Acciones de grupos finitos.
Grupos primitivos.

Jorge Lou Franco

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directora del trabajo: Paz Jiménez Seral
27 de junio de 2022

Abstract

In this project, we analize the relation between abstract groups, and groups of permutations, being these an example of the first ones, but with a remarkable importance, since every asbtract group can be seen as a permutation group. Furthermore, permutation groups historically precede the more geneneral contemporary notion of group we have now, and have had much interest, since Galois' approach to them, in the study of movements on both mathematical and physical objects.

We use Wielandt's book *Finite Permutation Groups* [5], to support all of our ideas about permutation groups, that is, chapters 1 and 2.

During chapter 1, we introduce the permutation groups, which rely on a finite set Ω, with which we define notions such as stabiliser and orbits, and tools to work with them, of great help to us. Likewise, orbits define the notion of transitivity of a group, a basic condition to the subsequent study of our groups, but it is not restrictive either, since every intransitive group can be studied through transitive groups. There lies the importance that the transitive permutation groups have.

In chapter 2, we introduce the notion of blocks, less general in the field of permutation groups, which are the central pillar of the definition of primitivity of groups, whose importance owes to them, being a permutation group primitive when it doesn't have any non trivial blocks, and imprimitive when it does.

When we have a non trivial block, every conjugate of it are also blocks, disjoint if not equal, and in the case of a transitive group, they form a particion of the set Ω, called a complete block system. Likewise, we can study any group through the permutation group on the set of the blocks, and the subgroups of permutations that fix a block, undesrtood as groups on the blocks itselfs. Since those groups' degrees are always less than the original group's degree, and this process can always be done while we have an imprimitive group, it follows that we can repeat this process, if necessary, until every group we obtain is primitive. Then, we can study any group through primitive groups.

Finally, we describe the correlation between the blocks containing a point, and the subgroups that contain the stabiliser of that point, having a bijection between them, and we establish the important property that the stabiliser of a point has to be maximal for the group to be primitive.

After that, in chapter 3, we finally introduce the notion of an asbtract group widely known, which share tons of properties with the permutations groups directly, and many more can be adapted due to the actions, which completely link every abstract group with a permutation group, and allow us to adapt every definition in which we rely on the set Ω, needing these considering an action to make sense in abstract groups. Likewise we introduce notions where we needed to make a step into the abstraction of groups, such as the direct and semidirect product, which will be useful to set up our examples of primitive groups.

Finally, we also define equivalent actions, and we see how every action is equivalent to the action on the cosets of a subgroup by right multiplication, so these actions earn great importance. The kernel of these actions is the largest normal subgroup contained in that subgroup. This subgroup is called the core, and then, the study of transitive permutation groups is equivalent to the study of core-free subgroups, since then, the action on the cosets will be inyective, and it establishes an isomorphism between an abstract group and a permutation group.

With all this, we have everything we need to enter the last chapter, where we support our ideas on the Ballester-Bolinches and Ezquerro's book *Classes of Finite Groups* [2].

In this chapter we adapt the definition of primitivity, to the case of abstract groups, which is, being isomorph to a primitive permutation group, and it translates as the existence of a core-free maximal subgroup. So the study of primitive permutation groups, is equivalent to the study of pairs (G,U), called a primitive pair, where U is a core-free maximal subgroup of G. To study these groups, we can use everything known about abstract groups.

Then, we will focus our attention on the study of these groups, and we state the Baer Theorem, a classification of the primitive groups into 3 types according to the structure of their socle, i.e. their minimal normal subgroups. That is, a primitive group can have an abelian minimal normal subgroup, an unique non-abelian minimal normal subgroup, or two distinct non-abelian minimal normal subgroups.

This theorem is one of the most important pieces for the study of the structure of groups, both abstracts and permutations. We will not cover it, but it's worth mentioning that the O'Nan-Scott Theorem provide us a complete description of primitive groups of type 2.

At last, to conclude this project, we give examples of all types of primitive groups, studying their core-free maximal subgroup, which determines the isomorphism to a primitive permutation group, and studying their minimal normal subgroups, to classify them.

Índice general

Capítulo 1

Grupos de permutaciones. Conceptos básicos

1.1. Grupos de permutaciones

El concepto de grupo aparece con Galois como grupos de permutaciones de las raíces de un polinomio, y desde entonces el estudio de las transformaciones biyectivas en distintos objetos matemáticos o físicos ha sido muy importante.

