# LECCIONES

**sobre**

# GRUPOS

## por


## María Jesús Iranzo Aznar

## y

## Francisco Pérez Monasor


Curso 2008-2009


Departamento de Algebra.

Facultad de Matemáticas. Universitat de València

**PROGRAMA**

**El Teorema de Burnside por teoría abstracta de grupos**

.

Este programa se ha impartido durante el primer cuatrimestre del curso 2008-09 en la asignatura optativa Teoría de Grupos (6 créditos).

**Lección 1**: Grupos nilpotentes. Estructura de los grupos finitos abelianos.

**Lección 2** : Los subgrupos de Fitting y de Frattini de un grupo finito.

**Lección 3**: Grupos actuando sobre grupos. Producto semidirecto.

**Lección 4**: Los teoremas de Baer, Zenkov y Lucchini.

**Lección 5**: El teorema de Schur-Zassenhaus.

**Lección 6**: Acción coprima. El $P \times Q$-lema de Thompson.

**Lección 7**: Preliminares para el $p^a q^b$-teorema.

**Lección 8**: Demostración del $p^a q^b$-teorema.

**Lección 1. Grupos nilpotentes. Estructura de los grupos finitos abelianos.**

.

**Definición 1**. Un grupo $G$ se dice **nilpotente** si posee una serie de subgrupos:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_n = 1$$

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

Los grupos nilpotentes son resolubles y los grupos abelianos son nilpotentes.

Notar que $G_i/G_{i+1} \leq Z(G/G_{i+1}) \Leftrightarrow [G/G_{i+1}, G_i/G_{i+1}] = 1 \Leftrightarrow [G, G_i]G_{i+1}/G_{i+1} = 1 \Leftrightarrow [G, G_i] \leq G_{i+1}$ $\forall i$.

Una serie de subgrupos normales $N_0 \leq N_1 \leq ... \leq N_r$ de un grupo $G$ se dice central si : $N_{i+1}/N_i \leq Z(G/N_i)$ $\forall i$. Así un grupo $G$ será nilpotente si posee una serie central que contiene a $G$ y a 1.

En cualquier grupo $G$ se pueden construir dos series centrales: $1 = Z_0(G)$ e inductivamente se define $Z_i(G)$ por $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$.

Dado que si $H/K \mathrm{car} G/K$ y $K \mathrm{car} G$ se sigue que $H \mathrm{car} G$, se obtiene así una serie de subgrupos característicos en $G$, que se conoce como la **serie central superior** de $G$.

De forma análoga se define : $G = \Gamma_1(G)$ e inductivamente $\Gamma_{i+1}(G) = [G, \Gamma_i(G)]$. Se obtiene así una serie de subgrupos característicos de $G$, que se conoce como **serie central inferior** de $G$.

**Teorema 2.** Sea $G$ un grupo y $n \geq 1$. Las siguientes afirmaciones son equivalentes:

i) $\Gamma_{n+1}(G) = 1$ ii) $Z_n(G) = G$.

Además $G$ es nilpotente si y solo si i) y ii) se cumplen para un cierto $n \geq 1$.

**Demostración**: Ciertamente si se cumple i) ó ii) $G$ es nilpotente.

Supongamos ahora que $G$ es nilpotente. Si $1 = N_0 \leq N_1 \leq ... \leq N_r = G$ es una serie central veamos que:

a) $\Gamma_i(G) \leq N_{r-i+1}$ $\forall i$. Notar que $\Gamma_1(G) = G = N_{r-1+1}$. Supuesto que $\Gamma_i(G) \leq N_{r-i+1}$, tenemos: $\Gamma_{i+1}(G) = [G, \Gamma_i(G)] \leq [G, N_{r-i+1}] \leq N_{r-i}$. En particular $\Gamma_{r+1}(G) = 1$.

b) $N_i \leq Z_i(G)$ $\forall i$. Se tiene que : $1 = N_0 \leq Z_0(G) = 1$. Suponer que $N_i \leq Z_i(G)$. Existe un epimorfismo $\phi : G/N_i \longrightarrow G/Z_i(G)$ dado por $\phi(xN_i) = xZ_i(G)$. Como $N_{i+1}/N_i \leq Z(G/N_i)$ se sigue que $N_{i+1}Z_i(G)/Z_i(G) \leq Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$, por lo tanto $N_{i+1} \leq Z_{i+1}(G)$. En particular $Z_r(G) = G$.

Veamos ahora que i) y ii) son equivalentes.

$i) \Longrightarrow ii)$. Sea $\mathrm{N}_0 = \Gamma_{n+1}$, $\Gamma_n(G) = N_1, .., N_n = \Gamma_1(G) = G$. Por lo probado en b) se tiene que $Z_n(G) = G$.

$ii) \Longrightarrow i)$. Sea $N_i = Z_i(G)\ \forall i$. En particular $N_n = Z_n(G) = G$ y por lo probado en a) se tiene que $\Gamma_{n+1}(G) = 1$.

Si $G$ es nilpotente, al menor $n$ tal que $Z_n(G) = G$, se le llama **clase de nilpotencia** de $G$

**Ejemplo**. Sabemos que $SL(2,3)/Z(SL(2,3) \cong A_4$ por lo tanto

$$Z(SL(2,3)/Z(SL(2,3)) \cong Z(A_4) = 1$$

, así $Z_2(SL(2,3)) = Z(SL(2,3))$, por lo que $SL(2,3)$ es un ejemplo de grupo resoluble con centro no trivial pero no nilpotente.

**Teorema 3**. Sea $G$ nilpotente y $H < G$, entonces $H < N_G(H)$

**Demostración**. Como $H < G$ existe $i$ tal que $\Gamma_{i+1}(G) \leq H$ pero $\Gamma_i(G) \nleq H$. Entonces : $[\Gamma_i(G), H] \leq [\Gamma_i(G), G] = \Gamma_{i+1}(G) \leq H$. Así $\Gamma_i(G) \leq N_G(H)$.

**Teorema 4**. Sea $G$ nilpotente y $1 \neq N \trianglelefteq G$, entonces i) $[G, N] < N$ ii)$N \cap Z(G) \neq 1$.

**Demostración**: Construyamos la serie: $N_1 = N$ , $N_2 = [G, N]$,.., $N_{i+1} = [G, N_i]$. Como $N_i \leq \Gamma_i(G)\ \forall i$ y existe $m$ tal que $\Gamma_m(G) = 1$, se tendrá que $N_m = 1$. Así $N_2 = [G, N] < N$, pues en caso contrario $N_i = N\ \forall i$ y se llegaría a contradicción con que $1 \neq N$. Sea $k$ tal que $N_k = 1$ pero $N_{k-1} \neq 1$. Se tiene que $[G, N_{k-1}] = N_k = 1$ luego $1 \neq N_{k-1} \leq N \cap Z(G)$.

En cuanto a las propiedades de la clase de grupos nilpotentes es sencillo probar que todo subgrupo y todo cociente de un grupo nilpotente es también nilpotente. Veamos ahora que la clase de los grupos nilpotentes tiene la Z-propiedad.

**Teorema 5.** Si $G/Z(G)$ es nilpotente entonces $G$ es nilpotente.

**Demostración**. Como $G/Z(G)$ es nilpotente existe una serie central

$$G/Z(G) = H_0/Z(G) \geq ... \geq H_r/Z(G) = 1$$

por lo tanto $[G/Z(G), H_i/Z(G)] \leq H_{i+1}/Z(G)$ $\forall i$, así $[G, H_i] \leq H_{i+1}$. Considerar la serie:

$$G = H_0 \geq ... \geq H_r = Z(G) \geq 1$$

para afirmar que $G$ es nilpotente.

**Teorema 6**. Todo $p$-grupo finito es nilpotente.

**Demostración**: Por inducción sobre el orden de $G$. Suponer $G \neq 1$. Sabemos que $Z(G) \neq 1$. Como $G/Z(G)$ es un $p$-grupo de orden estrictamente menor que el de $G$, por hipótesis de inducción se tiene que $G/Z(G)$ es nilpotente y por la Z-propiedad se sigue que $G$ es nilpotente.

**Ejercicio**. Comprobar que la clase de nilpotencia de $D_8$ y de $Q_8$ es 2.

**Teorema 7**. Si $G_1, G_2, ..., G_n$ son grupos nilpotentes entonces $G_1 \times G_2 \times ..G_n$ es nilpotente.

**Demostración**: Bastará probarlo para el caso $n = 2$.

Sea $G = H \times K$, con $H, K$ nilpotentes. Existen series centrales.

$$1 = H_0 \leq H_1 \leq ...H_m = H$$

$$1 = K_0 \leq K_1 \leq ...K_n = K$$

verificando que $[H, H_i] \leq H_{i-1}$ y que $[K, K_i] \leq K_{i-1}$ respectivamente. Repitiendo términos si es necesario, podemos suponer que $n = m$ y se tiene :

$$1 = H_0 \times K_0 \leq H_1 \times K_1 \leq .... \leq H_n \times K_n = H \times K$$

Como $[H \times K, H_i \times K_i] = [H, H_i] \times [K, K_i] \leq H_{i-1} \times K_{i-1}$, se concluye que $H \times K$ es nilpotente.

En el caso de grupos finitos, algunas de las propiedades anteriormente citadas caracterizan la nilpotencia del grupo.

**Teorema 8**. Si $G$ es finito, son equivalentes:

i) $G$ es nilpotente

ii) Si $H < G$ entonces $H < N_G(H)$

iii) Cada subgrupo maximal de $G$ es normal en $G$.

iv) Cada subgrupo de Sylow de $G$ es normal en $G$

v) $G$ es producto directo de $p$-grupos para algunos primos $p$.

**Demostración**: $i) \Longrightarrow ii)$ Demostrado en el Teorema 3 para grupos nilpotentes cualesquiera.

$ii) \Longrightarrow iii)$ Si $M <\cdot G$ como $M < N_G(M)$ necesariamente $N_G(M) = G$.

$iii \Longrightarrow iv)$ Si $P \in \mathrm{Syl}_p(G)$ y $N_G(P) < G$, sea $M <\cdot G$ tal que $N_G(P) \leq M$. Sabemos que entonces $M = N_G(M) = G$, lo que es una contradicción.

$iv) \Longrightarrow v)$ Notar que en tal caso $G$ es producto directo de sus subgrupos de Sylow.

$v) \Longrightarrow i)$ Basta aplicar los Teoremas 6 y 7 para concluir que $G$ es nilpotente.

**Teorema 9**. Sea $G$ finito $G = MN$ $M, N \trianglelefteq G$. Si $M, N$ son nilpotentes, entonces $G$ es nilpotente.

**Demostración:** Sea $P \in \mathrm{Syl}_p(G)$. Sabemos que $P = (P \cap M)(P \cap N)$. Por el teorema anterior $P \cap M \trianglelefteq M$ y $P \cap N \trianglelefteq N$. Más aún dichas intersecciones son subgrupos característicos de $M$ y $N$ respectivamente, por lo tanto son subgrupos normales de $G$. Concluimos que $P \trianglelefteq G$ y que por el teorema anterior $G$ es nilpotente.

Como consecuencia del resultado anterior si $G$ es finito se define el mayor subgrupo normal nilpotente de $G$, al que se denota por $F(G)$ y se llama **subgrupo de Fitting** de $G$.

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

**Teorema 10**. Si $G$ es un $p$-grupo finito abeliano y $C$ es un subgrupo de $G$ cíclico del orden mayor posible, existe un subgrupo $B$ de $G$ de forma que $G = C \times B$.

**Demostración**: Podemos suponer que $C < G$ y elegir $x \in G - C$ de orden el menor posible. Como $x \neq 1$ $o(x^p) < o(x)$, así $x^p \in C$. Si $< x^p >= C$ sería $| < x > | = p|C|$, lo que no es posible por la elección de $C$. Si $C =< c >$, existe $m$ tal que $x^p = c^m$ y por lo anterior necesariamente $p|m$. Sea $m = m'p$. Se tiene que $x^p = (c^{m\prime})^p$ . Llamemos $y = c^{m'}$, entonces $y \in C$ , $xy^{-1} \neq 1$ y $xy^{-1} \notin C$. Además $(xy^{-1})^p = x^p(y^p)^{-1} = 1$. Por la elección de $x$ tenemos que : $o(x) \leq o(xy^{-1}) = p$, así que $o(x) = p$. Sea $X =< x >$. Considerar el homomorfismo canónico $\phi$ de $G$ sobre $G/X = \bar{X}$. Como $|X| = p$ se tiene que $X \cap C = 1$ y $\phi(C) = \bar{C} = CX/X \cong C$, luego $\bar{C}$ es cíclico de igual orden que $C$. Si $\bar{G}$ tuviera un subgrupo cíclico $< \bar{g} >$ de orden mayor que $\bar{C}$, se tendría:

$$| < g > | = o(g) \geq o(\bar{g}) = | < \bar{g} > | > |\bar{C}| = |C|$$

lo que es una contradicción. Así $\bar{C}$ es un subgrupo cíclico de $\bar{G}$ de orden máximo. Trabajando por inducción, como $|\bar{G}| < |G|$, se concluye que $\bar{C}$ es un factor directo de $\bar{G}$, es decir que existe $\bar{B} \leq \bar{G}$ tal que $\bar{G} = \bar{C} \times \bar{B}$ siendo $\bar{B} = B/X$. Así $G = CB$ , $CX \cap B = X(C \cap B) = X$, luego $C \cap B \leq X \cap C = 1$ y $G = C \times B$.

**Teorema 11**. (Teorema de estructura de los grupos finitos abelianos). Si $G$ es un grupo finito abeliano, $G$ es producto directo de grupos cíclicos.

**Demostración**: Por inducción sobre el orden de $G$. Como $G$ es nilpotente, por el teorema 8, $G$ es producto directo de sus subgrupos de Sylow. Si el orden de $G$ es divisible por al menos dos primos distintos, por hipótesis de inducción cada uno de los correspondientes subgrupos de Sylow se expresará como producto directo de cíclicos y por tanto también $G$. Debemos suponer que $G$ es un $p$-grupo para algún primo $p$. Por el teorema anterior $G = C \times B$, siendo $C$ un subgrupo cíclico de orden máximo como tal. Si $B = 1$, $G$ es cíclico. Si $B \neq 1$ se expresará como producto directo de cíclicos y por tanto también $G$.

