Grupos finitos con subgrupos de Sylow cíclicos

Mireia Judith Sancho Nuez

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directora del trabajo: Paz Jiménez Seral
25 de junio de 2021

Introducción

El tema del presente trabajo se encuentra dentro del ámbito de la teoría clásica de los grupos finitos abstractos.

La teoría de grupos tiene sus orígenes en la teoría de números y la teoría de las ecuaciones algebraicas, las cuales surgieron a finales del siglo XVIII y en la geometría de comienzos del siglo XIX. Con todo esto, el concepto de grupo se formalizó en el siglo XX. En la teoría de las ecuaciones algebraicas tuvo una notable importancia el estudio de las permutaciones. Hasta 1770 se conocían las permutaciones como ordenaciones, pero en en ese año Lagrange introdujo el concepto de permutación como transformación de una ordenación a otra. Este concepto fue muy importante porque con las ordenaciones no se podía trabajar, pero considerando las permutaciones como transformaciones se puede componer, es decir, se puede operar con ellas. En 1832, Galois utilizó por primera vez la palabra "grupo", lo definió como un conjunto de permutaciones de manera que si estaban dos transformaciones también estaba su composición en el conjunto. En 1854, Cayley hizo un intento de definición de grupo abstracto y, en 1878, acabó demostrando que cualquier grupo finito puede describirse en términos de grupos de permutaciones, es decir, que todo grupo finito es isomorfo a un subgrupo de grupo de permutaciones. Así, el concepto con el que trabajó Galois es exactamente el actual. En el siglo XX se empezó a desarrollar la teoría de grupos en abstracto, considerando varias acciones fieles se llega a que un mismo grupo abstracto es un subgrupo de distintos grupos de permutaciones, pero todos estos, son isomorfos como grupos abstractos.
En todo el trabajo cuando hablemos de grupos, estos serán grupos finitos.

El objetivo del trabajo es la caraterización de los grupos que tienen todos sus subgrupos de Sylow cíclicos.

Sea p un primo, un grupo G se llama p-grupo si su orden es una potencia de p. Sea G un grupo tal que $|G| = p^a m$ donde p es primo y $(p,m) = 1$, es decir, $p \nmid m$, entonces un subgrupo S de G se llama p-subgrupo de Sylow de G cuando $|S| = p^a$. Por el Teorema de Lagrange un p-subgrupo de G no puede tener un orden mayor que p^a, un p-subgrupo de Sylow de G es un p-subgrupo de G que tiene este orden máximo p^a.

El estudio de los p-subgrupos de un grupo ya fue estudiado por Cauchy en 1845, el cual demostró que todo grupo cuyo orden es múltiplo de un primo p, contiene un elemento de orden p. En 1872, Peter Ludwig Sylow publicó un artículo llamado *Théorèmes sur les groupes de substitutions* en la revista *Mathematische Annalen* [3], donde generalizó el resultado de Cauchy, este enunció y demostró teoremas en grupos de permutaciones, los cuales fueron muy útiles en la clasificación de grupos finitos simples. Los teoremas de Sylow garantizan la existencia de p-subgrupos de Sylow de G para cualquier primo p que divide al orden del grupo G, establecen que todos los p-subgrupos de Sylow son conjugados, en particular, isomorfos, y nos aportan información sobre el número de p-subgrupos de Sylow. Más tarde, en 1887, Frobenius probó la existencia de subgrupos de Sylow evitando el teorema de Cauchy, para ello utilizó las clases de conjugación, y esta se convirtió en la prueba estándar de los teoremas de Sylow hasta que en 1959 Wielandt reconstruyó las demostraciones de los teoremas. [Véase [6]]

Hay programas de ordenador, como el GAP (Groups, Algorithms, Programming), que es un programa especializado en teoría de grupos, que calculan directamente los subgrupos de Sylow de un grupo. Este es un trabajo teórico de caracterización y por lo tanto no usaremos el GAP.

Summary

The objective of this dissertation is the characterization of the finite groups whose Sylow subgroups are all cyclic.

Let G be a finite group and p a prime, a subgroup $P \leq G$ is called a p-subgroup if its order is a power of p. A p-subgroup whose order is the maximum power of p that divides the order of G is called a Sylow p-subgroup.

First of all, we choose the results that we have already seen and that we are going to use in this dissertation, and then we introduce new concepts that have not appeared in the degree courses, such as the normaliser subgroup, the commutator subgroup, the derived subgroup, the derived series and the characteristic subgroup. We also state and demonstrate new results involving these concepts that we will need for our purpose. In addition, note that in the degree courses we have worked with the concept of the resolvable group as an extension of abelian groups, without mentioning the derived subgroup, and in the dissertation we give a characterization of the resolvable groups with the derived series.

In the next dissertation's chapter, we give the definition of p-subgroups and Sylow p-subgroups, and then we see some general results and properties about them.
Then, we state Sylow's theorems and some consequences that are easily deduced from them.

Later, we study the conditions that must be met by some group families to have cyclic all of their Sylow subgroups. Specifically, we study abelian, dihedral, symmetric and alternating groups. We also give some examples of these families of groups, in which we can see that they only have cyclic all their Sylow subgroups if they verify the conditions that we have given for each family.

In the last chapter of the dissertation we focused on seeing how is the structure of finite groups which have cyclic all of their Sylow subgroups.

First of all, we give two lemmas that we need to achieve our purpose. We see that subgroups and quotient groups of finite groups whose Sylow subgroups are all cyclic also have cyclic all of their Sylow subgroups. Then we see that if the Sylow p-subgroups of a finite group G are cyclic, all the p-groups of G are also cyclic.

For the purpose of the dissertation, *Theorem of Burnside* is essential. Let G be a finite group, if P is a p-Sylow subgroup and it's contained in the center of its normalizer, that is, $P \subseteq Z(N_G(P))$, then exists a normal complement, that is, exists $N \trianglelefteq G$ such that $N \cap P = 1$ and $G = NP$.

This theorem is very important because if a large group G has a subgroup $N \trianglelefteq G$ and a subgroup $H \leq G$ with $N \cap H = 1$ and $G = HN$, then G is a semi-direct product of H by N. If we know N and H, which are groups smaller than G, and we know how is the conjugation of an element of N by an element of H (since N is normal, n^h is another element of N), that is, we know n^h for all $n \in N$, $h \in H$, then we know the whole group G, and for this reason it is very important to detect which groups G are a semi-direct product.

For the proof of this theorem, a sophisticated homomorphism is constructed between the group and Sylow's subgroup. We will give that sophisticated construction called transfer between a finite group G and an abelian H/K section of the group ($K \trianglelefteq H \leq G$). First, the application is defined from a transversal of H in G, which is a set of representatives of the coset of H in G. Then we see that the definition is independent of the transversal. Therefore, a suitable transversal is chosen for each element in the group so that it is easier to control the image. Finally it is checked that the transfer is effectively a homomorphism.

To better understand this concept, we have put an example in which we have built the transfer of an element from two different transversals and we have effectively reached that the transfer of an element does not depend on the transversal we chose.

Once the *Theorem of Burnside* is known and proved, first we prove the resolubility of the finite groups whose Sylow subgroups are all cyclic and then we give a characterization. The finite groups whose Sylow subgroups are all cyclic are cyclic or they are a semi-direct product of two cyclic subgroups verifying some conditions with respect to the orders and conjugation. Specifically, they are in this way

$$G =< a,b \mid a^m = b^n = 1,\ b^{-1}ab = a^r >=< a >< b > \text{ where } | < a > | = m, | < b > | = n$$

with $m,r,n \in \mathbb{N}$ such that verify $r^n \equiv 1$ (mod m), $(m,n) = 1$ and $(r-1,m) = 1$.

Finally, we give an example of a finite group that is neither cyclic nor dihedral verifying these conditions and see that it has cyclic all its Sylow subgroups.

Índice general

Capítulo 1

Definiciones, propiedades y teoremas básicos.

En este capítulo seleccionamos algunos conceptos de la teoría de grupos que ya conocemos e introduciremos y explicaremos algunos nuevos. Los conceptos que no han aparecido en las asignaturas del grado son: normalizador, conmutador, subgrupo derivado, serie derivada y subgrupo característico. Todo lo que veamos en este capítulo podemos encontrarlo con más detalle en los libros de teoría de grupos, por ejemplo en el capítulo 1 del libro *Group Theory I* [2] y se usará en el resto del trabajo.

1.1. Grupos

Definición 1.1. *Un grupo G es un conjunto no vacío dotado de una operación binaria interna, usualmente denotada $' \cdot '$ que verifica:*

(i) *Es asociativa:* $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$

(ii) *Posee elemento neutro (y éste es único)* $1_G \equiv 1$ *tal que* $1 \cdot g = g \cdot 1 = g \quad \forall g \in G$

(iii) *Para cada elemento $g \in G$, existe $g^{-1} \in G$ elemento simétrico (se llama inverso y éste es único) tal que* $g \cdot g^{-1} = 1_G = g^{-1} \cdot g$

Si además la operación es conmutativa: $a \cdot b = b \cdot a$ para todo $a, b \in G$, el grupo se dice abeliano.

Definición 1.2. *Un grupo G se dice que es finito si tiene un número finito de elementos. A este número se le denomina orden de G y se le denota por $|G|$.*

Definición 1.3. *Un subgrupo H de un grupo G es un subconjunto de G que con la operación restringuida a dicho subconjunto es un grupo. Se denota $H \leq G$. Los elementos neutros coinciden $1_H = 1_G$. Se tiene que la intersección de una familia de subgrupos es subgrupo.*

Definición 1.4. *Sean $X, Y \subseteq G$, el producto de X por Y es el conjunto $XY = \{xy \,|\, x \in X, y \in Y\}$.*

Proposición 1.5. *Sean $H, K \leq G$, se tiene que $HK \leq G$ si y solo si $HK = KH$.*

Definición 1.6. *Sea $H \leq G$ y $x \in G$, llamamos*

- *Coclase a derecha de x módulo H al conjunto $H\{x\} \equiv Hx = \{hx \,|\, h \in H\}$.*
- *Coclase a izquierda de x módulo H al conjunto $\{x\}H \equiv xH = \{xh \,|\, h \in H\}$.*

En general, $Hx \neq xH$ aunque ambos conjuntos contienen a x $(1 \in H)$. Si H es finito $|Hx| = |H| = |xH|$, y además se tiene que las coclases a derecha (o equivalentemente a izquierda) forman una partición de G. También se tiene que $Hx = H$ si y solo si $x \in H$.

Definición 1.7. *Sea G finito y $H \leq G$, llamamos índice de H en G al número de coclases a derecha (que coincide con el número de coclases a izquierda) y lo denotamos $|G:H|$.*

Por formar las coclases una partición se tiene inmediatamente el siguiente teorema:

Teorema 1.8. *(Lagrange). Sea G un grupo finito y $H \leq G$, se tiene:*

$$|G| = |G:H||H|$$

De aquí deducimos que el orden de un subgrupo siempre es divisor del orden del grupo.

Corolario 1.9. *Sea G un grupo finito y $H \leq K \leq G$, se tiene:*

$$|G:H| = |G:K||K:H|$$

Demostración. Basta aplicar el Teorema 1.8 de Lagrange a (G,H), (G,K) y (H,K). □

Definición 1.10. *Sea $X \subseteq G$ entonces se llama subgrupo generado por X al subgrupo*

$$< X >= \bigcap_{X \subseteq K \leq G} K$$

Definición 1.11. *Si existe $x \in G$ tal que $G =< x >$, el grupo G se dice cíclico o monógeno, y se dice que x genera G.*

Definición 1.12. *Sea $x \in G$, al menor entero positivo n tal que $x^n = 1$ se le denomina el orden de x y se denota $|x|$. Notar que si x tiene orden n, se tiene que $x^{-1} = x^{n-1}$ y así se tiene*

$$< x >= \{1, x, \ldots, x^{n-1}\}$$

Proposición 1.13. *Todo grupo G de orden primo es cíclico.*

Proposición 1.14. *Sea $G =< x >$ un grupo cíclico finito de orden $n \in \mathbb{N}$. Se tiene que G es abeliano y además*

a) El número de generadores de G es el número de enteros positivos menores o iguales a n que son primos con n (Función de Euler). Se tiene que $< x^m >=< x >$ si y solo si $m.c.d(n,m) = 1$.

b) Todo elemento de G tiene orden divisor de n. (Se deduce del Teorema 1.8 de Lagrange).

c) Para todo d divisor de n existe un único subgrupo de orden d que también es cíclico.

d) Todo subgrupo de G es también cíclico.