Consideremos un conjunto finito $\Omega = \{1, 2, \dots, n\}$. A los elementos de Ω les llamaremos puntos, y le diremos $|\Omega|$, cardinal de Ω, al número de puntos de Ω. Las permutaciones sobre este, serán las aplicaciones α: $\Omega \to \Omega$ biyectivas. Si $i \in \Omega$, denotaremos i^α a la imagen de i por α. Al conjunto de todas las permutaciones sobre Ω lo denominaremos S_Ω. Si $\Omega = \{1, 2, \dots, n\}$, entonces escribiremos S_n en lugar de S_Ω.

Así mismo, si α, β son permutaciones sobre Ω, podemos definir la composición de permutaciones, de forma que, si $i \in \Omega$, entonces la composición $\alpha\beta$ queda definida como $i^{\alpha\beta} = (i^\alpha)^\beta$. Esta es una operación binaria interna, que es asociativa, con elemento neutro, la biyección identidad, y cada permutación α tiene inversa α^{-1}, por ser biyecciones.

Definición. Un grupo de permutaciones G es un subconjunto no vacío de S_Ω t.q. si $\alpha, \beta \in G$, entonces $\alpha\beta \in G$. En este caso, denotaremos $G \leq S_\Omega$. Esta es la definición, adaptada, de la definición de grupo que dio Galois en sus memorias, la cual trabajaba con el concepto de ordenaciones de un conjunto, para referirse a lo que posteriormente normalizaríamos como permutaciones, como podemos ver en el apéndice del capítulo 14 de [4].

Observación 1. Notar que, con esto, parece que no estemos exigiendo que el elemento neutro esté en estos conjuntos, ni de que cada elemento tenga inverso. Sin embargo, estamos exigiendo que, si $1 \neq \alpha \in G$, entonces también estén todas las potencias de α, es decir, $\alpha^2, \alpha^3, \alpha^4$... Pero como G es finito, habrá algún momento en que estas potencias se repitan, es decir, $\exists m > n$ naturales t.q. $\alpha^m = \alpha^n$. Entonces, tenemos que $\alpha^{m-n} = 1_\Omega$, y $\alpha^{m-n-1} = \alpha^{-1}$.

Con esto, tenemos que si G es un grupo de permutaciones, entonces $1_\Omega \in G$, y si $\alpha \in G$, entonces $\alpha^{-1} \in G$.

Definición. Sea $H \subseteq G$ grupo de permutaciones. Diremos que H es un **subgrupo** de G, si H también es un grupo de permutaciones. En este caso denotaremos $H \leq G$. Notar que esto es coherente con la notación de $G \leq S_\Omega$ para decir que G es un grupo de permutaciones, ya que el propio S_Ω es un grupo de permutaciones, del cual G es un subgrupo.

Definición. Sea G un grupo de permutaciones. Este se dirá **abeliano**, si tenemos que para todas permutaciones α, β de G, entonces $\alpha\beta = \beta\alpha$. Notar que el propio S_Ω no es abeliano si $|\Omega| > 2$.

Seguiremos la notación de permutaciones aportada por Cauchy, como bien podemos ver en el capítulo 5.5 de [1], y en el cual se pueden ver los siguientes resultados sobre las formas de escribir una permutación.

Diremos que una permutación es un ciclo de longitud r, si existen r puntos distintos y ordenados, $i_1, \cdots i_r$, de Ω, de forma que mueve cada uno de ellos a la siguiente, y el último al primero, y fija al resto de puntos, es decir, $i_k^\alpha = i_{k+1}$ para $k = 1, \cdots r-1$, y $i_r^\alpha = i_1$, y además $i^\alpha = i$ para todo i distinto de los i_k. Este ciclo, de denota $\alpha = (i_1, \cdots, i_r)$, y esta notación es única salvo ordenación cíclica, es decir, $(i_1, \cdots, i_r) = (i_r, i_1, \cdots, i_{r-1})$. Llamaremos trasposiciones a los ciclos de longitud 2, es decir $\alpha = (i_1, i_2)$. Si tenemos $\alpha = (i_1, \cdots, i_r)$, $\beta = (j_1, \cdots, j_s)$ disjuntas, es decir, $i_{k_1} \neq j_{k_2}$ $\forall 1 \leqslant k_1 \leqslant r, 1 \leqslant k_2 \leqslant s$, entonces se tiene que α y β permutan, $\alpha\beta = \beta\alpha$.