## Lección 2. Los subgrupos de Fitting y de Frattini de un grupo finito

En toda la lección los grupos considerados son finitos.

**Definición 1**. El **subgrupo de Frattini** de un grupo $G$, denotado por $\phi(G)$, es la intersección de todos los subgrupos maximales de $G$.

**Notas**. Como consecuencia de la definición se tiene:

a) $\phi(G)$ es un subgrupo característico de $G$.

b) $G \neq 1 \Longrightarrow \phi(G) < G$.

c) Si $H \leq G$ y $G = H\phi(G)$, se sigue que $G = H$.

En efecto, si $H < G$ existe $M < .G$ tal que $H \leq M$. Así $G = M\phi(G) = M$, lo que no es posible.

d) Si $N \trianglelefteq G$, se tiene que $\phi(G)N/N \leq \phi(G/N)$

Un subgrupo maximal de $G/N$ es de la forma $M/N$ con $M < .G$, por lo tanto $\phi(G)N/N \leq \phi(G/N)$.

e) Si $N \trianglelefteq G$ se tiene que: $\phi(N) \leq \phi(G)$.

En efecto, si existe $M < .G$ tal que $\phi(N) \not\leq M$, $G = \phi(N)M$ luego $N = N \cap \phi(N)M = \phi(N)(N \cap M) = N \cap M$, luego $N \leq M$, que es una contradicción.

**Teorema 2**. Son equivalentes:

i) $G$ es nilpotente.

ii) $G/\phi(G)$ es abeliano.

iii) $G/\phi(G)$ es nilpotente.

**Demostración**: i)$\Longrightarrow$ *ii*).Si $M < .G$, por el Teorema 8 de la Lección 1 sabemos que $M \trianglelefteq G$, luego $G/M$ tiene orden primo y por tanto $G' \leq M$, luego $G' \leq \phi(G)$ y $G/\phi(G)$ es abeliano.

Es claro que ii)$\Longrightarrow$ iii).

iii) $\Longrightarrow$ i) Basta probar que cualquier subgrupo maximal de $G$ es normal en $G$. Sea $M < .G$. Como $M/\phi(G) < .G/\phi(G)$ es $M/\phi(G) \trianglelefteq G/\phi(G)$, así que $M \trianglelefteq G$.

**Ejercicio**. Demostrar que si $n \geq 2$ se tiene que $\phi(\Sigma_n) = 1$.

**Teorema 3**. Sea $N \trianglelefteq G$ y $\phi(G) \leq N$. Entonces $N$ es nilpotente si y solo si $N/\phi(G)$ es nilpotente.

**Demostración**: Si $N$ es nilpotente sabemos que también lo será $N/\phi(G)$. Suponer ahora que $N/\phi(G)$ es nilpotente. Sea $P \in \mathrm{Syl}_p(N)$, entonces:

$$P\phi(G)/\phi(G) \in \mathrm{Syl}_p(N/\phi(G))$$

luego $P\phi(G)/\phi(G) \trianglelefteq N/\phi(G)$, por lo tanto:

$$P\phi(G)/\phi(G) \mathrm{car} N/\phi(G) \trianglelefteq G/\phi(G)$$

luego $P\phi(G) \trianglelefteq G$. Por el argumento de Frattini se tiene: $G = P\phi(G)N_G(P) = N_G(P)$ y por el Teorema 8 de la Lección 1, se sigue que $N$ es nilpotente.

Como consecuencia del resultado anterior $\phi(G)$ es nilpotente y por tanto que $\phi(G) \leq F(G)$.

**Corolario 4**. $F(G/\phi(G)) = F(G)/\phi(G)$.

**Demostración**: Como todo cociente de un grupo nilpotente es también nilpotente, $F(G)/\phi(G) \leq F(G/\phi(G))$. Por otra parte si $F(G/\phi(G)) = H/\phi(G)$, por el Teorema anterior $H$ será subgrupo normal nilpotente de $G$, luego $H \leq F(G)$.

**Teorema 5**. Si $G$ es resoluble y $N .\!\trianglelefteq G$, existe $p$ primo tal que $N$ es $p$-elemental abeliano.

**Demostración**: Como $N' < N$ y $N' \mathrm{car} N \trianglelefteq G$, es $N' \trianglelefteq G$ y por la minimalidad de $N$ se tiene que $N' = 1$, luego $N$ es abeliano. Sea $p \mid |N|$. Consideremos el conjunto $\{x \in N | x^p = 1\}$. Dicho conjunto es un subgrupo característico de $N$ luego normal de $G$ y como no es trivial, debe coincidir con $N$. Así $N$ es $p$-elemental abeliano.

Observar que si $G \neq 1$ es resoluble, se tiene que $\phi(G) < F(G)$. En efecto basta tomar $N/\phi(G) .\!\trianglelefteq G/\phi(G)$. Por el Teorema anterior $N/\phi(G)$ es abeliano luego nilpotente. Por el Teorema 3 $N$ es nilpotente luego $\phi(G) < N \leq F(G)$.

**Teorema 6**. a) Si $G$ es resoluble $C_G(F(G)) \leq F(G)$ ($G$ es $N$-constricto).

b) Si $N .\!\trianglelefteq G$ se tiene que $F(G) \leq C_G(N)$.

**Demostración**. a) Si $C_G(F(G)) \nleq F(G)$ $A = C_G(F(G)) \cap F(G) < C_G(F(G))$. Sea $H$ minimal en cuanto a ser un subgrupo normal de $G$ contenido en $C_G(F(G))$ y conteniendo propiamente a $A$. Entonces $H/A .\!\trianglelefteq G/A$, luego, por el Teorema 5, es abeliano. Así $H' \leq A$

y $[H,H,H]=1$, por lo que $H$ es nilpotente luego $H \leq F(G)$. Por lo tanto $H \leq A$, lo que es una contradicción.

b) $[N, F(G)] \leq N \cap F(G)$. Si $N \cap F(G) = 1$, $F(G) \leq C_G(N)$. En otro caso $N \cap F(G) = N$ luego $N \leq F(G)$ y por el Teorema 4 de la Lección 1 $N \cap Z(F(G)) \neq 1$, luego $N \leq Z(F(G))$ y también $F(G) \leq C_G(N)$.

**Teorema 7**.(Gaschütz) $G' \cap Z(G) \leq \phi(G)$.

**Demostración**: Suponer que existe $M < .G$ tal que $G' \cap Z(G) \not\leq M$. Entonces $G = (G' \cap Z(G))M$, luego $M \trianglelefteq G$ y por tanto $G' \leq M$, lo que es una contradicción.

**Lección 3. Grupos actuando sobre grupos. Producto semidirecto.**

**Definición 1**. Se dice que un grupo $H$ actúa sobre un grupo $K$, cuando existe un homomorfismo de grupos $\phi : H \longrightarrow \mathrm{Aut}(K)$.

Dado $k \in K$ y $h \in H$, escribiremos $k^h$ para denotar a $\phi(h)(k)$.

**Ejemplos**

i) Si $H \leq \mathrm{Aut}(K)$, considerar la inmersión de $H$ en $\mathrm{Aut}(K)$.

ii) Si $K \trianglelefteq H$, considerar la acción de $H$ sobre $K$ vía conjugación, es decir el homomorfismo

$$\phi : H \longrightarrow \mathrm{Aut}(K)$$

dado por $\phi(h) = \phi_h$ siendo $\phi_h(k) = k^h$, cualesquiera que sean $h \in H$ y $k \in K$.

En particular si $H \leq G$, $N_G(H)$ actúa sobre H vía conjugación , siendo el núcleo de tal acción el $C_G(H)$.

iii) Dados dos grupos $H, K$, siempre existe una acción de $H$ sobre $K$, que es la acción trivial, considerando el homomorfismo trivial de $H$ en $\mathrm{Aut}(K)$.

**Teorema 2**. Sea $H$ actuando sobre $K$ vía $\phi$. Entonces el conjunto de los pares ordenados $(h, k)$ con $h \in H$ y $k \in K$, adquiere una estructura de grupo, con la siguiente operación interna:

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1^{h_2}k_2)$$

**Demostración**: Si $h_1, h_2, h_3 \in H$ y $k_1, k_2, k_3 \in K$, se tiene

$$(h_1, k_1)[(h_2, k_2)(h_3, k_3)] = (h_1, k_1)(h_2h_3, k_2^{h_3}k_3) = (h_1h_2h_3, k_1^{h_2h_3}k_2^{h_3}k_3)$$

$$[(h_1, k_1)(h_2, k_2)](h_3, k_3) = (h_1h_2, k_1^{h_2}k_2)(h_3, k_3)$$

$$= (h_1h_2h_3, (k_1^{h_2}k_2)^{h_3}k_3) = (h_1h_2h_3, k_1^{h_2h_3}k_2^{h_3}k_3)$$

por lo que la operación es asociativa. Es sencillo comprobar que el neutro es $(1, 1)$ y que $(h, k)^{-1} = (h^{-1}, (k^{-1})^{h^{-1}}$.

Dicho grupo se conoce como **producto semidirecto de** $H$ **por** $K$ vía la acción $\phi$ y se denota por $H \times_\phi K$.

Si consideramos a Aut(K) actuando sobre $K$ en la forma natural, al producto semidirecto resultante se le conoce como holomorfo de $K$: Hol($K$). Más generalmente , si $H \leq$ Aut(K), el correspondiente grupo semidirecto se conoce como un holomorfo relativo de $K$.

Si $A$ es un grupo abeliano tal que $b^2 \neq 1$, para algún $b \in A$, se define $\eta : A \longrightarrow A$ mediante $\eta(a) = a^{-1}$ $\forall a \in A$. Entonces $\eta \in \mathrm{Aut}(A)$ , $\eta \neq 1$ y al holomorfo relativo se le llama grupo diédrico generalizado asociado a $A$ y se denota por Dih($A$).

Si consideramos a $H$ actuando trivialmente sobre $K$, el producto semidirecto asociado a dicha acción es el producto directo $H \times K$.

**Teorema 3**. Sea $H$ actuando sobre $K$ vía $\phi$ y $G = H \times_\phi K$. Si consideramos $\bar{H} = \{(h, 1)|h \in H\}$ y $\bar{K} = \{(1, k)|k \in K\}$, se tiene que :

i) $\bar{H} \leq G$, $\bar{K} \trianglelefteq G$, $G = \bar{H}\bar{K}$, $\bar{H} \cap \bar{K} = 1$.

ii) $H \cong \bar{H}$ y $K \cong \bar{K}$.

iii) Tras las correspondientes identificaciones, la acción de $H$ sobre $K$, es la restricción a $H$ de la acción por conjugación de $G$ sobre $K$.

**Demostración**: Dada la sencillez de i) y ii), comprobaremos únicamente iii).

$$(h, 1)^{-1}(1, k)(h, 1) = (h^{-1}, 1)(1, k)(h, 1) = (h^{-1}, k)(h, 1) = (1, k^h)$$

**Definición 4**. Si $K \trianglelefteq G$, se dice que $G$ **se escinde sobre** $K$, si existe $H \leq G$ tal que $G = HK$ y $H \cap K = 1$. Dicho $H$ se dice que es un **complemento** de $K$ en $G$.

**Teorema 5**. i) Sea $H$ actuando sobre $K$ vía $\phi$ y $G = H \times_\phi K$. Entonces $G$ se escinde sobre $\bar{K}$ con complemento $\bar{H}$.

ii) Sea $K \trianglelefteq G$. Suponer que $G$ se escinde sobre $K$ con complemento $H$. Considerar la acción $\phi$ de $H$ sobre $K$ vía conjugación, entonces $G \cong H \times_\phi K$.

**Demostración**: i) Vista en el teorema anterior.

ii) Notar que cada elemento $g$ de $G$ es expresable de forma única como $g = hk$, con $h \in H$ y $k \in K$. Definamos la siguiente aplicación:

$$\alpha : G \longrightarrow H \times_\phi K$$

dada por $\alpha(g) = (h, k)$, supuesto que $g = hk$. Es sencillo probar que es un homomorfismo de grupos. En efecto:

$$\alpha(h_1k_1h_2k_2) = \alpha(h_1h_2k_1^{h_2}k_2) = (h_1h_2, k_1^{h_2}k_2) = (h_1, k_1)(h_2, k_2)$$

.

Es claro es un isomorfismo de grupos.

**Lección 4. Los teoremas de Baer, Zenkov y Lucchini.**

Los grupos considerados son finitos.

**Teorema 1** (Baer). Sea $x$ un $p$-elemento de un grupo $G$. Son equivalentes:

i) $x \in O_p(G)$

ii) $< x^h, x^g >$ es $p$-grupo, cualesquiera que sean $h, g \in G$.

**Demostración**: Seguiremos la demostración de Alperin y Lyons.

Es claro que $i) \Longrightarrow ii)$, ya que $O_p(G) \trianglelefteq G$.

$ii) \Longrightarrow i)$. Sea $G$ un contraejemplo y $C = x^G$ la clase de conjugación de $x$ en $G$. Sea $P \in \mathrm{Syl}_p(G)$. Si $C \subseteq P$ entonces $< C > \leq P$ y como $< C > \trianglelefteq G$ se tendría que $x \in < C > \leq O_p(G)$ y $G$ no sería contraejemplo. Podemos afirmar que $C - P \neq \emptyset$, así que existe $Q \in \mathrm{Syl_p(G)}$ tal que $(C \cap Q) - (C \cap P) \neq \emptyset$.

