(23) 2 ejems.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO.

# Grupos Simples de Suzuki.

T E S I S

Que para obtener el título de

MATEMATICO

presenta

Leopoldo Román Cuevas.

1981.

**TESIS CON FALLA DE ORIGEN**

Yo lo que buscaba
era un pueblito relojero
que me arreglara el corazón.

-Gilberto Owen-

A Laura Elisa.

# I N D I C E.

# INTRODUCCION

## i).- Pequeña reseña histórica de los grupos simples.

Evariste Galois (1811-1832) llamó a un grupo "simple" cuando sus únicos subgrupos normales son el subgrupo identidad y el mismo grupo. Es evidente que los grupos simples abelianos son los grupos de orden uno y los grupos cíclicos de orden primo; sin embargo, los grupos simples no-abelianos poseen generalmente estructuras complicadas. ¿Por qué son importantes los grupos simples?

Son importantes porque tienen un papel en la teoría de los grupos semejante al que tienen los números primos en la teoría de los números. Después de haber formulado la definición de grupo simple, Galois probó que el grupo alternante en 5 elementos era simple, de ahí en adelante numerosos matemáticos han tratado de encontrar todos los grupos simples.

En 1870, Camile Jordan (1838-1922) publicó el primer libro sobre la teoría de los grupos (Traité de Substitutions). En este libro estableció la existencia de cinco familias infinitas de grupos simples finitos. En 1892, Otto Hölder (1859-1937) inició el problema del "rango", es decir, planteó la tarea de encontrar todos los grupos simples cuyos órdenes estuviesen en un rango dado. El problema consistía en determinar qué enteros en cierto rango dado eran los órdenes de grupos simples, y para cada entero que cumplía esta condición describir todos los grupos simples que tenían ese orden. Hölder probó en 1892 que los únicos dos grupos simples cuyos órdenes estaban entre 1 y 200 eran $A_5$ (de orden 60) y $PSL(2,7)$ (de orden 168).

El problema del "rango" continuó desarrollándose hasta que en [illegible] Burnside obtuvo en [illegible] numerosos criterios aritméticos para los grupos simples. Hacia el año de 1893 el problema del "rango" había sido completado hasta grupos de orden entre 1 y 660. Como el próximo grupo simple conocido tenía orden 1092, Burnside decidió examinar a los enteros entre 661 y 1092. Para obtener sus resultados, Burnside usó representaciones en permutaciones de grupos. Ciertos grupos de permutaciones - transitivos, doblemente transitivos y primitivos - poseen un papel muy importante en la teoría de los grupos simples. La importancia de estos grupos es que la representación de un grupo como permutaciones de las clases laterales de un subgrupo es transitiva, y muchos de los grupos simples conocidos pueden ser representados como grupos de permutaciones doblemente transitivos.

Existe otra teoría creada durante la "búsqueda" de grupos simples: la teoría de los caracteres de un grupo. Esta teoría fué desarrollada por Georg Frobenius (1849-1917) en una serie de artículos que escribió a partir de 1896 (en [15,16] se puede encontrar el desarrollo histórico de la teoría de caracteres). A finales del siglo XIX, Burnside simplificó la teoría y encontró importantes aplicaciones de esta última. En los últimos años, la teoría de caracteres ha sido desarrollada y refinada por Brauer, Suzuki y Feit.

Durante el periodo de 1895-1901, Burnside se preguntó si existía algún grupo simple de orden impar. En el artículo [5] que escribió en 1895, Burnside demostró que no existía ningún grupo simple de orden impar menor que 1095. Años más tarde, extendió su afirmación hasta 9,000 [7] y luego hasta 40,000 [9].

Los resultados que demostró en [8] y [9] lo llevaron a convencerse que no existían grupos simples de orden impar; de hecho en [8] escribió lo siguiente: "Los resultados obtenidos en este artículo, me indican que una respuesta a la interesante pregunta de la existencia o no existencia de grupos simples de orden impar, podrá hacerse al haber estudiado más la teoría de los caracteres de grupos".

La siguiente etapa importante que se obtuvo en esta dirección apareció cincuenta años más tarde. En 1957 Michio Suzuki [19] usó la teoría de caracteres para probar que un grupo simple en el que el centralizador de cualquier elemento distinto de la identidad es abeliano, debe tener orden par. Tres años más tarde, en un trabajo más amplio [4], Walter Feit, Marshall Hall Jr. y Jhon Thompson obtuvieron una generalización del resultado de Suzuki al demostrar que la condición de ser abeliano podía ser sustituida por nilpotente. La demostración era análoga a la de Suzuki y la teoría de caracteres jugó un papel importante.

La conjetura de Burnside fue resuelta, finalmente, en 1963 cuando Feit y Thompson probaron en [illegible] que los grupos de orden impar son solubles. La demostración del "teorema del orden impar" ocupa 255 páginas en el Pacific Journal of Mathematics. Este ha sido uno de los resultados más importantes que ~~se~~ han probado en la teoría de los grupos simples finitos.

Diversos grupos simples contienen otros grupos simples como subgrupos. Por ejemplo, $A_5 = A_5$... Un grupo simple mínimo es aquél en el que todos sus subgrupos son solubles. Los grupos simples mínimos son básicos y su clasificación completa será de gran valor. Thompson decidió atacar este problema de una manera más general. El normalizador de un grupo soluble distinto de la identidad de un grupo E, se llama un subgrupo local de E; y un N-grupo es aquél en el que todos sus subgrupos locales son solubles. Evidentemente todo subgrupo simple mínimo es también un N-grupo.

En 1963 Thompson demostró que salvo algunas excepciones, los N-grupos simples son $PSL(2,q)$ $(q>3)$ y los grupos de Suzuki. La clasificación completa de todos los N-grupos solubles, sin embargo, apareció años más tarde, entre 1968 y 1974, en una serie de seis artículos que Thompson escribió. La demostración de este importante teorema se puede encontrar en [illegible].

En el párrafo anterior se mencionaron los grupos de Suzuki. Michio Suzuki encontró esta nueva familia de grupos simples en 1960 cuando trataba de clasificar cierto tipo de grupos de permutaciones doblemente transitivos. ¿Por qué son importantes los grupos de Suzuki?

Porque dan el primer ejemplo de grupos simples cuyos órdenes no son divisibles por 3; además, Thompson demostró en un trabajo reciente [illegible] que los grupos de Suzuki son los únicos grupos simples cuyos órdenes no son divisibles por 3. Una lista de los órdenes de los grupos simples clásicos se puede encontrar en [illegible].

He tratado de dar un paranama general de lo que es la teoría de los grupos simples. Si se desea conocer más a fondo la historia de esta teoría, se podría consultar [13].

ii).- Objetivos.

El propósito de este trabajo es demostrar que los grupos de Suzuki son simples. Se consultaron tres artículos de Suzuki ([20] [21] y [illegible]) en donde mencionaba todos los resultados que se probarán aquí más adelante; sin embargo se demuestran algunas cosas de otra manera y se les da un tratamiento diferente al que les dió Suzuki en sus artículos originales.

El trabajo está dividido en tres partes. En (I).A se demuestran algunos resultados que se usarán más adelante. En (I).B se prueba que todo p-grupo finito que tiene un único subgrupo de orden p es cíclico o un grupo de cuaternios generalizado; en (I.C) se definen grupos transitivos, doblemente transitivos, grupos de Frobenius y se prueban algunos resultados acerca de estos últimos en especial.

En (II) se define un (ZT)- grupo y se demuestra que todo (ZT)-grupo es simple. Finalmente, en (III) se definen los grupos de Suzuki y se prueba que es un (ZT)-grupo.

Todas las demostraciones que se encuentran en I.A, [illegible] y [illegible] se tomaron de [illegible] y [illegible] (salvo algunos resultados que aparecían como ejercicios en [illegible]). En (I).C se mencionan tres teoremas que no se demuestran. La demostración de estos tres teoremas necesitaría de la teoría de caracteres que rebasa los objetivos de este trabajo.

Una palabra acerca de los dos teoremas de Brauer y Suzuki; me gustaría hacer notar que ninguno de los libros sobre Teoría de los Grupos que conozco, demuestra estos dos teoremas. El libro de Huppert [illegible], demuestra un caso particular del primer teorema de Brauer y Suzuki en la página 624. Las demostraciones de estos dos teoremas se pueden encontrar en [2], [3] y [4].

Por último, las referencias para (II) y (III) son los tres artículos de Suzuki que se mencionaron anteriormente.

Agradecimiento.

Agradezco al señor profesor, Dr. Francisco Tomás Pons, Director de esta Tesis, su paciencia y su valiosa ayuda, tanto en lo referente a la elaboración de ésta, como en la aclaración de varios de los resultados que se mencionan en ella.

Todos los grupos que se consideran en [illegible] son finitos. Daremos a continuación una lista de símbolos que se usarán durante el desarrollo de los temas:

Sean $G$ un grupo y $H$ un subgrupo de $G$:

| | |
|---|---|
| $\lvert G\rvert$ | orden de $G$ |
| $[G:H]$ | índice de $H$ en $G$ |
| $H \triangleleft G$ | $H$ es un subgrupo normal de $G$ |
| $\langle x_1, \ldots, x_n\rangle$ | subgrupo generado por $x_1, \ldots, x_n$ |
| $Z(G)$ | centro de $G$ |
| $G'$ | subgrupo conmutador de $G$ |
| $C_G(x)$ | centralizador de $x$ en $G$ |
| $C_G(H)$ | centralizador del subgrupo $H$ en $G$ |
| $N_G(H)$ | normalizador del subgrupo $H$ en $G$ |
| $G^{\#}$ | conjunto de elementos de $G$ distintos de la identidad |
| $\mathrm{Aut}\, G$ | Grupo de automorfismos de $G$ |
| [illegible] | subconjunto [illegible] |
| $H < G$ | $H$ es un subgrupo de $G$ |
| $\lvert x\rvert$ | orden de un elemento $x$ de $G$ |

Si $\pi$ es un conjunto de números primos, diremos que el elemento $x$ de $G$ es un $\pi$-elemento si $\lvert x\rvert$ es divisible sólo por primos que pertenecen a $\pi$. En particular, se tiene la noción de un $p$-elemento, $p$ un primo. Análogamente, un grupo $H$ se llama un $\pi$-grupo si $\lvert H\rvert$ es divisible sólo por primos en $\pi$.

El complemento del conjunto $\pi$ se denotará por $\pi'$. Entonces también se tiene la noción de $\pi'$ y $p'$-elementos, así como $\pi'$ y $p'$-grupos. Por ejemplo, un $2'$-elemento es simplemente un elemento de orden impar.

I).-

A

Demostraremos algunos resultados que se usarán en (II) y en (III)

Sean $G$ un grupo y $H \leq G$ entonces.

Teorema 1.-

Si $H \triangleleft G$ y $P$ es un $p$-subgrupo de Sylow de $H$

entonces $G = N_G(P)H$

Demostración.

Para $x \in G$, tenemos que $P^x = x^{-1}Px \subseteq x^{-1}Hx = H$ ya

que $H \triangleleft G$. Como $|P^x| = |P|$, $P^x$ también es un $p$-subgrupo de Sylow

de $H$ y por lo tanto es conjugado de $P$ por un elemento $y$ de $H$. Por-

lo consiguiente $P^x = P^y$ y $P^{xy^{-1}} = P$, entonces $xy^{-1} \in N_G(P)$. Como

$x = (xy^{-1})y$ y $x$ es arbitrario, el teorema queda demostrado.

Teorema 2.-

Si $H \triangleleft G$ y $P$ es un $p$-subgrupo de Sylow de $G$,

entonces $H \cap P$ es un $p$-subgrupo de Sylow de $H$.

Demostración.

Tenemos que $|G| = |H|_p |G/H|_p$ donde $|H|_p$ denota

la máxima potencia del primo $p$ que divide a $|H|$. Análogamente para

$|G/H|_p$. Por el segundo teorema de isomorfismo $|PH/H| = |P/P \cap H|$

Pero $PH/H$ es un $p$-subgrupo de Sylow de $G/H$. Concluimos por lo

tanto que $|P \cap H| = |H|_p$ y por lo tanto $P \cap H$ es un $p$-subgrupo de

Sylow de $H$.

Lema 1.-

Si todos los subgrupos de Sylow de un grupo abeliano $G$

son cíclicos, entonces $G$ es cíclico.

Demostración.

Sea $G$ un grupo abeliano con subgrupos de Sylow

$P_i = \langle x_i \rangle$ $1 \leq i \leq r$ y $n = |G|$. Como $G$ es un grupo abeliano finito

entonces $G$ es isomorfo al producto directo de sus subgrupos

de Sylow. Por lo tanto, como $x = x_1 \cdots x_r$ tiene orden $n = \prod_{i=1}^{r} |P_i|$ y

$n = |G|$ se tiene entonces que $G$ es cíclico.

Definición

Sea $G$ un grupo, se dice que un elemento $x$

en $G$ es una involución si su orden es 2.

Probaremos dos resultados importantes que involucran

a las involuciones de un grupo.

Teorema 3.-

Si $x, y$ son involuciones de $G$ entonces $x, y$ son conjugados en $\langle x, y\rangle$ ó existe una involución $z$ de $\langle x, y\rangle$ que conmuta con $x$ e $y$.

Demostración.

Sean $H = \langle x, y\rangle$, $u = xy$ y $m = |u|$. Como $H = \langle x, u\rangle$ y $x^{-1}(xy)x = yx = (xy)^{-1}$ entonces $|H| = 2m$. Pero entonces, si $m$ es impar $\langle x\rangle$, $\langle y\rangle$ son 2-subgrupos de Sylow de $H$, por lo tanto $x$ e $y$ son conjugados en $H$ por los teoremas de Sylow. Por otra parte, si $m = 2k$ entonces $z = u^k$ es una involución y $xz = zx$, $yz = zy$ ya que $x(xy) = (yx)x$, $y(xy) = (yx)y$ "k-veces"

Teorema 4.-

Si un 2-subgrupo de Sylow $S$ de $G$ es disjunto de sus conjugados entonces $S \triangleleft G$ ó dos involuciones arbitrarias de $G$ son conjugadas.

Demostración.

Supongamos que $S \triangleleft G$ y sea $T$ un 2-subgrupo de Sylow de $G$ distinto de $S$. Sean $x, y$ involuciones de $S$ y $T$ respectivamente. Si $x$ no es conjugada de $y$, entonces por el teorema 3 existe una involución $z$ en $\langle x, y\rangle$ que conmuta con $x$ e $y$. Como el 2-subgrupo de Sylow es ajeno de sus conjugados, $z$ está en un único 2-subgrupo $R$ de $G$ y además $S, T$ son los únicos 2-subgrupos de Sylow que contienen a $x$ e $y$ respectivamente. Pero $\langle z, x\rangle$ es un 2-grupo y por lo tanto pertenece a un 2-subgrupo de Sylow, que por la afirmación anterior debe de ser, por un lado, $R$ y por el otro $S$. Entonces $R = S$. Análogamente $R = T$ y por lo tanto $S = T$, esto es una contradicción. Concluimos que toda involución de $S$ es conjugada con $y$. Por lo tanto todas las involuciones de $S$ son conjugadas y por lo tanto dos involuciones de $G$ son conjugadas.

Definición.

Un automorfismo $\phi$ de un grupo $G$ se dice que no tiene punto fijo si la identidad de $G$ es el único elemento que fija $\phi$.

Probaremos a continuación, un lema que nos ayudará a demostrar algunos resultados importantes.

Lema 4.-

Si un grupo $G$ tiene un automorfismo $T$ de orden 2 que no tiene punto fijo entonces $gT = g^{-1}$ para toda $g$ en $G$ y $G$ es abeliano.

Demostración.

Sea $U: G \longrightarrow G$ la función tal que:

$$gU = g^{-1}(gT)$$

Si $gU = hU$ para alguna pareja $\{g,h\} \subseteq G$ entonces $g^{-1}(gT) = h^{-1}(hT)$, por lo tanto $hg^{-1} = (hg^{-1})T \Rightarrow hg^{-1} = e \Rightarrow h = g$. Concluimos que $U$ es una función inyectiva; como $G$ es finito $U$ es biyectiva.

Sea $x \in G$ entonces $x = gU$ para alguna $g \in G$

$$\therefore\ xT = (gU)T = (g^{-1}(gT))T = (gT)^{-1}g = (g^{-1}(gT))^{-1} = x^{-1}$$

Si además, $y$ está en $G$ obtenemos que:

$$(xT)(yT) = x^{-1}y^{-1} = (yx)^{-1} = (yx)T = (yT)(xT)$$

$$\therefore\ x^{-1}y^{-1} = y^{-1}x^{-1};\ \therefore\ yx^{-1} = x^{-1}y;\ \therefore\ xy = yx$$

Por lo tanto $G$ es abeliano.

Definición.-

Un grupo $G$ que no tiene subgrupos característicos propios se llama <u>característico simple</u>.

El siguiente resultado describe la estructura de tales grupos.

Teorema 5.-

Un grupo característico simple es el producto directo de grupos simples isomorfos.

Demostración.

Sea $G$ un grupo característico simple y sea $G_1$ un subgrupo normal no-trivial de $G$ de orden lo más pequeño posible (posiblemente $G_1 = G$). Sea $H$ un subgrupo de $G$ de orden máximo de la forma $H = G_1 \times G_2 \times \cdots \times G_r$, donde $G_i \trianglelefteq G$ y $G_i$ es isomorfo a $G_1$, $1 \leq i \leq r$. Claramente $H \trianglelefteq G$. Afirmamos que $H = G$.

Si $\phi \in Aut(G)$, tenemos que $\phi(G_i) \trianglelefteq G$ y $\phi(G_i)$ es isomorfo a $G_i$, por lo tanto, es isomorfo a $G_1$. Supongamos

que existen $i$ y $\varphi$ tales que $\varphi(G_i) \not\subseteq H$. Entonces $\varphi(G_i) H = \varphi(G_i)$
$|\varphi(G_i) \cap H| < |G_i|$. Pero $\varphi(G_i) \cap H \triangleleft G$, por lo tanto $\varphi(G_i) \cap H = 1$ por nuestra
elección de $G_1$. Por lo tanto $H\varphi(G_i) = H \times \varphi(G_i)$ satisface las mismas condi-
ciones que $H$ pero tiene orden más grande, lo cual contradice la defini-
ción de $H$. Se sigue entonces que $\varphi(G_i) \subseteq H$ para toda $i$, $1 \le i \le r$, y
todo $\varphi \in \mathrm{Aut}\, G$, por lo tanto $\varphi H = H$ para todo $\varphi$ en $\mathrm{Aut}\, G$. Enton-
ces $H$ es característico en $G$ y al ser $G$ característico simple con-
cluimos que $G = H = G_1 \times G_2 \times \cdots \times G_n$.