Definición 1.15. *Sean G_1 y G_2 grupos. $G_1 \times G_2$ con la operación $(x_1,x_2)(y_1,y_2) = (x_1y_1, x_2y_2)$ para cada $x_1, y_1 \in G_1$, $x_2, y_2 \in G_2$ es un grupo que se llama producto directo de G_1 y G_2.*

Definición 1.16. *Un homomorfismo de un grupo G en un grupo H es una aplicación $f : G \to H$ tal que para todo $a,b \in G$ se verifica $f(ab) = f(a)f(b)$. Un homomorfismo biyectivo se llama isomorfismo. Un automorfismo es un isomorfismo de un grupo en sí mismo. El conjunto de todos los automorfismos de G con la composición de aplicaciones es un grupo que denotamos por Aut(G). En este grupo, si $f, g \in Aut(G)$ escribiremos $fg = g \circ f$ el automorfismo que primero aplica f y luego g.*

En el libro *A Course in the Theory of Groups* de Derek J.S.Robinson [1], podemos encontrar un capítulo dedicado exclusivamente a grupos abelianos, el capítulo 4.

Proposición 1.17. *Sean C_n y C_m dos grupos cíclicos, su producto es un grupo cíclico si y solo si $m.c.d(n,m) = 1$.*
Es decir, $C_n \times C_m \simeq C_{nm}$ si y solo si $m.c.d(n,m) = 1$.

Teorema 1.18. *Todo grupo abeliano finito G es producto directo de cíclicos de orden una potencia de primo. Es decir, si G abeliano, $G = C_{p_1{}^{r_1}} \times C_{p_2{}^{r_2}} \times \cdots \times C_{p_n{}^{r_n}}$ donde p_i son primos y $r_i \geq 0$ para $i = 1, ..., n$.*

De la proposición anterior deducimos que si $p_i \neq p_j$ con $i \neq j$ entonces G es un grupo cíclico. Y si por el contrario $p_i = p_j$ para algunos i, j con $i \neq j$ entonces G no es un grupo cíclico. En otras palabras, si en la descomposición de un grupo abeliano G como producto de cíclicos de orden una potencia de primo se repite algún primo, G no es cíclico, y si son todos los primos distintos, G sí es cíclico.

Corolario 1.19. *Sea G un grupo abeliano de orden pq con (p,q)=1 tal que existe $a, b \in G$ con $|a| = p$ y $|b| = q$ entonces G es cíclico de orden pq.*

Definición 1.20. *Un subgrupo N de G, se dice subgrupo normal y se denota $N \trianglelefteq G$ si coinciden las coclases a derecha y a izquierda, es decir, si*

$$xN = Nx \quad \forall x \in G$$

Para probar que un subgrupo N es normal, basta probar $x^{-1}Nx \subseteq N \ \forall x \in G$.

Proposición 1.21. *Se tiene*

a) En un grupo abeliano todos sus subgrupos son normales.

b) Todo subgrupo de índice 2 es normal.

c) Sea $N \trianglelefteq G$ y $H \leq G$, se tiene que $NH \leq G$.

Definición 1.22. *Sea $N \trianglelefteq G$. El conjunto $G/N = \{Nx \,|\, x \in G\}$ es grupo con la operación $(Nx)(Ny) = Nxy$ para $x, y \in G$. Se denomina grupo cociente y el neutro de G/N es N.*

Teorema 1.23. *(Primer Teorema de isomorfía). Sea $f : G \to H$ homomorfismo. Se tiene*

$$G/kerf \simeq Imf$$

Teorema 1.24. *(Segundo Teorema de isomorfía). Sea G un grupo, $H \leq G$ y $N \trianglelefteq G$. Entonces $H \cap N \trianglelefteq H$, $NH \leq G$ y se tiene*

$$\frac{H}{H \cap N} \simeq \frac{NH}{N}$$

Teorema 1.25. *(Tercer Teorema de isomorfía). Sea G un grupo, $N \trianglelefteq G$, $M \trianglelefteq G$ y $N \leq M$. Entonces $M/N \trianglelefteq G/N$ y se tiene*

$$(G/N)/(M/N) \simeq G/M$$

Proposición 1.26. *Si $C_n =< x >$ es un grupo cíclico de orden n, entonces $Aut(C_n) \simeq \mathbb{U}(\mathbb{Z}_n)$ (grupo multiplicativo de las unidades de $\mathbb{Z}_n$).*

Demostración. Si $f \in Aut(C_n)$, f viene determinado por $f(x)$. La aplicación

$$\begin{array}{rccccc} \psi\colon & \mathbb{U}(\mathbb{Z}_n) & \longrightarrow & Aut(C_n) & & \\ & \bar{i} & \longmapsto & f_i : C_n & \longrightarrow & C_n \\ & & & x & \longmapsto & x^i \end{array}$$

Se comprueba que está bien definida, es homomorfismo y es biyectiva.
Se tiene $\mathbb{U}(\mathbb{Z}_n) \simeq Aut(C_n)$.

□

Definición 1.27. *Sea G un grupo y $g, x \in G$. Llamamos conjugado de x por g al elemento $x^g = g^{-1}xg$.*
Sea $H \leq G$, llamamos conjugado de H por g a $H^g = g^{-1}Hg = \{g^{-1}hg \,|\, h \in H\}$.
Sean $H, K \leq G$ decimos que K es conjugado con H en G si existe $g \in G$ tal que $H^g = K$. Si se cumple esto, se sigue que $K^{g^{-1}} = H$ y decimos que H y K son conjugados en G.

Proposición 1.28. *La aplicación $\alpha_g : G \to G$ definida por $\alpha_g(x) = x^g$ es un automorfismo de G, es decir, conjugar es un automorfismo, y por tanto todo subgrupo H es isomorfo a H^g. A α_g se le llama automorfismo interno en G. La composición de automorfismos internos es un automorfismo interno.*

Definición 1.29. *Sean $N \trianglelefteq G$ y $H \leq G$ tales que $G = HN$ y $H \cap N = 1$, podemos definir $\alpha : H \to Aut(N)$ dado por $\alpha(h)(n) = n^h$ para cada $h \in H$, entonces se dice que G es producto semidirecto de H y N. Esto quiere decir, que si conocemos un subgrupo $N \trianglelefteq G$ y otro subgrupo $H \leq G$ tales que $G = HN$ y $H \cap N = 1$ y conocemos la conjugación de N por H, entonces sabemos operar en G.*
Los elementos de G se escriben de manera única como uno de H por uno de N y por otra parte, si $x, y \in G$, $x = h_1n_1$, $y = h_2n_2$ con $h_1, h_2 \in H, n_1, n_2 \in N$, tenemos que $xy = h_1n_1h_2n_2 = h_1h_2n_1^{h_2}n_2 \in HN = G$.

Definición 1.30. *Una permutación de un conjunto Ω no vacío es una aplicación biyectiva de Ω en sí mismo. A los elementos de Ω los llamamos cifras. Para indicar que la permutación α aplica la cifra i en la j utilizamos la notación $i\alpha = j$. El conjunto de todas las permutaciones de Ω tiene estructura de grupo respecto del producto de permutaciones, usualmente se denomina grupo simétrico de grado n, siendo n el número de elementos de Ω y se denota S_n. Si Ω tiene n elementos, S_Ω tiene n! elementos.*

Definición 1.31. *Una permutación α se dice que es un ciclo de longitud r si existen r cifras distintas y ordenadas $c_1, c_2, \dots c_r$, de tal forma que $c_i\alpha = c_{i+1}$ para $i = 1, \dots, r-1$, $c_r\alpha = c_1$ y $c_j\alpha = c_j$ si $j \notin \{1, ..., r\}$. Se denota de la forma $\alpha = (c_1\, c_2 \dots c_r)$. Un 2-ciclo se denomina trasposición.*

Definición 1.32. *Un elemento de S_n se dice que es par si es producto de un número par de trasposiciones. En otro caso, se dice impar.*
El conjunto de las permutaciones pares es un subgrupo de S_n que se llama grupo alternado de grado n y se denota A_n. Se tiene que $|A_n| = |S_n|/2$.

1.2. Acciones de grupos

Definición 1.33. *Decimos que el grupo G actúa sobre el conjunto Ω si tenemos un homomorfismo de grupos $\varphi : G \to S_\Omega$. Para cada $i \in \Omega$ y $g \in G$, escribiremos i^g en lugar de $i^{\varphi(g)}$. Notar que $(i^g)^h = i^{gh}$. Se dice que G actúa fielmente sobre Ω si φ es inyectiva. Llamamos:*

- *Órbita de $i \in \Omega$ al conjunto $\mathcal{O}(i) = \{i^g \,|\, g \in G\} \subseteq \Omega$. Cada letra está en su órbita $(1 \in G)$.*
- *Estabilizador de $i \in \Omega$ al conjunto $St(i) = \{g \in G \,|\, i^g = i\} \leq G$.*

Se tiene que el conjunto de todas las órbitas forman una partición de Ω y que $|\mathcal{O}(i)| = \frac{|G|}{|St(i)|}$.

Definición 1.34. *Se dice que la acción es transitiva cuando todos los elementos de Ω están en la misma órbita, es decir, si para cada par de elementos $i, j \in \Omega$ existe $g \in G$ tal que $i^g = j$.*

Definición 1.35. *La aplicación $\varphi : G \to Per_G$ definida por $\varphi(g) : x \to x^g$ para cada $g, x \in G$, es decir $\varphi(g) = \alpha_g$ es una acción. Llamamos:*

- *Centro de G, $Z(G)$ al núcleo de esta acción: $Z(G) = \{x \in G \,|\, gx = xg \ \ \forall g \in G\}$.*
  Notar que $Z(G) \trianglelefteq G$.
- *Clase de conjugación de x: $Cl(x) = \{x^g \,|\, g \in G\}$ (es la órbita de x).*
- *Centralizador de x: $C_G(x) = \{g \in G \,|\, xg = gx\} \leq G$ (es el estabilizador de x).*
  Notar que $< x > \leq C_G(x)$.

Definición 1.36. *Para cada $H \leq G$ definimos la acción por conjugación de G sobre el conjunto de los subgrupos conjugados de H.*

$$\Omega = \{H^x \,|\, x \in G\}, \qquad \varphi : G \to S_\Omega \quad \text{definida por } \varphi(g) : H^x \to H^{xg}$$

Llamamos normalizador de H en G al subgrupo $N_G(H) = \{g \in G \,|\, H^g = H\} \leq G$ (es el estabilizador de H). Observar que $H \leq N_G(H)$ ya que $H^h = H$ para cada $h \in H$.

Proposición 1.37. *Sea $H \leq G$*

a) El conjunto de conjugados de H en G tiene cardinal $|G : N_G(H)|$, y por lo tanto divide a $|G|$.

b) $N_G(H)$ es el subgrupo más grande de G en el que H es normal.

Demostración.

a) Los subgrupos conjugados de H son los que están en la misma órbita que H con la acción de la definición anterior. Así que la acción es transitiva, la órbita coincide con Ω.

Se tiene que $|G : N_G(H)| = \frac{|G|}{|N_G(H)|}$ es el número de subgrupos conjugados de H en G.

□

Proposición 1.38. *Sea G un grupo, los automorfismos internos de G con la composición forman un grupo isomorfo al grupo cociente de G por su centro. Es decir,*

$$G/Z(G) \simeq Int(G) \leq Aut(G)$$

Demostración. Consideramos la acción de la Definición 1.35

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & Per_G \\ & g & \longmapsto & \alpha_g \end{array}$$

Si llamamos $\varphi(G) = Int(G)$, tenemos por la Proposición 1.28, $Int(G) \leq Aut(G)$.
Por el Primer Teorema de Isomorfía 1.23, $G/Z(G) \simeq Int(G)$.

□

Ahora, vamos a enunciar y demostrar una proposición similar a esta que nos será de gran ayuda para demostrar que todos los grupos finitos que tienen todos sus subgrupos de Sylow cíclicos, son resolubles. (Teorema 3.9).