Sea $\mathcal{M} = \{(P, Q) | C \cap P \neq C \cap Q\}$, que por lo anterior no es vacío. Elijamos $(P, Q) \in \mathcal{M}$ con $|C \cap P \cap Q|$ lo mayor posible. Sea $D =< C \cap P \cap Q >$, notar que $< C \cap D >= D$, ya que es claro que $< C \cap D > \leq D$ y como $C \cap P \cap Q \subseteq C \cap D$, se tiene que $D \leq < C \cap D >$. Sea $g \in G$ tal que $P^g = Q$, entonces $(C \cap P)^g = C \cap Q$, así $|C \cap P| = |C \cap Q|$ y como $C \cap P \neq C \cap Q$, se tiene que $C \cap P \not\subseteq Q$, así $C \cap P \not\subseteq D$, ya que si $C \cap P \subseteq D$ se tendría que $C \cap P \subseteq < C \cap P > \leq D \leq Q$, que no es posible. Consideremos la serie:

$$D = P_0 \leq P_1 \leq ... \leq P_n = P$$

con $|P_i / P_{i-1}| = p$ para todo $i$. Como $C \cap P_n \not\subseteq D$ pero $C \cap P_0 \subseteq D$, sea $i$ el menor posible tal que $C \cap P_i \not\subseteq D$ $(i \geq 1)$. Sea $u \in (C \cap P_i) - D$. Como $u$ normaliza a $C \cap P_{i-1} = C \cap D$, también normaliza a $< C \cap D >= D$. Así

$$u \in (C \cap P \cap N_G(D) - D$$

De igual forma existe

$$v \in (C \cap Q \cap N_G(D) - D$$

Como por la hipótesis $< u, v >$ es $p$-grupo, también $< u, v > D$ es $p$-grupo, luego existe $R \in \mathrm{Syl}_p(G)$ tal que $< u, v > D \leq R$. Así

$$C \cap P \cap R \supseteq C \cap P \cap < u, v > D \supseteq (C \cap D) \cup \{u\}$$

y por tanto :

$$|C \cap P \cap R| > |C \cap D| \geq |C \cap P \cap Q|$$

luego por la elección de $(P, Q)$ se concluye que $(P, R) \notin \mathcal{M}$, es decir que $C \cap P = C \cap R$.

Un argumento análogo lleva a que $C \cap Q = C \cap R$, así $C \cap P = C \cap Q$, lo que es una contradicción.

**Corokario 2**. Sea $t$ una involución de un grupo $G$. Si $t \notin O_2(G)$ existe un $2'$-elemento $h \neq 1$ tal que $h^t = h^{-1}$.

**Demostración:** Por el teorema anterior existe $g \in G$ tal que $< t, t^g >$ no es 2-grupo. Asì como $t^{-1}(tt^g)t = t^g t = (t^g)^{-1}t^{-1} = (tt^g)^{-1}$, $t$ invierte a cada elemento de $< tt^g >$, que no es un 2-grupo ya que si lo fuera, $< t, t^g >=< t, tt^g >=< t >< tt^g >$ sería 2-grupo.

**Teorema 3** (Zenkov). Sean $A, B$ subgrupos abelianos de un grupo $G$. Si $M$ es minimal en el conjunto $\{A \cap B^g | g \in G\}$, entonces $M \leq F(G)$.

**Demostración:** $\{A \cap B^g | g \in G\}$, es el mismo que si sustituimos $B$ por un conjugado suyo arbitrario, así que puede suponerse que $M = A \cap B$. Veamos por inducción sobre el orden de $G$ que $M \leq F(G)$.

Supongamos que $G =< A, B^g >$, para algún $g \in G$. Como $A$ y $B^g$ son abelianos, $A \cap B^g \leq Z(G)$ y por tanto $(A \cap B^g)^{g^{-1}} = A \cap B^g \leq B$ luego $A \cap B^g \leq A \cap B = M$ y por la minimalidad de $M$ es $M = A \cap B^g \leq Z(G) \leq F(G)$.

Podemos por tanto suponer que $< A, B^g >< G$ para cualquier $g \in G$. Para probar que $M \leq F(G)$ basta razonar que si $P \in \mathrm{Syl}_p(M)$ se tiene que $P \leq F(G)$, para cualquier $p \in \pi(M)$, o lo que es lo mismo que $P \leq O_p(G)$. Por el teorema de Baer basta con probar que $< P, P^g >$ es $p$-grupo para cualquier $g \in G$.

Dado $g \in G$, sea $H =< A, B^g >< G$ y $C = H \cap B$. Si $h \in H$ se tiene:

$$A \cap C^h = A \cap (B \cap H)^h = A \cap B^h \cap H = A \cap B^h$$

en particular $M = A \cap B = A \cap C$ es minimal en $\{A \cap C^h | h \in H\}$. Por hipótesis de inducción $P \leq M \leq F(H)$, es decir $P \leq O_p(H)$. Como $P^g \leq B^g \leq H$, $P^g$ normaliza a $O_p(H)$, así $P^g O_p(H)$ es $p$-grupo, que contiene a $P$ y a $P^g$, así que $< P, P^g >$ es $p$-grupo, como queríamos probar.

Observar que si $G$ es un grupo con $p$-subgrupos de Sylow abelianos, por el teorema de Zenkov existe $g \in G$ tal que $P \cap P^g \leq O_p(G)$, siendo $P \in \mathrm{Syl}_p(G)$. Por tanto $P \cap P^g = O_p(G)$ y así $O_p(G)$ se puede expresar como la intersección de $P$ y $P^g$, ambos subgrupos de Sylow de $G$. Este resultado se conoce como teorema de Brodkey.

**Corolario 4**. Sea $A \leq G \neq 1$, $A$ abeliano . Suponer que $|G : A| \leq |A|$. Entonces $A \cap F(G) \neq 1$.

**Demostración:** Podemos suponer que $A < G$ y que por tanto $AA^g \neq G$, ya que si $G = AA^g$, $g = ab$ con $a \in A$ y $b \in A^g$, así $gb^{-1} = a$ y $A^g = (A^g)^{b^{-1}} = A^a = A$, lo que no es posible pues $A < G$.

Si $g \in G$ $|A||A^g| = |A|^2 \geq |A||G : A| = |G|$. Por lo tanto:

$$|G| > |AA^g| = |A||A^g|/|A \cap A^g| \geq |G|/|A \cap A^g|$$

luego $A \cap A^g \neq 1$ y por el teorema de Zenkov con $B = A$, se sigue que $A \cap F(G) \neq 1$.

Se ha probado que si $A \leq G \neq 1$, $A$ abeliano con $|G : A| \leq |A|$, entonces $A$ contiene un subgrupo subnormal no trivial de $G$, es decir un subgrupo de $G$ que forma parte de una serie normal de $G$. Si $A$ es cíclico, probaremos a continuación que $A$ contiene un subgrupo normal no trivial de $G$.

**Teorema 5** (Lucchini). Sea $A$ un subgrupo cíclico propio de un grupo $G$ y $K = \mathrm{core}_G(A)$. Entonces :

$$|A : K| < |G : A|$$

En particular si $|G : A| \leq |A|$, se sigue que $K \neq 1$.

**Demostración:** Por inducción sobre el orden de $G$. Si $K \neq 1$, como $A/K$ es subgrupo cíclico de $G/K$ y $\mathrm{core}_{G/K}(A/K) = 1$, por hipótesis de inducción se tendría que $|A/K| < |G/K : A/K| = |G : A|$. Podemos por tanto suponer que $K = 1$ y probaremos que $|A| < |G : A|$. Suponer que $|G : A| \leq |A|$. Como $A < G$ , $G$ no es trivial y por el Corolario anterior $A \cap F(G) \neq 1$, en particular $F(G) \neq 1$. Sea $N.\trianglelefteq G$, $N \leq F(G)$. Sabemos que $N \leq Z(F(G))$ luego $N$ es $p$-elemental abeliano para algún primo $p$. Además $N$ normaliza a $A \cap F(G))$, así $A \cap F(G)) \trianglelefteq AN$ y como $K = 1$ debe de ser $AN < G$.

Sea $\bar{G} = G/N$ y $\bar{M} = \mathrm{core}_{\bar{G}}(\bar{A}) = M/N \leq AN/N < G/N$. Entonces $AM = AN$. Por hipótesis de inducción se tiene que : $|\bar{A} : \bar{M}| < |\bar{G} : \bar{A}|$ luego $|AN : M| < |G : AN|$.

Sea $B = A \cap M$, se tiene:

$$|AN : A| = |AM : A| = |M : A \cap M| = |M : B|$$

así:

$$|AN : M| = |A : B|$$

y se concluye que:

$$|M : B| = |AN : A| = |G : A|/|G : AN| < |G : A|/|AN : M| =$$

$$= |G : A|/|A : B| \leq |A|/|A : B| = |B|$$

Suponer que $M$ es abeliano y $\phi : M \longrightarrow M$ dada por $\phi(x) = x^p$. Se tiene que $N \subseteq \mathrm{Ker}(\phi)$ y $N \leq M \leq AN$, así que $M = NB$ y $\phi(M) = \phi(B) \leq B \leq A$. Como $M \trianglelefteq G$ es $\phi(M) \trianglelefteq G$. Así $\phi(M) = 1$ pues $K = 1$. Por lo tanto $\phi(B) = 1$ y como $B$ es cíclico, debe ser $|B| \leq p$ y $|M/B| < |B| \leq p$ y como $M/B$ es $p$-grupo, se sigue que $M = B$, luego $M \leq A$ y como $K = 1$, debe ser $M = 1$ y $N = 1$ lo que no es posible.

Como consecuencia $M$ no es abeliano y dado que $M/N$ es cíclico debe ser $N \not\leq Z(M)$, así $N \cap Z(M) < N$, luego $N \cap Z(M) = 1$ y $Z(M) \cong Z(M)N/N$ cíclico. Por el resultado anterior como $B$ es subgrupo abeliano de $M$ y $|M : B| < |B|$ se tiene que $B \cap F(M) \neq 1$. Ahora bien $F(M) \leq F(G)$ así $N$ centraliza a $F(M)$ y $B \cap F(M)$ es un subgrupo no trivial central de $BN = M$. Puesto que $Z(M)$ es cíclico, $B \cap F(M) \operatorname{car} Z(M) \trianglelefteq G$, por lo que $B \cap Z(M)$ es un subgrupo normal no trivial de $G$ contenido en $A$, lo que no es posible.

**Corolario 6**. (Horosevskii). Sea $\sigma \in \mathrm{Aut}(G)$, $G \neq 1$, entonces $o(\sigma) < |G|$.

**Demostración:** Considerar el producto semidirecto $< \sigma > \times_i G$. Por el teorema anterior se tiene que $| < \sigma >: K| < | < \sigma > \times_i G :< \sigma > |$, con $K = \mathrm{core}_{<\sigma>\times_i G} < \sigma >$. Como $K \cap G \leq < \sigma > \cap G = 1$, cada elemento de $K$ centraliza a cada elemento de $G$, luego $K = 1$ y $o(\sigma) = | < \sigma > | < |G|$.

**Lección 5. El teorema de Schur-Zassenhaus.**

Los grupos considerados son finitos.

La búsqueda de complementos de subgrupos normales de un grupo tiene una gran importancia en la teoría de grupos. El teorema de Schur-Zassenhaus afirma la existencia y conjugación de tales complementos si se cumple que $(|N|, |G/N|) = 1$. Comenzamos analizando el caso $N$ abeliano.

Previamente recordar que si $G$ actúa sobre un conjunto $\Omega$, $a \in \Omega$ y $g \in G$ se tiene que $G_a^g = G_{ag}$. Así si la acción es transitiva, todos los estabilizadores son conjugados en $G$. Además si $N \trianglelefteq G$ y $N$ actúa transitivamente sobre $\Omega$, dados $a \in \Omega$ y $g \in G$ existe $n \in N$ tal que $ag = an$ luego $gn^{-1} \in G_a$ es decir $g \in NG_a$, por lo tanto $G = NG_a$.

Sea $\mathcal{S}$ el conjunto de todos los transversales de $N$ en $G$. Si $R, S \in \mathcal{S}$, definamos:

$$R|S = \sqcap rs^{-1} (\in N)$$

donde $(r, s) \in R \times S$ y $Nr = Ns$.

Notar que como $N \trianglelefteq G$ no hace falta distinguir entre transversal a izquierda o a derecha. Además en la definición de $R|S$, no importa el orden de los factores, dado que $N$ es abeliano.

Para $R, S, T \in \mathcal{S}$ se tiene:

1) $(R|S)^{-1} = S|R$

2) $(R|S)(S|T) = R|T$

Si $R \in \mathcal{S}$ y $g \in G$, entonces $gR \in \mathcal{S}$. En efecto si $x \in G$, existen $r \in R$ y $n \in N$ tales que $x = rn = g(g^{-1}rn) = gr'n'$ siendo $g^{-1}rN = r'N$, $r' \in R$. Además si $grN = gr'N$ se sigue que $rN = r'N$ luego $r = r'$ y $G$ es unión disjunta de las clases $grN$ cuando $r$ recorre $R$. Así puede definirse una acción de $G$ sobre el conjunto $\mathcal{S}$ :

$$\rho : G \longrightarrow \Sigma(\mathcal{S})$$

siendo $\rho(g)(R) = g^{-1}R$. Es sencillo comprobar que $\rho$ es un homomorfismo de grupos.

3) Si $n \in N$ se tiene:

$$nR|S = n^{|G:N|} R|S$$

Como $xR|xS = \sqcap xrs^{-1}x^{-1} = x(R|S)x^{-1}$, se tiene:

4) Si $x \in G$ se tiene: $R|S = 1 \Leftrightarrow xR|xS = 1$

Supongamos ahora que además $(|N|, |G/N|) = 1$ y definamos $\alpha : N \longrightarrow N$ dada por $\alpha(n) = n^{|G:N|}$, es claro que $\alpha$ es un homomorfismo y como existen enteros $z, z'$ tales que $1 = z|N| + z'|G : N|$ se tiene que $n = n^{z'|G:N|}$ luego si $n^{|G:N|} = 1$ se tiene que $n = 1$. Así $\alpha \in \mathrm{Aut}(N)$.

5) Dados $R, S \in \mathcal{S}$ sea $n = \alpha^{-1}((R|S)^{-1})$, entonces

$$nR|S = n^{|G:N|}R|S = \alpha(\alpha^{-1}(R|S)^{-1})R|S = 1$$

6) Si $n \in N$ y $R|S = 1 = nR|S$ entonces:

$$1 = nR|S = n^{|G:N|}R|S = n^{|G:N|} \Rightarrow n = 1$$

Las afirmaciones 1) a 6) son necesarias para probar el siguiente resultado.