Como todo subgrupo normal de $G_1$ es de hecho normal en $G$, $G_1$ debe ser simple por la elección mínima de $G_1$. Entonces $G$ es el producto directo de grupos simples isomorfos, tal como se afirmaba.

## Lema de Burnside.-

Si $P$ es un $p$-subgrupo de Sylow de $G$, entonces dos subconjuntos normales de $P$ son conjugados en $G$ sii son conjugados en $N_G(P)$. En particular, dos elementos de $Z(P)$ son conjugados en $G$ sii son conjugados en $N_G(P)$.

## Demostración.

Todo elemento de $Z(P)$ es un subconjunto normal de $P$ y también dos subconjuntos de $P$ conjugados en $N_G(P)$ son conjugados en $G$. Por lo tanto, lo único que falta probar es que si $X$, $Y$ son subconjuntos normales de $P$ con $Y = X^u$, $u \in G$, entonces $Y = X^z$ con $z \in N_G(P)$. Sea $N = N_G(Y)$, por lo tanto $P \subseteq N$ ya que $Y$ es normal en $P$. Pero como $Y$ es un subconjunto normal de $P^u$ puesto que $X^u = Y$ y $X$ es un subconjunto normal de $P$, entonces $P^u \subseteq N$. Por lo tanto $P, P^u$ son $p$-subgrupos de Sylow de $N$ y $P^{uv} = P$ para alguna $v \in N$. Si hacemos $z = uv$, tenemos entonces que $z \in N_G(P)$ y $X^z = X^{uv} = Y^v = Y$.

## Definición.

Si $P$ y $Q$ son $p$-subgrupos de Sylow de $G$, diremos que la intersección $P \cap Q$ es <u>suave</u> si $N_P(P \cap Q)$ y $N_Q(P \cap Q)$ son $p$-subgrupos de Sylow de $N_G(P \cap Q)$.

Sea $P$ un $p$-subgrupo de Sylow de $G$. Entonces, si $Q$, $R$ son dos $p$-subgrupos de Sylow de $G$ diremos que $R$ está relacionado con $Q$ con respecto a $P$ si existen $p$-subgrupos de Sylow $Q_i$, $1 \le i \le n$, tales que:

i).- $P \cap Q_i$ es una intersección suave $1 \le i \le n$.

ii).- Existen $p$-elementos $x_i$ de $N_G(P \cap Q_i)$, tal que $R^x = Q$ donde $x = x_1 \cdots x_n$.

iii).- $P \cap R \subseteq P \cap Q_1$ y $(P \cap R)^{x_1 \cdots x_i} \subseteq P \cap Q_{i+1}$ $1 \le i \le n-1$

En tal caso escribimos $S \sim R$ y si no existe alguna confusión $S \sim R$. Nos referiremos al elemento $x$ como [illegible] vía $x$.

Notemos que,

$(P \cap S)^{x} = (P \cap S)^{x_1 \cdots x_n} \subseteq$ [illegible] $(P \cap R)$ ya que $x_i \in N_G(P \cap Q_i)$

Demostraremos algunos lemas que nos servirán para demostrar el teorema de Alperin.

Lema 3.-

Si $S, R, Q$ son $p$-subgrupos de Sylow tales que $S \sim R$ y $R \sim Q$ entonces $S \sim Q$.

Demostración.

Supongamos que $y_i, T_i$, $1 \le i \le m$ y $z_i, U_i$, $1 \le i \le r$ son los elementos y los $p$-subgrupos de Sylow de $G$ que satisfacen las relaciones $S \sim R$ y $R \sim Q$ con respecto a $P$ respectivamente. Sea $n = m + r$ y definimos:

$$x_i = \begin{cases} y_i \\ z_{i-m} \end{cases} \quad y \quad Q_i = \begin{cases} T_i & 1 \le i \le m \\ U_{i-m} & m+1 \le i \le n \end{cases} \quad --- (1)$$

Afirmamos que los elementos $x_i$ y los $p$-subgrupos $Q_i$, $1 \le i \le n$ cumplen la condición requerida $S \sim Q$.

$P \cap Q_i$ es una intersección suave y $x_i$ es un $p$-elemento de $N_G(P \cap Q_i)$ para toda $i$ puesto que las afirmaciones correspondientes se cumplen para $P \cap T_i$, $P \cap U_i$, $y_i$ y $z_i$. Además, si $y = y_1 y_2 \cdots y_m$ y $z = z_1 z_2 \cdots z_r$ entonces $x = yz = x_1 x_2 \cdots x_n$. Como $S^y = R$ y $R^z = Q$, tenemos que $S^x = Q$. Por lo tanto las condiciones (i) y (ii) se cumplen en la definición de $S \sim Q$.

Como $P \cap S \subseteq P \cap T_1 = P \cap Q_1$; si $1 \le i \le m-1$ entonces

$$(P \cap S)^{x_1 \cdots x_i} = (P \cap S)^{y_1 \cdots y_i} \subseteq P \cap T_{i+1} = P \cap Q_{i+1} \quad --- (2)$$

$$(P \cap S)^{x_1 \cdots x_m} = (P \cap S)^{y} \subseteq P \cap R$$

$$(P \cap S)^{x_1 \cdots x_m} \subseteq P \cap U_1 = P \cap Q_{m+1} \quad \text{ya que } P \cap R \subseteq P \cap U_1 \quad ---(3)$$

Finalmente, para $m+1 \le i \le n-1$ tenemos

$$(4) --- \quad (P \cap S)^{x_1 \cdots x_i} = ((P \cap S)^{y})^{x_{m+1} \cdots x_i} \subseteq (P \cap R)^{z_1 \cdots z_{i-m}} \subseteq P \cap U_{i-m+1} = P \cap Q_{i+1}$$

Por (2), (3) y (4) deducimos que (iii) se cumple.

Por lo tanto $S \sim Q$.

Lema 4.-

Sean $Q, R$ $p$-subgrupos de Sylow de $G$ tal que $P \cap R \subseteq P \cap Q$, $R \sim P$ vía $x$ y $Q^x = P$. Entonces $Q \sim P$.

Demostración.

Basta demostrar que $Q \sim R$ por el lema 3.

Sean $x = x_1 \cdots x_n$ y $Q_i$, $1 \le i \le n$ que cumplen con la definición $R \sim P$ vía $x$.

Afirmamos que $Q \sim P$ está dado por los mismos elementos $x_i$ y los $p$-subgrupos $Q_i$.

Las condiciones (i) y (ii) se cumplen claramente puesto que $Q_i$ es conjugado de $Q^x$ por elemento $x$. Como [illegible] por hipótesis y $P \cap R \geq P \cap Q$, entonces $P \cap Q \geq P \cap Q_i$. Entonces

$$(P \cap Q)^{x_1 \cdots x_i} \text{ [illegible] } \qquad 1 \leq i \leq n$$

tal como se deseaba.

Lema 5.-

Sean $Q, R$ $p$-subgrupos de Sylow de $G$ tales que $R \cap Q > P \cap Q$ y $R \sim P$. Supongamos que $S \sim P$ para todos los $p$-subgrupos de Sylow $S$ de $G$ con la propiedad $|S \cap P| > |Q \cap P|$. Entonces $Q \sim P$.

Demostración

Sea $R \sim P$ vía $x$, por lo tanto $R^x = P$. Entonces $P \cap Q^x = R^x \cap Q^x = (R \cap Q)^x$. Por hipótesis $|R \cap Q| > |P \cap Q|$ por lo tanto $|P \cap Q^x| > |P \cap Q|$. Por lo consiguiente $Q^x \sim P$ por nuestra segunda suposición. Como $R \sim P$, la conclusión deseada se obtendrá del lema 4, si demostramos que $P \cap R \geq P \cap Q$. Como $P \cap R \geq P \cap (R \cap Q) \geq P \cap (P \cap Q) = P \cap Q$ tal como se necesitaba.

Lema 6.-

Sea $Q$ un $p$-subgrupo de Sylow de $G$ tal que $P \cap Q$ es una intersección suave. Si $S \sim P$ para todo $p$-subgrupo de Sylow $S$ de $G$ con la propiedad $|S \cap P| > |Q \cap P|$, entonces $Q \sim P$.

Demostración

Si $Q = P$, entonces sabemos que $Q \cap P$ es una intersección suave y que $Q \sim P$; por lo tanto, podemos suponer que $Q \neq P$, en tal caso $P \cap Q < P$. Sea $P_0 = N_P(P \cap Q)$ y $Q_0 = N_Q(P \cap Q)$, por lo tanto $P_0, Q_0$ son $p$-subgrupos de Sylow de $N = N_G(P \cap Q)$ ya que $P \cap Q$ es una intersección suave. Sea $K$ el subgrupo de $N$ generado por todos sus $p$-elementos. Entonces claramente $Q_0$ y $P_0$ son subgrupos de Sylow de $K$, por lo tanto $Q_0^x = P_0$ para alguna $x$ en $K$. Podemos escribir $x = x_1 \cdots x_n$, donde cada $x_i$ es un $p$-elemento de $K$. Tomamos $Q_i = Q$ para $1 \leq i \leq n$. Entonces $P \cap Q_i$ es una intersección suave para toda $i$ y se sigue inmediatamente de la definición que $Q \sim Q^x$.

Por otra parte, $P \cap Q^x \geq P_0 \cap Q_0^x = P \cap P_0 = P_0$. Pero $P_0 > P \cap Q$ ya que $P \cap P \cap Q$. Por lo tanto $|P \cap Q^x| > |P \cap Q|$ y por lo tanto $Q^x \sim P$ por hipótesis. Entonces tenemos que $Q \sim Q^x$ y $Q^x \sim P$, concluimos entonces que $Q \sim P$ por el lema 4.

Con la ayuda de estos lemas, podemos probar ahora el siguiente teorema.

Teorema 1.-

Para toda pareja $P$ y $Q$ de $p$-subgrupos de Sylow de $G$, tenemos que $Q \sim_P P$.

Demostración.

Por inducción sobre $|P : P\cap Q|$. Si $|P : P\cap Q| = 1$, entonces $P = Q$ y el teorema se cumple, por lo tanto, podemos suponer que $P\cap Q \neq P$. Sea $D$ un p-subgrupo de $N_G(P\cap Q)$ que contenga a $N_P(P\cap Q)$ y sea $S$ un p-subgrupo de $G$ que contiene a $D$. Entonces $P\cap S \geq P\cap D = N_P(P\cap D) > P\cap Q$, por lo tanto $|P : P\cap S| < |P : P\cap Q|$. Por hipótesis de inducción $S \sim P$. Supongamos que $S^x = P$ con el elemento $x$. Bastará demostrar que $Q^x \sim P$, pues por el lema 4 con $S$ en lugar de $R$ se obtendrá la conclusión deseada $Q \sim P$.

Ahora bien, $P\cap Q^x \geq P\cap (P\cap Q)^x$, como $(P\cap Q)^x \leq S^x = P$ concluimos que $P\cap (P\cap Q^x) = (P\cap Q)^x$ y por lo consiguiente

$$(P\cap Q^x) \geq (P\cap Q)^x \quad --- (5)$$

Si $P\cap Q^x > (P\cap Q)^x$ entonces $|P : P\cap Q^x| < |P : P\cap Q|$ puesto que $(P\cap Q)^x$ y $(P\cap Q)$ tienen el mismo orden. Pero entonces $Q^x \sim P$ por inducción. Por lo tanto podemos suponer que (5) es una igualdad.

Como $D$ es un p-subgrupo de Sylow de $N_G(P\cap Q)$ se sigue entonces que $D^x$ es un p-subgrupo de Sylow de $N_G((P\cap Q)^x)$. Sea $E$ un p-subgrupo de Sylow de $N_G(P\cap Q^x)$ que contenga a $N_{Q^x}(P\cap Q^x)$ y sea $T$ un p-subgrupo de Sylow de $G$ que contenga a $E$. Entonces $T\cap Q^x \geq E\cap Q^x \geq N_{Q^x}(P\cap Q^x)$. Si $T\sim P$, entonces la primera condición del lema 5 se satisface con $T, Q^x$ en lugar de $R, Q$ respectivamente. Como la segunda condición del lema se sigue por nuestra hipótesis de inducción, se sigue entonces que $Q^x \sim P$, tal como se deseaba. Por lo tanto bastará probar que $T \sim P$. Pero $P\cap T \geq P\cap Q^x$, por lo tanto si $P\cap T > P\cap Q^x$, la afirmación se seguirá de la hipótesis de inducción. Por lo consiguiente, podemos suponer que $P\cap T = P\cap Q^x$.

Bajo estas condiciones afirmamos que $P\cap T$ es una intersección suave, en tal caso la conclusión $T\sim P$ se seguirá del lema 6 en vista de nuestra hipótesis de inducción. Notemos primero que $D^x \leq P$ y que $D^x$ es un p-subgrupo de Sylow de $N_G(P\cap Q^x) = N_G(P\cap T)$. Además, como $E \leq T$ y $E$ es un p-subgrupo de Sylow de $N_G(P\cap Q^x)$, también tenemos que $N_T(P\cap T)$ es un p-subgrupo de Sylow de $N_G(P\cap T)$. Por lo tanto $P\cap T$ es una intersección suave y el teorema está probado.

A partir del teorema 6 podemos demostrar el teorema de Alperin.

Teorema 7 (Alperin).-

Sean $A$ y $B$ dos subconjuntos de un $p$-subgrupo de Sylow $P$ de $G$ y supongamos que $A^x = B$. Entonces existen elementos $x_i$ y $p$-subgrupos de Sylow $Q_i$ de $G$, $1 \leq i \leq n$, y un elemento $y$ de $N_G(P)$ que satisfacen las siguientes condiciones:

i).- $x = x_1 \cdots x_n y$

ii).- $P \cap Q_i$ es una intersección suave para $1 \leq i \leq n$

iii).- $x_i$ es un $p$-elemento de $N_G(P \cap Q_i)$ $\quad 1 \leq i \leq n$

iv) - $A \leq P \cap Q_1$, además $A^{x_1 \cdots x_i} \leq P \cap Q_{i+1}$ $\quad 1 \leq i \leq n-1$

Demostración.

Por el teorema 6 $P^{x^{-1}} \sim P$ vía algún elemento $u$. Sean $Q_i$ y $x_i$, $1 \leq i \leq n$, $p$-subgrupos de Sylow y elementos de $G$ que satisfacen esta relación, por lo tanto en particular $u = x_1 \cdots x_n$ y $(P^{x^{-1}})^u = P$. Haciendo $y = u^{-1}x$, se sigue que $y \in N_G(P)$ y $x = uy$. Como $B = A^x \leq P$, tenemos que $A \leq P \cap P^{x^{-1}}$. Por lo tanto $A^{x_1 \cdots x_i} \leq (P \cap P^{x^{-1}})^{x_1 \cdots x_i} \leq P \cap Q_{i+1}$ $\quad 1 \leq i \leq n-1$, por la definición de $P^{x^{-1}} \sim P$ vía $u$ y por nuestra elección de $Q_i$ y $x_i$. Por la misma razón $P \cap Q_i$ es una intersección suave y $x_i \in N_G(P \cap Q_i)$ $\quad 1 \leq i \leq n$, y el teorema está probado.

Existe otra versión del teorema de Alperin que es más conveniente para algunas aplicaciones. Observamos que si hacemos $Q_{n+1} = P$ tenemos que $P \cap Q_{n+1}$ es una intersección suave. Además, como se ha visto antes $A^u \leq P$, por lo tanto $A^u = A^{x_1 \cdots x_n} \leq Q_{n+1}$. Además si hacemos $y = x_{n+1}$, entonces $x_{n+1} \in N_G(P \cap Q_{n+1})$. Ahora hagamos $A = A_0$ y $A_i = A^{x_1 \cdots x_i}$ $\quad 1 \leq i \leq n+1$, por lo tanto $A_{n+1} = B$. Nuestras condiciones implican que $A_{i-1}$ y $A_i$ están en $P \cap Q_i$ y son conjugados por el elemento $x_i$. Entonces tenemos (substituyendo $n+1$ por $n$).

Teorema 8 (Alperin) -

Si $A, B$ son subconjuntos del $p$-subgrupo de Sylow $P$ de $G$ que son conjugados en $G$, entonces existen $p$-subgrupos de Sylow $Q_i$ de $G$ donde $P \cap Q_i$ es una intersección suave $1 \leq i \leq n$ y subconjuntos $A = A_0, A_1, A_2, \ldots, A_n = B$ tal que:

i).- $A_{i-1} \leq P \cap Q_i$, $\quad A_i \leq P \cap Q_i$

ii).- $A_i = A_{i-1}^{z_i}$, para alguna $z_i$ en $N_G(P \cap Q_i)$ $\quad 1 \leq i \leq n$

Lema 7.-

Sea $P = \langle x \rangle$ un $p$-grupo cíclico de orden $p^n$, $n \geq 1$ y hagamos $A = \mathrm{Aut}\, P$. Entonces tenemos que

i).- Si $p = 2$ y $n = 2$, entonces $A = \langle \alpha \rangle$, donde $x\alpha = x^{-1}$ y $|A| = 2$.

ii).- Si $p = 2$ y $n > 2$, entonces $A$ es un grupo abeliano de tipo $(2^{n-2}, 2)$ y orden $2^{n-1}$ con base $\alpha, \beta$, donde $x\alpha = x^5$ $x\beta = x^{-1}$

iii).- Si $p$ es impar, $A$ es abeliano de orden $p^{n-1}(p-1)$ y un $p$-subgrupo de Sylow de $A$ es cíclico con generador $\alpha$, donde $x\alpha = x^{1+p}$.

Demostración.

Demostraremos en general, que si un grupo $G$ es cíclico entonces $\mathrm{Aut}\, G$ es abeliano.