Proposición 1.39. *Sea G un grupo, $H \leq G$. Entonces $C_G(H) \trianglelefteq N_G(H)$ y*

$$N_G(H)/C_G(H) \simeq K, \quad con \;\; K \leq Aut(H)$$

Demostración. Sea $g \in N_G(H)$, $\alpha_g : H \to H$ definida por $\alpha_g(h) = h^g$ está bien definida por ser $H^g = H$, ya que $g \in N_G(H)$.

$$\begin{array}{rccccc} f: & N_G(H) & \longrightarrow & Aut(H) & & \\ & g & \longmapsto & \alpha_g : H & \longrightarrow & H \\ & & & h & \longmapsto & h^g \end{array}$$

f es homomorfismo puesto que $\alpha_{gg'}(h) = h^{gg'} = (h^g)^{g'} = \alpha'_g \circ \alpha_g(h)$.
$Ker f = \{g \in N_G(H) \,|\, f(g) = Id\} = \{g \in N_G(H) \,|\, hg = gh \;\; \forall h \in H\} = C_G(H)$.
Por el Primer Teorema de Isomorfía 1.23, $N_G(H)/C_G(H) \simeq K$.

□

Proposición 1.40. *Si el grupo cociente $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. $G/Z(G) = \{Z(G)x \,|\, x \in G\}$
Si $G/Z(G)$ es cíclico, existe $Z(G)x$ tal que $G/Z(G) =< Z(G)x >$.
Sean $a, b \in G$, como las coclases me forman una partición, existen i, j tal que $a \in Z(G)x^i$ y $b \in Z(G)x^j$.
Así tenemos que $a = c_1x^i$, con $c_1 \in Z(G)$ y $b = c_2x^j$ con $c_2 \in Z(G)$.
$ab = c_1x^ic_2x^j = c_2c_1x^jx^i = c_2x^jc_1x^i = ba$, y así G es abeliano. □

1.3. Grupos resolubles, conmutadores y subgrupos característicos

Definición 1.41. *Un grupo G se dice simple si no tiene subgrupos normales propios. Es decir, si $N \trianglelefteq G$ implica $N = 1$ o $N = G$.*

Teorema 1.42. *Si $n > 4$, A_n es simple.*

Definición 1.43. *Un grupo G se dice resoluble si existen subgrupos G_i verificando*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{k-1} \trianglelefteq G_k = G$$

con G_{i+1}/G_i abeliano para $i = 0, 1, ..., k-1$.

Proposición 1.44. *Sea G un grupo*

a) Si $H \leq G$ y G es resoluble, entonces H es resoluble.

b) Si $N \trianglelefteq G$, entonces G es resoluble si y solo si N y G/N lo son.

Proposición 1.45. *Un grupo finito G es resoluble si y solo si existen subgrupos G_i verificando*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{k-1} \trianglelefteq G_k = G$$

con G_{i+1}/G_i cíclico de orden primo para $i = 0, 1, ..., k-1$.

Definición 1.46. *Sea G un grupo, $a, b \in G$, llamamos conmutador de a y b al elemento $[a,b] = a^{-1}b^{-1}ab$.*
Observar que $[a,b] = 1$ si y solo si a y b conmutan.
Sean $A, B \leq G$, definimos $[A,B] = <[a,b] \,|\, a \in A, b \in B> \leq G$.
Llamamos subgrupo conmutador o subgrupo derivado al subgrupo $G' \equiv G^{(1)} \equiv [G,G] = <[a,b] \,|\, a,b \in G>$.
El subgrupo derivado del subgrupo derivado se llama segundo subgrupo derivado y se denota por G'' o $G^{(2)}$. En general, el subgrupo derivado de $G^{(i)}$ se denota $G^{(i+1)}$ y se define como $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.
La serie

$$G^{(n)} \leq G^{(n-1)} \leq \cdots \leq G'' \leq G' \leq G$$

se llama serie derivada de G.

Proposición 1.47. *G' es el subgrupo normal más pequeño de G tal que G/G' es abeliano.*

Demostración. Primero veamos que el subgrupo G' está contenido en todos los subgrupos normales N tales que G/N es abeliano.
Sea $N \trianglelefteq G$ tal que G/N es abeliano y sea $[a,b] \in G'$, $[a,b]N = a^{-1}b^{-1}abN = a^{-1}Nb^{-1}NaNbN$ y como G/N es abeliano, $a^{-1}Nb^{-1}NaNbN = a^{-1}NaNb^{-1}NbN = N$, es decir, $[a,b]N = N$, y así $[a,b] \in N$, luego $G' \subseteq N$. Así, deducimos que $G' \subseteq \cap\{N \trianglelefteq G \,|\, \text{G/N es abeliano}\}$.

Por otra parte, veamos que G' es un subgrupo normal de G.
Para cada $g \in G, [a,b] \in G'$ se tiene $[a,b]^g = (a^{-1}b^{-1}ab)^g = a^{-1^g}b^{-1^g}a^g b^g = a^{g^{-1}}b^{g^{-1}}a^g b^g = [a^g, b^g] \in G'$.

Para ver el otro contenido, veamos que G/G' es un grupo abeliano.
Sean $aG', bG' \in G/G'$, tenemos que comprobar que $aG'bG' = bG'aG'$ que es lo mismo que comprobar que $a^{-1}G'b^{-1}G'aG'bG' = 1G'$.

$$a^{-1}G'b^{-1}G'aG'bG' = 1G' \Leftrightarrow (a^{-1}b^{-1}ab)G' = G' \Leftrightarrow [a,b] \in G'$$

Por definición de G', se tiene que $[a,b] \in G'$. Por lo tanto, G/G' es un subgrupo abeliano.

Así, hemos deducido que G' es un subgrupo normal tal que G/G' es abeliano, y por lo tanto, $G' = \cap\{N \trianglelefteq G \,|\, \text{G/N es abeliano}\}$. □

Proposición 1.48. *G es resoluble si y solo si $G^{(n)} = 1$ para algún n.*

Demostración.

$\Rightarrow$) Supongamos que G es resoluble y veamos que $G^{(n)} = 1$ para algún n.
Si G es resoluble, existen subgrupos G_i verificando

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

con G_{i+1}/G_i abeliano para $i = 0, 1, ..., n-1$.

Como $G_n/G_{n-1} = G/G_{n-1}$ es un grupo abeliano y $G_{n-1} \trianglelefteq G$, tenemos por la Proposición anterior que $G' \leq G_{n-1}$. En general, como G_{n-i}/G_{n-i-1} es abeliano, $G'_{n-i} \leq G_{n-i-1}$, y si $G^{(i)} \leq G_{n-i}$, se deduce que $G^{(i+1)} = (G^{(i)})' \leq G'_{n-i} \leq G_{n-i-1}$.

Como se verifica para $i = 1$, por inducción se tiene que $G^{(i)} \leq G_{n-i}$ para $i = 0, 1, ..., n$.

En particular, $G^{(n)} \leq G_0 = 1$, por lo tanto, $G^{(n)} = 1$.

$\Leftarrow$) Supongamos que $G^{(n)} = 1$ para algún n, y veamos que G es resoluble.
Consideramos la serie derivada

$$1 = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq ... \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

Por la Proposición anterior deducimos que G/G', G'/G'', G''/G''',..., $G^{(i)}/G^{(i+1)}$ son cocientes abelianos, y que $G^{(i+1)} \trianglelefteq G^{(i)}$ para todo $i = 0, 1, ..., n-1$.
Por la Definición 1.43, tenemos que G es resoluble.

□

Definición 1.49. *Si G es un grupo, $H \leq G$ se dice subgrupo característico si para todo $\phi : G \to G$ automorfismo, $\phi(H) = H$, y se escribe $H\,Char\,G$.*
Es decir, H es un subgrupo característico de G si cada automorfismo de G transforma a H en sí mismo.

Proposición 1.50. *Sea G un grupo finito*

a) $(G^{(i)}/G^{(n)})' = G^{(i+1)}/G^{(n)}$ *para* $i < n$.

b) G' *es característico en G.*

Demostración.

a) Por la Proposición 1.47, sabemos que $(G^{(i)}/G^{(n)})' \trianglelefteq G^{(i)}/G^{(n)}$, por lo tanto, $(G^{(i)}/G^{(n)})' = M/G^{(n)}$ para algún $M \trianglelefteq G^{(i)}$. Por la misma Proposición, sabemos que $(G^{(i)}/G^{(n)})/(M/G^{(n)})$ es abeliano, y por tanto, por el Tercer Teorema de Isomorfía 1.25, $(G^{(i)}/G^{(n)})/(M/G^{(n)}) \simeq G^{(i)}/M$ abeliano. Luego, $G^{(i+1)} \leq M$.
Para ver el otro contenido, como $G^{(i)}/G^{(i+1)}$ es abeliano, por el Tercer Teorema de Isomorfía 1.25, $G^{(i)}/G^{(i+1)} \simeq (G^{(i)}/G^{(n)})/(G^{(i+1)}/G^{(n)})$ abeliano. Luego, $M/G^{(n)} \leq G^{(i+1)}/G^{(n)}$, y por lo tanto, $M \leq G^{(i+1)}$.
Así, $M = G^{(i+1)}$, y se tiene que $(G^{(i)}/G^{(n)})' = G^{(i+1)}/G^{(n)}$ para $i < n$.

b) Sea $\phi : G \to G$ un automorfismo, $G' = < [a,b] \,|\, a,b \in G >$.
$\phi([a,b]) = \phi(a^{-1}b^{-1}ab) = (\phi(a))^{-1}(\phi(b))^{-1}\phi(a)\phi(b) = [\phi(a), \phi(b)]$. Luego, $\phi(G') \subseteq G'$, y por el orden, se tiene que $\phi(G') = G'$, y así $G'\,Char\,G$.

□

Proposición 1.51. *Sea G un grupo finito*

a) Si $H \leq G$ es subgrupo característico de G, $H \trianglelefteq G$.

b) Si G es cíclico, todos sus subgrupos son característicos.

c) Si H Char K y K $\trianglelefteq$ G, entonces H $\trianglelefteq$ G.

Demostración.

a) Sea $g \in G$, la conjugación $\alpha_g : G \to G$ definida por $\alpha_g(x) = x^g$ es un automorfismo. Como $H\ Char\ G$, $\alpha_g(H) = H$, equivalentemente, $g^{-1}Hg = H$ para cada $g \in G$, es decir, $H^g = H$ para cada $g \in G$, y así $H \trianglelefteq G$.

b) Sea $G =< a >$ un grupo cíclico con $| < a > | = n$, y sea ϕ un automorfismo de $< a >$. Sea $d|n$, por la Proposición 1.14, sabemos que existe un único subgrupo de $< a >$ de orden d. Sea H ese único subgrupo de orden d, como ϕ es un automorfismo, ϕ es biyectivo, y por tanto $\phi(H)$ tiene el mismo orden que H, es decir d, pero como solo hay un sugrupo de orden d tenemos que $\phi(H) = H$, y así H es un subgrupo característico de G.

c) Sea $g \in G$ y sea $\alpha_g : G \to G$ el automorfismo definido en el apartado a). Como $K \trianglelefteq G$, tenemos que $\alpha_g(K) = K$, por lo tanto, la restricción $\alpha_{g|K} \in Aut(K)$. Como $H\ Char\ K$, $\alpha_{g|K}(H) = H$, o equivalentemente $g^{-1}Hg = H$ para todo $g \in G$, luego $H \trianglelefteq G$.