**Teorema 1**. Sea $N \trianglelefteq G$, $N$ abeliano, tal que $(|N|, |G/N|) = 1$, entonces $N$ tiene complemento en $G$ y dos complementos cualesquiera de $N$ en $G$ son conjugados en $G$.

**Demostración:** Se define en $\mathcal{S}$ la relación:

$$R \sim S \text{ si } R|S = 1$$

Por 1) y 2) dicha relación es de equivalencia. Sea $[R]$ la clase de equivalencia de $R$ y $\mathcal{S}/\sim$ el conjunto de dichas clases. Se define una acción de $G$ sobre dicho conjunto :

$$\tilde{\rho} : G \longrightarrow \Sigma(\mathcal{S}/\sim)$$

en la forma $\tilde{\rho}(g)([R]) = [g^{-1}R]$. Notar que por 4):

$$[R] = [S] \Leftrightarrow R|S = 1 \Leftrightarrow g^{-1}R|g^{-1}S = 1 \Leftrightarrow [g^{-1}R] = [g^{-1}S]$$

Es claro que $\tilde{\rho}$ es un homomorfismo de grupos.

Por 5) dados $[R], [S]$ existe $n \in N$ tal que $\tilde{\rho}(n^{-1}) = [nR] = [S]$, es decir que $N$ actúa transitivamente sobre $\mathcal{S}/\sim$. Veamos el estabilizador en $N$ de un elemento de dicho conjunto. Suponer que existe $n \in N$ tal que $\tilde{\rho}(n)([R]) = [n^{-1}R] = [R]$. Entonces $R|R = 1 = n^{-1}R|R$. Por 6) se tiene que $n = 1$ y por tanto dicho estabilizador es trivial. Así el estabilizador de $[R]$ en $G$ es un complemento de $N$ en $G$.

Sea ahora $H$ un complemento de $N$ en $G$. $H$ es un transversal de $N$ en $G$. Como $hH = H \ \forall h \in H$ se tiene que $hH|H = 1$ luego $\tilde{\rho}(h^{-1})([H]) = [hH] = [H]$ es decir $H$ es un subgrupo del estabilizador de $[H]$ en $G$ y necesariamente deben coincidir.

Finalmente, sabemos que todos los estabilizadores en $G$ son conjugados en $G$.

Pasamos a demostrar el caso general.

**Teorema 2** (Schur-Zassenhaus).

a) Sea $N \trianglelefteq G$ tal que $(|N|, |G/N|) = 1$, entonces $N$ tiene complemento en $G$.

b) Si además $N$ ó $G/N$ es resoluble, dos complementos cualesquiera de $N$ en $G$ son conjugados en $G$.

**Demostración :**

a) Sea $G$ un contraejemplo de orden minimal.

1) $N$ es nilpotente.

Sea $P \in \mathrm{Syl}_p(N)$. Por el argumento de Frattini se tiene que $G = NN_G(P)$. Si $N_G(P) < G$, $N \cap N_G(P)$ tendría complemento $D$ en $N_G(P)$ y $|D| = |N_G(P)/N_G(P) \cap N| = |G/N|$ por lo que $D$ sería complemento de $N$ en $G$, lo que no es posible. Así que $N_G(P) = G$ y por el Teorema 8 de la Lección 1 se sigue que $N$ es nilpotente.

2) $N$ es abeliano.

Si $N' \neq 1$, como $|G/N'| < |G|$, sea $M/N'$ un complemento de $N/N'$ en $G/N'$. Así $|M/N'| = |G/N'/N/N'| = |G/N|$ y $|M| = |M/N'||N'| = |G/N||N'| < |G|$ pues $N' < N$. Por tanto existirá un complemento de $N'$ en $M$ de orden $|G/N|$ y llegaríamos a contradicción. Así $N$ es abeliano y aplicando el Teorema 1 llegaríamos a la contradicción final.

b) De nuevo podemos suponer que $G$ es un contraejemplo de orden minimal.

Si $N$ es resoluble se tiene que $N' < N$. Si $N' = 1$, $N$ es abeliano y basta aplicar el Teorema 1 para llegar a una contradicción. Si $N' \neq 1$ sean $D_1, D_2$ complementos de $N$ en $G$. Se tiene:

$$|D_i N'/N'| = |D_i/D_i \cap N'| = |D_i| = |G/N| = |G/N'/N/N'|$$

luego los $D_i N'/N'$ son complementos de $N/N'$, luego son conjugados y existe $x \in G$ tal que $D_2 N' = (D_1 N')^x = D_1^x N'$ y como $D_1^x$ y $D_2$ son complementos de $N'$ en $D_2 N'$ y

$|D_2N'| < |G|$, se sigue que son conjugados en $D_2N'$, asi $D_2 = (D_1^x)^y = D_1^{xy}$, que es una contradicción.

Si $G/N$ es resoluble sea $M/N.\trianglelefteq G/N$. Si $M < G$ como $M = M \cap D_iN = N(M \cap D_i)$ y $M/N$ es resoluble existirá $x \in M$ tal que $D_2 \cap M = (D_1 \cap M)^x = D_1^x \cap M$. Podemos suponer que $D_2 \cap M = D_1 \cap M = H \neq 1$. Entonces $D_i \leq N_G(H)$ $i = 1, 2$ y $N_G(H) = D_i(N_G(H) \cap N)$ y

$$N_G(H)/H = (D_i/H)\,(N_G(H) \cap N)H/H$$

con $D_i \cap (N_G(H) \cap N)H = H$, luego los $D_i/H$ son complementos y como $|N_G(H)/H| < |G|$ y

$$N_G(H)/H/(N_G(H) \cap N)H/H \cong N_G(H)/(N_G(H) \cap N)H = N_G(H)/N_G(H) \cap HN \cong$$

$$\cong N_G(H)N/HN \cong N_G(H)N/N/HN/N$$

que es resoluble, se seguiría que los $D_i$ son conjugados en $G$, lo que no es posible.

Si $M = G$ es que $G/N$ es simple y resoluble, luego $G/N \cong C_p$ para algún primo $p$ y como $p \nmid |N|$, los complementos son $p$-subgrupos de Sylow de $G$, que sabemos que son conjugados en $G$, lo que es la contradicción final.

Como $(|N|, |G/N|) = 1$ alguno de los órdenes es impar, luego, por el teorema de Feit-Thompson, $N$ ó $G/N$ es resoluble, por lo que en la parte b) del Teorema anterior podría suprimirse dicha condición.

## Lección 6. Acción coprima.

Para facilitar la exposición, supondremos que los grupos considerados son finitos.

Sea $G$ un grupo sobre el que actúa un grupo $A$ ($G$ es un $A$-grupo). Se definen dos subgrupos de $G$ en la forma siguiente:

$$[G, A] =< [g, a] | g \in G, a \in A >$$

siendo $[g, a] = g^{-1}g^a$,

$$C_G(A) = \{g \in G | g^a = g, \forall a \in A\}$$

Es sencillo probar que $[G, A]$ es un subgrupo normal $A$-invariante de $G$. En efecto, si $x \in G$

$$(g^{\cdot 1}g^a)^x = x^{-1}g^{-1}g^a x = x^{-1}g^{-1}g^a x^a x^{-a} x = (gx)^{-1}(gx)^a(x^{-1}x^a)^{-1} \in [G, A]$$

Si $a_1 \in A$:

$$(g^{-1}g^a)^{a_1} = g^{-a_1}g^{aa_1} = g^{-a_1}gg^{-1}g^{aa_1} = (g^{-1}g^{a_1})^{-1}g^{-1}g^{aa_1} \in [G, A]$$

Es claro que $C_G(A)$ es $A$.invariante, pero no necesariamente normal en $G$. Basta pensar en $< \alpha >$ actuando sobre $\Sigma_3$ en la forma

$$\alpha((1, 2, 3)) = (1, 3, 2), \alpha((1, 2)) = (1, 2)$$

entonces $C_{\Sigma_3}(< \alpha >) =< (1, 2) >$ que no es normal en $\Sigma_3$.

Si $G$ es un $A$.grupo y $N \trianglelefteq G$ , es $A$-invariante, queda inducida una acción de $A$ sobre $G/N$ en la forma siguiente:

$$\tilde{\phi} : A \longrightarrow \mathrm{Aut}(G/N)$$

$\tilde{\phi}(a)(xN) = x^a N$.

Diremos que $A$ actúa coprimamente sobre $G$ cuando $(|A|, |G|) = 1$.

Pasamos a demostrar un primer resultado sobre acción coprima que tiene muchas aplicaciones y que es una consecuencia del teorema de Schur-Zassenhaus.

**Teorema 1 (Lema de Glauberman).** Sea $\pi$ un conjunto de números primos, $A$ un $\pi$-grupo actuando sobre un $\pi'$-grupo $G$ ($A$ ó $G$ resoluble). Suponer que ambos actúan sobre un conjunto $\Omega$ de forma que:

a) $(\alpha g)a = (\alpha a)g^a$, cualesquiera que sean $\alpha \in \Omega, g \in G, a \in A$.

b) $G$ es transitivo sobre $\Omega$.

Entonces $A$ fija algún elemento de $\Omega$ y $C_G(A)$ actúa transitivamente sobre el conjuntom de elementos fijados por $A$.

**Demostración**: Sea $\Gamma = [G]A$ el producto semidirecto de $G$ por $A$ bajo la acción dada. Definimos una acción de $\Gamma$ sobre $\Omega$ en la forma:

$$\alpha(ag) = (\alpha a)g$$

En efecto, es una acción de $\Gamma$ sobre $\Omega$ ya que :

$$(\alpha(a_1g_1))(a_2g_2) = ((\alpha a_1)g_1)a_2)g_2 = ((\alpha a_1)a_2)g_1^{a_2})g_2 = (\alpha(a_1a_2))g_1^{a_2}g_2$$

y

$$\alpha(a_1g_1)(a_2g_2) = \alpha(a_1a_2g_1^{a_2}g_2) = (\alpha(a_1a_2))g_1^{a_2}g_2$$

Sea $\alpha \in \Omega$ y $H = \Gamma_\alpha$, entonces:

$$|\Omega| = |G : G_\alpha| = |G : G \cap \Gamma_\alpha| = |G : G \cap H| = |\Gamma : H|$$

pues la acción de $\Gamma$ sobre $\Omega$ será también transitiva.

Como $G \cap H \leq H \leq \Gamma$ y $G \cap H \leq G \leq \Gamma$, se sigue por lo anterior que

$$|A| = |\Gamma : G| = |H : H \cap G|$$

y como $H \cap G \trianglelefteq H$, por el teorema de Schur-Zassenhaus existe $D$ complemento de $H \cap G$ en $H$. Como $|D| = |A|$ será $D$ complemento de $G$ en $\Gamma$ y de nuevo aplicando dicho teorema, $D$ será conjugado con $A$ en $\Gamma$. Asi existe $g \in G$ tal que $A = D^g$. Por tanto $A \leq H^g = \Gamma_{\alpha g}$.

Veamos ahora la acción transitiva de $C_G(A)$ sobre el conjunto de elementos fijados por $A$. Sean $\beta, \gamma$ elementos de $\Omega$ fijados por $A$. Por b) sabemos que existe $y \in G$ tal que $\beta y = \gamma$ por lo tanto $A, A^y \leq \Gamma_\gamma \leq \Gamma = [G]A$, luego $\Gamma_\gamma = G_\gamma A = G_\gamma A^y$ y por tanto $A$ y

$A^y$ son conjugados en $\Gamma_\gamma$, luego existe $z \in G_\gamma$ tal que $A^z = A^y$ así $yz^{-1}$ normaliza a $A$. Como consecuencia tenemos:

$$[< yz^{-1} >, A] \leq A \cap G = 1$$

así que $yz^{-1} \in C_G(A)$ y $\beta yz^{-1} = \gamma z^{-1} = \gamma$.

El siguiente resultado viene a decir que si $A$ actúa coprimamente sobre $G$ ($A$ ó $G$ resoluble) y $N$ es un subgrupo normal $A$-invariante de $G$, los puntos fijos de $G/N$ por la acción inducida provienen de los puntos fijos de $G$.

**Teorema 2**. Si $A$ actúa coprimamente sobre $G$ ($A$ ó $G$ resoluble ) y $N$ es un subgrupo normal $A$-invariante de $G$, entonces:

$$C_{G/N}(A) = C_G(A)N/N$$

**Demostración**: sea $\Omega = \{Nx | x \in G\}$. $G$ actúa transitivamente sobre $\Omega$ y $A$ actúa en la forma inducida comentada en la introducción, de forma que:

$$(Nx)ga = (Nxg)a = N(xg)^a = Nx^a g^a = (Nx)ag^a$$

Por el lema de Glauberman sabemos que $A$ fija algún elemento de $\Omega$ y que $C_G(A)$ actúa transitivamente sobre el conjunto de puntos fijos por $A$. Así al considerar $N \in C_{G/N}(A)$ y hacer actuar $C_G(A)$, recorremos todos los puntos fijos por $A$ de $G/N$.

**Corolario 3**. Si $A$ actúa coprimamente sobre $G$ ($A$ ó $G$ resoluble) se tiene que

$$G = C_G(A)[G, A]$$

**Demostración**: Considerar a $A$ actuando sobre $G/[G, A]$. Como $x^{-1}x^a \in [G, A]$, cualesquiera que sean $x \in G, a \in A$, $A$ fija a cada elemento de $G/[G, A]$, luego

$$G/[G, A] = C_{G/[G,A]}(A) = C_G(A)[G, A]/[G, A]$$

luego G=C$_G(A)[G, A]$.

**Ejercicio**. i) Si $A, B \leq G$ se tiene que: $[A, B] \trianglelefteq < A, B >$. ii) Si $A, B, C$ son subgrupos de un grupo $G$ y $B \leq N_G(A) \cap N_G(C)$, entonces: $[AB, C] = [A, C][B, C]$.