Sea $G = \langle x \rangle$ de orden $n$. Si $\phi \in \mathrm{Aut}(G)$, entonces $(x)\phi$ tiene también orden $n$ y por lo tanto $(x)\phi = x^k$ con $(k, n) = 1$. Hacemos $\phi_k = \phi$. Recíprocamente, para cada entero $k$ primo con $n$ el mapeo $x^i \longrightarrow x^{ik}$ es un automorfismo de $G$. Además, si $\phi_h$ y $\phi_k$ están en $\mathrm{Aut}\, G$, tenemos que $(x)\phi_h\phi_k = (x^h)^k = x^{hk} = x^{\overline{hk}}$ donde $\overline{hk}$ denota el residuo de $hk$ módulo $n$. Por lo tanto $\phi_h \phi_k = \phi_{\overline{hk}}$ y se sigue que $\mathrm{Aut}\, G$ es isomorfo al grupo multiplicativo de clases residuales módulo $n$. Como el último grupo es evidentemente abeliano $\mathrm{Aut}\, G$ también lo es.

Por lo tanto $A$ es abeliano en todos los casos. Además, todo elemento $\alpha$ de $A$ está determinado por su efecto en $x$; también $x\alpha = x^i$ donde $(p^n, i) = 1$. Recíprocamente, para cada $i$ existe un elemento de $A$ que lleva $x$ en $x^i$. Por lo tanto $|A| = |\phi(p^n)|$, donde $\phi$ es la $\phi$-función de Euler, y en consecuencia $|A| = p^{n-1}(p-1)$.

Supongamos que $p = 2$, en tal caso $|A| = 2^{n-1}$. Si $n = 2$ $|A| = 2$ y el único automorfismo notrivial de $P$ está dado por $x\alpha = x^3 = x^{-1}$ por lo tanto (i) se cumple. Para probar (ii) observemos que:

$$5^{2^{n-2}} = (1 + 2^2)^{2^{n-2}} \equiv 1 \pmod{2^n} \quad \text{---} (6)$$

y

$$5^{2^j} \not\equiv 1 \pmod{2^n} \quad \text{si } j < n-2 \quad \text{---} (7)$$

Sea $\alpha$ un automorfismo de $P$ determinado por $x\alpha = x^5$. Entonces $x\alpha^i = x^{5^i}$. Como $|x| = 2^n$, (6) y (7) implican que $x\alpha^{2^j} \neq x$ si $1 \leq j < n-2$ y que $x\alpha^{2^{n-2}} = x$. Por lo tanto $|\alpha| = 2^{n-2}$. Por otro lado, también tenemos que:

$$5^j \not\equiv -1 \quad \mathrm{mod}(2^n), \quad \forall_j \quad --- (8)$$

Por lo tanto $\alpha^j \neq \beta$ para toda $j$, donde $\beta \in A$ y $x\beta = x^{-1}$. Como $|A| = 2^{n-1}$ se sigue que $\alpha, \beta$ es una base de $A$, por lo tanto (ii) se cumple.

Supongamos finalmente que $p$ es impar. Entonces el orden de un $p$-subgrupo de Sylow $A_p$ de $A$ es $p^{n-1}$. Observamos ahora que:

$$(1+p)^{p^j} \equiv 1 \quad (\mathrm{mod}\ p^{j+1}) \quad --- (9)$$

$$(1+p)^{p^j} \not\equiv 1 \quad (\mathrm{mod}\ p^{j+2}) \quad --- (10)$$

si $p$ es impar. Pero entonces, como en el párrafo anterior, el elemento $\alpha \in A$ dado por $x\alpha = x^{1+p}$ es de orden $p^{n-1}$. Por lo tanto $A_p = \langle\alpha\rangle$ es cíclico y (iii) también se cumple.

Definición.

Si $E$ es un $p$-grupo, denotaremos por $\Omega_i(E)$ al subgrupo de $E$ generado por todos los elementos de orden $p^i$. Análogamente, usamos el símbolo $\mho^i(E)$ que denota al subgrupo de $E$ generado por los elementos $x^{p^i}$ con $x$ en $E$.

Un corolario del lema 7 es el siguiente:

Corolario 1 .-

Las siguientes condiciones se cumplen:

i).- Si $p = 2$ y $n > 2$, hagamos $\gamma = \alpha^{2^{n-3}}$. Entonces $\Omega_1(A)$ es abeliano de tipo (2, 2) con base $\gamma, \beta$ y

$$x\beta = x^{-1} \qquad x\gamma = x^{5^{2^{n-3}}} = x^{1+2^{n-1}} \qquad x(\gamma\beta) = x^{-1-2^{n-1}} = x^{-1+2^{n-1}}$$

Además, $\gamma$ es el único elemento de $A^{\#}$ que actúa trivialmente en $\mho^1(P) = \langle x^2\rangle$.

ii).- Si $p$ es impar $\langle\gamma\rangle$ es el único subgrupo distinto de la identidad, de $A_p$ que actúa trivialmente en $\mho^1(P) = \langle x^p\rangle$

Teorema 9.-

Sea $P$ un $p$-subgrupo de Sylow de $G$. Entonces:

i).- Existe un subgrupo normal $K$ de $G$ tal que $G/K$ es isomorfo a $P/P\cap G'$.

ii).- Si $K$ es un subgrupo normal de $G$ tal que $G/K$ es un $p$-grupo abeliano entonces $P\cap G' \leq K$ y $G/K$ es isomorfo a la imagen homomorfa de $P/P\cap G'$.

Demostración.

Supongamos que $K \lhd G$ y $G/K$ es un $p$-grupo abeliano entonces $G' \leq K$ ya que $G/K$ es abeliano y $G = KP$ puesto que $G/K$ es un $p$-grupo. En particular $P\cap G' \leq K$ y por el tercer teorema de isomorfismo $G/K$ es isomorfo a $P/P\cap K$ lo cual implica que $P/P\cap K$ es la imagen homomorfa de $P/P\cap G'$. Por lo tanto (ii) se cumple.

$P\cap G'$ es un $p$-subgrupo de Sylow de $G'$ ya que $G' \lhd G$; además $\bar{G} = G/G'$ es abeliano. Si $K$ denota la imagen inversa del único $p'$-subgrupo normal máximo que denotaremos por $O_{p'}(\bar{G})$ entonces $P\cap G' = P\cap K$, $K \lhd G$ y $G/K$ es un $p$-grupo abeliano isomorfo a $P/P\cap G'$ y (i) se cumple ($O_{p'}(\bar{G})$ existe ya que el producto de dos $p$-subgrupos normales de un grupo $G$ es un $p$-grupo).

Teorema 10.-

Sea $G$ un grupo, $H$ un subgrupo de $G$ y $\phi$ un homomorfismo de $H$ en un grupo abeliano $A$. Sea $y_i$, $1 \leq i \leq n$ un conjunto completo de representantes de $H$ en $G$ si $y_i x \in H y_{i'(x)}$ escribimos

$$y_i x = h_i(x)\, y_{i'(x)}$$

para algún elemento $h_i(x)$ apropiado de $H$. Entonces tenemos que:

i).- El mapeo $x\tau = \prod_{i=1}^{n} h_i(x)\phi$ es un homomorfismo de $G$ en $A$.

ii).- $\tau$ está determinada independientemente de la elección de los representantes $y_i$, $1 \leq i \leq n$ de $H$ en $G$.

Demostración.

Como $\phi$ es un homomorfismo podemos reescribir $x\tau$ como

$$x\tau = \left(\prod_{i=1}^{n} h_i(x)\right)\phi \qquad ---(11)$$

Por lo tanto para $x_1, x_2$ en $G$ tenemos que

$$(x_1\tau)(x_2\tau) = \left(\prod_{i=1}^{n} h_i(x_1)\right)\phi \left(\prod_{i=1}^{n} h_i(x_2)\right)\phi = \left(\prod h_i(x_1) \prod h_i(x_2)\right)\phi \quad ---(12)$$

Por otro lado

$$(x_1 x_2)\tau = \left(\prod_{i=1}^{n} h_i(x_1 x_2)\right)\phi \quad ---(13)$$

Si $u, v$ denotan los términos de los paréntesis de (12) y (13) respectivamente, $\tau$ será un homomorfismo si probamos que $u\phi = v\phi$ ó equivalentemente $u = kv$ para algún elemento del núcleo $K$ de $\phi$. Como $A$ es abeliano, $H' \leq K$. Por lo tanto, bastará probar que $u \equiv v \mod(H')$. Supongamos que podemos demostrar que $v$ es igual al producto de $2n$ elementos $h_i(x_1)\, h_i(x_2)$ $1 \leq i \leq n$ dispuestos de algún modo. Como todo rearreglo de estos términos no afecta a la clase $H'$ en el que el producto esté, la conclusión deseada $v \equiv u \mod(H')$ se seguirá ya que según (12) $u$ es por definición un producto de $2n$ elementos.

Para probar la afirmación, notemos primero que por definición de $h_i(x_1 x_2)$ tenemos que:

$$y_i(x_1, x_2) = h_i(x_1 x_2)\, y_{i'(x_1 x_2)} \quad ---(14)$$

Por otra parte

$x_1$

$$y_i(x_1 x_2) = (y_i x_1) x_2 = h_i(x_1)\, y_{i'(x_1)} x_2 = h_i(x_1)(y_j x_2) \quad ---(15)$$

donde $j = i'(x_1)$

Por lo tanto $y_i(x_1 x_2) = h_i(x_1)\, h_j(x_2)\, y_{j'(x_2)}$ --- (16)

con lo que por (14)

$$h_i(x_1 x_2) = h_i(x_1)\, h_j(x_2) \qquad 1 \leq i \leq n \quad ---(17)$$

Como $v = \prod_{i=1}^{n} h_i(x_1 x_2)$, la conclusión deseada se seguirá de (17) si demostramos que $j$ "corre" sobre el conjunto $S = \{1, 2, \ldots, n\}$ (en algún orden) cuando $i$ lo hace también. Pero el mapeo $\pi_{x_1}$ de $S$ en $S$ definido por:

$$(i)\pi_{x_1} = i'(x_1) \quad ---(18)$$

es claramente una permutación de $S$. Como $i'(x_1) = j$ por definición, $j$ corre sobre $S$ y concluimos que $\tau$ es un homomorfismo.

Supongamos ahora que $\bar{y}_i$, $1 \leq i \leq n$ es otro conjunto de representantes de las clases de $H$ en $G$, sea $\bar{\tau}$ el homomorfismo correspondiente de $G$ en $A$, definido por los elementos correspondientes $\bar{h}_i(x)$ para $x$ en $G$, $1 \leq i \leq n$. Debemos de probar que $\bar{\tau} = \tau$. Sean

$$u = \prod_{i=1}^{n} h_i(x) \qquad \bar{u} = \prod_{i=1}^{n} \bar{h}_i(x) \qquad \text{---} (19)$$

y como en la demostración de [illegible], bastará demostrar que $u \equiv \bar{u}$ [illegible]. Si $\bar{y}_i$ es una permutación de $y_i$ entonces $\bar{h}_i$ [illegible] es una permutación de $h_i(x)$ y la conclusión se sigue en este caso. Por lo tanto, substituyendo $\bar{y}_i$ por alguna permutación adecuada de ella, podemos asumir sin perder generalidad, que $y_i$ y $\bar{y}_i$ están en la misma clase de $H$, $1 \leq i \leq n$. Por lo tanto, $\bar{y}_i = z_i y_i$ $\quad z_i \in H \quad 1 \leq i \leq n$ entonces:

$$\bar{y}_i(x) = z_i y_i x = z_i h_i(x)\, y_{i'(x)} = z_i h_i(x)\, z^{-1}_{i'(x)} z_{i'(x)} y_{i'(x)} = (*)$$

$$(*) = z_i h_i(x)\, z^{-1}_{i'(x)} \bar{y}_{i'(x)} \qquad \text{---} (20)$$

Se obtiene por (20) y la definición de $\bar{h}_i(x)$ que:

$$\bar{h}_i(x) = z_i h_i(x)\, z^{-1}_{i'(x)} \qquad 1 \leq i \leq n \qquad \text{---} (21)$$

Pero (19) y (21) implican que:

$$\bar{u} \equiv u \left(\prod_{i=1}^{n} z_i\right)\left(\prod z^{-1}_{i'(x)}\right) \qquad \mathrm{mod}(H')$$

Sin embargo, el mapeo $(i)\pi_x = i'(x)$ es una permutación de $S = \{1, 2, \ldots, n\}$ y por lo tanto el segundo producto es simplemente el inverso del primero. Entonces $\bar{u} \equiv u$ mod $(H')$ y el teorema está probado.

El homomorfismo $\tau$ se llama el "transfer" de $G$ en $A$ (relativo a $H$ y $\varphi$).

Teorema 11.-

Sea $\tau$ el "transfer" de $G$ en un grupo abeliano $A$ relativo al subgrupo $H$ de $G$ y $\varphi$ el homomorfismo de $H$ en $A$. Entonces para todo elemento $x$ en $G$ existe un conjunto de $t$ elementos $x_i$ de $G$ $1 \leq i \leq t$ con $t$ y $x_i$ que dependen de $x$ con las siguientes propiedades:

i).- $x_i x^{r_i} x_i^{-1} \in H$ para ciertos enteros $r_i$ [illegible]

ii).- $\sum_{i=1}^{t} r_i = n = [G : H]$

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

Demostración

Con la notación del teorema [illegible] y los representantes [illegible] de las clases de $H$ en [illegible], [illegible], consideremos la permutación [illegible] de [illegible] dada por ([illegible]). Descompongamos a $\Pi_x$ como el producto de ciclos ajenos y renumeramos [illegible] de tal manera que la descomposición de $\Pi_x$ tenga la forma

$$(1\ 2 \ldots r_1)(r_1+1 \ldots r_1+r_2)(r_1+r_2+1 \ldots r_1+r_2+r_3)\ldots \qquad ---(22)$$

Sea [illegible] el número de ciclos de $\Pi_x$. Entonces sus longitudes respectivas son $r_i$ y $\sum_{i=1}^{t} r_i = n = [G:H]$. Entonces ([illegible]) se cumple para estos enteros $r_i$

Sean $x_1, x_2, \ldots, x_t$ los representantes de las clases numeradas por $1, r_1+1, \ldots, r_1+r_2+\ldots+r_{t-1}+1$ respectivamente. Entonces por la definición de $\Pi_x$ tenemos que $x_i x^j$ es un representante de $H$ en $G$ correspondiente a la [illegible]-ésima clase del $i$-ésimo ciclo de $\Pi_x$ y por lo tanto los elementos

$$\{x_i x^j \mid 1 \leq i \leq t \quad 0 \leq j \leq r_i - 1\} \qquad ---(23)$$

forman un conjunto completo de representantes de las clases de $H$ en $G$. Además, $x_i x^{r_i} \in Hx_i$ por la definición de $r_i$, por lo tanto $x_i x^{r_i} x_i^{-1} \in H$ y entonces (i) se cumple.

Sea $y_k = x_i x^j$ ($k$ una función de $j$ e $i$) y consideremos $y_k x = h_k(x)\, y_{k'(x)}$. Si $j < r_i - 1$, entonces $y_k x = x_i x^{j+1} = y_{k'(x)}$ de los representantes. Pero esto implica que $h_k(x) = 1$ si $j < r_i - 1$. Entonces [illegible] es el producto de aquellas $(h_k(x))\phi$ que corresponden a los elementos $y_k = x_i x^{r_i - 1}$. Para tales $y_k$, $y_k x = x_i x^{r_i} \in Hx_i$, por lo tanto $y_k x = (x_i x^{r_i} x_i^{-1}) x_i$ con $x_i x^{r_i} x_i^{-1} \in H$ y $x_i = y_{k'(x)}$. Se sigue que $h_k(x) = x_i x^{r_i} x_i^{-1}$ para cada una de las $y_k$ y concluimos que:

$$x\tau = \prod_{i=1}^{t} (x_i x^{r_i} x_i^{-1})\phi \qquad ---(24)$$

Como $\phi$ es un homomorfismo (ii) se sigue de (24) y el teorema está probado.

Teorema [illegible].-

Si $P$ es un $p$-subgrupo de Sylow de $G$ entonces el subgrupo $P\cap G'$ está generado por todos los elementos $x^{-1}y$ con $x\in P$, $y\in P$ y $y$ es conjugado de $x$ en $G$.

Demostración.

Sea $P^* = \langle x^{-1}y \mid x\in P,\ y\in P,\ y \text{ conjugado de } x\rangle$. Debemos demostrar que $P^* = P\cap G'$. Como $x^{-1}y = x^{-1}g^{-1}xg \in G'$, es claro que $P' \subseteq P^* \subseteq P\cap G'$. En particular $P/P^*$ es abeliano.

Sea $\theta$ el homomorfismo natural de $P$ en $P/P^*$ y sea $\tau$ el "transfer" de $G$ en $P/P^*$ relativo a $P$ y a $\theta$. Si $K$ denota el núcleo de $\tau$, bastará demostrar que $G/K$ es isomorfo a $P/P^*$. Si esto se cumple entonces $P/P^*$ será la imagen homomorfa de $P/P\cap G'$ por el teorema 9, lo cual implicará que $|P/P\cap G'| \geq |P/P^*|$. Pero como $P^* \subseteq P\cap G'$, la desigualdad inversa también se cumple, lo que dará la conclusión deseada $P^* = P\cap G'$.

Sea $x$ en $P$ y escogemos elementos $x_i$ de $G$ y enteros $r_i$, $1\leq i\leq t$ que cumplan las ecuaciones del teorema 11. Entonces si $n=|G:P|$, tenemos que:

$$x_i x^{r_i} x_i^{-1} \in P \qquad 1\leq i\leq t \quad \text{---}(25)$$

$$x\tau \equiv \prod_{i=1}^{t} x_i x^{r_i} x_i^{-1} \quad \operatorname{mod}(P^*) \quad \text{---}(26)$$

Como $P/P^*$ es abeliano podemos reescribir (26) como:

$$x\tau = \prod_{i=1}^{t} x_i x^{r_i} x_i^{-1} = \prod x^{r_i} x^{-r_i} x_i x^{r_i} x_i^{-1} \equiv \left(\prod x^{r_i}\right)\left(\prod x^{-r_i} x_i x^{r_i} x_i^{-1}\right) \operatorname{mod}(P^*) \quad \text{---}(27)$$

Pero $x^{-r_i} x_i x^{r_i} x_i^{-1} = (x^{r_i})^{-1} x_i x^{r_i} x_i^{-1} \in P^*$ ya que $x^{r_i}$ y $x_i x^{r_i} x_i^{-1}$ están en $P$ y son conjugados en $G$. Entonces (27) se reduce a:

$$x\tau \equiv \prod_{i=1}^{t} x^{r_i} = x^{\sum_{i=1}^{t} r_i} = x^{n} \quad \operatorname{mod}(P^*) \quad \text{---}(28)$$

Por otro lado $(n,p)=1$ ya que $|G:P| = n$ es primo relativo con $p$. Si $x \notin P^*$, se sigue por (28) que $x\tau \notin P^*$. En otras palabras $\tau$ mapea representantes de las distintas clases de $P^*$ en $P$ en clases distintas de $P^*$ en $P$; por lo tanto $\tau$ mapea $P$ **sobre** $P/P^*$. Entonces $(G)\tau = P/P^*$, por lo tanto $G/K \cong P/P^*$.