□

Proposición 1.52. *Sea G un grupo finito, cada subgrupo derivado de la serie derivada es normal en G.*

Demostración. Procedemos por inducción. Por la Proposición 1.47, $G' \trianglelefteq G$. Supongamos que $G^{(i)} \trianglelefteq G$, como $G^{(i+1)}\ Char\ G^{(i)}$, por la Proposición 1.51 c), $G^{(i+1)} \trianglelefteq G$. □

Capítulo 2

p-Grupos y Teoremas de Sylow

Definición 2.1. *Si p es primo, un grupo finito G se llama p-grupo si su orden es una potencia de p. Por el Teorema de Lagrange 1.8, el orden de cada elemento de un p-grupo también debe ser una potencia de p.*

Definición 2.2. *Sea G un grupo finito y p un primo. Si $|G| = p^a m$ donde $(p,m) = 1$, es decir, $p \nmid m$, entonces por el Teorema de Lagrange 1.8, un p-subgrupo de G no puede tener un orden mayor que p^a. Un p-subgrupo de G que tiene este orden máximo p^a se llama p-subgrupo de Sylow de G. Al conjunto de los p-subgrupos de Sylow de G lo denotamos $Syl_p(G)$.*

Proposición 2.3. *$P \in Syl_p(G) \Leftrightarrow$ P es p-grupo y $p \nmid |G : P|$*

Demostración. Sea $|G| = p^a m$ donde $p \nmid m$.
$\Rightarrow$) Si $P \in Syl_p(G)$, $|P| = p^a$. Por el Teorema de Lagrange 1.8, $|G| = |G : P||P|$, es decir,
$|G : P| = \frac{p^a m}{p^a} = m$, luego $p \nmid |G : P| = m$.
$\Leftarrow$) Sea P un p-grupo tal que $p \nmid |G : P|$, $p \nmid \frac{|G|}{|P|}$, luego $|P| = p^a$ y por lo tanto $P \in Syl_p(G)$. □

Proposición 2.4. *Sea $N \trianglelefteq G$ y $P \in Syl_p(G)$.*

a) $P \cap N \in Syl_p(N)$.

b) $\frac{PN}{N} \in Syl_p(\frac{G}{N})$.

Demostración.

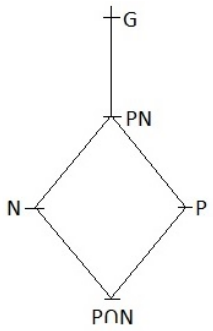
a) Como $P \cap N \leq P$, $|P \cap N|$ es una potencia de p. Por el Segundo Teorema de Isomorfía 1.24, $PN/N \simeq P/P \cap N$, luego $|PN : N| = |P : P \cap N|$.

Por otra parte,

$$|PN : N||N : P \cap N| = |PN : P \cap N| = |PN : P||P : P \cap N|$$

Y por lo tanto $|N : P \cap N| = |PN : P|$.
Como $P \leq PN \leq G$, por el Corolario 1.9, tenemos que $|PN : P|$ es un divisor de $|G : P|$. Como P es un p-Sylow, por la Proposición anterior 2.3 tenemos que $p \nmid |G : P|$, entonces $p \nmid |PN : P| = |N : P \cap N|$ y así, de nuevo por la misma Proposición tenemos que $P \cap N \in Syl_p(N)$.

b) Por el Segundo Teorema de Isomorfía 1.24, $PN/N \simeq P/P \cap N$. Luego, $PN/N = \{pN \mid p \in P\}$. Por lo tanto, todo elemento de PN/N tiene orden potencia de p, y así, PN/N es un p-grupo de G/N.



Como $N \subseteq PN \subseteq G$, tenemos que $|\frac{G}{N} : \frac{PN}{N}| = |G : PN|$. Por el Corolario 1.9, $|G : PN|$ es un divisor de $|G : P|$, y como por la Proposición 2.3, $p \nmid |G : P|$ porque P es un p-Sylow de G, tenemos que $p \nmid |\frac{G}{N} : \frac{PN}{N}|$, y por la misma Proposición, tenemos que $\frac{PN}{N}$ es un p-Sylow de $\frac{G}{N}$.

□

2.1. Teoremas de Sylow

En el capítulo 4 del libro de Zassenhaus, *The Theory of Groups* [4], podemos encontrar los enunciados y demostraciones de los teoremas de Sylow con una notación más clásica y en el capítulo 2 del libro de Michio Suzuki, *Group Theory I* [2], podemos encontrar los teoremas de Sylow y sus demostraciones según Wieldlant.

Teorema 2.5. ***Primer Teorema de Sylow*** *Sea G un grupo finito y p un primo. Si $|G| = p^a m$ donde $(p,m) = 1$. Entonces:*

Para cada entero r tal que $0 \leq r \leq a$, G tiene por lo menos un subgrupo de orden p^r.

Teorema 2.6. ***Segundo Teorema de Sylow*** *Sea G un grupo finito y p un primo. Si $|G| = p^a m$ donde $(p,m) = 1$. Entonces:*

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

(b) Todos los p-subgrupos de Sylow son conjugados en G.

Corolario 2.7. *Sea G un grupo finito y p un primo. Si $|G| = p^a m$ donde $(p,m) = 1$. Entonces:*

(a) El número de p-subgrupos de Sylow es $n_p = |G : N_G(P)|$ donde P es un p-subgrupo de Sylow, y además se tiene por lo tanto que $n_p \,||G|$.

(b) Existe un único p-subgrupo de Sylow de G si y solo si $P \trianglelefteq G$.

Demostración.

(a) Se deduce directamente de la Proposición 1.37 a), ya que todos los p-subgrupos de Sylow son conjugados.

(b) $n_p = 1 \Leftrightarrow G = N_G(P) \Leftrightarrow P \trianglelefteq G$.

□

2.2. Ejemplos concretos de grupos con sus subgrupos de Sylow

Vamos a estudiar en algunas familias de grupos las condiciones para tener todos sus subgrupos de Sylow cíclicos. También hallaremos el número de subgrupos de Sylow que hay en los grupos que veamos.

2.2.1. Grupos Cíclicos

Sea $< x >$ un grupo cíclico tal que $| < x > | = n$, $n \in \mathbb{N}$ vamos a ver como son sus subgrupos de Sylow.

Proposición 2.8. *Para cada primo p que divide al orden de un grupo cíclico existe un único p-subgrupo de Sylow, y éste es cíclico.*

Demostración. Sea $G =< x >$ un grupo cíclico de orden n, los p-subgrupos de Sylow de G tienen orden p^r con $r \in \mathbb{N}$ la máxima potencia de p tal que $p^r \mid n$. Como G es cíclico, por la Proposición 1.14, existe un único subgrupo de orden p^r que será también cíclico y que será el p-subgrupo de Sylow. □

Por lo tanto, un grupo cíclico tiene todos sus subgrupos de Sylow cíclicos, y solo tiene uno para cada primo p que divide al orden de G.

Ejemplo 2.9. *Sea $G =< x >$, con $|G| = 12$.*

$|G| = 12 = 2^2 \times 3$. Por el Primer Teorema de Sylow 2.5 y por la Proposición 2.8, existe un único 2-Sylow de orden $2^2 = 4$ y un único 3-Sylow de orden 3, y ambos son cíclicos.

2.2.2. Grupos Abelianos

Por las Proposiciones 1.17 y 1.18, tenemos que si G es un grupo abeliano finito, G es isomorfo al producto directo de grupos cíclicos de orden potencia de un primo.
Esas potencias de orden primo son invariantes y determinan el grupo salvo isomorfismos.

Proposición 2.10. *Todo grupo abeliano G tiene un único p-Sylow para cada primo p que divide al orden del grupo.*

Demostración. Como en un grupo abeliano todos sus subgrupos son normales, los p-Sylow son normales, y por tanto, por el Corolario 2.7 (b), solo hay un p-subgrupo de Sylow para cada p que divide al orden de G. □

Proposición 2.11. *Los únicos grupos abelianos que tienen todos sus p-Sylow cíclicos son los cíclicos.*

Demostración. Consideramos la descomposición como producto directo de grupos cíclicos de orden potencia de primo. Para cada primo p que divide al orden de G, el p-Sylow es el producto de los cíclicos cuyo orden es potencia de ese primo p. Luego, si tiene dos factores cíclicos cuyo orden es potencia del mismo primo p, por la Proposición 1.17, el p-Sylow no es cíclico, sin embargo si solo hay un factor cuyo orden es potencia de ese primo p, el p-Sylow sí es cíclico.

Si todos los p-Sylow son cíclicos quiere decir que para cada primo p que divide al orden de G solo aparece un factor cíclico cuyo orden es potencia de ese primo p en la descomposición de G como producto de cíclicos. Y por lo tanto, si solo hay un factor cíclico para cada primo p, G es un producto de cíclicos de ordenes primos entre sí, y por la Proposición 1.17, G es cíclico de orden el producto del orden de esos grupos cíclicos de orden potencia de primo. □

Ejemplo 2.12. *Sea G un grupo abeliano tal que $G = C_{2^2} \times C_{5^3} \times C_7$*

Por el Primer Teorema de Sylow 2.5 y la Proposición 2.10, sabemos que existe un único 2-Sylow de orden $2^2 = 4$, un único 5-Sylow de orden $5^3 = 125$ y un único 7-Sylow de orden 7.

Como en la descomposición de G como producto de cíclicos cada cíclico tiene orden potencia de un primo distinto, por la Proposición 1.17, G es cíclico, y por lo tanto por la Proposición que acabamos de ver 2.11, sus subgrupos de Sylow son cíclicos.

Ejemplo 2.13. *Sea G un grupo abeliano tal que* $G = C_{2^2} \times C_2 \times C_5$

Por el Primer Teorema de Sylow 2.5 y la Proposición 2.10, sabemos que existe un único 2-Sylow de orden $2^3 = 8$ *y un único 5-Sylow de orden* 5.

Como en la descomposición de G como producto de cíclicos aparecen dos factores cíclicos cuyo orden es potencia del mismo primo (2)*, por la Proposición 1.17, G no es cíclico, y por lo tanto por la Proposición que acabamos de ver 2.11, no todos sus p-Sylow son cíclicos. El* 2*-Sylow no es cíclico ya que hay dos factores cíclicos de orden potencia de* 2*, el 2-Sylow tiene orden* 8 *pero en G no hay ningún elemento de orden* 8*, el mayor orden de un elemento de G potencia de* 2 *es* 4 *(ya que* $G \simeq C_{2^2} \times C_2 \times C_5$*). En cambio, como solo aparece un factor cíclico de orden potencia de* 5*, el* 5*-Sylow sí es cíclico.*

2.2.3. Grupos Diédricos

Denotaremos D_{2n} al grupo diédrico de orden $2n$

$$D_{2n} =< x,y \mid x^n = 1, y^2 = 1, x^y = x^{-1} >=< x >< y > \text{ con } | < x > | = n \text{ y } | < y > | = 2.$$

Proposición 2.14. *En el grupo diédrico* D_{2n} *los p-subgrupos de Sylow para* $p \geq 3$ *son cíclicos y normales.*

Demostración. $|D_{2n}| = 2n$ con $| < x > | = n, | < y > | = 2$. Sabemos que $| < x > |$ es un subgrupo cíclico y normal. Llamando S al p-subgrupo de Sylow, $|S| = p^r, r \in \mathbb{N}$, luego $|S|$ es impar. Sabemos que $y, x^i y$ para $i = 1, ..., n-1$ son elementos de orden 2, luego $y, x^i y \notin S$. Así, $S \leq < x >$ y como $< x >$ es un grupo cíclico, por la Proposición 1.14, S es cíclico. Por la Proposición 1.51 b), $SChar < x >$. Como $SChar < x >$ y $< x > \trianglelefteq G$, por la Proposición 1.51 c), $S \trianglelefteq G$. De hecho, cualquier subgrupo de orden impar de D_{2n} es cíclico y normal. □

Veamos que pasa ahora con los 2-subgrupos de Sylow de D_{2n}

Proposición 2.15. *Sea* D_{2n}

- *Si* $2 \nmid n$*,* D_{2n} *tiene todos sus subgrupos de Sylow cíclicos.*
- *Si* $2|n$*,* D_{2n} *no tiene todos sus subgrupos de Sylow cíclicos.*

Demostración. Sea $D_{2n} =< x,y >$ con $| < x > | = n$, $| < y > | = 2$, $x^y = x^{-1}$, y sabemos que $< x >$ es un subgrupo normal. Por la Proposición anterior 2.14, si $p \geq 3$ los p-subgrupos de Sylow son cíclicos. Por lo tanto, nos queda ver cómo son los 2-subgrupos de Sylow.

- Si $2 \nmid n$, $|D_{2n}| = 2n$, y por lo tanto, los 2-subgrupos de Sylow son de orden 2, es decir, están formados por la identidad y un elemento de orden 2, por lo que son cíclicos. Además, como hay n elementos de orden 2, tenemos que D_{2n} tiene n 2-subgrupos de Sylow.
- Si $2|n$, $|D_{2n}| = 2n = 2^k c$, con $k, c \in \mathbb{N}$. Sea $P \in Syl_2(D_{2n})$ un 2-subgrupo de Sylow, $|P| = 2^k$. Por la Proposición 2.4, $P \cap < x > \in Syl_2(< x >)$. $| < x > | = n = 2^{k-1}c$, por lo tanto $|P \cap < x > | = 2^{k-1}$. Luego, $y \in P$ con $y \notin < x >$, $|y| = 2$.

  $$P =< y > (P \cap < x >)$$

  Denotando $< \bar{x} >= P \cap < x >$ tenemos $\bar{x}^y = \bar{x}^{-1}$.