**Corolario 4**. Si $A$ actúa coprimamente sobre $G$ ($A$ ó $G$ resoluble) se tiene:

$$[G, A, A] = [G, A]$$

**Demostración**: $[G, A] = [[G, A]C_G(A), A] = [[G, A], A]$.

**Teorema 5.** Si $A$ actúa coprimamente sobre $G$ y $G$ es abeliano entonces:

$$G = [G, A] \times C_G(A)$$

**Demostración**: Basta probar que $[G, A] \cap C_G(A) = 1$, para lo cual construiremos un endomorfismo $\phi$ de $G$ tal que $\phi(x) = x$ para cada $x \in C_G(A)$ y $\phi(x) = 1$ para cada $x \in [G, A]$.

Sea $|A| = n$, como $(n, |G|) = 1$, la aplicación que asocia a cada elemento $x \in G$ el elemento $x^n$, es un automorfismo $\alpha$ de $G$. En efecto, como $G$ es abeliano $(xy)^n = x^n y^n$, para cualesquiera $x, y \in G$. Además existen $s, t \in \mathbf{Z}$ tales que $1 = sn + t|G|$, luego si $x^n = 1$, $x = x^{sn+t|G|} = 1$. Considerar $\alpha^{-1}$ y definir

$$\phi : G \longrightarrow G$$

en la forma:

$$\phi(x) = \alpha^{-1}(\prod_{a \in A} x^a)$$

Es claro que $\phi$ es un endomorfismo de $G$. Además si $x \in C_G(A)$ se tiene que $\phi(x) = \alpha^{-1}(\alpha(x)) = x$ y si $a_1 \in A$ se tiene: $\phi(x^{a_1}) = \alpha^{-1}(\prod_{a \in A} x^{a_1 a}) = \phi(x)$, luego $\phi([x, a_1]) = \phi(x^{-1}x^{a_1}) = \phi(x)^{-1}\phi(x^{a_1}) = 1$, así $\phi(y) = 1$ para cualquier $y \in [G, A]$.

**Ejercicio**. (Lema de los tres subgrupos). Sean $A, B, C$ subgrupos de un grupo $G$. Demostrar que si $[A, B, C] = 1 = [B, C, A]$ entonces $[C, A, B] = 1$.

(Ayuda: usar la identidad de Hall-Witt: $[a, b^{-1}, c]^b [b, c^{-1}, a]^c [c, a^{-1}, b]^a = 1$, cualesquiera que sean $a, b, c \in G$.)

**Teorema 6 (El $P \times Q$- lema de Thompson)**. Sean $P, X$ $p$-grupos,$Q$ $p'$-grupo siendo $X$ un $P \times Q$-grupo. Si $[C_X(P), Q] = 1$ entonces $[X, Q] = 1$.

**Demostración**: Suponer que $[X, Q] \neq 1$ y sea $X_0$ minimal en el conjunto de los subgrupos $Y$ $P \times Q$-invariantes de $X$ que verifican $[Y, Q] \neq 1$.

Como $X_0$ y $P$ son $p$-grupos, el producto semidirecto $[X_0]P$ también lo es y por los Teoremas 3 y 6 de la Lección 1 se tiene que $[X_0, P[\leq [X_0, [X_0]P] < X_0$ y por la elección de $X_0$ se sigue que $[X_0, P, Q] = 1$ y como $[P, Q, X_0] = 1$, por el lema de los tres subgrupos se sigue que $[Q, X_0, P] = 1$ luego $[Q, X_0] \leq C_X(P)$ y por la hipótesis $[X_0, Q, Q] = 1$ y por el Corolario 4 se concluye que $[X_0, Q] = 1$, lo que es una contradicción.

**Corolario 7.** Si $P$ es un $p$-subgrupo de $G$, se tiene:

$$O_{p'}(N_G(P) \leq C_G(O_p(G))$$

siendo $O_{p'}(N_G(P)$ el mayor $p'$-subgrupo normal de $G$.

**Demostración**. Considerar $X = O_p(G), Q = O_{p'}(N_G(P))$ y el $p$-subgrupo $P$. Como se verifican las hipótesis del $P \times Q$-lema, y $[C_{O_p(G)}(P), O_{p'}(N_G(P)] \leq O_p(G) \cap O_{p'}(N_G(P) = 1$, sabemos que $[O_p(G), O_{p'}(N_G(P)] = 1$.

**Lema 8**. Sea $P$ un $p$.subgrupo de $G$ y $K$ un $p'$-subgrupo normal de $G$. Entonces:

$$N_{G/K}(PK/K) = N_G(P)K/K$$

**Demostración**: Es claro que $N_G(P)K/K \leq N_{G/K}(PK/K) = U/K$. Ahora bien, como $PK \trianglelefteq U$ y $P \in \mathrm{Syl}_p(PK)$, por el argumento de Frattini se tiene que:

$$U = PKN_U(P) = KN_U(P) \leq KN_G(P) = N_G(P)K$$

.

A continuación probaremos que si $G$ es resoluble puede obtenerse un resultado más fuerte que el obtenido en el Corolario 7.

**Teorema 9**. Sea $G$ resoluble y $P$ un $p$-subgrupo de $G$. Denotar con $C = C_G(P)$ y con $N = N_G(P)$. Entonces

$$O_{p'}(C) = O_{p'}(N) \leq O_{p'}(G)$$

**Demostración**: Como $O_{p'}(C) \mathrm{car} C \trianglelefteq N$ es $O_{p'}(C) \leq \mathrm{O}_{p'}(N)$. Además $[O_{p'}(N), P] = 1$, así que $O_{p'}(N) \leq C$ y por lo tanto $O_{p'}(N) \leq O_{p'}(C)$.

Veamos ahora que uno de tales subgrupos es subgrupo del $p'$-radical de $G$. La demostración será por inducción sobre $|G|$.

Si $K = O_{p'}(G) \neq 1$, se tiene que $|G/K| < |G|$ y por hipótesis de inducción se tiene que:

$$O_{p'}(N_{G/K}(PK/K)) \leq O_{p'}(G/K) = 1$$

Por el lema anterior sabemos que $N_{G/K}(PK/K) = N_G(P)K/K$, así que

$$O_{p'}(N_G(P))K/K \leq O_{p'}(N_G(P)K/K) = 1$$

por tanto $O_{p'}(N_G(P)) \leq K = O_{p'}(G)$.

Suponer ahora que $K = 1$. Así $F(G) = O_p(G)$ y como $G$ es resoluble, por el Teorema 6 de la Lección 2 sabemos que $C_G(O_p(G)) \leq O_p(G)$. Por el Corolario anterior se tiene que

$$O_{p'}(N_G(P)) \leq C_G(O_p(G)) \leq O_p(G)$$

y así $O_{p'}(N_G(P)) = 1$.

## Lección 7. Preliminares del $p^a q^b$-Teorema de Burnside.

**Teorema 1**. Sea $P$ un $p$-grupo que a lo más tiene un subgrupo de orden $p$. Si $p = 2$ suponer además que $P$ es abeliano. Entonces $P$ es cíclico.

**Demostración:** Por el Teorema 11 de la Lección 1 (Teorema de estructura de los grupos finitos abelianos) se sigue que si $P$ es abeliano, necesariamente $P$ será cíclico, por lo tanto podemos suponer que $|P| \geq p^3$. Procederemos por inducción sobre $|P|$.

Si $|P| = p^3$ , supongamos que $P$ no es cíclico, luego $P$ no es abeliano (luego $p$ impar), así que $P' = Z(P) \cong C_p$ y $P/Z(P) \cong C_p \times C_p$, luego $P/Z(P) = X/Z(P) \times Y/Z(P)$ con $|X/Z(P)| = |Y/Z(P)| = p$. Ambos $X, Y$ tienen por tanto orden $p^2$, luego serán cíclicos. Sea $X =< x >$, $Y =< y >$, entonces $X \cap Y =< x^p >=< y^p >= Z(P)$, el único subgrupo de orden $p$ de $P$. Como $y^{-p} = (x^p)^m = (x^m)^p$ para algún $m, 1 \leq m < p$, podemos suponer que $x^p y^p = 1$. Como $[x, y] \in P' = Z(P)$ se tiene que $[x, y] = 1$ ó $o([x, y]) = p$. Sabemos que:

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

Como $p$ es impar $2|p-1$ luego $(xy)^p = 1$, pero $xy \notin X \cap Y$ lo que es una contradicción.

Pasamos al caso general. Sea $N.\trianglelefteq P$. Entonces $N \leq Z(P)$ y $|N| = p$. Considerar $P/N$ y suponer que existen dos subgrupos de orden $p$: $R/N$ y $S/N$. Supongamos, sin pérdida de generalidad que $R/N \leq Z(P/N)$, entonces $RS$ es un subgrupo de $P$ de orden $p^3$ con un único subgrupo de orden $p$ y además, si $p = 2$, es abeliano. Por la parte anterior, sabemos que $RS$ es cíclico, luego tiene un único subgrupo de orden $p^2$, así $R = S$ lo que no es posible. Ahora, por hipótesis de inducción, $P/N$ es cíclico, luego $P/Z(P)$ es también cíclico, por lo tanto $P$ es abeliano y por la hipótesis es cíclico.

Es una consecuencia inmediata que un $p$-grupo $P$ no cíclico de orden impar contiene un subgrupo isomorfo a $C_p \times C_p$, pues $Z(P)$ siempre contiene un elemento de orden $p$.

**Lema 2**. Sea $P$ $p$-elemental abeliano no cíclico actuando sobre un $q$-elemental abeliano $Q$. Entonces existe $g \neq 1, g \in P$ tal que $C_Q(g) \neq 1$.

**Demostración:** Supongamos sin pérdida de generalidad que $|P| = p^2$, es decir que $P \cong C_p \times C_p$. $P$ tiene $p^2 - 1/p - 1$ subgrupos de orden $p$ y $P = \cup P_i$ donde $P_i$ recorre tales subgrupos. Consideremos a $Q$ como $\mathbf{Z}/q\mathbf{Z}$-espacio vectorial. Suponer que la tesis es falsa, así si $1 \neq g \in P$ y $x \in Q$ tal que $x^g = x$ entonces $x = 0$ (utilizamos notación aditiva en $Q$).

Sea $0 \neq y \in Q$ y $1 \neq h \in P$, entonces

$$(\sum_{g \in P} y^g)^h = \sum_{g \in P} y^{gh} = \sum_{g \in P} y^g$$

luego $\sum_{g \in P} y^g = 0$. Lo mismo sucede para $P_i$ en lugar de $P$, $i = 1, ..., p+1$, así:

$$0 = \sum_{g \in P} y^g = \sum_{i=1}^{p+1} (\sum_{g \in P_i} y^g) - py = -py$$

pero como $o(y) = q$, se sigue $p = q$. Entonces el producto semidirecto asociado $G = [Q]P$ es un $p$-grupo y sabemos que $Q \cap Z(G) \neq 1$, lo que no es posible.

**Lema 3.** Sean $p, q$ primos tales que $p \neq q$ y sea $P$ $p$-elemental abeliano no cíclico actuando sobre un $q$-grupo $Q$. Si

$$\eta(Q) =< C_Q(W) | W \leq P, |P : W| = p >$$

entonces $Q = \eta(Q)$. En particular

$$Q =< C_Q(x) | 1 \neq x \in P >$$

**Demostración:** Por inducción sobre $|P| + |Q|$.

Suponer primero que $Q$ tiene un subgrupo normal $P$-invariante no trivial propio $Q_0$. sea $W \leq P$ tal que $|P : W| = p$. Por el Teorema 2 de la Lección 6 sabemos que :

$$C_{Q/Q_0}(W) = C_Q(W)Q_0/Q_0$$

así que $\eta(Q/Q_0) \leq \eta(Q)Q_0/Q_0$ y como $|Q/Q_0| < |Q|$, se sigue por hipótesis de inducción que $\eta(Q/Q_0) = Q/Q_0$ y por tanto que $Q = \eta(Q)Q_0$. Asimismo, como $|Q_0| < |Q|$ es $Q_0 = \eta(Q_0) \leq \eta(Q)$, luego $Q = \eta(Q)$.

Supongamos ahora que $Q$ no posee subgrupos $P$-invariantes normales distintos de 1 y de $Q$. Así $Q$ es característicamente simple luego $\phi(Q) = 1$ y por tanto $Q$ es $q$-elemental abeliano. Por el lema anterior existe $1 \neq x \in P$ tal que $C_Q(x) \neq 1$. Como $P$ es abeliano, $C_Q(x)$ es $P$-invariante y por la hipótesis es $Q = C_Q(x)$. Podemos definir una acción en forma natural de $\bar{P} = P/ < x >$ sobre $Q$.

Si $\bar{P}$ es cíclico es $|\bar{P}| = p$ y $Q = C_Q(x) \leq \eta(Q)$.

Si $\bar{P}$ no es cíclico, por hipótesis de inducción se tiene:

$$Q =< C_Q(\bar{W}) || \bar{P} : \bar{W}| = p > \leq < C_Q(W) || P : W| = p >= \eta(Q)$$

Hemos probado que $Q$ viene generado por los subgrupos de puntos fijos de los subgrupos maximales de $P$. Es claro que si $1 \neq x \in P$, $< x >< P$, pues $P$ no es cíclico y existirá $M < .P$ tal que $< x > \leq M$ luego $C_Q(M) \leq C_Q(< x >)$ así en particular $Q =< C_Q(x) | 1 \neq x \in P >$.

**Lema 4.** Sean $p, q$ primos tales que $p \neq q$, ambos impares, $P$ un $p$-subgrupo y $Q$ un $q$-subgrupo de $G = \mathrm{GL}(2, q)$. Si $Q \leq N_G(P)$ entonces $Q \leq C_G(P)$.