Proposición 1.1. *Toda permutación α se puede escribir como producto de ciclos disjuntos. Esta forma de expresarla es única salvo el orden de los ciclos. Así, tenemos una notación para escribir cualquier permutación, de forma que $\alpha = (i_1, \cdots, i_r) \cdots (j_1, \cdots, j_s)$.*

Proposición 1.2. *Toda permutación se puede escribir como un producto de trasposiciones, cuya descomposición no es única, pero si que está unequívocamente determinado si es un número par o impar de trasposiciones.*

A estas permutaciones se les llaman pares o impares, respectivamente. Además, el conjunto de permutaciones pares, A_Ω, es un subgrupo de S_Ω, el llamado grupo alternado.

Como es claro que la intersección de grupos es un grupo, si tenemos un $K \subseteq S_\Omega$, entonces podemos considerar la intersección de todos los grupos de permutaciones que contienen a K, la cual será un subgrupo. Este es el llamado subgrupo generado por K, $\langle K \rangle$, y es el menor subgrupo de S_Ω que contiene a K.

Llamaremos grado de un grupo $G \neq 1$, al número de puntos que son movidos por alguna permutación de G. No confundir con el orden del grupo, este es $|G|$, el número de permutaciones de G. Así mismo, llamaremos grado de una permutación $\alpha \neq 1$, al grado de $\langle \alpha \rangle$. También tenemos el grado mínimo de G, el cual es el menor grado de todas las permutaciones $1 \neq \alpha \in G$.

Si $H \leq G$, definimos las coclases a derecha de β módulo H en G, a $H\beta = \{\alpha\beta \mid \alpha \in H\}$, con $\beta \in G$. De forma análoga se pueden definir las coclases a izquierda βH, pero trabajaremos siempre con coclases a derecha, aunque de forma análoga se podría realizar también todo con coclases a izquierda. Igualmente, hablaremos de coclases en general para referirnos a coclases a derecha, mientras no haya lugar a error. Como las coclases son disjuntas, y $\beta \in H\beta$ $\forall \beta \in G$, tenemos una partición de G, por medio de coclases de H.

Si $H \leq G$, llamaremos índice de H en G, $|G : H|$, al número de coclases de H que hay en G.

A continuación, daremos el importante teorema de Lagrange, del cual deducimos que el orden de todo subgrupo de G tiene que dividir al orden de G.

Teorema 1.3. $|G| = |G : H||H|$.

Demostración. Se deduce de ser las coclases una partición, y de ser $|H\alpha| = |H|$ para toda coclase $H\alpha$. □

Definición. Sea $N \leq G$. Este subgrupo se dice **normal** en G, si coinciden sus coclases a izquierda y a derecha, es decir, si $\beta N = N\beta$ $\forall \beta \in G$. En este caso, escribimos $N \trianglelefteq G$.

Diremos que un grupo es simple, si no tiene subgrupos normales propios.

Proposición 1.4. *Si n>4, entonces A_n es un grupo simple.*

Demostración. Ver capítulo 1.5. de [3]. □

Además, con los conceptos introducidos, podemos decir más de A_n, el cual será un subgrupo normal de S_n de índice 2, si n > 2.

Definición. Sean $H,K \leq S_\Omega$. Entonces, se tiene que $HK = \{\alpha\beta \mid \alpha \in H,\ \beta \in K\}$ es un subconjunto de G, el cual es un subgrupo si y solo si HK=KH. En caso de que $H \trianglelefteq G$, entonces esta igualdad se dará, y tendremos que dicho producto será un subgrupo, el **subgrupo producto** de H por K. Así, una forma de poder garantizar de que un producto de grupos formará un grupo, es exigir que uno de ellos sea normal, aunque cabe destacar que habrá casos de productos de grupos no normales que serán un grupo.

Proposición 1.5. *Ley de Dedekind.*
Sean $A,B,C \leq G$, con $A \subseteq B$ y tales que $AC \leq G$. Entonces $A(B \cap C) = B \cap AC$.

Demostración. Veamoslo por doble contenido.