  Así, $P \simeq D_{2^k}$ y como D_{2^k} no es cíclico, P no es cíclico.

  Además observar que por el Segundo Teorema de Isomorfía 1.24,

  $$2 = |\frac{P}{P \cap < x >}| \simeq |\frac{P < x >}{< x >}|$$

  Por lo tanto, $P < x >= D_{2n}$.

□

Ejemplo 2.16. $D_{12} =< x,y \mid x^6 = 1, y^2 = 1, x^y = x^{-1} >=< x >< y >$ *con* $| < x > | = 6$ *y* $| < y > | = 2$.
$|D_{12}| = 12 = 2 \cdot 6 = 2^2 \cdot 3,\ n = 6,\ 2|n$

El Primer Teorema de Sylow 2.5, garantiza la existencia de 2-subgrupos de Sylow, los cuales tienen orden $2^2 = 4$ *y de 3-subgrupos de Sylow, los cuales tienen orden 3.*

$D_{12} = \{1, x, x^2, x^3, x^4, x^5, y, xy, x^2y, x^3y, x^4y, x^5y\}$

Los elementos de la forma $x^iy,\ \ i = 0,1,..,5$*, tienen orden* 2*, ya que* $x^iyx^iy = x^i(x^i)^y = x^ix^{-i} = 1$.

En D_{12} *hay* 7 *elementos de orden* 2*:* $x^3, y, xy, x^2y, x^3y, x^4y, x^5y$ *y* 2 *elementos de orden* 3*:* x^2, x^4.

$H = \{1, x^3, y, x^3y\}$ *es un* 2*-subgrupo de Sylow. H no es un grupo cíclico ya que no hay ningún elemento de orden* 4 *en H. Por el Segundo Teorema de Sylow 2.6, sabemos que todos los* 2*-subgrupos de Sylow son conjugados con H en G, es decir, isomorfos a H, y por lo tanto ninguno de ellos será cíclico.*

Además, por el Corolario 2.7, sabemos que el número de 2*-subgrupos de Sylow es* $|G : N_G(H)|$*. Por otro lado, sabemos que* $H \leq N_G(H)$*, y como* $|H| = 4$*, se tiene que* $|N_G(H)|$ *es múltiplo de* 4*. También sabemos que* $H \leq G$ *y* $|G| = 12$*, luego* $|N_G(H)|$ *es divisor de* 12*. Juntando ambas tenemos que* $|N_G(H)|$ *es múltiplo de* 4 *y divisor de* 12*, luego* $|N_G(H)|$ *es igual a* 4 *o* 12*, pero* 12 *no puede ser porque H no es normal en G (*$H^x \lneq H$*). Como* $H \leq N_G(H)$ *y* $|H| = |N_G(H)|$ *tenemos que* $H = N_G(H)$*. Por lo tanto, hay* $|G : N_G(H)| = \frac{|G|}{|N_G(H)|} = \frac{12}{4} = 3$ *2-subgrupos de Sylow no cíclicos.*

$K = \{1, x^2, x^4\} =< x^2 >$ *es un 3-subgrupo de Sylow, el único que existe ya que solo hay* 2 *elementos de orden* 3 *en G, y es cíclico.*

Ejemplo 2.17. $D_{30} =< x,y \mid x^{15} = 1, y^2 = 1, x^y = x^{-1} >=< x >< y >$ *con* $| < x > | = 15$ *y* $| < y > | = 2$.
$|D_{30}| = 30 = 2 \cdot 15 = 2 \cdot 3 \cdot 5,\ n = 15,\ 2 \nmid n$

El Primer Teorema de Sylow 2.5, garantiza la existencia de 2*-subgrupos de Sylow, los cuales tienen orden* 2*, de* 3*-subgrupos de Sylow, los cuales tienen orden* 3 *y de* 5*-subgrupos de Sylow, los cuales tienen orden* 5*.*

$D_{30} = \{1, x^i, y, x^iy \mid i = 1,2,...,14\}$

Como hemos visto en el Ejemplo 2.16, los elementos de la forma $x^iy,\ \ i = 0,1,...,14$*, tienen orden* 2*.*

En D_{30} *hay* 15 *elementos de orden* 2*:* $x^iy,\ \ i = 0,1,...,14$*,* 2 *elementos de orden* 3*:* x^5, x^{10} *y* 4 *elementos de orden* 5*:* x^3, x^6, x^9, x^{12}.

Como tengo 15 *elementos de orden* 2*, y los* 2*-subgrupos de Sylow son de orden* 2*, cada elemento de orden* 2 *me genera un* 2*-subgrupo de Sylow, por lo tanto tengo* 15 *2-subgrupos de Sylow cíclicos:* $H_1 =< y >,\ H_i =< x^iy >\quad i = 1,2,...,14$.

$K = \{1, x^5, x^{10}\} =< x^5 >$ *es un* 3*-subgrupo de Sylow, el único que existe ya que solo hay* 2 *elementos de orden* 3 *en G, y es cíclico.*

$N = \{1, x^3, x^6, x^9, x^{12}\} =< x^3 >$ *es un* 5*-subgrupo de Sylow, el único que existe ya que solo hay* 4 *elementos de orden* 5 *en G, y es cíclico.*

2.2.4. Grupos Simétricos

Proposición 2.18. *Sea* $n \geq 4$ *y* $m > n$*. Si existe un p-subgrupo de Sylow de* S_n *que no es cíclico para algún p primo, entonces existe un p-subgrupo de Sylow de* S_m *que no es cíclico.*

Demostración. En S_m consideramos el subgrupo $H = \{\alpha \in S_m \mid \alpha(i) = i\ \forall i > n\}$, se tiene $H \leq S_m$ y $H \simeq S_n$. Sea P un p-sylow de H que no es cíclico, P es un subgrupo de S_m para todo $m > n$, luego P es un p-grupo en S_m para todo $m > n$. Por el Segundo Teorema de Sylow 2.6, sabemos que todo p-grupo de S_m está contenido en un p-Sylow de S_m, es decir, existe un Q subgrupo p-Sylow en S_m tal que $P \subseteq Q$. Si Q fuese cíclico, por la Proposición 1.14, P también sería cíclico y llegaríamos a una contradicción. Por lo tanto, el p-Sylow Q de S_m no puede ser cíclico. □

Proposición 2.19. *Los únicos grupos simétricos* S_n *que tienen todos sus subgrupos de Sylow cíclicos son* S_2 *y* S_3*. En particular, los* 2*-Sylow de* S_m *con* $m > 4$ *no son cíclicos.*

Demostración.

- $S_2 : |S_2| = 2$, $S_2 = \{1, (12)\}$. Por lo tanto, en S_2 solo hay un único 2-Sylow y claramente, éste es cíclico.
- S_3: $|S_3| = 3! = 2 \cdot 3$. En S_3 hay 3 2-Sylow de orden 2 que son cíclicos: $H_1 =< (12) >$, $H_2 =< (13) >$ y $H_3 =< (23) >$ y un único 3-Sylow de orden 3 que también es cíclico: $H_4 =< (123) >$. Luego S_3 tiene todos sus subgrupos de Sylow cíclicos.
- S_4: $|S_4| = 4! = 2^3 \cdot 3$. En S_4 hay 2-Sylow de orden $2^3 = 8$ y 3-Sylow de orden 3. Como en S_4 no hay elementos de orden 8, los 2-Sylow no pueden ser cíclicos. Por lo tanto, ya hemos encontrado el primer subgrupo simétrico que no tiene todos sus subgrupos de Sylow cíclicos.
- Por la Proposición anterior, como en S_4 los 2-Sylow no son cíclicos, tampoco lo serán en ningún S_n con $n > 4$, y de esta manera hemos deducido que S_n con $n > 4$ no tendrá todos sus subgrupos de Sylow cíclicos.

□

Ejemplo 2.20. $|S_4| = 4! = 24 = 2^3 \cdot 3$

- *Veamos qué forma tienen los elementos de S_4 y cuantos hay de cada tipo.*

  Elemento identidad: 1_{S_4}

  Elementos de orden 2 de la forma: $(12) \longrightarrow \frac{4 \cdot 3}{2} = 6$

  Elementos de orden 2 de la forma: $(12)(34) \longrightarrow \frac{\frac{4 \cdot 3}{2} \cdot \frac{2 \cdot 1}{2}}{2!} = 3$

  Elementos de orden 3 de la forma: $(123) \longrightarrow \frac{4 \cdot 3 \cdot 2}{3} = 8$

  Elementos de orden 4 de la forma: $(1234) \longrightarrow \frac{4 \cdot 3 \cdot 2 \cdot 1}{4} = 6$

- *Por el Primer Teorema de Sylow 2.5, sabemos que hay 2-subgrupos de Sylow de orden $2^3 = 8$ y 3-subgrupos de Sylow de orden 3.*

  Los 2-Sylow deben estar generados por un 4-ciclo y una trasposición, es decir, deben ser D_8. Por lo tanto, los 2-Sylow de S_4 no son cíclicos. Como en cada D_8 hay 2 elementos de orden 4; si x tiene orden 4, x y x^3, y hemos visto que hay 6 elementos de orden 4 en S_4, tenemos que hay 3 2-Sylow y que son los siguientes:

  $H_1 =< (1234), (24) >$, $H_2 =< (1243)(23) >$, $H_3 =< (1324)(34) >$

  $K =< (123) >$ es un 3-Sylow y es cíclico. Como hay 8 elementos de orden 3 en S_4 y un grupo cíclico de orden 3 tiene 2 generadores, hay 4 3-Sylow cíclicos.

Ejemplo 2.21. $|S_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$

- *Veamos qué forma tienen los elementos de S_5 y cuantos hay de cada tipo.*

  Elemento identidad: 1_{S_5}

  Elementos de orden 2 de la forma: $(12) \longrightarrow \frac{5 \cdot 4}{2} = 10$

  Elementos de orden 2 de la forma: $(12)(34) \longrightarrow \frac{\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2}}{2!} = 15$

  Elementos de orden 3 de la forma: $(123) \longrightarrow \frac{5 \cdot 4 \cdot 3}{3} = 20$

  Elementos de orden 4 de la forma: $(1234) \longrightarrow \frac{5 \cdot 4 \cdot 3 \cdot 2}{4} = 30$

  Elementos de orden 5 de la forma: $(12345) \longrightarrow \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{5} = 24$

  Elementos de orden 6 de la forma: $(123)(45) \longrightarrow \frac{5 \cdot 4 \cdot 3}{3} \cdot \frac{2 \cdot 1}{2} = 20$

- *Por el Primer Teorema de Sylow 2.5, sabemos que hay* 2*-Sylow de orden* $2^3 = 8$*,* 3*-Sylow de orden* 3 *y* 5*-Sylow de orden* 5*.*

  De forma análoga que en S_4*, deducimos que hay* 15 2*-Sylow que son* D_8*, y por lo tanto, no cíclicos. Por ejemplo:* $H_1 =< (1235)(25) >$*,* $H_2 =< (1253)(23) >$ *son* 2*-Sylow.*

  Los 3*-Sylow son cíclicos, y como hay* 20 *elementos de orden* 3*, deducimos que hay* 10 3*-Sylow. Por ejemplo,* $K_1 =< (123) >$*,* $K_2 =< (124) >$ *son* 3*-Sylow.*

  Los 5*-Sylow son cíclicos, un grupo cíclico de orden* 5 *tiene* 4 *generadores, como tenemos* 24 *elementos de orden* 5*, tenemos* 6 5*-Sylow. Por ejemplo,* $L_1 =< (12345) >$*,* $L_2 =< (13245) >$ *son* 5*-Sylow.*

2.2.5. Grupos Alternados

Proposición 2.22. *El único grupo alternado* A_n *que tiene todos sus subgrupos de Sylow cíclicos es* A_3*.*

Demostración. Esta demostración es análoga a la de la Proposición 2.19 vista en la subsección anterior de grupos simétricos.