**Demostración:** Notar que $Q$ actúa coprimamente sobre $P$, así por el Corolario 4 de la Lección 6 : $[[P, Q], Q] = [P, Q, Q] = [P, Q]$, luego bastará probar que $Q$ centraliza a $P_0 = [P, Q] \trianglelefteq PQ$, $P_0 \leq P$. Es claro que $P_0 \leq [G, G] \leq \mathrm{SL}(2, q)$ ya que :

$$\mathrm{GL}(2, q)/\mathrm{SL}(2, q) \cong \mathrm{GF}(q)^* \cong C_{q-1}$$

Sea $V$ un $\mathrm{GF}(q)$-espacio vectorial 2-dimensional y consideremos a $\mathrm{GL}(2, q)$ actuando como es habitual sobre $V$. Supongamos que existen $x \in P_0$ y $v \in V$ tales que $v^x = v \neq 0$.

Sea $(v, w)$ base de $V$ y $X = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ la matriz coordenada de $x$ en dicha base. Como $\det(X) = 1$ es $b = 1$ y así $X^q = I$ luego $x = 1$ pues $P_0$ es $q'$-grupo. Por el Lema 2 $P_0$ no contiene subgrupos elementales abelianos no cíclicos así, por la nota posterior al Teorema 1, $P_0$ es cíclico. Como $p || \mathrm{GL}(2, q) = (q^2 - 1(q^2 - q) = q(q-1)^2(q+1)$ y $q \neq 2$ se tiene que $p < q$. Sea $|P_0| = p^a$, $a \geq 1$ entonces $|\mathrm{Aut} P_0| = p^{a-1}(p-1)$ que no es divisible por $q$. Como cada elemento de $Q$ induce un automorfismo de $\mathrm{P}_0$ de orden potencia de $q$, se concluye por el Corolario 4 de la Lección 6 que:

$$[P_0, Q] = 1 = [P, Q, Q] = [P.Q]$$

es decir $Q \leq C_G(P)$.

**Lema 5.** Sea $q$ un primo impar, $V$ $q$-elemental abeliano y $H$ un grupo de automorfismos resoluble de $V$. Suponer $|H|$ impar y $O_q(H) = 1$. Si $h$ es un $q$-elemento de $H$ tal que $|V : C_V(h)| \leq q$ entonces $h = 1$.

**Demostración:** Podemos suponer que $|V : C_V(h) = q$ pues si $|V : C_V(h)| = 1$ sería $h = 1$. También podemos suponer que $o(h) = q$, ya que si $o(h) = q^a$, $a > 1$ considerariamos $h^{q^{a-1}}$, $o(h^{q^{a-1}}) = q$ y como $C_V(h) \leq C_V(h^{q^{a-1}}) < V$, pues $h^{q^{a-1}} \neq 1$, se tendría $C_V(h) = C_V(h^{q^{a-1}})$.

Sea $H$ contraejemplo de orden minimal y $Q =< h >$. Como $O_q(H) = 1$, $F(H)$ es un $q'$-grupo. Como $H$ es resoluble, por el Teorema 6 a) de la Lección 2 $C_H(F(H)) \leq F(H)$ y existe $p \in \pi(H)$, $p \neq q$, tal que $[O_p(H), Q] \neq 1$ (notar que también $p$ es impar pues $|H|$ es impar). Sea $P = O_p(H)$, entonces $O_q(PQ) = 1$. Por la elección de $H$, debe de ser $H = PQ$. Como $Q$ no es un subgrupo normal de $H$ tomamos $x \in H - N_H(Q)$, así $Q$ y $Q^x$ son $q$-subgrupos de Sylow de $H$, $Q \neq Q^x$, luego también de $< Q, Q^x >$ y como $O_q(< Q, Q^x >) \leq Q \cap Q^x = 1$, de nuevo, por la elección de $H$, se tiene que $H =< Q, Q^x >$. así $C_V(H) = C_V(Q) \cap C_V(Q^x)$ y :

$$|V : C_V(H)| \leq |V : C_V(Q)||V : C_V(Q^x)| = q^2$$

Como $V$ es abeliano $C_V(H) \trianglelefteq V$. Además $H$ se representa fielmente sobre $W = V/C_V(H)$. En efecto si $L = \mathrm{Ker}(H\,\mathrm{sobre}\,W)$, $[L, W] = 1 \Longrightarrow [L, V] \leq C_V(H) \Longrightarrow [L, V, L] = 1 \Longrightarrow [V, L \cap P, L \cap P] = 1 = [V, L \cap P]$, por el Corolario 4 de la Lección 6. Por lo tanto $L \cap P = 1$ y $|L| = |LP/P|$, que divide a $|H : P| = q$, luego $L \leq O_q(H) = 1$.

En consecuencia, $H$ es isomorfo a un subgrupo de $\mathrm{GL}(2, q)$ y por el resultado anterior es $[P, Q] = 1$, lo que es una contradicción.

## Lección 8. Demostración del $p^a q^b$-Teorema de Burnside.

**Teorema**. Sea $G$ un grupo de orden $p^a q^b$, $p, q$ primos, entonces $G$ es resoluble.
**Demostración**: (Bender) Si $G$ es contraejemplo de orden minimal, analizaremos su estructura en varios pasos hasta llegar a que no puede existir dicho grupo.

1. $G$ es un grupo simple no abeliano cuyos subgrupos propios son todos resolubles.

En efecto $G$ no es abeliano y si $1 \neq N \lhd G$, la elección de $G$ fuerza a que tanto $N$ como $G/N$ son resolubles luego $G$ es resoluble, lo que no es posible. Además si $H < G$ por la misma razón $H$ es resoluble.

Necesariamente $p \neq q$ y podemos suponer que $p < q$. En la demostración $\{r, s\}$ denotará el par no ordenado $\{p, q\}$.

2. Si $G$ tiene subgrupos $A, B$ tales que $G = AB$ y $A \neq G$, entonces $B$ no normaliza a cualquier subgrupo no trivial de $A$.

Suponer que $B \leq N_G(H)$ siendo $1 \neq H \leq A$. Entonces:

$$1 \neq H^G = H^{BA} = H^A \leq A < G$$

donde $H^G$ denota la envoltura normal de $H$ en $G$. Como $H^G \lhd G$, esto no es posible por 1.

3. Si $R \in \mathrm{Syl}_r(G)$ , $R$ no normaliza a un $s$-subgrupo no trivial de $G$.

Si $1 \neq H \leq G$ es un $s$-subgrupo de $G$ y $R \leq N_G(H)$, como existe $S \in \mathrm{Syl}_s(G)$ tal que $H \leq S$ y $G = RS$ basta aplicar 2 para concluir que dicha suposición no puede darse.

4. Si $S \in \mathrm{Syl}_s(G)$, $1 \neq Y \trianglelefteq R \in \mathrm{Syl}_r(G)$, entonces $G =< S, Y >$.

En efecto, sea $1 \neq z \in Y \cap Z(R)$. Considerar los subgrupos $< S, z >$ y $C_G(z)$. Como $R \leq C_G(z)$ es $G =< S, z > C_G(z)$ y dado que $C_G(z)$ normaliza al subgrupo no trivial $< z >$ de $< S, z >$, concluimos por 2 que debe ser $G =< S, z >=< S, Y >$.

5. Sean $M, H$ subgrupos maximales de $G$. Suponer que existen $R$ $r$-subgrupo normal de $M$ y $S$ $s$-subgrupo normal de $M$ no triviales de forma que $R \times S \leq H$, entonces:

i) $R \times S \leq F(H) \leq M$

ii) $M = H$

Como $M \leq N_G(R) \leq G$, por la maximalidad de $M$ y por 1 se sigue que $M = N_G(R)$. Análogamente $M = N_G(S)$.

Por otra parte:

$$S \leq C_H(R) \leq C_G(R) \leq N_G(R) = M$$

así que $S \trianglelefteq C_H(R)$. Por el Teorema 9 de la Lección 6 sabemos que:

$$O_{r'}(C_H(R)) = O_{r'}(N_H(R)) \leq O_{r'}(H) = O_s(H)$$

pues $H$ es resoluble. Por tanto $1 \neq S \leq O_s(H)$. Análogamente $1 \neq R \leq O_r(H)$. Así $R \times S \leq O_r(H) \times O_s(H) = F(H)$. Además $O_r(H) \leq C_G(S) \leq M$ y también : $O_s(H) \leq C_G(R) \leq M$ por lo tanto $F(H) \leq M$.

Considerando ahora que, según hemos probado, $O_r(H) \times O_s(H) \leq M$, intercambiando los papeles de $M$ y $H$ se concluye que:

$$F(H) = O_r(H) \times O_s(H) \leq F(M) \leq H$$

Finalmente repitiendo lo que hemos hecho al principio con $R = O_r(M)$ y $S = O_s(M)$, concluiremos que $F(M) \leq F(H)$ y por tanto que:

$$F(M) = F(H)$$

Por tanto: $M = N_G(F(M)) = N_G(F(H)) = H$

6. Sea $M < .G$, entonces $F(M)$ tiene orden potencia de un primo.

Supongamos que $O_r(M) \neq 1 \neq O_s(M)$ y lleguemos a contradicción.

Sean $1 \neq R_0 = Z(O_r(M))$ y $1 \neq S_0 = Z(O_s(M))$. Es claro que $R_0, S_o \leq Z(F(M))$. Sea $1 \neq x \in F(M)$, entonces $R_0 \leq C_G(x) < G$ y $S_0 \leq C_G(x) < G$, así existe $H < .G$ tal que $R_0 \times S_0 \leq C_G(x) \leq H < G$. Por 5 sabemos que $H = M$, así que

$$C_G(x) \leq M, \ \forall\ 1 \neq x \in F(M)$$

Veamos que $R_0$ es cíclico. Si no fuera así, por el Teorema 11 de la Lección 1, existiría $T \leq R_0$ tal que $T \cong C_r \times C_r$.

Sea $R \in \mathrm{Syl}_r(M)$. Como $R \leq N_G(S_0)$, por 3 no puede ser $R$ un $r$-subgrupo de Sylow de $G$. Así existe $P \in \mathrm{Syl}_r(G)$ tal que $R < P$ luego $R < N_P(R)$. Sea $g \in N_P(R) - R$. Entonces $g \notin M$ pues si $g \in M$, $R << g > R$, $r$-subgrupo de $M$, lo que no es posible. Así:

$$T \leq R_0 \leq R = R^g \leq M^g \neq M$$

pues $M = N_G(M)$. por lo tanto $T$ normaliza a $S_0^g \trianglelefteq M^g$. Llamemos $S = S_0^g$. Como $T$ es un $r$-elemental abeliano no cíclico actuando sobre $S$, que es un $s$-grupo, por el Lema 3 de la Lección 7 sabemos que:

$$S =< C_S(x) | 1 \neq x \in T > \leq < C_G(x) | 1 \neq x \in T > \leq M$$

Además, como $R_0 \leq R$, se tiene: $R_0^g \leq R^g = R \leq M^g$ y $M$ contiene a $R_0^g \times S_0^g \trianglelefteq M^g$. Por 5 se tiene que $M = M^g$, lo que no es cierto.

Concluimos que $R_0$ es cíclico y análogamente $\mathrm{S}_0$ es cíclico.

Concretando, $P_0 = Z(O_p(M)$ es cíclico. Suponer que $|P_0| = p^c$, entoces $|\mathrm{Aut}(P_0)| = p^{c-1}(p-1)$. Sea $Q \in \mathrm{Syl}_q(M)$ actuando por conjugación sobre $P_0$. Como el grupo de automorfismos de $P_0$ inducido por $Q$ es un $q$-grupo y $p < q$ dicho grupo debe ser trivial. Así $Q$ centraliza a $P_0$ y $P_0 \times Q_0 \leq N_G(Q)$ siendo $1 \neq Q_0 = Z(O_q(M))$. Por 5 se sigue que $N_G(Q) \leq M$. Por la cuestión 11 de Teoría de Sylow, sabemos que $Q \in \mathrm{Syl}_q(G)$, lo que no es posible por 3, dado que $Q \leq N_G(P_0)$.

7. Sea $t$ un primo y $E$ un grupo finito . Un $t$-subgrupo $U$ de $E$ se dice **localmente central en** $E$ si $U \leq Z(T)$, siendo $T$ algún $t$-subgrupo de Sylow de $E$. Notar que el centro de cualquier $t$-subgrupo de Sylow de $E$ es ejemplo de localmente central y que si $U$ es $t$-localmente central, $C_E(U)$ contiene un $t$-subgrupo de Sylow de $E$. La existencia de subgrupos localmente centrales no triviales en subgrupos maximales de $G$, suministrará una información importante sobre la estructura de $G$.

8. (Matsuyama) Si $M < .G$ contiene algún $r$-subgrupo no trivial $Y$ localmente central en $G$ entonces $F(M)$ es un $r$-grupo.

Supongamos que $F(M)$ no es un $r$-grupo. Por el paso 6, $F(M)$ es un $s$-grupo. Elijamos un $s$-subgrupo de Sylow de $G$ conteniendo a $F(M)$ y sea $Z$ su centro. Entonces: $Z \leq C_G(F(M)) \leq N_G(F(M)) = M$, así que: $Z \leq C_M(F(M)) \leq F(M)$, por ser $M$ resoluble. Sea:

$$L =< Z^y | y \in Y >$$

entonces $L \leq F(M)$ y por tanto $L$ es un $s$-subgrupo normalizado por $Y$. Sea $\mathcal{M}$ el conjunto de los $s$-subgrupos de $G$ que satisfacen:

i) son normalizados por $Y$

ii) están generados por $G$-conjugados de $Z$

Claramente $1 \neq L \in \mathcal{M}$. Sea $K$ maximal de $\mathcal{M}$ conteniendo a $L$ y sea $S$ un $s$-subgrupo de Sylow de $G$ conteniendo a $K$. Como $Y$ es un $r$-subgrupo localmente central es normal en el $r$-subgrupo de Sylow en cuyo centro está contenido. Así por 4 $G =< S, Y >$. Como $Y \leq N_G(K)$ debe ser $S \nleq N_G(K)$, es decir $N_S(K) < S$ luego $N_S(K) < N_S(N_S(K))$ y podemos considerar $x \in N_S(N_S(K)) - N_S(K)$. Por tanto $K \neq K^x \leq N_s(K)$. Como $K^x$ está generado por conjugados de $Z$, sea $Z^g$ uno de ellos tal que $Z^g \nleq K$.