- $\subseteq$) Sea $\alpha \in A(B \cap C)$, entonces $\alpha = ab$ con $a \in A$ y $b \in B \cap C$. Así, $\alpha = ab \in AC$ y como $A \subseteq B$, tenemos que $a \in B$ y $\alpha \in B$.
- $\supseteq$) Sea ahora $\alpha \in B \cap AC$. Entonces $\alpha = ac$ con $a \in A, c \in C, ac \in B$. Así, como $a \in A \subseteq B$ y $ac \in B$, entonces $c \in B$, y tenemos que $\alpha \in A(B \cap C)$.

□

Definición. Sean dos grupos de permutaciones, G y H. No es necesario que sean subgrupos del mismo S_Ω. Un **homomorfismo** entre ellos, es una aplicación $\varphi : G \to H$, de forma que $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ $\forall \alpha, \beta \in G$, es decir, una aplicación que conserva la operación.

Se dice núcleo o kernel de φ a Ker(φ)=$\{\alpha \in G \mid \varphi(\alpha) = 1\}$, y este es claramente un subgrupo de G.

Si φ además es biyectiva, entonces además de homomorfismo, se dice **isomorfismo**. También, dos grupos se dicen isomorfos si existe un isomorfismo entre ellos. Un **automorfismo** será un isomorfismo de un grupo G en si mismo.

Sea G un grupo y $\alpha, \beta \in G$, entonces denotamos $\alpha^\beta = \beta^{-1}\alpha\beta$ y lo llamamos conjugado de α por β.

Para todo β en G, la $\varphi_\beta : G \to G$ dada por $\varphi_\beta(\alpha) = \alpha^\beta \forall \alpha$, es un isomorfismo.

También, si $H \leq G$, entonces $H^\beta = \beta^{-1}H\beta = \{\beta^{-1}\alpha\beta \mid \alpha \in H\}$, es un subgrupo de G, el conjugado de H por β. Notar que, si $N \leq G$, entonces $N \trianglelefteq G$ si y solo si $N = \beta^{-1}N\beta = N^\beta \ \ \forall \beta \in G$, es decir si los elementos de G dejan fijo a N por conjugación.

Proposición 1.6. *Sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces su núcleo es un subgrupo normal de G. Además, $\varphi(G) \leq H$, y tenemos que hay una biyección entre G/Ker(φ) y $\varphi(G)$, entendiendo G/Ker(φ) como el conjunto de las coclases módulo Ker(φ).*

Demostración. Sea $\varphi : G \to H$ un homomorfismo. Sea $K = Ker(\varphi)$, $\alpha \in K, \beta \in G$. Entonces

$$\varphi(\beta^{-1}\alpha\beta) = \varphi(\beta^{-1})\varphi(\alpha)\varphi(\beta) = \varphi(\beta^{-1})\varphi(\beta) = \varphi(\beta^{-1}\beta) = 1$$

Así, $\beta^{-1}\alpha\beta \in K$ y tenemos que K es normal.

Sean ahora $\overline{\alpha}, \overline{\beta} \in \varphi(G)$, entonces $\exists \alpha, \beta \in G$ tales que $\overline{\alpha} = \varphi(\alpha)$ y $\overline{\beta} = \varphi(\beta)$. Así,

$$\overline{\alpha}\overline{\beta} = \varphi(\alpha)\varphi(\beta) = \varphi(\alpha\beta) \in \varphi(G)$$

ya que $\alpha\beta \in G$, con lo que obtenemos que $\varphi(G) \leq H$.

Denotemos Ker(φ)=K. Consideremos la biyección que relaciona cada coclase Kα con el elemento $\varphi(\alpha)$. Para ver que está bien definida, consideremos α y β en G tales que Kα=Kβ. Así, $\alpha \in K\alpha = K\beta$, luego existe un $\gamma \in K$ t.q. $\alpha = \beta\gamma$. Así

$$\varphi(\alpha) = \varphi(\beta\gamma) = \varphi(\beta)\varphi(\gamma) = \varphi(\beta)$$

ya que $\gamma \in K$. Recíprocamente, consideremos ahora α y β tales que $\varphi(\alpha) = \varphi(\beta)$. Entonces

$$1 = \varphi(\alpha)\varphi(\beta)^{-1} = \varphi(\alpha)\varphi(\beta^{-1}) = \varphi(\alpha\beta^{-1})$$

con lo que $\alpha\beta^{-1} \in K$, o lo que es equivalente, $K\alpha = K\beta$. Así, obtenemos que esta biyección entre $\varphi(G)$ y G/Ker(φ), está bien definida, sea cual sea el respresentante que tomemos de la coclase o la antiimagen que tomemos de cada elemento de $\varphi(G)$. □

Definición. El **normalizador** de H en G, es $N_G(H) = \{\beta \in G \mid \beta H = H\beta\}$.