- $A_3 : |A_3| = \frac{|S_3|}{2} = 3$. En A_3 hay un único 3-Sylow y éste es cíclico (Es el mismo que el de S_3, ya que los elementos de orden 3 de S_3 son permutaciones pares y por lo tanto están también en A_3).
- $A_4 : |A_4| = \frac{|S_4|}{2} = 12 = 2^2 \cdot 3$. En A_4 hay 2-Sylow de orden 4. Como en A_4 no hay elementos de orden 4 ya que los elementos de la forma (1234) son permutaciones impares, deducimos que los 2-Sylow no pueden ser cíclicos. De este modo ya tenemos el primer grupo alternado que no tiene todos sus subgrupos de Sylow cíclicos.
- Utilizando el mismo razonamiento que en la demostración de la Proposición 2.19 llegamos a que los grupos alternados A_n con $n > 4$ tampoco tienen todos sus subgrupos de Sylow cíclicos.

□

Ejemplo 2.23. $|A_5| = \frac{5!}{2} = 60 = 2^2 \cdot 3 \cdot 5$.

- *Veamos qué forma tienen los elementos de* A_5 *y cuantos hay de cada tipo.*

  Elemento identidad: 1_{A_5}

  Elementos de orden 2 *de la forma:* $(12)(34) \longrightarrow \frac{\frac{5\cdot4}{2}\cdot\frac{3\cdot2}{2}}{2!} = 15$

  Elementos de orden 3 *de la forma:* $(123) \longrightarrow \frac{5\cdot4\cdot3}{3} = 20$

  Elementos de orden 5 *de la forma:* $(12345) \longrightarrow \frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$

- *El Primer Teorema de Sylow 2.5, garantiza la existencia de* 2*-subgrupos de Sylow, los cuales tienen orden* $2^2 = 4$*, de* 3*-subgrupos de Sylow, los cuales tienen orden* 3 *y de* 5*-subgrupos de Sylow, los cuales tienen orden* 5*.*

  Como en A_5 *no hay elementos de orden* 4 *y sabemos por el Segundo Teorema de Sylow 2.6, que todos los* 2*-subgrupos de Sylow son isomorfos, tenemos que ningún 2-subgrupo de Sylow de* A_5 *es cíclico.*

  El subgrupo

  $$H = \{1, (12)(34), (13)(24), (14)(23)\}$$

  es un 2*-subgrupo de Sylow de* A_5*.*

  Vamos a ver cuantos 2*-subgrupos de Sylow hay en* A_5*. Como los* 2*-subgrupos de Sylow tienen* 4 *elementos, sus elementos son de orden* 2 *o* 4*, pero no hay elementos de orden* 4 *en* A_5 *y los*

elementos de orden 2 *que están en* A_5 *son de la forma* $(12)(34)$*, de los cuales ya hemos visto que hay* 15*. Por lo tanto, todos los* 2*-subgrupos de Sylow son isomorfos a* $C_2 \times C_2$ *y están formados por la identidad y* 3 *elementos de orden* 2 *que conmutan entre sí. Tomamos por ejemplo el elemento* $x = (12)(34)$*, y observamos que este elemento no conmuta con ningún elemento que no fije* 5*. Por lo tanto, el único* 2*-Sylow al que pertenece x es H. De este modo, deducimos que hay exactamente* 5 2*-Sylow, cada uno de ellos formado por los elementos de orden* 2 *de* A_5 *que fijan, respectivamente, a* 1*,* 2*,* 3*,* 4 *y* 5*.*

$K =< (123) >$ *es un* 3*-subgrupo de Sylow, y éste es cíclico, luego los* 3*-subgrupos de Sylow de* A_5 *son todos cíclicos. Un subgrupo cíclico de orden* 3 *tiene* 2 *generadores; un elemento y su inverso. Como tenemos* 20 *elementos de orden* 3 *en* A_5 *tenemos que hay* 10 3*-subgrupos de Sylow en* A_5 *y que son cíclicos.*

$L =< (12345) >$ *es un* 5*-subgrupo de Sylow, y éste es cíclico, luego todos los* 5*-subgrupos de Sylow de* A_5 *son cíclicos. Como hay* 24 *elementos de orden* 5 *en* A_5 *y un subgrupo cíclico de orden* 5 *tiene* 4 *generadores, entonces hay* 6 5*-subgrupos de Sylow en* A_5 *y son cíclicos.*

Capítulo 3

Grupos cuyos subgrupos de Sylow son cíclicos

Este capítulo lo vamos a dedicar a ver cómo es la estructura de los grupos finitos que tienen todos sus subgrupos de Sylow cíclicos. Para ello, vamos a necesitar el Teorema de Burnside, el cual enunciaremos y demostraremos utilizando un concepto nuevo, el transfer. En el capítulo 5 del libro de Zassenhaus, *The Theory of Groups* [4], podemos encontrar la definición de transfer y el Teorema de Burnside. El libro de Zassenhaus data del año 1956, y en él se recogen resultados y conceptos que siguen siendo muy importantes en la teoría de grupos a día de hoy.

Lema 3.1. *Sea G un grupo finito que tiene todos sus subgrupos de Sylow cíclicos.*

a) Los subgrupos de G tienen todos sus subgrupos de Sylow cíclicos.

b) Los cocientes de G tienen todos sus subgrupos de Sylow cíclicos.

Demostración.

a) Sea $H \leq G$ y sea P un p-Sylow de H, P es un p-grupo de H, y por lo tanto, es un p-grupo de G. Por el Segundo Teorema de Sylow 2.6, P está contenido en un p-Sylow de G, y como por hipótesis, todos los p-Sylow de G son cíclicos, por la Proposición 1.14, P también es cíclico. Por lo tanto, H también tiene todos sus subgrupos de Sylow cíclicos.

b) Sea $N \trianglelefteq G$, $P \in Syl_p(G)$. Por la Proposición 2.4 b), sabemos que $\frac{PN}{N}$ es un p-Sylow del grupo cociente G/N. Por hipótesis P es cíclico, luego $P =< x >$, y entonces, $< xN >= \frac{PN}{N}$, y por lo tanto, $\frac{PN}{N}$ es un grupo cíclico. Así, los cocientes de G también tienen todos sus subgrupos de Sylow cíclicos.

□

Lema 3.2. *Si los p-Sylow de un grupo finito G son cíclicos, todos los p-grupos de G también son cíclicos.*

Demostración. Por el Segundo Teorema de Sylow 2.6, sabemos que todo p-grupo está contenido en un p-subgrupo de Sylow. Por lo tanto, si los p-Sylow son cíclicos, los p-grupos también lo son. □

3.1. Teorema de Burnside

Teorema 3.3. ***[Teorema de Burnside]*** *Sea G un grupo finito. Si un p-subgrupo de Sylow está contenido en el centro de su normalizador, entonces P tiene complemento normal. Es decir, si P un p-subgrupo de Sylow, y $P \subseteq Z(N_G(P))$ entonces existe $N \trianglelefteq G$ tal que $N \cap P = 1$ y $G = NP$.*

Notemos que si P está contenido en el centro de su normalizador, como el centro de un grupo siempre es abeliano esto implica que P es abeliano, y como P está contenido en $Z(N_G(P))$, los elementos de P además de conmutar con los de P, conmutan también con los de su normalizador $N_G(P)$. Si se da esa situación, existe $N \trianglelefteq G$ tal que $N \cap P = 1$ y $G = NP$, y como P es un p-subgrupo de Sylow de orden la máxima potencia de p que divide a G, $p \nmid N$.

Como caso particular de este Teorema tenemos que si P es abeliano y coincide con su normalizador, es decir, P es abeliano y $P = N_G(P)$ ya se da la situación de Burnside, porque P conmuta con todos los elementos de su normalizador, que solo son los de P, y por lo tanto existe un complemento normal de P.

Para demostrar este teorema tenemos que introducir un concepto nuevo, el transfer. Además de en el libro de Zassenhaus citado al principio de este capítulo, también podemos encontrar el concepto del transfer en el capítulo 10 del libro de Robinson, A Course in the Theory of Groups *[5], y en el capítulo 5 del libro de Michio Suzuki,* Group Theory II *[4].*

3.1.1. Transfer

Definición 3.4. *Sea $H \leq G$ finito y $K \trianglelefteq H$ tal que H/K es un cociente abeliano.*

Como $H \leq G$, las coclases de H forman una partición de G.

Sea $|G:H| = n$ y $\Omega = \{Ht_1, ..., Ht_n\}$ el conjunto de las distintas coclases a derecha de H (como H no tiene por qué ser normal en G, las coclases a derecha y a izquierda no tienen por qué coincidir). Se dice que $t_1, ...t_n$ es un transversal a derecha de H en G. Consideraremos transversales con $t_1 = 1$, es decir, en la coclase H elegimos el representante 1.

Consideramos la acción de G sobre las coclases a derecha de H por multiplicación a derecha.

$$\begin{array}{rccccc} \varphi\colon & G & \longrightarrow & S_\Omega & & \\ & x & \longmapsto & Ht_i & \longrightarrow & Ht_i x = Ht_j \end{array}$$

Para cada $x \in G$, llamamos π_x a la permutación de los elementos de Ω que me define x, π_x se puede ver como una permutación del conjunto $\{t_1, t_2, ..., t_n\}$, o simplemente como una permutación de $\{1, 2, ..., n\}$. Tal y como hemos definido la acción de arriba, tendríamos $\pi_x(i) = j$.

Sea $\{1 = t_1, ..., t_n\}$ un transversal a derecha de H en G. Para cada $x \in G$, el elemento $t_i x \in G$, y por lo tanto, está en una coclase a derecha de H. De este modo,

$$t_i x = h_i(x) t_{\pi_x(i)}$$

Definimos el transfer de x en H/K como el elemento

$$\prod_{i=1}^{n} h_i(x) K$$

(Nos pasamos al grupo cociente H/K para que estos elementos conmuten, ya que H/K es abeliano).

Proposición 3.5. *Sea $H \leq G$ finito y $K \trianglelefteq H$ tal que H/K es un cociente abeliano. Sea $x \in G$, el transfer de x en H/K no depende del transversal que tomemos.*

Demostración. Sea $x \in G$, como acabamos de ver, con el transversal $\{1 = t_1, ..., t_n\}$, tenemos que el transfer de x en H/K es $\prod_{i=1}^{n} h_i(x)K$. Sea ahora $\{1 = h_1 t_1, ..., h_n t_n\}$ otro transversal para ciertos $h_i \in H$. Observar que todos los transversales son así, de hecho hay exactamente $|H|^{n-1}$ transversales distintos de este tipo (con el 1 en la primera coclase). Tenemos que

$$h_i t_i x = h_i h_i(x) t_{\pi_x(i)} = h_i h_i(x) h_{\pi_x(i)}^{-1} h_{\pi_x(i)} t_{\pi_x(i)}$$

Y el transfer de x en H/K con este transversal es

$$\prod_{i=1}^{n} h_i h_i(x) h_{\pi_x(i)}^{-1} K$$

Como π_x es una permutación de $\{1,2,...,n\}$, tenemos que $\prod h_{\pi_x(i)}^{-1} = h_1^{-1} \cdot h_2^{-1} \cdot ... \cdot h_n^{-1}$ reordenados de alguna manera.

Por ser H/K abeliano, no importa el orden en que tomemos el producto de los h^{-1} y se tiene que

$$\prod_{i=1}^{n} h_i h_i(x) h_{\pi_x(i)}^{-1} K = \prod_{i=1}^{n} h_i(x) K$$

Por lo tanto, hemos demostrado que el transfer de x en H/K no depende del transversal que tomemos, ya que obtenemos el mismo elemento de H/K. □

Vamos a ilustrar la definición del transfer de un elemento con un ejemplo para entenderlo mejor, y comprobamos que efectivamente el transfer de un elemento no depende del transversal que tomemos (Proposición anterior).