Teorema 15.-

Sea $P$ un 2-subgrupo de Sylow cíclico de $G$. Entonces $G$ tiene un $p$-complemento normal.

Demostración.

Sea $N = N_G(P)$ y $C = C_G(P)$, tenemos que $N/C$ es un $2'$-grupo de automorfismos de $P$. Pero $A(P)$ es un 2-grupo por el lema (7) y por lo tanto $N = C$. Entonces $P \subseteq Z(N)$ y la conclusión deseada se sigue del teorema 14.

B

Definición.

Un grupo $E$ es abeliano elemental si $pE = E$ para algún primo $p$

Definiremos ahora al grupo de los cuaternios generalizados y al grupo diédrico.

Definición.-

Un grupo de <u>cuaternios generalizados</u> $Q_n$, $n \geq 3$ es un grupo de orden $2^n$ que tiene generadores $a$ y $b$, relaciones:

$$a^{2^{n-2}} = b^2 = (ab)^2$$

Si $n = 3$ entonces $Q_3$ es el grupo de los cuaternios que denotaremos por $Q$

El grupo <u>diédrico</u> $D_n$, $n \geq 2$ es un grupo de orden $2n$ generado por dos elementos $s, t$ que cumplen con las relaciones:

$$s^n = 1 \qquad t^2 = 1 \qquad tst = s^{-1}$$

Denotaremos al grupo cíclico de orden $n$ por $Z(n)$. En el teorema 16 se usará el hecho siguiente:

Existen 5 grupos distintos de orden 8 a saber:

3 grupos abelianos.

$D_4$

$Q$

Demostraremos el siguiente lema

Lema: [illegible]-

Sean [illegible] elementos de [illegible] y supongamos que [illegible] conmuta con [illegible] e [illegible]. Entonces, para toda [illegible]

i).- $[x,y]^{n} = [x^{n}, y]$

ii).- $(xy)^{n} = [\,\text{[illegible]}\,]^{\text{[illegible]}/2}\, x^{n} y^{n}$

Demostración

Para probar [illegible] usaremos inducción en $n$

Para $n=1$ es trivial.

$[x,y]^{n-1}[x,y] = x^{-1}[x,y]^{n-1}$ [illegible] por hipótesis

$= x^{-1}[x^{n-1}, y]\,y^{-1}xy$ por hipótesis de inducción

$= x^{-1}(x^{-(n-1)}y^{-1}x^{n-1}y)\,y^{-1}xy$

$= [x^{n-1}, y]$ [illegible]

Afirmamos que $[x^{-1},y]=[x,y]^{-1}$. Por hipótesis $x[y,x]=[y,x]x$, lo cual implica que $xy^{-1}x^{-1}y = y^{-1}x^{-1}yx$, es decir, $[x^{-1},y]=[y,x]$. Pero siempre se tiene que $[y,x]=[x,y]^{-1}$. Por lo tanto (i) se cumple para toda $n$.

Para probar la segunda identidad para $n \geq 0$ usaremos de nuevo inducción. Para $n=1$ es trivial.

Por hipótesis de inducción

$(xy)^{n}xy = [y,x]^{n(n-1)/2}$ [illegible] $= [y,x]^{n(n-1)/2}$ [illegible] $[x,y^{-n}]\,y^{n+1}$

Por (i),

$[x,y^{n}]$ [illegible] $^{-1} = [y,x]^{n}$

Entonces

$(xy)^{n+1} = [y,x]^{\text{[illegible]}}$ [illegible] $x^{n+1}y^{n+1}$

$= [\,\text{[illegible]}\,]^{\text{[illegible]}}$ [illegible] $y^{n+1}$

Si [illegible] la demostración es análoga.

Teorema [illegible].–

Sea $G$ un $p$-grupo con un único subgrupo de orden $p$ y que contenga más de un subgrupo cíclico de índice $p$. Entonces $G \cong Q$ los cuaternios.

Demostración.

Si $H$ es un subgrupo de índice $p$, entonces $H \triangleleft G$ ya que como $G$ es un $p$-grupo entonces es nilpotente y todo subgrupo de índice primo en un grupo nilpotente es normal. Por lo tanto, si $x \in G$ entonces $xH \in G/H$, un grupo de orden $p$. Por lo consiguiente $x^p \in H$.

Sean $A = \langle a \rangle$ y $B = \langle b \rangle$ subgrupos cíclicos distintos de índice $p$ y sea $D = A \cap B$; $D \triangleleft G$ al ser la intersección de subgrupos normales. Por la observación del párrafo anterior se tiene que:

$$G^p = \{x^p \mid x \in G\} \subset D$$

Al ser $A, B$ dos subgrupos normales máximos de $G$ entonces $G = AB$. Por lo tanto

$$[G:D] = p^2$$

Se sigue entonces que $G/D$ es abeliano, por lo tanto $G' \subset D$. Al ser $G = AB$, todo elemento $x$ en $G$ es el producto de potencias de $a$ y $b$. Por lo consiguiente, un elemento $d \in D$ es simultáneamente una potencia de $a$ y una potencia de $b$, por lo tanto $d$ conmuta con $x$. Entonces $D \subset Z(G)$; si $D \neq Z(G)$, para $p^2 = [G:D] = (*)$
$(*) = [G:Z(G)][Z(G):D]$ y $[G:Z(G)] \neq p$

Ahora bien, $G' \subset D = Z(G)$, por lo tanto las hipótesis del lema 8 se cumplen. Entonces, para toda $x, y \in G$

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

puesto que $y^p \in D = Z(G)$ y por lo tanto

$$(xy)^p = [y,x]^{p(p-1)/2}\, x^p y^p$$

Si $p$ es impar, tenemos que $(xy)^p = x^p y^p$, es decir $x \to x^p$ es un homomorfismo. Hacemos $G_p = \{x \in G \mid x^p = 1\}$, entonces, como $G_p$ y $G^p$ son subgrupos y $[G:G_p] = |G^p|$, entonces

$$|G_p| = [G:G_p] = [G:D][D:G^p] \geq p^2$$

Pero al contener $H_p$ un subgrupo abeliano elemental con al menos $p^2$ elementos, entonces tiene más de un grupo de orden $p$, lo cual es una contradicción. Por lo tanto $p = 2$.

Ahora, $H/D = H/Z(H)$ es el 4-grupo con generadores [illegible] y [illegible]. Podemos substituir $a$ y $b$ por otros generadores de $A = $ [illegible] y $B = \langle b \rangle$ respectivamente. En particular, $ab^m \notin$ [illegible] si $m$ es impar. Además, como [illegible] es cíclico y de índice 2 en $A \cap B$ tenemos que $\langle a^2 \rangle = D = \langle b^2 \rangle$, por lo tanto $a^{2} = b^{2m}$ para alguna $m$ impar. Finalmente, notamos que [illegible] y que $\langle ab^m \rangle$ es otro subgrupo cíclico de índice 2.

En efecto, como [illegible] tenemos entonces que [illegible], sabemos que $\forall\, x, y \in H$ $[x, y]^2 = 1$, por lo tanto $(xy)^2 = (xy)$ [illegible] $x^2 y^2 = x^2 y^2$

En particular $(ab^{-m})^2 = a^2 b^{-2m} = 1$, es decir, $\langle ab^{-m} \rangle$ tiene orden cuatro. Demostraremos que $D = \langle (ab^{-m})^2 \rangle$. Si esto último no fuese cierto entonces se tendría que $(ab^{-m})^2 = a^{4r}$. Consideremos $(ab^{-m})a^{-2r}$, entonces:

$$((ab^{-m})a^{-2r})^2 = a^{4r} \cdot a^{-4r} = 1$$

y como $((ab^{-m})^2)^2 = 1$ entonces $(ab^{-m})a^{-2r} = (ab^{-m})^2 \quad \therefore \quad a^{-2r} = ab^{-m}$

$$\therefore\ ab^m \in \langle a \rangle \text{ lo cual no es posible.}$$

Como $[\langle ab^{-m} \rangle : \langle (ab^{-m})^2 \rangle] = 2$, concluimos que $\langle ab^{-m} \rangle$ es un grupo cíclico de $H$ de índice 2.

Al generar $(ab^{-m})^2$ a $D$, se ha probado que $|D| = 2$, por lo tanto $|H| = 8$. Concluimos entonces que $H$ es isomorfo a $Q$.

Demostraremos ahora el "teorema importante" que se mencionó en la introducción.

**Teorema 17.-**

Un $p$-grupo finito $G$ que tiene un subgrupo único de de orden $p$ es cíclico ó un grupo de cuaternios generalizado.

Demostración

Se usará inducción sobre $n$, donde $n$ es tal que $|G| = p^n$. Es claro que el teorema es cierto si $n = 0$.

Supongamos primero que $p$ es impar. Si $n > 0$ entonces tiene un subgrupo (H) de índice $p$ que debe ser cíclico por la hipótesis de inducción. No puede existir otro subgrupo cíclico de índice $p$ distinto de $H$ ya que por el teorema 14, $G$ sería igual a los cuaternios. Por lo tanto $H$ es el único subgrupo máximo de $G$ y por lo consiguiente $H$ contiene a todo subgrupo propio de $G$. Supongamos ahora que $G$ no es cíclico, entonces para toda $x$ en $G$, $\langle x \rangle$ es un subgrupo propio. Por lo tanto $\langle x \rangle \subset H \quad \forall\, x \in G$ y $G \subset H$ lo cual no es posible. Podemos concluir entonces que $G$ es cíclico y el teorema ha sido probado si $p$ es impar.

Supongamos ahora que $|G| \geq 16$. Demostraremos que $G$ contiene un subgrupo cíclico de índice $2$, pero antes mostraremos que $G$ contiene un subgrupo normal $H$ de índice $4$. Si $|G| = 16$, entonces $G$ contiene un subgrupo normal de índice $4$ y por lo tanto, de orden cuatro. $H$ es cíclico ya que si no lo fuese tendría tres elementos de orden $2$. Si $|G| = 2^n > 16$, entonces un subgrupo $H$ de $G$ que tenga índice $2$ es cíclico ó un grupo de cuaternios generalizado por la hipótesis de inducción. En cualquier caso, $H$ contiene un único subgrupo cíclico de orden $2^{n-2}$ ya que si tuviese más de un subgrupo con esta propiedad, se tendría que $H$ es igual a $Q$ por el teorema $16$ y como $|Q| = 8 = 2^{n-1}$ entonces $n = 4$ lo cual no es posible.

Denotemos a este subgrupo por $\langle a \rangle$, entonces $\langle a \rangle$ es un subgrupo característico de $H$ y por lo tanto $\langle a \rangle$ es un subgrupo normal cíclico de $G$ de índice cuatro.

Es claro entonces que podemos suponer que $|G| = 2^n$ donde $n > 4$. Para encontrar un subgrupo cíclico de índice $2$, consideremos $G/\langle a \rangle$ que es un grupo de orden $4$. Tenemos entonces dos casos:

i).- $G/\langle a \rangle$ es cíclico

ii).- $G/\langle a \rangle$ tiene tres elementos de orden $2$.

Si $G/\langle a \rangle \cong \langle \bar{b} \rangle$ y $b \in G$ con $b \mapsto \bar{b}$, entonces $G = \langle a, b \rangle$ y $\langle a, b^2 \rangle$ es un subgrupo cíclico de índice $2$ de $G$. Si $\langle a, b^2 \rangle$ es abeliano entonces es cíclico ya que todo $p$-grupo abeliano que posee un único subgrupo de orden $p$ es cíclico. Si $\langle a, b^2 \rangle$ no es abeliano entonces, por hipótesis de inducción, es un grupo de cuaternios generalizado. En particular, podemos suponer que $b^{-2} a b^2 = a^{-1}$. Ahora bien, como $\langle a \rangle \triangleleft G$, se tiene que $b^{-1} a b = a^i$ para alguna $i$. Entonces:

$$a^{-1} = b^{-2} a b^2 = b^{-1}(b^{-1} a b) b = b^{-1} a^i b = a^{i^2}$$

Por lo tanto $i^2 \equiv -1 \mod(2^{n-2})$. Sin embargo esta congruencia no tiene solución para $n > 4$. (Si $n-2 = 2$ hacemos simplemente el cálculo, si $n-2 \geq 3$ usamos el lema 7).

Supongamos ahora que $G/\langle a \rangle$ tiene tres elementos de orden $2$. (Recordemos que nuestro propósito es demostrar que $G$ contiene un subgrupo cíclico de orden $2^{n-1}$). Entonces sabemos que [illegible] es un 2- grupo, por lo tanto existen elementos $b, c \in E$ con [illegible] y con $\langle a, b \rangle$, [illegible], [illegible] cada uno de índice 2 en [illegible]. Si $\langle a, b \rangle$ ó [illegible] es cíclico, la afirmación es cierta, de lo contrario, son cuaternios generalizados por hipótesis de inducción. En particular, existen ecuaciones [illegible] $= c^{-1} a$ [illegible]. Se sigue que [illegible] y [illegible] es abeliano, por lo tanto cíclico.

Hemos demostrado que $E$ debe contener un subgrupo cíclico $\langle \alpha \rangle$ de índice 2. Escogemos [illegible] $E$, $\beta \notin \langle \alpha \rangle$. Como $[E : \langle \alpha \rangle] = 2$ tenemos que $\beta^2 \in \langle \alpha \rangle$. Cambiando de generador, si es necesario, tenemos que

$$\beta^2 = \alpha^{2^r}$$

Notemos que $r \leq n-2$ (si $r > n-2$, entonces $\beta$ es un segundo elemento de orden 2). Además, podemos suponer que $\alpha$ y $\beta$ no conmutan ya que en caso contrario $E$ sería abeliano y por lo tanto cíclico. Por el lema 7, se tiene que:

$$\beta^{-1} \alpha \beta = \alpha^t$$

donde $t = -1, -1 + 2^{n-2}, 1 + 2^{n-2}$ (ya que $\alpha$ tiene orden $2^{n-1}$). Eliminaremos las dos últimas posibilidades de $t$.

Supongamos que $t = 1 + 2^{n-2}$. Para todo entero $m$

$$(\alpha^m \beta)^2 = \alpha^m \beta^2 (\beta^{-1} \alpha^m \beta) = \alpha^{2s}$$

donde $s = 2^{r-1} + m(1 + 2^{n-3})$. Como $1 + 2^{n-3}$ es impar $(n \geq 4)$ podemos resolver la congruencia

$$2^{r-1} + m(1 + 2^{n-3}) \equiv 0 \mod (2^{n-2})$$

Para esta elección de $m$, tenemos que $(\alpha^m \beta)^2 = \alpha^{2s}$ $\alpha^{2s} =$ [illegible] $^{2^{n-1}} = 1$. Entonces $\alpha^m \beta \notin \langle \alpha \rangle$ es un nuevo elemento de orden 2.

Supongamos que $t = -1 + 2^{n-2}$ entonces:

$$2^r \equiv 2^r (-1 + 2^{n-2}) \mod (2^{n-1})$$

Por lo tanto

$$2^{r} \equiv 0 \mod (2^{n-2})$$

y $r = n-2$. Pero entonces

$$(\alpha\beta)^2 = \alpha\beta^2(\beta^{-1}\alpha\beta) = \alpha^{[illegible]} = \alpha^{2^{n-2}} \alpha^{2^{n-2}} = 1$$

por lo tanto un segundo elemento de orden 2 ha sido exhibido.

Por lo tanto $E = \langle \alpha, \beta \rangle$, donde

$$\alpha^{2^{n-1}} = 1 \quad [illegible] \quad \beta^2 = \alpha^{2^r}$$

Falta demostrar que $r = n-2$. Como [illegible] $= -1$, entonces $2^r \equiv$ [illegible] $\mod (2^{[illegible]})$, por lo tanto $2^{r+1} \equiv 0 \mod (2^{[illegible]})$ y $r = n-2$.

C

Definición

Un grupo de permutaciones $G$ que actúa en un conjunto $S$ se dice que es <u>transitiva en $S$</u> si para $S$, $S'$ en $S$, existe un elemento $x$ en $G$ tal que $(S)x = S'$ y se dice que $G$ es <u>doble transitivo en $S$</u> si para todo conjunto de parejas $(S_1, S_2)$ y $(S_1', S_2')$ con $S_i, S_i' \in S$ $1 \le i \le 2$, $S_1 \neq S_2$, $S_1' \neq S_2'$, existe un elemento $x$ en $G$ tal que $(S_i)x = S_i'$ $1 \le i \le 2$. El entero $|S|$ se llama el <u>grado de $G$</u>.

En todo grupo de permutaciones $G$ que actúa en un conjunto $S$, el subconjunto de $G$ que deja invariante un subconjunto $T$ de $S$ es claramente un subgrupo de $G$.

Sea $H$ un subgrupo de $G$ y sea $Hx_i$, $x_i \in G$, $1 \le i \le n$, un conjunto completo de clases de $H$ en $G$. Denotemos al conjunto de esas clases por $S$. Entonces para $x$ en $G$, el mapeo $\pi_x$ definido por

$$(Hx_i)\pi_x = H(x_i x) \qquad 1 \le i \le n$$

es una permutación de $S$ ya que $H(x_i x) \in S$ y $H(x_i x) \neq H(x_j x)$ si $i \neq j$ pues si existiesen $i, j \in \{1, \ldots, n\}$ tales que $H(x_i x) = H(x_j x)$ con $i \neq j$ entonces se tendría que:

$Hx_i = Hx_j$ lo cual es una contradicción.