Recordar que $Y$ es un $r$-subgrupo no trivial localmente central de $G$ y $Z$ es un $s$-subgrupo no trivial localmente central de $G$, luego $G = C_G(Z)C_G(Y)$. Sean $u \in C_G(Z), v \in C_G(Y)$ tales que $g = uv$. Entonces $Z^g = Z^{uv} = Z^v$. Sea

$$L^* =< Z^{vy} | y \in Y >=< Z^{yv} | y \in Y >= L^v$$

Es claro que $L^*$ es un $s$-subgrupo normalizado por $Y$ y generado por ciertos conjugados de $Z$, por tanto $L^* \in \mathcal{M}$. Además como $Y \leq N_G(K)$ y $Z^v = Z^g \leq K^x \leq N_G(K)$ se tiene que $L^* \leq N_G(K)$ , luego $KL^*$ es un $s$-subgrupo de $G$, $KL^* \in \mathcal{M}$ y $K < KL^*$ lo que está en contra de la maximalidad de $K$.

9. Un $r$-subgrupo localmente central $Y \neq 1$ de $G$ no normaliza a un $s$-subgrupo no trivial de $G$.

Supongamos que $Y \leq N_G(S)$ siendo $S$ un $s$-subgrupo no trivial de $G$. Entonces $N_G(S)$ contiene a $Y$, que es un $r$-subgrupo localmente central no trivial y al centro de un $s$-subgrupo de Sylow que contiene a $S$, que es un $s$-subgrupo localmente central no trivial de $G$. Si $N_G(S) \leq M < .G$, por 8 sabemos que $F(M)$ es a la vez $r$-grupo y $s$-grupo, luego $F(M) = 1$, lo que no es posible pues $M$ es resoluble (ver la nota que sigue al Teorema 5 de la Lección 2).

10. $G$ tiene orden impar.

Recordar que como consecuencia del Teorema de Baer (Corolario 2 de la Lección 4) sabemos que si $t$ es una involución de un grupo $G$ y $t \notin O_2(G)$, existe un $2'$-elemento $1 \neq h \in G$ tal que $h^t = h^{-1}$.

Suponer que $2||G|$. Sea $t$ una involución del centro de un 2-subgrupo de Sylow de $G$, como $O_2(G) = 1$, por el resultado anterior $< t >$ normaliza a un $2'$-subgrupo de $G$ no trivial (es decir a un $q$-subgrupo no trivial de $G$), lo que no es posible por 9.

11. Si $E$ es un $p$-grupo, $\Omega(E)$ denota el subgrupo de $E$ generado por los elementos de orden $p$.

Sea $R_0$ un $r$-subgrupo no trivial de $G$ tal que $C_G(R_0) \leq L < G$. Además sea $R_0 \leq R_1 \leq R_2$ con $R_1 \in \mathrm{Syl}_r(L)$ y $R_2 \in \mathrm{Syl}_r(G)$. Entonces :

a) $F(L) = O_r(L)$

b) $\Omega(Z(R_2)) \leq \Omega(Z(O_r(L)))$

c) $C_G(\Omega(Z(O_r(L))))$ es un $r$-grupo

En efecto:

a) Como $1 \neq Z(R_2) \leq C_G(R_0) \leq L$ y $Z(R_2)$ es un $r$-subgrupo localmente central de $G$, por 9 se sigue que $O_s(L) = 1$. así $F(L) = O_r(L)$.

b) Como $O_r(L) \leq R_1 \leq R_2$ se sigue que $Z(R_2) \leq C_L(F(L) \leq F(L)$ pues $L$ es resoluble.

Por tanto $Z(R_2) \leq Z(O_r(L))$ y de ahí que $\Omega(Z(R_2)) \leq \Omega(Z(O_r(L)))$

c) Si $S \in \mathrm{Syl}_s(C_G(\Omega(Z(O_r(L)))))$, por b) se tiene que $[S, \Omega(Z(R_2))] = 1$ y como $\Omega(Z(R_2))$ es un $r$-subgrupo localmente central de $G$, por 9 se sigue que $S = 1$ y así $C_G(\Omega(Z(O_r(L))))$ es un $r$-grupo.

12. Sea $P_0$ un $p$-subgrupo de $G$ no trivial, entonces $N_G(P_0)$ tiene $q$-subgrupos de Sylow cíclicos.

En particular si $F(M)$ es $p$-grupo, siendo $M < .G$, $M = N_G(F(M))$ tiene $q$-subgrupos de Sylow cíclicos

Suponer que sucede lo contrario y sea $V = \Omega(Z(P_0))$. Por la consecuencia del Teorema 1 de la Lección 7, dichos $q$-subgrupos de Sylow contendrán un subgrupo del tipo $C_q \times C_q$ y como $N_G(P_0) \leq N_G(V)$, este último contendrá un tal subgrupo.

Sea $\mathcal{N}$ el conjunto de pares $(A, V)$ que satisfacen:

i) $A \cong C_q \times C_q$

ii) $V$ es un subgrupo no trivial $p$-elemental abeliano $A$-invariante maximal de $G$

Por lo anterior, $\mathcal{N}$ no es vacío. Sea $(A, V) \in \mathcal{N}$ con $|C_V(A)|$, lo mayor posible.

Podemos afirmar que :

$$C_V(A) < V$$

Para ello, consideremos $Y = \Omega(Z(O_p(N_G(V))))$. Apliquemos 11 con $R_0 = V$ y

$L = N_G(V)$, entonces $C_G(Y)$ es $p$-grupo. $Y$ es un $A$-invariante $p$-elemental abeliano subgrupo de $Z(O_p(N_G(V)))$ y $V \leq O_p(N_G(V))$, así $VY$ es un $A$-invariante $p$-elemental abeliano. Por lo tanto, por la elección de $V$ es $Y \leq V$ y se sigue que $C_G(V) \leq C_G(Y)$. Así $C_G(V)$ es un $p$-grupo y si $V = C_V(A)$, se seguiría que $A \leq C_G(V)$, llegando a contradicción.

Por el Lema 3 de la Lección 7 se tiene que:

$$V =< C_V(x) | 1 \neq x \in A >$$

y existirá $1 \neq x \in A$ tal que $C_V(A) < C_V(x) = U$. Como $A$ centraliza a $x$, $U$ es $A$-invariante y no centralizado por $A$. Así $A$ induce sobre $U/C_V(A)$ un $q$-grupo de automorfismos no trivial, ya que en otro caso : $[U, A] \leq C_V(A)$ luego $[U, A, A] = 1 = [U, A]$, por el Corolario 4 de la Lección 6. Como $|\mathrm{Aut} C_p| = p - 1$ y $p < q$, se concluye:

$$|U/C_V(A)| \geq p^2$$

Sea $Z_1 = \Omega(Z(O_q(C_G(x))))$, entonces como $< x > \trianglelefteq C_G(x)$ es $< x > \leq O_q(C_G(x))$ y finalmente $< x > \leq Z(O_q(C_G(x)))$, luego $x \in Z_1$. Por 11 c) con $< x >, C_G(x)$ y $q$ en lugar de $R_0, L$ y $r$, tenemos que $C_G(Z_1)$ es $q$-grupo. Como $1 \neq U \leq C_G(x)$ se tiene que $Z_1$ es normalizado pero no centralizado por $U$, pues $U$ es $p$-grupo. Así $< x >< Z_1$ y $U$ induce sobre $Z_1/ < x >$ un grupo de automorfismos no trivial, pues en otro caso sería $[U, Z_1] \leq < x >$ luego: $[Z_1, U, U] = 1 = [Z_1, U]$, lo que no es posible.

Como $U$ no puede ser cíclico, por el Lema 3 de la Lección 7 se tiene:

$$Z_1/ < x > =< C_{Z_1/<x>}(W) || U : W| = p >$$

luego existe $W \leq U$ tal que $|U : W| = p$ que centraliza a un subgrupo $1 \neq Z_2/ < x >$ de $Z_1/ < x >$, es decir$[Z_2, W] \leq < x >$ luego $[Z_2, W, W] = 1 = [Z_2, W]$. Como $Z_1$ es elemental abeliano, existe $A_1 \leq Z_2$, $A_1 \cong C_q \times C_q$ y como $A_1$ centraliza a $W$, podemos encontrar un $A_1$-invariante $p$-elemental abeliano maximal, sea $V_1$, conteniendo a $W$. Entonces $(A_1, V_1) \in \mathcal{N}$ y $W \leq C_{V_1}(A_1)$. Ahora bien:

$$|W| = |U|/p > |C_V(A)|$$

lo que está en contradicción con la elección del par $(A, V)$.

13. Sea $M < .G$ con $F(M)$ $r$-grupo. Entonces $M/F(M)$ tiene $r$-subgrupos de Sylow cíclicos.

Considerar:

$$F(M/F(M)) = F(M/O_r(M)) = O_s(M/O_r(M)) = L/O_r(M)$$

así $L = O_r(M)S$ con $S \in \mathrm{Syl}_s(L)$.

Por el argumento de Frattini $M = SO_r(M)N_M(S) = O_r(M)N_M(S)$.

Si $S = 1$ se tiene que $M/F(M) = 1$ y 13 se cumple.

Si $S \neq 1$, tenemos dos posibilidades:

i) $s = p$. Entonces por 12 $N_G(S)$ tiene $q$-subgrupos de Sylow cíclicos, de ahí que $M/F(M) = O_r(M)N_M(S)/O_r(M) \cong N_M(S)/N_{O_r(M)}(S)$ tiene $q$-subgrupos de Sylow cíclicos.

ii) $s = q$. Entonces $r = p$ y como $1 \neq F(M)$ es un $p$-subgrupo de $G$ y $M = N_G(F(M))$, por 12 se sigue que $M$ tiene $q$-subgrupos de Sylow cíclicos luego se sigue que $S$ es cíclico y como $2 < q$ es conocido que $\mathrm{Aut}(S)$ es también cíclico.

Considerar $M^* = M/F(M)$, entonces $F(M^*) \cong S$, luego $C_{M^*}(F(M^*)) = F(M^*)$ y por tanto $M^*/F(M^*)$ es isomorfo a un subgrupo de $\mathrm{Aut}(F(M^*))$. Por lo tanto $M^*/F(M^*)$ es cíclico y si $P^* \in \mathrm{Syl}_p(M^*) \Longrightarrow P^* \cong P^*F(M^*)/F(M^*)$ es también cíclico.

14. Si $R$ es un $r$-grupo, denotaremos por $J_0(R)$ al subgrupo de $R$ generado por todos sus subgrupos elementales abelianos de orden maximal. Claramente $J_0(R)\mathrm{car}R$ y si $J_0(R) \leq U \leq R$ entonces $J_0(R) = J_0(U)$.

(El subgrupo de Thompson $J(R)$ es similar, omitiendo la palabra "elemental" en la definición. Subgrupos de este tipo juegan un papel importante en la teoría de grupos no resolubles).

15. Sea $M < .G$ con $F(M)$ $r$-grupo. Si $R \in \mathrm{Syl}_r(M)$, entonces $M = N_G(J_0(R))$ y $R \in \mathrm{Syl}_r(G)$.

Sea $K = F(M) = O_r(M)$. Supongamos que $J_0(R) \not\leq K$ y llegaremos a contradicción. Sea $A$ un subgrupo elemental de orden maximal de $R$ no contenido en $K$. Por 13 $AK/K$ es cíclico y así $|A : A \cap K| = r$.

Sea $V = \Omega(Z(K))$, observar que $(A \cap K)V$ es subgrupo elemental abeliano de $R$. De ahí que:

$$|A| \geq |(A \cap K)V| = |A \cap K||V|/|A \cap V| = |A||V|/r|A \cap V|$$

Así $|V : A \cap V| \leq r$.

Como $1 \neq V \mathrm{car} K \trianglelefteq M$ y $M < .G$ es $M = N_G(V)$. Como consecuencia $C_G(V) \leq M$ y por 11, tomando $V$ como $R_0$ y $M$ como $L$, tenemos que $C_G(V)$ es un $r$-grupo, de hecho es $r$-subgrupo normal de $M$ y así $C_G(V) \leq K \leq C_G(V)$ y por tanto $K = C_G(V)$.

Sea $H = M/K = M/C_M(V)$ grupo de automorfismos de $V$. además $O_r(H) = O_r(M/O_r(M)) = 1$. Sea $a \in A - (A \cap K)$ y $h = aK$, entonces $A \cap V \leq C_V(h)$ y como $|V : A \cap V| \leq r$, se sigue que $|V : C_V(h)| \leq r$. Por el Lema 5 de la Lección 7 se sigue que $h = 1$, luego $a \in K$ lo que es una contradicción.

Por tanto $J_0(R) \leq K \leq R$ y así $J_0(R) = J_0(K) \mathrm{car} K \trianglelefteq M$, luego $M = N_G(J_0(R))$.

Si $R < R^* \in \mathrm{Syl}_r(G)$ sería $J_0(R) \mathrm{car} R < N_{R^*}(R)$, pero esto no puede ser pues se tendría que: $N_{R^*}(R) \leq N_G(J_0(R)) = M$ y $R \in \mathrm{Syl}_r(M)$. Así $R \in \mathrm{Syl}_r(G)$.

16. Sea $M < .G$ con $F(M)$ $r$-grupo. Si $g \in G - M$ entonces $M \cap M^g$ es un $s$-grupo.

Notar que $M \neq M^g$ pues $N_G(M) = M$.

Suponer que la afirmación no es cierta y elegir $g \in G - M$ de forma que un $r$-subgrupo de Sylow $R$ de $M \cap M^g$ tenga el orden mayor posible. Si $R \in \mathrm{Syl}_r(M)$ se sigue que $R \in \mathrm{Syl}_r(M^g)$. Así, por 15, $M = N_G(J_0(R)) = M^g$, que no es posible. Por lo tanto $1 < R < R_1$ para algún $R_1 \in \mathrm{Syl}_r(M)$, y de ahí que $R < N_{R_1}(R)$. Sea $H < .G$ conteniendo a $N_G(R)$. Por 11 a) $F(H)$ es $r$-grupo y por 15 $H = N_G(J_0(R_2))$, para algún $R_2 \in \mathrm{Syl}_r(G)$. También por 15 tenemos que $R_1 \in \mathrm{Syl}_r(G)$ y se sigue que $J_0(R_2)$ es conjugado a $J_0(R_1)$ en $G$. Como consecuencia $H$ es conjugado con $N_G(J_0(R_1)) = M$.