Proposición 1.7. *$N_G(H) \leq G$. Además, este es el mayor subgrupo de G en el que H es normal.*

Demostración. Sea $N = N_G(H)$. Entonces, si $\alpha, \beta \in N$, tenemos que $H^{\alpha\beta} = (H^\alpha)^\beta = H^\beta = H$, y así $\alpha\beta \in N$, y deducimos que efectivamente, N es un subgrupo de G.

Ahora consideremos $H \trianglelefteq M$ y $\alpha \in M$, entonces $H^\alpha = H$, con lo que $\alpha \in N$, y obtenemos que $M \leq N$, y así N será el mayor subgrupo de G en el que H es normal. □

Definición. El **centralizador** de H en G, $C_G(H)$, son los elementos que conmutan con todos los de H, es decir, $C_G(H) = \{\beta \in G \mid \beta\alpha = \alpha\beta \ \ \forall \alpha \in H\}$. Este es un subgrupo de G, tal que $C_G(H) \leq N_G(H)$. Notar que $H \leq G$ es abeliano si y solo si $C_G(H) \supseteq H$.

Teorema 1.8. *Sea $G \leq S_\Omega$. Sea p primo t.q. p^m divide a $|G|$, pero p^{m+1} no lo divide. Entonces, tenemos que $\exists P \leq G$ de orden p^m. Estos subgrupos P, son los llamados p-subgrupos de Sylow de G. Además, si P,Q son p-subgrupos de Sylow (para un mismo p), entonces son conjugados, esto es, $\exists \alpha \in G$ t.q. $P = Q^\alpha$.*

Demostración. Ver el capítulo 1.6. de [3] □

Ejemplo 1. Grupos diédricos D_{2n}.

Sea S_n el grupo de permutaciones de n puntos. Consideremos α un n-ciclo, y β un producto de trasposiciones tales que $\alpha^\beta = \alpha^{-1}$. Por ejemplo, si consideramos $\alpha = (1, 2, \cdots, n)$, entonces podemos tomar, si n es impar:

$$\beta = (1,n)(2,n-1)\cdots((n-1)/2,(n+1)/2)$$

o bien si n es par:

$$\beta = (1,n)(2,n-1)\cdots(n/2,(n/2)+1)$$

Notar que así, al conjugar α con β, obtendremos $(n, n-1, \cdots, 1) = \alpha^{-1}$.

Ahora bien, como $\alpha^\beta = \alpha^{-1}$, tenemos que $\langle\beta\rangle \leq N_G(\langle\alpha\rangle)$, con lo que

$$\langle\alpha\rangle\langle\beta\rangle = \langle\beta\rangle\langle\alpha\rangle$$

y así, podemos considerar el producto de $\langle\alpha\rangle$ y $\langle\beta\rangle$. Este, es un subgrupo de orden 2n y grado n denominado el diédrico de orden 2n, D_{2n}. Estos son:

$$D_{2n} = \{1, \alpha, \cdots, \alpha^{n-1}, \beta, \alpha\beta, \cdots, \alpha^{n-1}\beta\}$$

Notar que si consideramos elementos de la forma $\beta\alpha^k$, entonces $\beta\alpha^k = \beta\alpha^k\beta\beta = \alpha^{-k}\beta$. Así, si operamos $(\alpha^{k_1}\beta)(\alpha^{k_2}) = \alpha^{k_1}\alpha^{-k_2}\beta = \alpha^{k_1-k_2}\beta$, y $(\alpha^{k_1}\beta)(\alpha^{k_2}\beta) = \alpha^{k_1-k_2}$, luego siempre obtenemos elementos de la forma $\alpha^{k_1}\beta^{k_2}$.

Este grupo, se corresponde con el grupo de movimientos que fijan un polígono regular de n lados, si numeramos cada vértice del 1 al n, y consideramos que cada permutación es el movimiento que permuta los vértices de dicha manera. Las permutaciones de la forma α^k se corresponden con los giros, y las permutaciones de la forma $\alpha^k\beta$ se corresponden con las simetrías. Notar que el producto de 2 giros o de 2 simetrías, es un giro, y el producto de una simetría con un giro es una simetría.