Además, para $x, y$ en $G$ $\pi_{xy} = \pi_x \pi_y$ ya que $\forall i$ tal que $1 \le i \le n$ $(Hx_i)\pi_{xy} = H(x_i(xy)) = H((x_i x)y) = (H(x_i x))\pi_y = (Hx_i)\pi_x \pi_y$

Por lo tanto el mapeo $\pi_H$ de $x$ en $\pi_x$ es un homomorfismo de $G$ en el grupo simétrico $S_n$ en el conjunto $S$. El núcleo $K$ de $\pi_H$ es el conjunto de elementos $x$ en $G$ que fijan a toda $Hx_i$. Equivalentemente, $x \in K$ sii $x \in x_i^{-1} H x_i$ $\forall\, 1 \le i \le n$.

En efecto $x \in K \Leftrightarrow \pi_H(x) = \pi_x = 1 \Leftrightarrow (Hx_i)\pi_x = Hx_i$ $\forall i, 1 \le i \le n \Leftrightarrow H(x_i x) = Hx_i$ $\forall i, 1 \le i \le n \Leftrightarrow x_i x x_i^{-1} \in H \Leftrightarrow x \in x_i^{-1} H x_i$ $\forall i$

$$\therefore K = \bigcap_{i=1}^{n} x_i^{-1} H x_i$$

Por lo tanto tenemos que $G/K$ es isomorfo a un grupo de permutaciones de $S$. Además, $G/K$ actúa transitivamente en $S$. Si $Hx_i$, $Hx_j$ son dos elementos de $S$ y hacemos $x = x_i^{-1} x_j$ entonces $\pi_x$ transforma $Hx_i$ en $Hx_j$.

Demostraremos ahora que $H^{x_i}$ es el subgrupo que fija a la letra $Hx_i$ de $S$.

Sea $x \in H^{x_i}$ $\therefore$ $x = x_i^{-1} h x_i$ con $h \in H$

$(Hx_i)\pi_x = Hx_i x = Hx_i(x_i^{-1}hx_i) = Hhx_i = Hx_i$

Si $x$ es tal que $(Hx_i)\pi_x = Hx_i x = Hx_i$ entonces $x_i x x_i^{-1} \in H$ $\therefore$ $x \in x_i^{-1}Hx_i = H^{x_i}$.

Llamamos a $\pi_H$ la representación en permutaciones transitiva de $G$ en las clases laterales derechas de $H$. Claramente $\pi_H$ está determinada totalmente por $H$ y es independiente de la elección de los representantes $x_i$ de $H$ en $G$.

En general, todo homomorfismo $\pi$ de $G$ en el grupo simétrico de un conjunto $S$ se llama una representación en permutaciones de $G$ en $S$. El entero $|S|$ se llama el grado de $\pi$. Decimos que $\pi$ es transitiva si $G\pi$ actúa transitivamente en $S$; análogamente se define que $\pi$ sea doble transitiva.

Si $\theta$ es un mapeo inyectivo de $S$ en un conjunto $S'$, entonces claramente la composición $\pi' = \theta^{-1}\pi\theta$ da una representación de $G$ en $S'$. Claramente la acción $G\pi'$ en $S'$ está determinada por la acción $G\pi$ en $S$ (junto con $\theta$) y viceversa. Bajo esta situación podremos decir que $\pi$ y $\pi'$ son equivalentes o son representaciones en permutaciones isomorfas de $G$.

Probaremos el siguiente teorema:

Teorema.-

Toda representación en permutaciones transitiva de $G$ es equivalente a una de las clases laterales derechas de un subgrupo $G$.

Demostración.

Sea $\pi$ una representación en permutaciones transitiva de $G$ en $S$, identificamos a $S$ con $\{1, \ldots, n\}$. Como antes, denotamos a la imagen de $x$ por $\pi_x$. Sea $H$ el subgrupo que fija a la letra $1$. Demostraremos que $\pi$ y $\pi_H$ son equivalentes.

Como $\pi$ es transitiva, existen elementos $x_i$ en $G$ tales que $(1)\pi_{x_i} = i$ con $1 \leq i \leq n$. Entonces como $\pi$ es un homomorfismo $(1)\pi_{hx_i} = i$ para toda $h$ en $H$. Recíprocamente, si $(1)\pi_x = i$ entonces $(1)\pi_{xx_i^{-1}} = 1$ y por lo tanto $x \in Hx_i$. Concluimos entonces que $Hx_i$ es el conjunto de elementos que transforman $1$ en $i$. En particular $Hx_i \neq Hx_j$ si $i \neq j$.

Además, como un elemento de $G$ transforma $1$ en $i$ para alguna $i$, todo elemento de $G$ pertenece a $Hx_i$ para alguna $i$, $1 \le i \le n$. Por lo tanto, el conjunto $\{Hx_i \mid 1 \le i \le n\}$ es un conjunto completo de clases laterales derechas de $H$ en $G$.

Hagamos ahora $(i)\theta = Hx_i$, $1 \le i \le n$, $\pi' = \theta^{-1}\pi\theta$. Entonces $\pi'$ es una representación en permutaciones de $G$ en $S'$ que es equivalente a $\pi$. Además, sea $x \in G$ e $i \in S$, supongamos que $H(x_i x) = Hx_j$, en tal caso $(1)\pi_{x_i x} = j$ y por lo tanto $(i)\pi_x = j$. Aplicando $\theta$ obtenemos que $(Hx_i)\pi'_x = Hx_j = H(x_i x)$; por lo tanto $\pi' = \pi_H$ y el teorema está probado.

El siguiente resultado nos dá un criterio importante para decidir cuando un grupo de permutaciones transitivo es doble transitivo.

Teorema 9.-

Sea $G$ un grupo de permutaciones transitivo que actúa en un conjunto $S$ y sea $H$ el subgrupo de $G$ que fija una letra. Entonces se tiene que:

i).- $G$ es doble transitivo sii $H$ actúa transitivamente en las letras restantes.

ii).- Si $G$ es doble transitivo y $|G:H| = n$, entonces $|G| = dn(n-1)$ donde $d$ es el orden de un subgrupo que fija a dos letras.

Demostración.

Sea $S = \{1, 2, \ldots, n\}$ y supongamos que $H$ fija a la letra $1$. Sean $\{i, j\}$, $\{i', j'\}$ dos parejas de $S$ con $i \neq j$, $i' \neq j'$ y supongamos que $H$ actúa transitivamente en $\{2, \ldots, n\}$. Entonces $i' = ix$ para alguna $x$ en $G$. Hagamos $k = jx$, entonces $k \neq i'$ si $i \neq j$, ya que si $k = i'$ entonces $i = j$. Ahora bien, el subgrupo que fija a la letra $i'$ es conjugado de $H$.

Denotemos por $H'$ al subgrupo que fija a la letra $i'$; existe $y \in G$ tal que $1y = i'$. Por lo tanto, $y^{-1}H'y$ ... $y^{-1}xy'$ fija a la letra $i'$. Si $z \in H'$ entonces $yzy^{-1}$ fija a la letra $1$ y por lo tanto pertenece a $H$, i.e., $z \in H^y$. Por lo tanto $H'$ es transitivo en las letras diferentes de $i'$. Podemos concluir, entonces que existe un elemento $z$ de $G$ que fija a la letra $i'$ y transforma $k$ en $j'$ (ya que $k$ y $j'$ son distintos de $i'$).

El elemento $g = xy$ transforma [illegible] en [illegible] y [illegible] en [illegible]. Por lo tanto [illegible] es doble transitivo. Además, si [illegible] denota al subgrupo de H que fija a la letra [illegible], se sigue por el teorema anterior que [illegible] y por la misma razón [illegible]. Por lo tanto [illegible], donde [illegible].

Si [illegible] es doble transitivo e [illegible] entonces existe un elemento $x$ en H tal que [illegible]. (Consideramos las parejas [illegible] e [illegible]). Por lo tanto H es transitivo en [illegible].

Mencionaremos ahora algunos resultados que no se demostrarán pero se darán las referencias en donde se puede encontrar las demostraciones de estos últimos.

Definición.

Sea G un grupo de permutaciones transitivo tal que la identidad de G es el único elemento que fija más de una letra, pero el subgrupo que fija una letra es no-trivial, entonces G es un grupo de Frobenius.

Teorema de Frobenius.

Sea G un grupo de Frobenius y sea H el subgrupo que fija una letra. Entonces el subconjunto de G que consiste de la identidad y aquellos elementos que no fijan letras forman un subgrupo normal K de G de orden [illegible].

El subgrupo K se llama usualmente el núcleo de Frobenius de G, el subgrupo de G que fija a una letra se llamará un complemento de Frobenius.

La demostración de este importante teorema se puede encontrar, por ejemplo, en [illegible].

Una consecuencia inmediata del teorema de Frobenius es el siguiente resultado.

Proposición [illegible].-

Sea [illegible] un grupo de Frobenius con complemento H y núcleo K. Entonces [illegible] con [illegible], es decir, es el producto semidirecto de K por H.

Demostración.

Como los elementos, distintos de la identidad, de $X$ no fijan letras entonces $H\cap X=1$. Pero $|X|=|G:H|$, por el teorema de Frobenius y por lo tanto $|G|=|HX|$. Entonces $G=HX$.

Daremos ahora una condición para que un grupo $G$ sea de Frobenius con complemento $H$ que es independiente del teorema de Frobenius.

Teorema 20.-

Sea $H$ un subgrupo no trivial de $G$. Entonces $G$ es un grupo de Frobenius con complemento $H$ sii $H$ es ajeno de sus conjugados y es su propio normalizador en $G$.

Demostración.

Sea $Hx_i$, $x_i\in G$, $x_1=1$, $1\le i\le n$, un conjunto completo de clases de $H$ en $G$. Si algún elemento de $G$ fija dos clases de $H$, entonces por transitividad algún elemento de $H$, distinto de uno, fija una de las clases $Hx_i$ con $i>1$. Por lo tanto $G$ es un grupo de Frobenius con complemento $H$ sii ningún elemento, distinto de la identidad, de $H$ fija cualquier $Hx_i$ con $i>1$. Pero para $1\neq h\in H$, $Hx_i=Hx_ih$ sii $x_ihx_i^{-1}\in H$, o equivalentemente, $h\in H\cap H^{x_i}$. Por lo tanto $G$ y $H$ tienen las propiedades dadas sii

$$H\cap H^{x_i}=1 \qquad 2\le i\le n \quad --- (1)$$

Afirmamos que (1) es equivalente a las dos condiciones del teorema. Supongamos (1). Si $N_G(H)\supset H$, podemos tomar $x_2$ en $N_G(H)-H$ para obtener $H\cap H^{x_2}=H$, una contradicción; por lo tanto $N_G(H)=H$. Además, si $x\in G-H$, entonces $x\in Hx_i$ para alguna $i>1$ $H\cap H^{x}=H\cap H^{x_i}=1$. Recíprocamente, si $N_G(H)=H$ y es ajeno de sus conjugados, entonces $H\cap H^{x}=1$ para toda $x\in G-H$ y por lo tanto (1) se cumple.

Definición.

Un grupo no trivial $A$ de automorfismos de $G$ se dice que es un grupo regular de automorfismos si todo elemento de $A$ distinto de la identidad, sólo deja invariante al elemento identidad de $G$.

Probaremos a continuación una proposición importante que se usará en (II).

Proposición [illegible].-

Si $A$ es un grupo regular de automorfismos de $G$ entonces el producto semidirecto de $A$ por $G$ es un grupo de Frobenius con núcleo $G$ y complemento $A$.

Demostración

Sea $Ax_i$, $x_i \in G$, $x_1 = 1$, $1 \leq i \leq n$ un conjunto completo de clases de $A$ en $AG$. Deseamos demostrar que $A \cap A^{x_i} = \{1\}$ para $2 \leq i \leq n$. Supongamos que existe $i \neq 1$ tal que $A \cap A^{x_i} \neq \{1\}$ y sea $\varphi \in A \cap A^{x_i}$ ∴ $\varphi = x_i^{-1} \psi x_i$ con $\psi \in A$. Como $\forall h \in G$ $\psi^{-1} h \psi = (h)\psi$ entonces:

$$x_i^{-1} \psi^{-1} x_i h x_i^{-1} \psi x_i = x_i^{-1} (x_i h x_i^{-1}) \psi x_i = (h)\varphi$$

Sea $g \in G$ tal que $g = (x_i^{-1})\psi x_i$ ∴ $(h)\varphi = g^{-1} (h)\psi g$

Por lo tanto $\varphi = i_g \psi$ donde $i_g$ es el automorfismo interno definido por $g$. Entonces $i_g \in A$.

Si $i_g = 1$ entonces $\varphi = \psi$ ∴ $\psi = x_i^{-1} \psi x_i$ ∴ $1 = \psi^{-1} x_i^{-1} \psi x_i$ ∴ $(x_i^{-1})\psi = x_i^{-1}$ ∴ $x_i = 1$ lo cual no es posible.

Por lo tanto $i_g \in A^{\#}$, i.e., $i_g$ no fija a algún elemento distinto de la identidad. Ahora bien, existe $g_1 \in G$ tal que $(g_1)\psi = x_i$

$$\therefore (h)\varphi = (g_1^{-1} x_i h x_i^{-1} g_1)\psi \quad \forall h \in G$$

La fórmula es en particular, cierta si $h = x_i^{-1} g_1$

$$\therefore (x_i^{-1} g_1)\varphi = (g_1^{-1} x_i (x_i^{-1} g_1) x_i^{-1} g_1)\psi = (x_i^{-1} g_1)\psi$$

$x_i^{-1} g_1 \neq 1$ ya que si $x_i^{-1} g_1 = 1$ entonces $g_1 = x_i$. Por lo tanto obtendríamos que $\psi(x_i) = x_i$ y como $\psi$ pertenece a $A^{\#}$, concluiríamos que $x_i = 1$, que es contrario a la hipótesis.

Sin embargo, $(x_i^{-1} g_1)\varphi = (g_1^{-1})\psi (x_i)\psi (x_i^{-1} g_1)\psi (x_i^{-1})\psi (g_1)\psi$

$$= x_i^{-1} (x_i)\psi (x_i^{-1} g_1)\psi (x_i^{-1})\psi x_i = g^{-1} \psi (x_i^{-1} g_1) g = (x_i^{-1} g_1)\varphi$$

Por lo tanto $i_g \in A^{\#}$ fija a $(x_i^{-1} g_1)\varphi$. Como $x_i^{-1} g \neq 1$ entonces $x_i = 1$ lo cual es una contradicción.

Por lo tanto $AG$ es un grupo de Frobenius con complemento $A$ y núcleo $G$.

Teorema 21.-

Sea $G$ un grupo de Frobenius con complemento $H$ y núcleo $K$. Entonces:

i).- Todo elemento distinto de la identidad de $H$ induce por conjugación un automorfismo de $K$ que fija sólo al elemento identidad de $K$

ii).- $C_G(y) \leq K$ para todo $1 \neq y \in K$

Este teorema nos dará la clave para analizar la estructura de un (ZT)-grupo; este tipo de grupos se estudiarán ampliamente en (II).

Demostración.

Como $G$ es transitivo y $H$ es el subgrupo que fija una letra, nuestra representación es equivalente a una de las clases de $H$. En este caso, podemos tomar elementos de $K$ como representantes de las clases de $H$ en $G$. Supongamos que $h^{-1}kh=k$ para alguna $1\neq h$ en $H$ y $1\neq k$ en $K$. Entonces es inmediato que $h$ fija a la clase $Hk$ así como a la clase $H$. Pero por la definición de un grupo de Frobenius, sólo la identidad fija más de una letra. Entonces $h^{-1}kh\neq k$ para todo $1\neq h$ en $H$ y $1\neq k$ en $K$. En particular (i) se cumple.

Ahora bien, por (i) ningún elemento de $K$ distinto de la identidad, centraliza algún elemento de un conjugado de $H^{\#}$. Pero los conjugados de $H$ son simplemente los subgrupos que fijan a una letra y por lo tanto por el teorema de Frobenius $K$ consiste precisamente de aquellos elementos de $G$ que no están en ningún conjugado de $H^{\#}$. Concluimos que $C_G(y)\leq K$ para toda $y$ en $K^{\#}$, lo cual prueba (ii).

Teorema 22.-

Sea $G$ un grupo de Frobenius con núcleo $K$. Si $A\triangleleft G$ entonces $A<K$ ó $K<A$.

demostración.

Supongamos que $A\not< K$. Entonces existe $h\in A$ tal que $h\notin K$. $h$ define un automorfismo de $K$ por conjugación.

En efecto, sea $\varphi_h: K\longrightarrow K$ tal que

$$(k)\varphi_h = h^{-1}kh \qquad \forall\, k\in K$$

$h^{-1}kh\in K$ ya que $K\triangleleft G$

$\varphi_h$ es un automorfismo que no tiene punto fijo ya que si existe $k\in K^{\#}$ tal que $(k)\varphi_h=k$ entonces $h^{-1}kh=k$. Por lo tanto $h\in C_G(k)<K$, lo cual no es posible.

Definimos ahora $\varphi: K\longrightarrow K$ la función tal que:

$$(k)\varphi = k^{-1}\,(k)\varphi_h$$

Si $k, k_1\in K$ son tales que $(k)\varphi=(k_1)\varphi$ entonces $k^{-1}(k)\varphi_h = k_1^{-1}(k_1)\varphi_h \Rightarrow k_1k^{-1}=(k_1k^{-1})\varphi_h \Rightarrow k_1k^{-1}=1 \Rightarrow k=k_1$. Por lo tanto $\varphi$ es una función biyectiva.

$\therefore$ $K=\{k^{-1}h^{-1}kh \ldots\} \ldots K < A$ ya que $A\triangleleft G$.

Teorema [illegible] (Brauer y Suzuki).-

Sea [illegible] un grupo de orden par. Si [illegible] es un 2-subgrupo de Sylow de [illegible] que es un [illegible], [illegible]. Entonces [illegible] no es simple.

Teorema [illegible] (Brauer y Suzuki) -

Sea [illegible] un grupo finito cuyo 2-subgrupo de Sylow es un [illegible], [illegible]. Si [illegible] es el único subgrupo máximo de orden impar entonces [illegible] tiene centro de orden 2.

Las demostraciones de estos dos teoremas se pueden encontrar en [illegible].