Ejemplo 3.6. *Sea* $D_{12} = < x,y \mid x^6 = 1, y^2 = 1, x^y = x^{-1} > = < x >< y >$ *con* $| < x > | = 6 y | < y > | = 2$.
Tomamos $H = < y >$, $K = 1$, *así* $H/1$ *es un cociente abeliano.*
$|D_{12} : H| = 6$ *y las coclases a derecha de H forman una partición de* D_{12}*:*

$$\{1,y\},\ \{x,yx\},\ \{x^2,yx^2\},\ \{x^3,yx^3\},\ \{x^4,yx^4\},\ \{x^5,yx^5\}$$

Sea $\{1 = t_1,...,t_6\} = \{1, x, yx^2, yx^3, x^4, x^5\}$ *un transversal a derecha de H en* D_{12}. *Sea* $g = xy \in G$.
$t_1 g = xy = yx^5 = h_1(g) t_{\pi_g(1)}, \quad h_1(g) = y,\ t_{\pi_g(1)} = x^5,\ \pi_g(1) = 6$

$t_2 g = x^2 y = yx^4 = h_2(g) t_{\pi_g(2)}, \quad h_2(g) = y,\ t_{\pi_g(2)} = x^4,\ \pi_g(2) = 5$

$t_3 g = yx^3 y = (x^y)^3 = x^3 = yyx^3 = h_3(g) t_{\pi_g(3)}, \quad h_3(g) = y,\ t_{\pi_g(3)} = yx^3,\ \pi_g(3) = 4$

$t_4 g = yx^4 y = (x^y)^4 = x^2 = yyx^2 = h_4(g) t_{\pi_g(4)}, \quad h_4(g) = y,\ t_{\pi_g(4)} = yx^2,\ \pi_g(4) = 3$

$t_5 g = x^5 y = yx = h_5(g) t_{\pi_g(5)}, \quad h_5(g) = y,\ t_{\pi_g(5)} = x,\ \pi_g(5) = 2$

$t_6 g = x^6 y = y = y1 = h_6(g) t_{\pi_g(6)}, \quad h_6(g) = y,\ t_{\pi_g(6)} = 1,\ \pi_g(6) = 1$

Así, $\pi_g = (16)(25)(34)$
Por lo tanto, el transfer de $g = xy$ *en H con este transversal es*

$$\prod_{i=1}^{6} h_i(x) K = \prod_{i=1}^{6} h_i(x) = y^6 = 1$$

Sea ahora $\{1 = t_1,...,t_6\} = \{1, yx, x^2, yx^3, yx^4, x^5\}$ *otro transversal a derecha de H en* D_{12}.
$t_1 g = xy = yx^5 = h_1(g) t_{\pi_g(1)}, \quad h_1(g) = y,\ t_{\pi_g(1)} = x^5,\ \pi_g(1) = 6$

$t_2 g = yx^2 y = (x^y)^2 = x^4 = yyx^4 = h_2(g) t_{\pi_g(2)}, \quad h_2(g) = y,\ t_{\pi_g(2)} = yx^4,\ \pi_g(2) = 5$

$t_3 g = x^3 y = yx^3 = 1yx^3 = h_3(g) t_{\pi_g(3)}, \quad h_3(g) = 1,\ t_{\pi_g(3)} = yx^3,\ \pi_g(3) = 4$

$t_4 g = yx^4 y = (x^y)^4 = x^2 = 1x^2 = h_4(g) t_{\pi_g(4)}, \quad h_4(g) = 1,\ t_{\pi_g(4)} = x^2,\ \pi_g(4) = 3$

$t_5 g = yx^5 y = x = yyx = h_5(g)t_{\pi_g(5)}, \quad h_5(g) = y,\ t_{\pi_g(5)} = yx,\ \pi_g(5) = 2$

$t_6 g = x^6 y = y = y1 = h_6(g)t_{\pi_g(6)}, \quad h_6(g) = y,\ t_{\pi_g(6)} = 1,\ \pi_g(6) = 1$

Así, $\pi_g = (16)(25)(34)$
Por lo tanto, el transfer de $g = xy$ *en* H *con este otro transversal es*

$$\prod_{i=1}^{6} h_i(x)K = \prod_{i=1}^{6} h_i(x) = y^4 = 1$$

Observamos que el transfer del elemento $g = xg$ *sale* 1 *con ambos transversales.*

Teorema 3.7. *Sea* $H \leq G$ *finito y* $K \trianglelefteq H$ *tal que* H/K *es un cociente abeliano. La aplicación*

$$V : G \longrightarrow H/K$$

que asocia a cada $x \in G$ *el transfer de* x *en* H/K *es un homomorfismo de grupos.*

Demostración. Sean $x, y \in G$, $\{1 = t_1, ..., t_n\}$ un transversal a derecha de H en G.

$$t_i xy = h_i(x)t_{\pi_x(i)}y = h_i(x)h_{\pi_x(i)}(y)t_{\pi_y(\pi_x(i))}$$

Por lo tanto,

$$V(xy) = \prod_{i=1}^{n} h_i(x)h_{\pi_x(i)}(y)K$$

Y por ser π_x una permutación del conjunto $\{1, 2, ..., n\}$ y H/K abeliano se tiene que

$$V(xy) = \prod_{i=1}^{n} h_i(x)h_{\pi_x(i)}(y)K = \prod_{i=1}^{n} h_i(x)K \prod_{i=1}^{n} h_{\pi_x(i)}(y)K = \prod_{i=1}^{n} h_i(x)K \prod_{i=1}^{n} h_i(y)K = V(x)V(y)$$

□

Nota 3.8. *Vamos a ver un transversal interesante para calcular el transfer.*
π_x *considerada como permutación del conjunto de coclases de* H *se puede escribir como producto de r ciclos disjuntos.*
Consideramos uno de esos ciclos de longitud f_i

$$(Ht_i, Ht_i x, Ht_i x^2, ..., Ht_i x^{f_i - 1})$$

donde las coclases que aparecen son distintas, y por tanto, $t_i, t_i x, t_i x^2, ..., t_i x^{f_i - 1}$ *son representantes de coclases distintas.*
Podemos considerar el transversal que resulta de unir los transversales que aparecen en los r ciclos disjuntos, y calcular con este transversal el transfer.
Notemos que las $h(x)$ *correspondientes a los elementos del transversal son todas* 1 *salvo la correspondiente a* $t_i x^{f_i - 1}$*, y ésta se obtiene con la igualdad* $t_i x^{f_i - 1} x = h t_i$*, de donde se obtiene* $h = t_i x^{f_i - 1} x t_i^{-1}$.
Así,

$$V(x) = \prod_{1}^{r} t_i x^{f_i - 1} x t_i^{-1} K = \prod_{1}^{r} t_i x^{f_i} t_i^{-1} K$$

con $\sum_{i=1}^{r} f_i = |G : H|$

Ahora que ya hemos definido el concepto del transfer, y hemos visto que la aplicación que asocia a cada $x \in G$ el transfer de x en H/K es un homomorfismo, veamos la demostración del Teorema de Burnside utilizando el transversal que acabamos de ver.

Demostración del Teorema de Burnside 3.3

Como P es un grupo abeliano, podemos considerar la aplicación $V : G \longrightarrow P$ que asocia a cada elemento de $x \in G$ el transfer de x en P.

Llamamos $N \trianglelefteq G$ al núcleo de V. Veamos que V es sobreyectiva, como $V(G) \subseteq P$, basta ver que $V(P) = P$.

Para $x \in P$, consideramos su transfer en P calculado con el transversal que hemos descrito en la Nota anterior 3.8, y así tenemos

$$V(x) = \prod_1^r t_i x^{f_i - 1} x t_i^{-1} = \prod_1^r t_i x^{f_i} t_i^{-1}$$

con $t_i x^{f_i} t_i^{-1} \in P$.

Como $x^{f_i} \in P$ y $t_i x^{f_i} t_i^{-1} \in P$, se tiene que $x^{f_i} \in P \cap P^{t_i^{-1}}$.

Por ser P abeliano, $P \leq C_G(x^{f_i})$ y $P^{t_i^{-1}} \leq C_G(x^{f_i})$, y por ser P un p-subgrupo de Sylow, por el Segundo Teorema de Sylow 2.6, tenemos que existe $y \in C_G(x^{f_i})$ tal que $P^y = P^{t_i^{-1}}$.

Así, $yt_i \in N_G(P)$, y como por hipótesis, $P \subseteq Z(N_G(P))$, tenemos que yt_i conmuta con todos los elementos de P. Luego, $x^{f_i} = (x^{f_i})^{yt_i} = (x^{f_i})^{t_i}$.

De este modo, nuestro transfer queda

$$V(x) = \prod_1^r x^{f_i}$$

$\sum_{i=1}^r f_i = |G : P|$ es coprimo con p por la Proposición 2.3, por tanto, también es coprimo con el orden de x ya que el orden de x es una potencia de p por ser $x \in P$.

Por lo tanto, $< V(x) >=< x >$, y como x era un elemento cualquiera de P, se tiene que $V(P) = P$, y así V es sobreyectiva.

Como V es sobreyectiva, por el Primer Teorema de Isomorfía 1.23, tenemos que $G/N \simeq P$, luego $|G/N| = |P|$, es decir, G/N tiene orden la máxima potencia de p que divide al orden del grupo G. Por lo tanto, $N \cap P = 1$ y $G = NP$.

3.2. Estructura de los grupos finitos G que tienen todos sus subgrupos de Sylow cíclicos.

Teorema 3.9. *Un grupo finito G que tiene todos sus subgrupos de Sylow cíclicos, es resoluble.*

Demostración. Procedemos por inducción sobre el número de primos que divide al orden de G.
Caso base: si solo hay un primo que divide al orden de G, $|G| = p^r$ para algún primo p, $r \in \mathbb{N}$, así G es un subgrupo de Sylow de orden p^r y por hipótesis es cíclico. Por lo tanto, como G es un grupo cíclico, G es abeliano, y por la Definición 1.43, G es resoluble. En realidad, es fácil de probar que todos los p-grupos son resolubles.
Supongamos que nuestro teorema se cumple cuando hay n primos que dividen al orden de G y veamos que se cumple para $n+1$ primos.
Sea el orden de G, $|G| = p_1^{r_1} p_2^{r_2} ... p_{n+1}^{r_{n+1}}$ con $p_i \neq p_j$ si $i \neq j$ y $r_i > 0, i = 1, ..., n+1$ y $p_1 < p_2 < ... < p_{n+1}$.
Sea $p \equiv p_1$ el primo más pequeño que divide a $|G|$ y sea P un p-subgrupo de Sylow de G, $|P| = p_1^{r_1} \equiv p^r$, P es cíclico por hipótesis. Por la Proposición 1.26, sabemos que el grupo de automorfismos de P tiene orden igual a la función de Euler de p^r, que es $p^r - p^{r-1} = p^{r-1}(p-1)$. Por la Proposición 1.39, $N_G(P)/C_G(P)$ es isomorfo a un subgrupo de los automorfismos de P, y por lo tanto $|N_G(P)/C_G(P)|$

es un divisor de $p^{r-1}(p-1)$. Como $N_G(P)/C_G(P) \leq G/C_G(P)$ y $|G/C_G(P)|||G|$, $|N_G(P)/C_G(P)|$ es divisor del orden de G, es decir, $|N_G(P)/C_G(P)|$ es divisor de $p_1^{r_1}p_2^{r_2}...p_{n+1}^{r_{n+1}}$. De este modo tenemos que $|N_G(P)/C_G(P)|$ es divisor de $p^{r-1}(p-1)$ y también es divisor de $p_1^{r_1}p_2^{r_2}...p_{n+1}^{r_{n+1}}$. Como $p_1 = p$ es el primo más pequeño que divide al orden de G, tenemos que $|N_G(P)/C_G(P)||p^{r-1}$.

Por otra parte, como P es un grupo cíclico tenemos que $P \leq C_G(P)$ ya que P conmuta con todos los elementos de P. Por la Proposición 1.39, tenemos que $C_G(P) \leq N_G(P)$. Así, tenemos que $P \leq C_G(P) \leq N_G(P) \leq G$. Luego $|N_G(P)/C_G(P)|$ es divisor de $|G:P|$ y como P es un p-Sylow de G, $p \nmid |G:P|$, luego p no puede dividir a $|N_G(P)/C_G(P)|$, y así $|N_G(P)/C_G(P)| = 1$. Por lo tanto, $N_G(P) = C_G(P)$.

Como P conmuta con todos los elementos de $C_G(P)$ y $C_G(P) = N_G(P)$, P conmuta con todos los elementos de $N_G(P)$, y así se tiene $P \leq Z(N_G(P))$, y por el Teorema de Burnside 3.3 existe $N \trianglelefteq G$ tal que $N \cap P = 1$ y $G = NP$. Como $N \leq G$, por el Lema 3.1, N también tiene todos sus subgrupos de Sylow cíclicos. Los primos que dividen al orden de N son los mismos que dividen al orden de G salvo p, luego le dividen n primos y por hipótesis N es resoluble. Por otra parte, por el Segundo Teorema de Isomorfía 1.24, $G/N = NP/N \simeq P/P\cap N = P$, y por tanto, G/N es un p-grupo, luego por el caso base es resoluble. De este modo, por la Proposición 1.44, concluimos que G es resoluble. Así nuestro enunciado es cierto para $n+1$ primos que dividen al orden de G y por tanto es cierto para todo $n \geq 1$.