Observación 2. Podemos considerar grupos diédricos de orden 2n, contenidos en subgrupos simétricos de grado m > n siguiendo el mismo procedimiento. Sin embargo, lo hemos considerado contenido en S_n, para hacer ver que siempre podemos encontrar un diédrico de orden 2n contenido en él. Además, todos los grupos diédricos de orden 2n son isomorfos, asi que, en ámbitos generales, podemos considerar siempre $D_{2n} \leq S_n$.

1.2. Componentes transitivas

Sea $\Delta \subseteq \Omega$, $K \subseteq S_\Omega$. Entonces denotaremos $\Delta^K = \{i^\alpha \mid i \in \Delta \text{ , } \alpha \in K\}$. Notar que podemos utilizar esta notación aunque K no sea un grupo de permutaciones.

Definición. Sea $G \leq S_\Omega$. $\Delta \subseteq \Omega$ se dice que es un **bloque fijo o fijado** por G si $\Delta^G = \Delta$. En este caso, tenemos que cada $\alpha \in G$ induce una permutación en Δ, que denotaremos por $\alpha^\Delta \in S_\Delta$.

Se dice **componente** de G en Δ a $G^\Delta = \{\alpha^\Delta \mid \alpha \in G\}$, y entonces tenemos el siguiente homomorfismo:

$$\varphi : G \to G^\Delta, \alpha \mapsto \alpha^\Delta$$

Si φ es un isomorfismo, o dicho de otra forma, si $|G| = |G^\Delta|$, entonces se dice que la componente G^Δ es **fiel**.

Proposición 1.9. *Notar que si $A, B \subseteq \Omega$ son bloques fijos, entonces tanto $A \cup B$ como $A \cap B$ son bloques fijos también. Además, para todo $\Gamma \subseteq \Omega$, se tiene que Γ^G es el menor bloque fijo que contiene a Γ.*

Definición. $\emptyset, \Omega$ son bloques fijos $\forall G \leq S_\Omega$. A parte de estos bloques fijos triviales, un grupo G se dice **transitivo** si no tiene más bloques fijos. En caso contrario se dice **intransitivo**.

Una componente G^Δ se dice **transitiva** si Δ es minimal, es decir. si no contiene ningún bloque fijo no trivial. En este caso Δ se dice **órbita o conjunto de transitividad** de G.

Lema 1.10. *Para todo $i \in \Omega$, existe una órbita Δ de G, que es única, t.q. $i \in \Delta$. Se tiene que $\Delta = i^G$. Además $i, j \in \Delta$ órbita de $G \Leftrightarrow j = i^\alpha$ para algún $\alpha \in G$*

Demostración. Notar que efectivamente, por la proposición 1.9, i^G es el menor bloque fijo que contiene a i, es decir, es una órbita de G t.q. $i \in i^G$. Además, si tomamos otra órbita que contenga a i, en particular será un bloque fijo también minimal, por lo que, necesariamente será la misma órbita.

Probemos ahora la segunda parte del lema:

$\Rightarrow$) $i \in \Delta$ órbita $\Rightarrow \Delta = i^G$. Luego como $j \in \Delta = i^G$, entonces $\exists \alpha \in G$ t.q. $j = i^\alpha$

$\Leftarrow$) Tenemos que la órbita de i es i^G. Luego como $j = i^\alpha$ con $\alpha \in G$, se tiene que j está en la misma órbita que i.

□

Notar que esto nos dice que las órbitas de G forman una partición de Ω.

Observación 3. En caso de que tengamos un grupo G intransitivo, tenemos que contiene bloques fijos no triviales, y en particular, podemos considerar la partición de Ω por órbitas $\Delta_1, \cdots, \Delta_n$, con n > 1. Entonces, tenemos los homomorfismos $\varphi_k : G \to G^{\Delta_k}$ para $1 \leqslant k \leqslant n$.