II).-

Definición.

Un grupo $G$ se dice que es un (ZT)-grupo si:

i).- $G$ es un grupo doble transitivo en $N+1$ letras.

ii).- La identidad es el único elemento que deja invariante a tres letras distintas.

iii).- $G$ no contiene un subgrupo normal de orden $N+1$.

iv).- $N$ es par.

Grupos finitos que satisfacen las condiciones (i) (ii) y (iii) han sido estudiados por Zassenhaus en [24] y por Feit en [30]. El teorema principal de Feit en [30] es que bajo las suposiciones (i), (ii) y (iii), el número $N$ debe de ser una potencia de un número primo. Por lo tanto, en (ZT)-grupos, $N$ es una potencia de 2.

Probaremos ahora la siguiente proposición:

Proposición 3

Sea $G$ un (ZT)-grupo y sea $F$ el subgrupo que fija una letra, entonces tenemos que:

i).- $F$ es un grupo de Frobenius con núcleo $Q$ de orden $N$ y complemento $K$.

ii).- $F = N_G(Q)$ y $C_G(\sigma) \subseteq Q$ $\forall\, \sigma \in Q$, $\sigma \neq 1$

iii).- $Q$ es un 2-subgrupo de Sylow de $G$ y un elemento distinto de uno de $K$ induce un automorfismo de $Q$ que fija sólo a la identidad.

iv).- $|G| = e \cdot N(N+1)$ donde $e = |K|$ y $e$ divide a $N-1$.

Demostración.

Sea $G$ un (ZT)-grupo que actua en $S = \{1, \ldots, N+1\}$ y sea $F$ el subgrupo de $G$ que fija a $1$.

Como $G$ es doble transitivo y sólo la identidad fija a tres letras distintas, entonces $F$ actúa transitivamente en $T = S - \{1\}$ y únicamente la identidad de $F$ fija a dos letras. Por la definición de un (ZT)-grupo, el subgrupo que fija a dos letras de $S$ y por lo tanto el subgrupo que fija una letra en $T$ es no trivial. Por lo tanto $F$ es un grupo de Frobenius en su acción en $T$, entonces por el teorema de Frobenius $F$ posee un subgrupo normal $Q$ de orden $N = [illegible]$, donde todo elemento de $Q$ distinto de la identidad no fija a ninguna letra de $F$. Además, existe un complemento de Frobenius $K$ en $F$ que es el subgrupo que fija a una letra de $F$, digamos $1 = 2$. Por lo tanto $K$ fija dos letras ($1$ y $2$).

Sea $y \in Q$ tal que $y \neq 1$ $\therefore (1)y = 1$ $\therefore (1)yx = (1)x$ con $x \in G$; $\therefore ((1)x)x^{-1}yx = (1)x$ $\therefore x^{-1}yx$ fija a la letra $(1)x$. Supongamos que $(a)x^{-1}yx = a$ con $a \in Q$

$\therefore (a)x^{-1}y = x^{-1}(a)$ $\quad \therefore (a)x^{-1} = 1$ ya que $y \in Q$ $\quad \therefore a = (1)x$

$\therefore x^{-1}yx$ sólo fija a la letra $(1)x$

$\therefore$ Si $x^{-1}yx \in Q$ entonces $(1)x = 1$ $\quad \therefore x \in F$

$\therefore N_G(Q) \subseteq F$; como $Q$ es un subgrupo normal de $F$ entonces $F \subseteq N_G(Q)$ $\quad \therefore N_G(Q) = F$

Sea $\pi \in C_G(y)$ donde $1 \neq y \in Q$ entonces sabemos que:

$$(1)\pi y = (1)y\pi = (1)\pi$$

es decir, $(1)\pi$ es invariante por $y$; al pertenecer $y$ a $Q$ se sigue que $(1)\pi = 1$.

Supongamos que $\pi$ deja otro símbolo $b$ invariante ($b \neq 1$) entonces:

$$(b)y\pi = (b)\pi y = (b)y$$

$\therefore \pi$ deja a $(b)y$ invariante. Como $b \neq (b)y$, entonces $\pi$ deja invariante a tres símbolos distintos. Por lo tanto $\pi$ es la identidad.

Podemos concluir entonces que todo elemento $\pi$ de $C_G(y)$ deja fijo sólo a la identidad y por lo consiguiente $\pi \in Q$.

$$\therefore C_G(y) \subseteq Q \quad \forall\, 1 \neq y \in Q$$

Sea $1 \neq k \in K$ y consideremos el automorfismo interno de $Q$ definido por $k$, i.e.:

$$\varphi_k(q) = k^{-1}qk \quad \forall q \in Q$$

Si existe $1 \neq q \in Q$ tal que $\varphi_k(q) = q$ entonces [illegible] $qk = kq$ [illegible] $k \in Q$ lo cual es imposible.

Por lo tanto, todo elemento, distinto de la identidad, de $K$ induce un automorfismo de $Q$ que fija sólo a la identidad.

Para $1 \neq 1$ [illegible] fija, el conjunto $\Gamma_q$ [illegible] debe consistir de [illegible] $|K|$ elementos distintos de [illegible], pero claramente para $q, q' \neq 1$ [illegible] se tiene que $\Gamma_q = \Gamma_{q'}$ ó $\Gamma_q \cap \Gamma_{q'} = \emptyset$.

En efecto, si para alguna $q \in Q$ [illegible] con [illegible] $\in K$ entonces [illegible] deja fijo a [illegible] lo cual no es posible (se ha supuesto que $h \neq h_1^{-1}$, si $h = h_1^{-1}$ entonces [illegible] fija a $q$).

Si existen $k, k_1 \in K$ tales que [illegible] entonces [illegible] $= q_1$ [illegible]

$\therefore \Gamma_{q_1} = \Gamma_q$. Análogamente $\Gamma_{q_1} = \Gamma_q$

$\therefore \Gamma_q = \Gamma_{q_1}$

Por lo tanto $|Q| - 1$ es un múltiplo de $e$. Por el teorema 17 tenemos que $|Q| = e(n+1)/K$ donde $e = |K|$. Como $F$ es un grupo de Frobenius $F = QK$ y como $e$ divide a $n-1$ entonces $e$ es un entero impar y el índice de $Q$ en $G$ es también impar. Por lo tanto $Q$ es un 2-subgrupo de Sylow de $G$.

Proposición 4.-

El grupo $K$ es un grupo cíclico y el normalizador $N_G(K)$ contiene una involución $\tau$.

Demostración.

Demostraremos primero que todos los p-subgrupos de Sylow de $K$ son cíclicos. Sabemos que $Q$ es un 2-subgrupo de Sylow. Consideremos el centro $Z(Q)$ de $Q$. En $Z(Q)$ tomemos a todos los elementos de orden 2, denotaremos por $Q'$ al subgrupo generado por todas las involuciones de $Z(Q)$. Entonces $Q'$ es un subgrupo característico de $Q$ abeliano cuyos elementos tienen orden 2 (excepto $e$).

Supongamos, si es posible, que $K$ contiene un subgrupo no cíclico de orden $q^2$, donde $q$ es un primo. El correspondiente grupo de automorfismos debe permutar los elementos de $Q'$ transitivamente en conjuntos de $q^2$ elementos; y al afectar un conjunto, sus generadores $Q_1$, $Q_2$ pueden tomarse como:

$$(P_{11}, P_{12} \dots P_{1q}) \dots (P_{21} \dots P_{2q}) \dots (P_{q1} \dots P_{qq})$$

y $$(P_{11}, P_{21} \dots P_{q1}) \dots (P_{12} \dots P_{q2}) \dots (P_{1q} P_{2q} \dots P_{qq})$$

Entonces en [illegible] el ciclo que contiene a $P_{11}$ es:

$$(P_{11}\ P_{1+i,2}\ P_{1+2i,3} \dots P_{1-i,q})$$

Como ninguno de estos automorfismos cambia a algún elemento (excepto la identidad), en sí mismo, el producto de los elementos en cualquier ciclo debe de ser la identidad. Por lo tanto:

$$P_{11} P_{12} \dots P_{1q} = e$$
$$P_{11} P_{21} \dots P_{q1} = e$$
$$P_{11} P_{1+i,2} \dots P_{1-i,q} = e \qquad (i = 1, 2, \dots, q-1)$$

y entonces $P_{11}^{q} \prod P_{ij} = e$ ó $P_{11}^{q} = e$. Esto no es posible y por lo tanto $K$ no contiene subgrupos no cíclicos de orden $q^2$. Demostraremos ahora que $K$ es abeliano y que $N_G(K)$ contiene una involución $\tau$.

Sean $a$ y $b$ los dos símbolos que son fijados por los elementos de $K$. Como $G$ es doble transitivo existe un elemento $\tau$ que intercambia a $a$ y $b$.

$\therefore \tau(a) = b$ y $\tau(b) = a$ [illegible] $(\tau^2)(a) = a$ $\forall\, n \in N$

$\therefore \tau^2(a) = \tau(\tau(a))$ [illegible]

Por lo tanto el orden de $\tau$ es par ya que si fuese impar se tendría que:

$$[illegible]$$ lo cual no es posible.

Entonces alguna potencia de $\tau$ es una involución $\pi$. Por la proposición 7, el centralizador [illegible] está contenido en un 2-subgrupo de Sylow de [illegible]. Como $\tau$ pertenece a [illegible], $\tau$ está contenido en un 2-subgrupo de Sylow y por lo tanto $\tau$ deja invariante un símbolo, digamos $c$. El elemento $\tau^2$ fija por lo tanto a tres símbolos distintos $a, b$ y $c$. Por la condición (ii) de los [illegible]-grupos, $\tau^2$ es la identidad.

Hemos demostrado que $\tau$ es una involución. Sea $k$ un elemento distinto de uno de $K$. Entonces tenemos que:

$$\tau^{-1} k \tau(a) = \tau^{-1} k(b) = [illegible] = a$$

y análogamente $\tau^{-1} k \tau(b) = b$. Estas identidades implican que $\tau$ está en el normalizador $N_G(K)$. Como $K$ es de orden impar, por la proposición tres $\tau$ no conmuta con ningún elemento distinto de la identidad de $K$. Por lo tanto el automorfismo interno definido por $\tau$ es de orden 2 y no tiene punto fijo; por el lema 2 concluimos que $K$ es abeliano y $\tau$ transforma todo elemento de $K$ en su inverso. Como todos los subgrupos de Sylow son cíclicos $K$ es cíclico.

Sabemos entonces que [illegible] ---(1). Si denotamos por $b$ la imagen de $a$ entonces el grupo $\tau^{-1} F \tau$ consiste de los elementos que dejan a $b$ invariante. Por lo tanto tenemos que:

$$F \cap \tau^{-1} F \tau = [illegible] \quad \text{ó} \quad Q \cap \tau^{-1} F \tau = [illegible] \quad \text{---(2)}$$

Proposición 5.-

Un elemento fuera de $F$ puede escribirse de manera única en la forma [illegible] con $\eta \in F$ y $\pi \in Q$.

Demostración.

Supongamos que se tiene [illegible] con $\eta, \eta' \in F$ y [illegible]. Entonces [illegible]. El lado izquierdo pertenece a [illegible] y el lado derecho a [illegible]. La ecuación (2) afirma que [illegible]. Por lo tanto $\pi = \pi'$ y [illegible]. Esto prueba la unicidad de la expresión. Al mismo tiempo hay exactamente [illegible] elementos de la forma [illegible] con $\eta \in F$ y [illegible] donde $h$ es el orden de $F$. Todos estos elementos están fuera de $F$ ya que si existiesen [illegible] tales que [illegible] entonces [illegible] lo cual no es posible.

Como el orden de [illegible] es [illegible], existen exactamente [illegible] elementos distintos fuera de $F$. Por lo tanto todo elemento fuera de $F$ puede escribirse como $\eta z\pi$, lo cual prueba la afirmación.

Probaremos ahora la siguiente proposición que se refiere a las involuciones de [illegible].

Proposición 6.- Un elemento $\eta z\pi$ de [illegible] $- F$ es una involución sii $\pi\eta \in K$.

Demostración

Si $\eta z\pi$ es una involución entonces se tiene que

$\eta z\pi\eta z\pi = 1$ ó $z\pi\eta z = \eta^{-1}\pi^{-1}$

Como $F \cap z^{-1}Fz = K$ por (1) concluimos que $\pi\eta \in K$. Por otra parte, si $\pi\eta \in K$ podemos escribir $\pi\eta = k^2$ con $k \in K$. Entonces:

$$\eta z\pi = \pi^{-1}k^2 z\pi = \pi^{-1}k^{-1}zk\pi$$

Por lo tanto $\eta z\pi$ es conjugada con $z$ y ciertamente es una involución.

La proposición anterior demuestra que una involución fuera de $F$ es conjugada con $z$ en [illegible]. El grupo [illegible] está fuera de $F$ y es un 2-subgrupo de Sylow. Tenemos entonces la siguiente proposición.

Proposición 7.- Toda involución de [illegible] es conjugada con $z$. Si $t$ es una involución de [illegible], $t$ está en el centro de [illegible] y toda involución de [illegible] distinta de $t$ puede escribirse como [illegible] con $k \in K$. El orden de [illegible] coincide con el número de involuciones de [illegible]

Demostración

Si [illegible] es una involución de [illegible] entonces [illegible] es una involución fuera de [illegible] tales que

[illegible] donde [illegible]

Por lo tanto, toda involución de [illegible] es conjugada con [illegible]

Como el centro de $Q$ contiene una involución [illegible] es un $2$-subgrupo de Sylow de $H$. Por otra parte, por la proposición 3 $C_H(\pi)$ está contenido en $Q$. Por lo tanto $C_H(\pi)$ coincide con $Q$. Si $\pi'$ es otra involución, $\pi'$ está también contenida en el centro de $Q$. Por lo tanto por el lema de Burnside, es conjugada con $\pi$ en el normalizador de $Q$ que es $F$ en nuestro caso. Como $F = QK$, existe un elemento $k \in K$ tal que $\pi' = k^{-1}\pi k$. Ningún elemento, distinto de la identidad, de $K$ conmuta con $\pi$ por lo tanto la última afirmación se sigue inmediatamente.

Lema 7.-

Si $N$ es un subgrupo normal de $H$ que contiene a $Q$, entonces dos involuciones de $N$ son conjugadas en $N$.

Demostración.

Toda involución de $H$ está contenida en $N$ ya que $N$ es un subgrupo normal que contiene a un $2$-subgrupo de Sylow. Como $Q$ no es normal en $H$ existe un subgrupo conjugado $Q'$ de $Q$ que es diferente de $Q$. Sean $\pi, \pi'$ dos involuciones de $Q$ y $Q'$ respectivamente y consideremos el producto $\pi\pi'$.

Si el orden de $\pi\pi'$ es par ($o(\pi\pi') = 2n$) entonces la involución $\alpha = \underbrace{\pi\pi' \cdots \pi\pi'}_{\text{"n-veces"}}$ conmuta con $\pi$ y $\pi'$. Por la proposición 3 $\pi$ y $\pi'$ deben de estar en el mismo $2$-subgrupo de Sylow de $H$. Esto contradice la elección de $\pi$ y $\pi'$.

Por lo tanto el orden de $\pi\pi'$ es impar y $\pi$ es conjugada de $\pi'$ en el grupo generado por $\{\pi, \pi'\}$.

$$\underbrace{\pi\pi' \cdots \pi\pi'}_{\text{"2n+1 veces"}} = 1 \Rightarrow \pi^{\alpha} \cdots = \pi' \qquad \alpha \in \langle \pi, \pi' \rangle$$

Si $\pi''$ es otra involución de $Q$, $\pi$ es conjugada con $\pi'$ en $N$, por lo tanto $\pi''$ es conjugada con $\pi$ en $N$.

Ahora bien, como el número de involuciones de $Q$ es igual al orden de $K$ (proposición 7) entonces el subgrupo normal del lema 7 contiene a $F$. Como $Q$ es un $2$-subgrupo de Sylow entonces [illegible]. Concluimos por lo tanto que $H$ es el único subgrupo normal que contiene a $Q$.

Definición.

Un grupo $G$ se dice que es un (CIT)-grupo si su orden es par y el centralizador de cualquier involución es un 2-grupo.

Demostraremos ahora el siguiente teorema.

Teorema 25.- Un (ZT)-grupo $G$ es un (CIT)-grupo simple no abeliano.

Demostración.

Por el inciso ii) de la proposición anterior $G$ es un (CIT)-grupo. Demostraremos ahora que $G$ es un grupo simple.

Supongamos que $G$ no es simple y sea $H$ el subgrupo normal propio mínimo de $G$. Por la observación anterior $H$ no contiene al subgrupo $Q$. $H$ no está contenido en $Q$ ya que $\tau^{-1}F\tau \cap F = K$. Sea $R_1$ igual a la intersección $H\cap Q$. El grupo $H\cap F$ es un subgrupo normal de $F$. Como $F$ es un grupo de Frobenius, $H\cap F$ está contenido en $Q$ por el teorema 22. Por lo tanto tenemos que $H\cap F = H\cap F\cap Q = R_1$. Tenemos entonces dos casos:

i).- $R_1 \neq \{e\}$

ii).- $R_1 = \{e\}$

Supongamos que $R_1 \neq \{e\}$. Entonces $H$ contiene a todas las involuciones de $G$ ya que dos involuciones de $G$ son conjugadas y $R_1$ contiene una involución. Si $R_1$ contiene más de una involución, tenemos que $N_H(R_1) \neq R_1$ ya que las involuciones de $R_1$ son conjugadas en $N_H(R_1)$.

En efecto, supongamos que $R_1$ es un subgrupo normal en $H$ entonces:

$$(h\tau\pi)^{-1} R_1 h\tau\pi = \pi^{-1}\tau h^{-1} R_1 h\tau\pi = \pi^{-1}\tau R_1 \tau\pi = R_1 \quad \text{ya que } H\cap F \trianglelefteq F$$

y $H$ no está contenido en $Q$.

$$\therefore \tau R_1 \tau = R_1$$

Pero como $F\cap \tau F\tau = K$ y $R_1 \subset F$ entonces

$$\tau R_1 \tau \subset \tau F \tau \quad \therefore \tau R_1 \tau \cap R_1 = R_1 \subset F \cap \tau F \tau = K$$

$\therefore R_1 = \{e\}$ lo cual es absurdo.