Como $R < N_{R_1}(R) \leq H \cap M$, la elección de $R$ y $M^g$ fuerza a que $H = M$. Un argumento análogo aplicado a $R$ como subgrupo de $M^g$, lleva a que $H = M^g$ y así a la contradicción $M = M^g$.

17. Conclusión.

Sea $r$ el primo para el que un $r$-subgrupo de Sylow de $G$ tiene mayor orden que un $s$-subgrupo de Sylow de $G$. Sea $C_G(Z(R)) \leq M < .G$. Por 11 a) $F(M)$ es un $r$-grupo. Si $g \in G - M$, por 16 tenemos que $R \cap R^g = 1$, así $RR^g$ es un subconjunto de $G$ conteniendo

$|R||R^g| = |R|^2$ elementos. Sin embargo $|R|^2 > |R||S| = |G|$, y así la contradicción final completa la demostración.

## Prácticas de Teoría de Grupos

## Práctica 1

1. Si $[[a,b],a]=1$, $a,b\in G$, probar que para cualquier $n\geq 1$ se tiene:

$$[a^n,b]=[a,b]^n$$

2. Si $[[a,b],a]=1=[[a,b],b]$, $a,b\in G$, probar que para cualquier $n\geq 1$ se tiene

$$(ab)^n=a^nb^n[b,a]^{\binom{n}{2}},$$

3. Probar que si $|G/Z(G)|=4$, entonces $|G'|=2$.

4. Si $x\in G$, $G$ grupo finito, con $o(x)=2$ y los 2-subgrupos de Sylow de $C_G(x)$ son cclicos, probar que son 2-subgrupos de Sylow de $G$.

5. Demostrar que si en un grupo finito $G$ existe $x$ tal que $|C_G(x)|=p$, entonces cada $p$-subgrupo de Sylow de $G$ tiene orden $p$.

6. Sea $|G|=p^n$ y $|G:C_G(x)|\leq p, \forall x\in G$. Probar:

i) $C_G(x)\trianglelefteq G\,, \forall x\in G$

ii) $G'\leq Z(G)$

iii) $|G'|\leq p$

7. Sea $G$ finito, $p$ el menor primo dividiendo a $|G|$ , $p$ impar y $G'\cong C_p\times C_p$, entonces $G$ es nilpotente.

8. Sea $G$ finito, $H\leq G$ tal que $C_G(x)\leq H\,, \forall x\in H-\{1\}$. Probar que:

$$(|H|,|G:H|)=1$$

es decir que $H$ es un subgrupo de Hall de $G$.

9. Sea $G$ un grupo finito nilpotente y sea $A$ maximal entre todos los subgrupos normales abelianos de $G$. Probar que $A=C_G(A)$.

10. Demostrar:

i) Si $N\trianglelefteq G$, entonces: $\phi(N)\leq\phi(G)$.

ii) Si $N\trianglelefteq G$ , $N$ nilpotente y $G/N'$ nilpotente, entonces $G$ es nilpotente.

iii) $F(G/Z(G))=F(G)/Z(G)$.

## Práctica 2

11. (M. Isaacs) Si $G$ es un grupo finito, tal que todas las clases de conjugación fuera de $Z(G)$ tienen cardinal $p$ y $G/Z(G)$ es abeliano, probar que $|G'| = p$. (Confrontar con los problemas 3 y 6 de la Práctica 1). .

12. Si $m \neq 1$ es un divisor de $p-1$, siendo $p$ primo, usar el producto semidirecto para construir un grupo de orden $pm$, no abeliano, que contiene un subgrupo normal de orden $p$.

13. Sea $G$ un $p$-grupo finito. Probar que $\phi(G)$ es el menor normal de $G$ que da cociente $p$-elemental abeliano.

14. Considerar el producto semidirecto $G =< \alpha > \times_i < a >$ con $o(a) = 5$ y $\alpha(a) = a^2$. Comprobar que:

i) $\phi(G) = 1$

ii) $\phi(< \alpha >) =< \alpha^2 >\cong C_2$

iii) $\phi(G) < a > / < a >< \phi(G/ < a >)$

15. Se considera el grupo cuaternio de orden ocho: $Q_8$, comprobar que la aplicación de dicho grupo en sí mismo $\alpha$ tal que $\alpha(i) = j$ y $\alpha(j) = ij$ es un automorfismo. Si $G =< \alpha > \times_i Q_8$, es el correspondiente producto semidirecto, se pide:

i) Obtener $Z(G), G', F(G), \phi(G)$.

ii) Describir los subgrupos nilpotentes de $G$.

16. Sea $A =< a >\cong C_8$ y $\alpha \in \mathrm{Aut}(A)$ dado por $\alpha(a) = a^3$, entonces $o(\alpha) = 2$. Sea $G$ el holomorfo relativo correspondiente. Entonces $G$ se llama semidiédrico de orden 16. Encontrar en $G$ subgrupos $H_1, H_2, H_3$ tales que $H_1 \cong C_8$, $H_2 \cong D_8$, $H_3 \cong Q_8$. Demostrar que la clase de nilpotencia de $G$ es 3.

17. Se considera $C_3 \times C_3$ como un $\mathbf{Z}/3\mathbf{Z}-$espacio vectorial de dimensión 2. Sea

$$A =< \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} >\leq \mathrm{GL}(2,3)$$

En una base previamente fijada, cada una de dichas matrices representa un automorfismo. Considerar el holomorfo relativo correspondiente $G$. Hallar $F(G), \phi(G), G'$.

18. Sea $G = NH$ con $N \trianglelefteq G$, $N$ abeliano y $N \cap H = 1$. Probar que

$$C_G(N) = N \times \mathrm{core}_G(H)$$

19. Sea $K$ un grupo abeliano y $G = \mathrm{Hol}(K)$. Probar que

$$C_G(K) = K$$

.

20. Sea $K$ un grupo abeliano, $H \leq \mathrm{Aut}(K)$, y $G = [K]H$ el holomorfo relativo asociado. Probar que:

$$Z(G) = C_K(H)$$

## Práctica 3

21. Es conocido que un grupo $G$ tal que $x^2 = 1$, cualquiera que sea $x \in G$, es abeliano. Se trata ahora de encontrar ejemplos de grupos no abelianos verificando $x^p = 1$ para cualquier $x \in G$ , $p$ primo $(p > 2)$. Considerar $C_3 \times C_3$ como $\mathbf{Z}/3\mathbf{Z}$- espacio vectorial. Sea $\alpha$ el automorfismo que en una base de $C_3 \times C_3$ tiene a la matriz $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ como matriz coordenada. Considerar el holomorfo relativo: $G =< \alpha > \times_i (C_3 \times C_3)$. Probar que $x^3 = 1\ \forall x \in G$, pero que $G$ no es abeliano. Hallar $Z(G), \phi(G), G'$. (Este grupo es un ejemplo de grupo extraespecial).

22. Sea $K = C_p, H = \mathrm{Aut}(K)$ y $G = \mathrm{Hol}(K)$, donde $p$ es un primo. Se pide razonar que:

i) $H < .G$ y $\mathrm{core}_G(H) = 1$

ii) $F(G) = K$ y $\phi(G) = 1$

iii) Para $p = 5$ $\phi(G/K)$ no es trivial.

23. Sea $\alpha \in \mathrm{Aut}(\Sigma_3)$ dado por :

$$\alpha((1,2,3)) = (1,2,3),\ \alpha((1,2)) = (2,3)$$

Comprobar que $o(\alpha) = 3$ y considerar el holomorfo relativo $G =< \alpha > \times_i \Sigma_3$. Obtener $G', F(G), \phi(G), Z(G)$.

24. Sea $K =< a >\cong C_{13}$ y $H =< \alpha >\leq \mathrm{Aut}(K)$ dado por $\alpha(a) = a^{10}$ Comprobar que $o(\alpha) = 6$ y obtener $G', \phi(G), F(G)$ y $Z(G)$.

25. Considerar a $C_3 \times C_3$ como $\mathbf{Z}/3\mathbf{Z}$- espacio vectorial. Sea $\alpha$ el automorfismo que en una base de $C_3 \times C_3$ tiene a la matriz $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Considerar el holomorfo relativo $G =< \alpha > \times_i (C_3 \times C_3)$ y hallar $G', F(G), \phi(G)$ y $Z(G)$.

## Práctica 4

26. Si $G$ es un grupo finito demostrar que: $\pi(G/\phi(G)) = \pi(G)$

27. Sea $G$ finito, $A \trianglelefteq G$, $A$ abeliano tal que $A \cap \phi(G) = 1$. Probar que $A$ tiene com plemento en $G$.

(Ayuda: Considerar $\{S | S \leq G, G = AS\}$. Sea $L$ minimal en dicho conjunto. Probar que $A \cap L \trianglelefteq G, A \cap L \leq \phi(L), A \cap L \leq \phi(G)$, obteniendo finalmente que $L$ es complemento de $A$ en $G$.)

28. Demostrar que si $G$ es finito y $N . \trianglelefteq G$, $N$ abeliano y $H$ un complemento de $N$ en $G$, entonces $H . < G$.

29. Sea $N . \trianglelefteq G$, $N$ abeliano, entonces $N$ tiene complemento en $G$ si y solo si $N \not\leq \phi(G)$.

30. i) Sea $F$ un cuerpo. Considerar la acción de $F^*$ sobre $F^+$ vía multiplicación. Razonar que dicha acción es irreducible, es decir que los únicos subgrupos que quedan invariantes por dicha acción son $\{0\}$ y el propio $F^+$.

ii) Razonar que para cada primo $p$ y cualquier entero $n$, $n \geq 1$, existe un grupo resoluble finito con un maximal de ìndice $p^n$.

31. Sea $H(k) = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} | a, b, c \in k\} \leq \mathrm{GL}(3, k)$

Comprobar:

i) $Z(H(k)) = \{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} | b \in k\}$.

ii) $H(\mathbf{Z}/2\mathbf{Z}) \cong D_8$.

iii) En general $H(k)$ es nilpotente de clase 2.

Este grupo es conocido como grupo de Heisenberg y si $k = \mathbf{R}$ juega un importante papel en mecánica cuántica.

32. El grupo de Pauli. Sea $P =< a = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, c = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} > \leq \mathrm{GL}(2, \mathbf{C})$. Observar que $o(a) = 4, o(b) = o(c) = 2, a^b = a = a^c, b^c = ba^2$. Comprobar que $|P| = 16$. Hallar $Z(P), P', \phi(P)$.

### Cuestiones sobre Teoría de Sylow

1. Si $P \in \mathrm{Syl}_p(G)$ y $N \trianglelefteq G$, entonces $PN/N \in \mathrm{Syl}_p(G/N)$.

2. Si $P \in \mathrm{Syl}_p(G)$ y $N \trianglelefteq G$, entonces $P \cap N \in \mathrm{Syl}_p(N)$.

3. SI $G/N$ es un $p$-grupo y $P \in \mathrm{Syl}_p(G)$ se tiene que $G = PN$.

4. Si $P \in \mathrm{Syl}_p(G)$ y $M, N \trianglelefteq G$, entonces $P \cap MN = (P \cap M)(P \cap N)$.

5. Si $G/N$ y $G/M$ son $p$-grupos entonces $G/N \cap M$ es también un $p$-grupo.

6. Si $P \in \mathrm{Syl}_p(G)$ y $M, N \trianglelefteq G$, entonces $PN \cap PM = P(N \cap M)$.

7. Argumento de Frattini. Si $P \in \mathrm{Syl}_p(N)$ , $N \trianglelefteq G$, entonces $G = NN_G(P)$.

8. $N_{G/N}(PN/N) = N_G(P)N/N$ siendo $P \in \mathrm{Syl}_p(G)$ y $N \trianglelefteq G$.

9. $\cap P^g$, cuando $g$ recorre los elementos de $G$, es el mayor $p$-subgrupo normal de $G$. Se denota $O_p(G)$.

10. Si $N_G(P) \leq A \leq G$, con $P \in \mathrm{Syl}_p(G)$, entonces $A = N_G(A)$. En particular: $N_G(N_G(P)) = N_G(P)$.

11. Sea $P$ un $p$-subgrupo de $G$, entonces : $P \in \mathrm{Syl}_p(G) \Leftrightarrow P \in \mathrm{Syl}_p(N_G(P))$.

12. Si $\nu_p(G) > 1$ y $P_1, P_2 \in \mathrm{Syl}_p(G)$ se eligen de forma que $P_! \neq P_2$ y $|P_1 \cap P_2|$ sea el mayor posible, entonces $\nu_p(N_G(P_1 \cap P_2)) > 1$.

13. Todo grupo de orden $p^a q$, con $p, q$ primos , es resoluble.

14. Todo grupo de orden $pqr$, con $p, q, r$ primos, es resoluble.

15. Todo grupo de orden $p^2 q^2$ , con $p, q$ primos, es resoluble.

16. Si $|G| = p(p+1)$, con $p$ primo , entonces $G$ tiene un subgrupo normal de orden $p$ o un subgrupo normal de orden $p+1$.

17. Si $|G| = pn$ con $p$ primo tal que $p > n$ y $H \leq G$ con $|H| = p$, entonces $H \trianglelefteq G$.

**BIBLIOGRAFIA.**

1. Doerk-Hawkes. Finite Soluble Groups. Walter de Gruyter, 1992.

2. Gorenstein. Finite Groups. Harper Row, 1968

3. Isaacs. Algebra. A graduate course. Brooks/Cole Pub. Comp. 1994

4. Isaacs. Finite Group Theory. Graduate Studies in Mathematics v.92 A.M.S., 2008.

5. Kurzweil-Stellmacher. The Theory of Finite Groups. Springer, 2004

6. Rose. A course on group theory. Cambridge Univ. Press, 1978.