□

Teorema 3.10. *Sea G un grupo finito. Si dos factores consecutivos de la serie derivada de G, digamos $G^{(i)}/G^{(i+1)}$ y $G^{(i+1)}/G^{(i+2)}$ son cíclicos, entonces $G^{(i+1)} = G^{(i+2)}$.*

Demostración. Sea $G^{(n)} \leq G^{(n-1)} \leq \cdots G^{(i)} \cdots \leq G'' \leq G' \leq G$ la serie derivada de G. Teniendo en cuenta la Proposición 1.50, que nos dice que $(G^{(i)}/G^{(n)})' = G^{(i+1)}/G^{(n)}$ para $i < n$ y tomando $\bar{G} = \frac{G^{i-1}}{G^{i+2}}$, tenemos que $\bar{G}' = \frac{G^i}{G^{i+2}}$, $\bar{G}'' = \frac{G^{i+1}}{G^{i+2}}$ y $\bar{G}''' = 1$.
De este modo podemos tomar sin pérdida de generalidad $G''' = 1$ y demostar que

Si G es un grupo finito tal que G'/G'' y G''/G''' son cíclicos. Entonces $G'' = G'''$.

Siendo $G''' = 1$ queremos ver que $G'' = 1$.
Por la Proposición 1.52, tenemos que $N_G(G'') = G$. Por la Proposición 1.39, $G/C_G(G'')$ es isomorfo a un subgrupo del grupo de automorfismos de G'' y como G'' es cíclico ya que hemos supuesto G''/G''' cíclico y $G''' = 1$, tenemos que $G/C_G(G'')$ es isomorfo a un subgrupo de automorfismos de un grupo cíclico, y por lo tanto, $G/C_G(G'')$ es abeliano.

Por la Proposición 1.47, $G' \subseteq C_G(G'')$. Por definición, sabemos que $C_G(G'') = \{x \in G \,|\, gx = xg \ \forall g \in G''\}$, luego que G' esté contenido en $C_G(G'')$, quiere decir que los elementos de G' conmutan con los elementos de G'', y como $Z(G') = \{x \in G' \,|\, xg = gx \ \forall g \in G'\}$ y $G'' \leq G'$ entonces $G'' \subseteq Z(G')$.

Como G'/G'' es cíclico y $G'' \subseteq Z(G')$ entonces $G'/Z(G')$ también es cíclico y por la Proposición 1.40, G' es abeliano, y por lo tanto $G'' = 1$.

□

Teorema 3.11. *Un grupo finito G que tiene todos sus subgrupos de Sylow cíclicos se puede expresar como un producto semidirecto de grupos cíclicos:*

$$G = < a,b \mid a^m = b^n = 1, b^{-1}ab = a^r > = < a >< b > \ \textit{donde} \mid < a > \mid = m, \mid < b > \mid = n$$

con $m,r,n \in \mathbb{N}$ tales que cumplen:

a) $|G| = mn$

b) $r^n \equiv 1$ *(mód m)*

c) $(m,n) = 1$

d) $(r-1,m) = 1$

También es cierto el recíproco: un grupo que cumpla estas condiciones tiene todos sus subgrupos de Sylow cíclicos.

Demostración. Si G es abeliano, como por hipótesis G tiene todos sus subgrupos de Sylow cíclicos, por la Proposición 2.11, G es cíclico y tomando $m = 1$, $r = 1$, G se puede expresar como en el enunciado y se cumplen las condiciones. Luego el resultado ya está probado en el caso de que G sea abeliano.

Supongamos ahora que G no es abeliano, como tiene todos sus subgrupos de Sylow cíclicos, por el Teorema 3.9, tenemos que G es resoluble. Por el Lema 3.1, como $G^i \leq G$ y G tiene todos sus subgrupos de Sylow cíclicos, entonces G^i también tiene todos sus subgrupos de Sylow cíclicos. Y por la misma Proposición, $\frac{G^i}{G^{i+1}}$ también tiene todos sus subgrupos de Sylow cíclicos. Por la Proposición 1.47, tenemos que $\frac{G^i}{G^{i+1}}$ es un grupo abeliano, y como tiene todos sus subgrupos de Sylow cíclicos, de la Proposición 2.11, deducimos que $\frac{G^i}{G^{i+1}}$ es un grupo cíclico, y análogamente que $\frac{G^{i+1}}{G^{i+2}}$ también es cíclico. Luego, por el Teorema anterior 3.10, $G^{i+1} = G^{i+2}$ para todo i, y como G es resoluble la única opción es que $G'' = 1$. Por lo tanto, G' y G/G' son grupos cíclicos.

Como G' es cíclico, existe $a \in G'$ tal que $G' =< a >$, supongamos que $|G'| = | < a > | = m$ y como G/G' es cíclico, existe $bG' \in G/G'$ tal que $G/G' =< bG' >$, supongamos que $|G/G'| = | < bG' > | = n$. Como $G' \leq G$ y las coclases forman una partición de G, tenemos que todo elemento $g \in G$ pertenece a alguna coclase $b^r G'$, luego $g = b^r a^j$ para algún $a^j \in G'$, por lo tanto, $G =< a,b >$. Como $b \in G$ y $G' \trianglelefteq G$, tenemos que $a^b \in G'$, es decir, $b^{-1}ab = a^r$ para algún $r \in \mathbb{N}$. Conjugando n veces tenemos que $a^{b^n} = b^{-n}ab^n = a^{r^n}$, y así, $a = a^{r^n}$, y por lo tanto $r^n = 1 + km$, con $k \in \mathbb{Z}$, luego $r^n \equiv 1$ (mód m).

Por otra parte, como $G =< a,b >$, los conmutadores de G son de la forma $[a^k, b^l]$.
$[a^k,b^l] = a^{-k}b^{-l}a^k b^l = a^{-k}a^{k^{b^l}} = a^{-k}a^{b^{kl}} = a^{-k}a^{rk^l} = a^{k(r^l-1}$ y $r-1|r^l-1$, luego $[a^k,b^l] = a^{kh(r-1)}$, es decir, todo conmutador de G es una potencia de a^{r-1}, luego $G' =< a^{r-1} >$ y como G' es cíclico y de orden m, se tiene que $(r-1,m) = 1$ o equivalentemente $r-1 \equiv 1$ (mód m).

Como $G/G' =< bG' >$ tenemos que $(bG')^n = G'$, luego $b^n G' = G'$ y esto quiere decir que $b^n \in G'$. Por lo tanto, b^n es una potencia de a, supongamos a^s, que conmuta con b, así tenemos que $1 = [a^s,b] = a^{-s}b^{-1}a^s b = a^{-s}a^{rs} = a^{rs-s} = a^{s(r-1)} = a^{r-1^s}$, luego $s(r-1) \equiv 0$ (mód m). Y como $r-1 \equiv 1$ (mód m), se tiene que $s \equiv 0$ (mód m), así s es múltiplo de m y $a^s = b^n = 1$.

Si m y n tienen un divisor primo p común, por la Proposición 1.51, $< a^{\frac{m}{p}} >$ es un subgrupo característico de $< a >$, y además como $G' =< a >$ es un subgrupo normal en G, por la misma Proposición tenemos que $< a^{\frac{m}{p}} > \trianglelefteq G$. Así, $< b^{n/p} >< a^{m/p} >$ es un subgrupo de G de orden p^2 no cíclico, ya que $|b^{n/p}| = | < a^{m/p} > | = p$ y por la Proposición 1.14, sabemos que los grupos cíclicos solo tienen un subgrupo de orden p. De este modo tenemos un p-grupo de orden p^2 no cíclico, pero por el Lema 3.2, tenemos que se contradice la hipótesis, ya que este p-grupo estará contenido en algún p-Sylow cíclico. Luego, $(n,m) = 1$.

Ahora veamos que si un grupo finito G cumple esas condiciones entonces tiene todos sus subgrupos de Sylow cíclicos. Sea $G =< a >< b >$, cumpliendo las condiciones citadas en el teorema, y P un p-Sylow. $< a > \trianglelefteq G$ y $|G| = mn$, entonces $P \leq < a >$ o $P \cap < a >= 1$ ya que $(m,n) = 1$. Y en cualquiera de estos casos, P es un grupo cíclico. □

Corolario 3.12. *Este Teorema confirma lo que ya habíamos visto para grupos diédricos en la Proposición 2.15:*

Los grupos diédricos D_{2m} se pueden poner como

$$D_{2m} =< x,y \mid x^m = y^2 = 1, b^{-1}ab = a^{m-1} >$$

En este caso, con la notación del Teorema anterior 3.11, $m = m$, $n = 2$ y $r = m-1$. Veamos ahora si se cumplen el resto de condiciones del Teorema. Las condiciones a) y b) se cumplen ya que $|D_{2m}| = 2m$ y $(m-1)^2 = m^2 - 2m + 1 \equiv 1$ (mód m). Para ver si se cumplen las condiciones c) y d) distinguimos 2 casos:

- *Si $2|m$, no se cumple la condición c) del Teorema, luego D_{2m} no puede tener todos sus subgrupos de Sylow cíclicos.*
- *Si $2 \nmid m$, se cumple la condicón c) del Teorema ya que $(m,2) = 1$ y la condición d) ya que, sea d tal que $d|r-1 = m-2$ y $d|m$, entonces $d|m-(m-2) = 2$, si $d|2$, se tiene que $d = 1$ o $d = 2$, pero como estamos en el caso de que $2 \nmid m$, forzosamente d tiene que ser 1, y así se cumple la condición d) del Teorema $(m-2,m) = 1$, y el grupo D_{2m} tiene todos sus subgrupos de Sylow cíclicos.*

Por último, vamos a dar un ejemplo de grupo finito G que no es cíclico ni diédrico que cumple las condiciones del Teorema 3.11, y vamos a ver que tiene todos sus subgrupos de Sylow cíclicos.

Ejemplo 3.13. *Tomando en S_{13}, $r = 3$, $n = 3$, $m = 13$, $a = (1,2,3,4,5,6,7,8,9,10,11,12,13)$ y $b = (2,4,10)(5,13,11)(6,3,7)(8,9,12)$, tenemos que se cumplen las condiciones del Teorema 3.11 con*

$$G =< a,b \mid a^{13} = b^3 = 1, a^b = a^3 >=< a >< b > \text{ donde } | < a > | = 13, | < b > | = 3$$

$r = 3, n = 3, m = 13$ cumplen las condiciones $(a)-(d)$ del Teorema.

Como $|G| = 3 \cdot 13$, por el Primer Teorema de Sylow 2.5, sabemos que hay 3-subgrupos de Sylow, los cuales tienen orden 3 y 13-subgrupos de Sylow, los cuales tienen orden 13.

$H =< b >$ es un 3-Sylow y es cíclico. Por el Segundo Teorema de Sylow 2.6, sabemos que todos los 3-Sylow son isomorfos, entonces se tiene que todos los 3-Sylow son cíclicos.

$K =< a >$ es un 13-Sylow y es cíclico. Del mismo modo, por el Segundo Teorema de Sylow 2.6, se tiene que todos los 13-Sylow son cíclicos.

Asi, G tiene todos sus subgrupos de Sylow cíclicos.

Bibliografía

[1] P. LUDWIG SYLOW (1872) MATHEMATISCHE ANNALEN, *Théorèmes sur les groupes de substitutions*, 5, 584–594, disponible en `https://gdz.sub.uni-goettingen.de/id/PPN235181684_0005?tify`.

[2] H. WIELANDT (1959) Ein Beweis für die Existenz von Sylowgruppen. Arch. Math. 10, 401-402.

[3] MICHIO SUZUKI (1980) *Group Theory I*. Springer-Verlag.

[4] MICHIO SUZUKI (1985) *Group Theory II*. Springer-Verlag.

[5] DEREK J. S. ROBINSON (1980) *A Course in the Theory of Groups*. Urbana, Illinois, Springer-Verlag.

[6] ZASSENHAUS (1956) *The Theory of Groups*. McGill University, Chelsea.