Por lo tanto $R_1$ no es un subgrupo normal de $H$, por el teorema 4 y el lema de Burnside obtenemos la afirmación deseada.

Sin embargo, $R_1$ no puede contener más de una involución pues:

$$R_1 \neq N_H(R_1) = N_G(R_1)\cap H = H\cap F = R_1$$

Por lo tanto $R_1$ contiene sólo una involución. Por el teorema 17, $R_1$ es cíclico ó un cuaternio generalizado. Si $R_1$ es cíclico, el teorema 15 demuestra la existencia de un subgrupo normal $H_1$ de $H$ tal que $H = R_1 H_1$. Esto contradice la minimalidad de $H$

Si $Q$ es un cuaternio generalizado, $H$ no es simple por el teorema 24 de Brauer y Suzuki. Como $H$ es mínimo, $H$ es característico simple. Por el teorema [illegible], $H$ es un producto directo de grupos simples isomorfos. Tal grupo contiene más de una involución en un 2- subgrupo de Sylow ([illegible]). Esto es una contradicción. Por lo tanto se debe cumplir que [illegible].

Sea $\pi$ una involución de $Q$, por lo tanto $\pi$ induce un automorfismo de orden 2 (por conjugación) en $H$ que no tiene punto fijo. Por el lemma 2, $H$ es abeliano y $\pi$ mapea todo elemento de $H$ en su inverso. Si $Q$ contiene otra involución $\pi'$, $\pi'$ mapea todo elemento de $H$ en su inverso. Entonces el producto $\pi\pi'$ es una involución de $Q$ que conmuta con todo elemento de $H$. Esto contradice el hecho de que $G$ sea un (CIT)-grupo. Por lo tanto $Q$ contiene sólo una involución. Dicho grupo es cíclico ó un cuaternio generalizado. Es claro que $H$ es un subgrupo normal de orden impar.

Demostraremos ahora la siguiente proposición.

Proposición 2.-

Supongamos que un 2-subgrupo de Sylow $S$ de un (CIT)-grupo $G$ es un grupo cíclico ó un cuaternio generalizado. Entonces $G$ contiene un subgrupo abeliano $A$ normal de orden impar tal que $G = AS$ y ningún elemento, distinto de la identidad, de $S$ conmuta con algún elemento de $A$ distinto de uno. En particular $G$ es un grupo de Frobenius.

Demostración.

Sea $A$ un subgrupo normal de $G$ con orden impar lo más grande posible. Como antes $A$ es abeliano. Si $S$ es cíclico, por el teorema (15) $G = AS$. Por otro lado, si $S$ es un cuaternio generalizado, el grupo $G/A$ contiene una involución central por el teorema 24 de Brauer y Suzuki. Existe una involución $z$ de $S$ tal que la clase $zA$ está en el centro de $G/A$. Si $\tau$ es un elemento de $G$, el elemento $\tau^{-1}z\tau$ genera un 2- subgrupo de Sylow del subgrupo generado por $\{A, z\}$. Por lo tanto, por los teoremas de Sylow existe un elemento $\rho$ de $A$ tal que $\tau^{-1}z\tau = \rho^{-1}z\rho$. El elemento $\tau\rho^{-1}$ pertenece al centralizador de $z$ en $G$ que es por hipótesis el grupo $S$. Por lo tanto $\tau\rho^{-1} \in S$ y por lo consiguiente $G = SA$. Como todo elemento, distinto de la identidad, de $S$ induce un automorfismo sin punto fijo de $A$, el grupo $G$ es un grupo de Frobenius.

Si aplicamos este resultado a nuestro (CIT)- grupo $G$ obtenemos por lo tanto una contradicción.

Podemos concluir entonces que $G$ es simple y el teorema está probado.

III).-

Definiremos ahora, los grupos de Suzuki que denotaremos por $Sz(q)$.

Sea $F$ un campo finito de $q$ elementos, donde $q = 2^{2n+1}$. Si $\theta = 2^{n+1}$, entonces el mapeo $\theta : F \to F$ dado por $x^{\theta} = x^{\theta}$ es un automorfismo de $F$ tal que $\theta^2 = 2$.

Sean $\alpha, \beta$ elementos arbitrarios de $F$ y sea $(\alpha, \beta)$ la matriz de $4 \times 4$ $(\alpha_{ij})$ definida como sigue:

$$\alpha_{ij} = 0 \quad \text{si } i < j$$

$$\alpha_{ii} = 1 \qquad \alpha_{21} = \alpha_{43} = \alpha \qquad \alpha_{32} = \alpha^{\theta} \qquad \alpha_{42} = \beta$$

$$\alpha_{31} = \alpha^{1+\theta} + \beta \qquad \alpha_{41} = \alpha^{2+\theta} + \alpha\beta + \beta^{\theta}$$

es decir, la matriz $(\alpha, \beta)$ tiene la siguiente forma:

$$(\alpha, \beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \alpha^{1+\theta} + \beta & \alpha^{\theta} & 1 & 0 \\ \alpha^{2+\theta} + \alpha\beta + \beta^{\theta} & \beta & \alpha & 1 \end{pmatrix}$$

Sean $\gamma, \delta$ elementos arbitrarios de $F$ y consideremos la matriz $(\gamma, \delta)$, entonces:

$$(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha + \gamma, \alpha\gamma^{\theta} + \beta + \delta) \quad \text{---} \ (1)$$

$$(\alpha, \beta) \cdot (0, 0) = (\alpha + 0, \alpha \cdot 0^{\theta} + 0 + \beta) = (\alpha, \beta) = (0, 0) \cdot (\alpha, \beta)$$

$$(\alpha, \beta) \cdot (\alpha, \alpha^{1+\theta} + \beta) = (\alpha + \alpha, \alpha^{1+\theta} + \beta + \alpha^{1+\theta} + \beta) = (0, 0) = (\alpha, \alpha^{1+\theta} + \beta) \cdot (\alpha, \beta)$$

$$((\alpha, \beta) \cdot (\gamma, \delta)) (\alpha_1, \beta_1) = (\alpha + \gamma, \alpha\gamma^{\theta} + \beta + \delta) \cdot (\alpha_1, \beta_1) = (*)$$

$$(*) = (\alpha + \gamma + \alpha_1, (\alpha + \gamma)\alpha_1^{\theta} + \alpha\gamma^{\theta} + \beta + \delta + \beta_1) = (\alpha, \beta) \cdot ((\gamma, \delta) \cdot (\alpha_1, \beta_1))$$

$\therefore$ las matrices $(\alpha, \beta)$ con la multiplicación usual de matrices forman un grupo que denotaremos por $Q(q)$.

Lema 10.-

El grupo $Q(q)$ tiene orden $q^2$, el centro de $Q(q)$ consiste de las matrices de la forma $(0, \beta)$. Un elemento es una involución sii está contenido en el centro.

Demostración.

Sea $(0, \beta)$ una matriz de $Q(q)$ y $(\gamma, \delta)$ un elemento arbitrario de $Q(q)$. Por (1) se tiene que:

$$(0, \beta) \cdot (\gamma, \delta) = (\gamma, 0 \cdot \gamma^{\theta} + \beta + \delta) = (\gamma, \beta + \delta)$$

$$(\gamma, \delta) \cdot (0, \beta) = (\gamma + 0, \gamma \cdot 0^{\theta} + \delta + \beta) = (\gamma, \beta + \delta)$$

Por lo tanto $(0, \beta) \cdot (\gamma, \delta) = (\gamma, \delta) \cdot (0, \beta)$

$\therefore$ toda matriz de la forma $(0, \beta)$ está en el centro de $Q(q)$.

Si $(\alpha, \beta)$ está en el centro de $Q(q)$ entonces:

$$(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha + \gamma, \alpha\gamma^{\theta} + \beta + \delta) = (\alpha + \gamma, \gamma\alpha^{\theta} + \delta + \beta)$$

$$(*) = (\gamma, \delta) \cdot (\alpha, \beta)$$

$$\alpha\gamma^{\theta} = \gamma\alpha^{\theta} \quad \forall \gamma \in F$$

En particular, la igualdad es válida si $\gamma = 1$

$\therefore \alpha^{\theta} = \alpha$

Como $\theta \neq 1$ existe un elemento tal que $\gamma \neq \gamma^{\theta}$. Por lo tanto $\alpha$ es igual a cero. $\therefore (\alpha, \beta) = (0, \beta)$

Sea $(0, \beta)$ un elemento arbitrario del centro de $Q(q)$

$$(0, \beta) \cdot (0, \beta) = (0+0,\ 0 \cdot 0^{\theta} + \beta + \beta) = (0, 0)$$

$\therefore (0, \beta)$ es una involución.

Si $(\alpha, \beta)$ es una involución entonces:

$$(\alpha, \beta)(\alpha, \beta) = (\alpha + \alpha,\ \alpha^{1+\theta} + \beta + \beta) = (0, 0)$$

$$\therefore \alpha^{1+\theta} = 0 \qquad \therefore \alpha = 0$$

$$\therefore (\alpha, \beta) = (0, \beta)$$

Es claro que el orden de $Q(q)$ es $q^2$.

A cada elemento $k$ distinto de cero de $F$ le asociamos una matriz diagonal, denotada por la misma letra $k$, donde $z_1, z_2, z_3, z_4$ están en la diagonal y cumplen con lo siguiente:

$$z_1^{\theta} = k^{1+\theta} \qquad z_2^{\theta} = k \qquad z_3 = z_2^{-1} \qquad z_4 = z_1^{-1}$$

$$k = \begin{pmatrix} z_1 & 0 & 0 & 0 \\ 0 & z_2 & 0 & 0 \\ 0 & 0 & z_3 & 0 \\ 0 & 0 & 0 & z_4 \end{pmatrix} \quad --- \ (2)$$

Lema 11.-

Las matrices definidas arriba forman un grupo cíclico de orden $q-1$ isomorfo al grupo multiplicativo de elementos distintos de cero de $F$

Demostración.

$$k \cdot k' = \begin{pmatrix} z_1 & 0 & 0 & 0 \\ 0 & z_2 & 0 & 0 \\ 0 & 0 & z_3 & 0 \\ 0 & 0 & 0 & z_4 \end{pmatrix} \begin{pmatrix} z_1' & 0 & 0 & 0 \\ 0 & z_2' & 0 & 0 \\ 0 & 0 & z_3' & 0 \\ 0 & 0 & 0 & z_4' \end{pmatrix} = \begin{pmatrix} z_1 z_1' & 0 & 0 & 0 \\ 0 & z_2 z_2' & 0 & 0 \\ 0 & 0 & z_3 z_3' & 0 \\ 0 & 0 & 0 & z_4 z_4' \end{pmatrix}$$

$$(z_1 z_1')^{\theta} = k^{1+\theta} \cdot (k')^{1+\theta} = (k k')^{1+\theta} \qquad (z_2 z_2')^{\theta} = k \cdot k'$$

$$z_4 z_4' = (z_1 z_1')^{-1} \qquad z_3 z_3' = (z_2 z_2')^{-1}$$

Si $k$ es igual a $\begin{pmatrix} z_1 & 0 & 0 & 0 \\ 0 & z_2 & 0 & 0 \\ 0 & 0 & z_3 & 0 \\ 0 & 0 & 0 & z_4 \end{pmatrix}$ entonces:

$$k^{-1} = \begin{pmatrix} z_1^{-1} & 0 & 0 & 0 \\ 0 & z_2^{-1} & 0 & 0 \\ 0 & 0 & z_3^{-1} & 0 \\ 0 & 0 & 0 & z_4^{-1} \end{pmatrix} \text{ es tal que } \quad k k^{-1} = k^{-1} k = 1$$

donde $1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$$k \cdot 1 = 1 \cdot k = k$$

$\therefore$ las matrices definidas en (2) forman un grupo que denotaremos por $K(q)$.

Sea $\alpha$ un generador de $(F-\{0\})$.

$\therefore$ $\alpha = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & \alpha_3 & 0 \\ 0 & 0 & 0 & \alpha_4 \end{pmatrix}$ donde $\alpha_1^{\theta} = \alpha^{1+\theta}$ $\alpha_2^{\theta} = \alpha$ $\alpha_3 = \alpha_2^{-1}$ $\alpha_4 = \alpha_1^{-1}$

genera al grupo $K(q)$.

Sea $k \neq 1$ un elemento arbitrario de $K(q)$

$\therefore$ $z_1 = k \cdot k^{\theta}$ $\therefore$ $\exists\, s \in \mathbb{Z} \ni k = \alpha^{s}$

$\therefore$ $z_1^{\theta} = \alpha^{s} \cdot (\alpha^{s})^{\theta}$ $z_2^{\theta} = k = \alpha^{s}$

Consideramos

$$\alpha^{s} = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & \alpha_3 & 0 \\ 0 & 0 & 0 & \alpha_4 \end{pmatrix}^{s}$$ P.D. $k \cdot \alpha^{-s} = 1$

P.D. $z_1 \alpha_1^{-s} = 1 \iff (z_1 \alpha_1^{-s})^{\theta} = 1 \iff z_1^{\theta} \cdot (\alpha_1^{\theta})^{-s} = 1 \iff (\alpha^{1+\theta})^{s} \cdot (\alpha^{1+\theta})^{-s} = 1$

$z_2 \cdot \alpha_2^{-s} = 1 \iff z_2^{\theta} \cdot (\alpha_2^{-s})^{\theta} = 1 \iff \alpha^{s} \cdot \alpha^{-s} = 1$

$\therefore$ $k \cdot \alpha^{-s} = 1$

$\therefore$ $\alpha$ genera al grupo $K(q)$

$\therefore$ $K(q)$ es un grupo cíclico de orden $q-1$.

La función $\varphi : F-\{0\} \longrightarrow K(q)$ definida por:

$$\varphi(\alpha) = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & \alpha_3 & 0 \\ 0 & 0 & 0 & \alpha_4 \end{pmatrix}$$ donde $\alpha_1^{\theta} = \alpha^{1+\theta}$ $\alpha_2^{\theta} = \alpha$ $\alpha_3 = \alpha_2^{-1}$ $\alpha_4 = \alpha_1^{-1}$

es un isomorfismo.

Consideremos un elemento $(\alpha, \beta)$ de $Q(q)$ y $k \in K(q)$, entonces

$k^{-1}(\alpha, \beta) k = (\alpha k, \beta k^{1+\theta})$ --- (3)

esto se sigue del hecho de que $z_3 z_1 = k$ y $z_1 z_2 = k^{1+\theta}$.

Por lo tanto el grupo $H(q)$ generado por $Q(q)$ y $K(q)$ es un grupo de orden $q^2(q-1)$.

Sea $\tau = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ y denotemos por $G(q)$ al grupo generado por $H(q)$ y $\tau$.

Lema 12.-

Si $(0, \beta)$ es una involución de $Q(q)$ entonces existe $k \in K(q)$ tal que $k^{-1}(0,1) k = (0, \beta)$

Demostración.

Por (3) $k^{-1}(0,1)k = (0, k^{[illegible]}) = (0, \beta)$. Sea $\gamma$ un generador del grupo multiplicativo de elementos distintos de cero de $F$.

$\therefore \beta = \gamma^{u}$ para alguna $u \in \mathbb{Z}$

Sabemos que $q = 2^{2n+1}$ $\therefore r^2 = 2q = 2^{2n+2}$ $\therefore r = 2^{n+1}$

Ahora bien, deseamos que exista $k \in F - \{0\}$ tal que $k^{1+\theta} = \beta$, i.e., debe de existir $t \in \mathbb{Z}$ tal que $\gamma^{t(2^{n+1}+1)}$ sea igual a $\gamma^{u}$.

$$\therefore \gamma^{t(2^{n+1}+1)} = \gamma^{u}$$

Como $t(2^{n+1}+1) \equiv u \mod (2^{2n+1}-1)$ tiene solución entonces existe $k \in K(q)$ tal que $k^{-1}(0,1)k = (0, k^{1+\theta}) = (0, \beta)$.

Probaremos ahora el siguiente teorema.

Teorema [illegible].-

Si $q > 2$, el grupo $G(q)$ es un $(ZT)$-grupo de orden $q^2(q-1)(q^2+1)$.

Demostración.

Sea $L$ la totalidad de las matrices triangulares inferiores de $4\times 4$ con coeficientes en el campo $F$. $L$ consiste de las matrices $(\alpha_{ij})$ con $\alpha_{ij} = 0$ si $i<j$. Por definición, $H(q)$ está contenido en $L$. Si $U$ denota a las matrices triangulares superiores de $4\times 4$ con coeficientes en $F$, entonces $z^{-1}Lz = U$. La intersección $D = L\cap U$ es la totalidad de las matrices diagonales sobre $F$. Tenemos que:

$$H(q) \cap D = K(q)$$

Como $H(q) \subset L$ y $z^{-1}Lz = U$, concluimos que

$$H(q) \cap z^{-1}H(q)z = K(q)$$
$$H(q) \cap z^{-1}G(q)z = [illegible] \quad --- (4)$$

Como $z = z^{-1}$ y todo elemento $k \in K(q)$ es de la forma $k = \begin{pmatrix} \xi_1 & 0 & 0 & 0 \\ 0 & \xi_2 & 0 & 0 \\ 0 & 0 & \xi_3 & 0 \\ 0 & 0 & 0 & \xi_4 \end{pmatrix}$ entonces

[illegible]

$$\therefore zkz = k^{[illegible]} \quad \forall\, k \in K(q) \quad --- (5)$$

Probaremos el siguiente lema.

Lema 13.-

Todo elemento de $\bar{G}(q) - H(q)$ puede escribirse como $\eta\tau\pi$ con $\eta \in H(q)$ y $\pi \in Q(q)$, además, la expresión es única.

Demostración.

Si $\eta \in H(q)$ y $\pi \in Q(q)$, el elemento $\eta\tau\pi$ pertenece a $\bar{G}(q)$. Si $\eta\tau\pi \in H(q)$ entonces se tendría que $\tau \in H(q)$, lo cual es imposible. Por lo tanto $\eta\tau\pi$ es un elemento de $\bar{G}(q) - H(q)$. Si

$$\eta\tau\pi = \eta_1\tau\pi_1 \qquad \text{para } \eta, \eta_1 \in H(q) \text{ y } \pi, \pi_1 \in Q(q)$$

entonces $\eta_1^{-1}\eta = \tau\pi_1\pi^{-1}\tau$ es un elemento de $H(q) \cap \tau^{-1}Q(q)\tau$. Por (4) concluimos que $\eta = \eta_1$ y $\pi = \pi_1$. Por lo tanto, la expresión es única y en particular sabemos que hay $q^4(q-1)$ elementos de la forma $\eta\tau\pi$.

Queremos probar, recíprocamente, que todo elemento de $\bar{G}(q) - H(q)$ puede escribirse como $\eta\tau\pi$, con $\eta \in H(q)$ y $\pi \in Q(q)$. Como el grupo $\bar{G}(q)$ está generado por $H(q)$ y $\tau$, basta demostrar que el conjunto de elementos de la forma $\eta\tau\pi$ junto con $H(q)$ forman un grupo.

Si $\eta_1 \in H(q)$, entonces $\pi\eta_1 \in H(q)$ y $\eta_1(\eta\tau\pi) = (\eta_1\eta)\tau\pi$ el elemento $\pi\eta_1$ está en $H(q)$ por lo tanto es de la forma $k\pi'$ con $k \in K(q)$ y $\pi' \in Q(q)$. Entonces por (5) tenemos que:

$$(\eta\tau\pi)\eta_1 = \eta\tau(\pi\eta_1) = \eta\tau(k\pi') = (\eta k^{\tau})\tau\pi'$$

Si $\pi_1 \in Q(q)$, entonces

$$(\eta\tau\pi)(\eta_1\tau\pi_1) = (\eta\tau\pi)(\eta_1\tau\pi_1) = \eta\tau(\pi\eta_1)\tau\pi_1 = (*)$$

$(*) = \eta k^{\tau}\tau\pi'\tau\pi_1$.

Para probar nuestra afirmación basta probar entonces que $\tau\pi\tau = \eta_2\tau\pi_2$ $\quad (\eta_2 \in H(q), \pi_2 \in Q(q))$ $\forall \pi \neq 1$ de $Q(q)$ ya que si se cumple lo anterior entonces $(\eta\tau\pi)(\eta_1\tau\pi_1) = \eta k^{\tau}\eta_2\tau\pi_2\pi_1$ y $\eta k^{\tau}\eta_2 \in H(q)$ $\pi_2\pi_1 \in Q(q)$; que era lo que deseábamos demostrar.

P.D. $\quad \tau\pi\tau = \eta_2\tau\pi_2 \quad (\eta_2 \in H(q)\ \pi_2 \in Q(q)) \quad \forall \pi \neq 1$ de $Q(q)$ - - - (6)

Sean $\pi = (\alpha, 1)$ y $\rho = (1, c)$ elementos de $Q(q)$ entonces se cumple la siguiente igualdad:

[illegible] - - - (7)

Consideremos $\pi(k) = [illegible]$ para $k \neq 1$ de $K(q)$, entonces tenemos que:

$$[illegible] = (*)$$

$(*) = [illegible]$ por (5) y (7)

Ahora bien, por (3) $Q(q)$ es un subgrupo normal de $H(q)$ por lo tanto el elemento $k^{-1}(k^{-1}\tau k\tau)k$ es un elemento de $Q(q)$.

Como $\tau=(0,1)$ entonces por (3) $k^{-1}\tau k=(0,k^{1+q})$

$\therefore\ k^{-1}\tau k\tau=(0,k^{1+q})\cdot(0,1)=(0,k^{1+q}+1)$

Por el lema 11 $k^{-1}\tau k\tau$ es una involución de $Q(q)$

$k^{-1}(k^{-1}\tau k\tau)k$ es una involución de $Q(q)$.

$$k\tau=\begin{pmatrix} k_1 & 0 & 0 & 0\\ 0 & k_2 & 0 & 0\\ 0 & 0 & k_3 & 0\\ 0 & 0 & 0 & k_4\end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 1 & 1 & 1 & 0\\ 1 & 1 & 0 & 1\end{pmatrix} = [illegible]$$

$$\tau k=\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 1\end{pmatrix}\begin{pmatrix} k_1 & 0 & 0 & 0\\ 0 & k_2 & 0 & 0\\ 0 & 0 & k_3 & 0\\ 0 & 0 & 0 & k_4\end{pmatrix} = \begin{pmatrix} k_1 & 0 & 0 & 0\\ 0 & k_2 & 0 & 0\\ k_1 & 0 & k_3 & 0\\ k_1 & k_2 & 0 & k_4\end{pmatrix}$$

Como $k\neq 1$, el elemento $k^{-1}\tau k\tau$ no es la identidad y por el lema 12, existe un elemento $\lambda=\lambda(k)$ de $K(q)$ tal que

$$k^{-1}(k^{-1}\tau k\tau)k=\lambda^{-1}\tau\lambda$$

$$\tau\pi(k)\tau=\rho k^{-2}\tau k^{-1}(k^{-1}\tau k\tau)k\tau\rho^{-1}k^{-1}=\rho k^{-2}\lambda\tau\tau\tau\lambda^{-1}k\rho^{-1}k^{-1}=(*)$$

$$(*)=\rho k^{-2}\lambda\rho^{-1}\tau\rho\lambda^{-1}k\rho^{-1}k^{-1}=\rho k^{-2}\lambda\rho^{-1}\lambda^{-1}\lambda\tau\lambda^{-1}\lambda\rho\lambda^{-1}k\rho^{-1}k^{-1}=(*)$$

$$(*)=\rho k^{-2}\lambda\rho^{-1}\lambda\tau\lambda\rho\lambda^{-1}k\rho^{-1}k^{-1}=h_2\tau\pi_2$$

Hemos demostrado entonces que para todo elemento $k$, distinto de la identidad, de $K(q)$ $\tau\pi(k)\tau=h_2\tau\pi_2$ con $h_2\in H(q)$ y $\pi_2\in Q(q)$.

Probaremos ahora el siguiente lema:

Lema 14-

Todo elemento de $Q(q)-\{1\}$ es transformado por un elemento de $K(q)$ en alguno de los siguientes elementos: $\tau,\rho,\rho^{-1}$ ó $\pi(k)$ $(1\neq k\in K(q))$.

Demostración.

Sea $(\alpha,\beta)$ un elemento arbitrario de $Q(q)-\{1\}$. Si $\alpha=0$ entonces el lema 12 nos asegura la existencia de un elemento $k$ tal que $k^{-1}(\alpha,\beta)k=\tau$

Si $\alpha$ es distinto de cero entonces por (3) $k^{-1}(\alpha,\beta)k=(\alpha k^{q},\beta k^{1+q})$, si deseamos que $k^{-1}(\alpha,\beta)k$ sea igual a $\rho$ entonces si $\beta=0$ y $k=\alpha^{-1}$ se tiene que

$$k^{-1}(\alpha,\beta)k=[illegible]=(1,0)=\rho$$

Supongamos ahora que $\alpha$ y $\beta$ son distintos de cero. Queremos ahora que:

$$k^{-1}(\alpha,\beta)k = (k\alpha, k^{1+\theta}\beta) = (t+1, t^{\theta}(t+1)) = \pi(t) \text{ para alguna}$$

$t \in F$

$$\therefore\ k\alpha = t+1 \Rightarrow t = k\alpha - 1$$

$$\therefore\ (k\alpha-1)^{\theta}k\alpha = t^{\theta}(t+1) = k^{1+\theta}\beta$$

$$\therefore\ (k\alpha-1)^{\theta}\alpha = k^{\theta}\beta$$

$$\therefore\ k^{\theta}(\alpha^{1+\theta}-\beta) = \alpha$$

$$\therefore\ k^{\theta} = \frac{1}{\alpha^{1+\theta}-\beta} \quad \text{si } \beta \neq \alpha^{1+\theta}$$

Por lo consiguiente, escogemos $k \in F$ tal que $k^{\theta} = \frac{1}{\alpha^{1+\theta}-\beta}$; es claro entonces que $k^{-1}(\alpha,\beta)k$ es igual a $\pi(t)$

Si $\alpha^{\theta+1}$ es igual a $\beta$ entonces $\beta^{-1} = \alpha^{-(1+\theta)}$

$$\therefore\ k^{-1}(\alpha,\beta)k = (k\alpha, k^{1+\theta}\beta) = (1,1) \quad \text{donde } k = \alpha^{-1} \quad (1,1) = \rho^{-1}$$

Por lo tanto, todo elemento de $Q(q)-\{1\}$ es trasformado por un elemento de $H(q)$ en alguno de los siguientes elementos:

$$\tau, \rho, \rho^{-1}, \pi(k) \quad (1 \neq k \in K(q)).$$

Ahora bien, los elementos $\tau, \rho, \rho^{-1}, \pi(k)$ satisfacen (6) ya que:

$$\tau\tau\tau = \rho^{-1}\tau\rho \qquad \tau\rho^{-1}\tau = \tau\tau\rho^{-1}$$

$$\tau\rho\tau = \rho\tau\tau \qquad \tau\pi(k)\tau = \eta_2\tau\pi_2$$

Demostraremos ahora que si $\pi \in Q(q)$ satisface (6) entonces su conjugado $k^{-1}\pi k$ $(k \in H(q))$ satisface también (6).

En efecto, si $\pi \in Q(q)$ satisface (6) se tiene que:

$$\tau\pi\tau = \eta_2\tau\pi_2 \qquad \eta_2 \in H(q) \quad \pi_2 \in Q(q)$$

$$\therefore\ \tau^{-1}k^{-1}\pi k\tau = k\tau\pi\tau k^{-1} = k\eta_2\tau\pi_2k^{-1} = k\eta_2\tau k^{-1}k\pi_2k^{-1} = (*)$$

$(*) = k\eta_2\tau k\pi_2k^{-1}$ y $k\eta_2 \in H(q)$, $k\pi_2k^{-1} \in Q(q)$, ya que $Q(q) \lhd H(q)$

Por el lema 14 concluimos que la ecuación (6) se cumple para todos los elementos de $Q(q)-\{1\}$

Hemos demostrado que todo elemento de $E(q)-H(q)$ puede escribirse como $\eta\tau\pi$ con $\eta \in H(q)$, $\pi \in Q(q)$ y además esta expresión es única. Por lo tanto el orden de $E(q)$ es $q^{2}(q-1)(q^{2}+1)$ y tenemos una descomposición de $E(q)$ en clases dobles de la forma:

$$E(q) = H(q) \cup H(q)\tau Q(q).$$

La última fórmula implica que la representación transitiva de $H(q)$ en las clases de $H(q)$ es doble transitiva de grado $q^{2}+1$.

El subgrupo que consiste de los elementos que fijan dos clases $H(q)$ y $H(q)z$ coincide con $K(q)$ ya que $K(q) = H(q) \cap z^{-1}H(q)z$. Sea $H(q)z\pi$ una clase ($\pi \in Q(q)$) y supongamos que [illegible] $= H(q)z\pi$ para alguna $k \in K(q)$. Entonces tenemos que $z\pi k = \eta z\pi$ para alguna $\eta \in H(q)$. Se sigue entonces que [illegible] por la unicidad de la expresión obtenemos que

$$k^{-1}\pi k = \pi$$

Si $\pi = (\alpha, \beta)$ entonces por (I)

$$k^{-1}\pi k = (\alpha, \beta) = (k\alpha, k^{1+\theta}\beta)$$

$$\therefore k\alpha = \alpha \text{ y } k^{1+\theta}\beta = \beta$$

Estas ecuaciones implican que $\pi = (0,0)$ ó $k^{1+\theta} = 1$

Si $k^{1+\theta} = 1 \Rightarrow k^{\theta} = k^{-1}$ $\therefore k^{\theta^{2}} = k^{-\theta} = k \Rightarrow k = 1$

Por lo tanto la identidad es el único elemento que deja fijos a tres símbolos distintos.

Demostraremos ahora lo siguiente:

Lema 15.-

Si $1 \neq \pi \in Q(q)$ el centralizador $C_{G(q)}(\pi)$ está contenido en $Q(q)$.

Demostración.

Sea $1 \neq \pi \in Q(q)$ y consideremos su centralizador $C_{G(q)}(\pi)$.

Sea $\tau \in C_{G(q)}$ $\therefore$ $\tau \in H(q)$ ó $\tau = \eta z \pi_1$ con $\eta \in H(q)$ y $\pi_1 \in Q(q)$.

Si $\tau = \eta z \pi_1$ entonces

[illegible]

$\therefore$ $\eta z \pi_1 \pi \pi_1^{-1} z = \pi\eta$ $\therefore$ $z\pi_1\pi\pi_1^{-1}z = \eta^{-1}\pi\eta$

Por (∗) $\eta^{-1}\pi\eta = 1 \Rightarrow \pi = 1$ lo cual es una contradicción.

$\therefore \tau \in H(q)$ $\therefore$ $\tau = \pi_1 k_1$ con $\pi_1 \in Q(q)$ $1 \neq k_1 \in K(q)$.

Si [illegible] y [illegible] entonces

[illegible]

[illegible]

[illegible] $(\alpha, \beta)$

$\therefore$ [illegible]

$\therefore$ [illegible]

$\therefore (\alpha, \beta) = (\alpha', \beta')$ $\quad \therefore$ [illegible]

$\therefore$ [illegible] $= \alpha \quad$ [illegible] $= \beta \Rightarrow k = 1$ lo cual es una contradicción.

$\therefore \quad C_{G(q)}(\pi) \subset Q(q)$

Si $G(q)$ contiene un subgrupo normal $N$ de orden $1+q^2$, entonces el grupo $Q(q)$ actúa en $N$ de la siguiente manera:

$$\varphi_q : N \longrightarrow N \qquad q \neq 1$$
$$\varphi_q(n) = q^{-1} n q$$

$\forall q \neq 1 \quad \varphi_q$ es un automorfismo sin punto fijo por el lema 16

Sea $\tau$ una involución de $Q(q)$, por lo tanto $\tau$ induce un automorfismo de orden 2 en $N$ que fija sólo a la identidad. Por el lema 2 $N$ es abeliano y $\tau$ mapea todo elemento de $N$ en su inverso. Si $Q(q)$ contiene otra involución $\tau'$, $\tau'$ mapea todo elemento de $N$ en su inverso. Entonces el producto $\tau\tau'$ es una involución de $Q(q)$ que conmuta con todo elemento de $N$. Esto contradice el hecho de que el centralizador de todo elemento, distinto de la identidad, de $Q(q)$ esté contenido en $Q(q)$. Por lo tanto $Q(q)$ contiene sólo una involución. Pero como $q > 2$ y toda involución de $Q(q)$ es de la forma $(0, \beta)$ con $0 \neq \beta \in F$ entonces $Q(q)$ contiene más de una involución, por lo consiguiente $G(q)$ no puede contener un subgrupo normal de orden $q^2+1$.

Por lo tanto $G(q)$ es un $(ZT)$ grupo.

# Referencias.


[1].- E. Artin. The orden of the classical simple groups, Comm. Pure Appl. Math. [illegible] ([illegible]) [illegible].

[2].- R. Brauer, Some Applications of the Theory of Blocks of Characters of Finite Groups I, Journal of Algebra 1, [illegible], ([illegible]).

[3].- R. Brauer, Some Applications of the Theory of Blocks of Characters of Finite Groups II, Journal of Algebra 1 [illegible], (1964).

[4].- R. Brauer and M. Suzuki, On finite whose 2-Sylow group is a generalized quaternion group, Proc. Nat. Acad. Sci. USA vol. 45 (1959) pp. [illegible].

[5].- W. Burnside, Notes on the Theory of groups of finite orden Proc. London Math. Soc. 26 ([illegible]) [illegible]

[6].- ———, On a class of groups defined by congruences, Proc. London Math. Soc. 25 (1894) 113-139

[7].- ———, On transitive groups of degree n and class n-1, Proc. London Math. Soc. [illegible] ([illegible]) [illegible].

[8].- ———, On some properties of groups of odd orden, Proc. London Math. Soc. [illegible] ([illegible]) [illegible].

[9].- ———, On some properties of groups of odd orden (second paper), Proc London Math Soc., [illegible] ([illegible]) [illegible]

[10].- W Feit, On a class of doubly transitive permutation groups, Illinois J. Math, 4 (1960), [illegible].

[11].- W. Feit, M. Hall Jr., J. G. Thompson, Finite groups in wich the centralizer of any non-identity element is nilpotent, Math. Z., 74 ([illegible]), 1-17.

[12].- W Feit and J. G. Thompson, Solvability of groups of odd orden Pacific J. Math., [illegible] ([illegible]) 775-[illegible].

[13].- J. A. Gallian, The Search for finite simple groups, Mathematics Magazine, Vol 49 N. 4 ([illegible]) [illegible]

[14].- D. Gorenstein, Finite Groups, Harper and Row; Publishers New York, Evanston and London ([illegible]), [illegible]-pp

[15].- T. Hawkins, the origins of the Theory of group characters, Archive Hist, Exact. Sci. 7 (1971) [illegible]

[16].- ________, New light on Frobenius creation of the Theory of Group characters. Archive Hist. Exact. Sci, [illegible] ([illegible]) [illegible]

[17].- O. Hölder, Die einfachen Gruppen im ersten und zweiten Hundert der Ordnung zahlen. Math. Ann. [illegible] ([illegible]) [illegible].

[18].- J. Rotman, the theory of Groups; an introduction. Allyn and Bacon Inc, Boston Mass. ([illegible]) [illegible] pp.

[19].- M. Suzuki, The non existence of a certain type of simple groups of odd order, Proc. Amer. Math. Soc., [illegible] ([illegible]) [illegible]

[20].- ________, A new type of simple groups of finite order, Proc. Nat. Acad. Sci. USA, 46 ([illegible]) [illegible].

[21].- ________, Finite groups with nilpotent centralizers, Trans. Amer. Math. Soc, 99 ([illegible]) [illegible]-470.

[22].- ________, On a class of doubly transitive groups, Ann. of Math. Vol. 75 N. 1 ([illegible]) [illegible].

[23].- J. G. Thompson, Non solvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. [illegible] ([illegible]) [illegible]; Pacific J. Math. 33 (1970) [illegible]; Pacific J. Math. [illegible] (1971) [illegible]; Pacific J. Math. [illegible] ([illegible]) 511-592; Pacific J. Math. 50 (1974) [illegible]; Pacific J. Math. [illegible] ([illegible]) [illegible].

[24].- H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, Abh. Math. Sem. Univ. Hamburg, 11 ([illegible]) 17-40