En caso de que $Ker(\varphi_k) = 1$, para algún k, entonces tenemos que la órbita Δ_k es fiel, y tenemos que nuestro grupo G es isomorfo a un grupo transitivo G^{Δ_k}. En caso de que ninguna órbita sea fiel, nuestro grupo no será isomorfo a un grupo transitivo. Aún así, siempre podremos estudiar un grupo a través de sus componentes transitivas, de la siguiente forma:

Sea $\alpha \in G$. Entonces tenemos α^{Δ_k} las restricciones de α a cada bloque Δ_k. Entonces, si queremos ver como funciona α, podemos verlo a través de los α^{Δ_k}, ya que si tomamos $i \in \Omega$, tenemos que $i \in \Delta_k$ para algún $1 \leqslant k \leqslant n$, y solo uno, ya que forman una partición. Así, tenemos que $i^\alpha = i^{\alpha^{\Delta_k}}$, y podemos estudiar el grupo de permutaciones G a través de los grupos de permutaciones transitivos G^{Δ_k}. Por esta razón son particularmente importantes los grupos de permutaciones transitivos.

Ejemplo 2. Sea S_6 y consideremos G = $\langle \alpha, \beta \rangle \leq S_6$ con α = (1,2,3)(4,5,6) y β = (1,2)(4,5). Entonces, si tomamos $A = \{1,2,3\}$ y $B = \{4,5,6\}$, tenemos que $A^G = A$ y $B^G = B$. Luego A y B son bloques fijos por G. Como estos son minimales, tenemos que estos son las órbitas de G, y nuestro grupo es intransitivo. Pero si consideramos $\varphi_A : G \to G^A$, dada por $\alpha^m \beta^n \mapsto (\alpha^A)^m (\beta^A)^n$, con α^A = (1,2,3) y β^A = (1,2). Entonces tenemos que $Ker(\varphi_A) = 1$, y tenemos que la componente G^A es fiel, y así G es isomorfo a un grupo transitivo $G^A = \langle (1,2,3), (1,2)) \rangle = D_6 \leq S_3$.

Ejemplo 3. Sea S_8, y α=(1,2,3), β=(4,5,6), γ=(7,8) y consideremos G=$\langle \alpha, \beta, \gamma \rangle \leq S_8$. Este es un grupo abeliano de 18 elementos. Sean $A = \{1,2,3\}$, $B = \{4,5,6\}$ y $C = \{7,8\}$. Entonces, como antes, tenemos que A, B y C son las órbitas de G, y tenemos que G es intransitivo. Notar que las órbitas no son necesariamente del mismo tamaño. Así mismo, notar que tenemos más bloques fijos, por ejemplo el $A \cup B$, los cuales no son órbitas por no ser minimales.

Entonces podemos considerar, $\varphi_A : G \to G^A$, de forma que $\varphi(\alpha^m \beta^n \gamma^s) = (\alpha^A)^m$, y de forma análoga consideramos φ_B y φ_C. Notar que las componentes G^A, G^B y G^C no son fieles, ya que estos homomorfismos no son inyectivos. Sin embargo, podremos estudiar cada elemento de G, por sus imagenes en ellas, ya que $\forall \delta \in G$, tenemos que δ^A, δ^B y δ^C nos definen perfectamente δ.

Lema 1.11. *Sea $G \leq S_\Omega$, Δ órbita de G, $\alpha \in S_\Omega$. Entonces Δ^α es una órbita de $\alpha^{-1} G \alpha$.*

Demostración. Sea $i \in \Delta$. Entonces tenemos que $\Delta = i^G$. También tenemos que $i^\alpha \in \Delta^\alpha$.

Veamos que $\Delta^\alpha = (i^\alpha)^{\alpha^{-1} G \alpha}$ por doble contenido:

$\subseteq$) $j \in \Delta^\alpha = (i^G)^\alpha \Rightarrow \exists \beta \in G$ t.q. $j = (i^\beta)^\alpha = i^{\beta\alpha} = i^{\alpha\alpha^{-1}\beta\alpha} = (i^\alpha)^{\alpha^{-1}\beta\alpha} \in (i^\alpha)^{\alpha^{-1} G \alpha}$

$\supseteq$) $j \in (i^\alpha)^{\alpha^{-1} G \alpha} \Rightarrow \exists \beta \in G$ t.q. $j = (i^\alpha)^{\alpha^{-1}\beta\alpha} = (i^\beta)^\alpha \in \Delta^\alpha$.

Luego obtenemos que Δ^α es una órbita de $\alpha^{-1} G \alpha$. □

1.3. Estabilizadores

Definición. Sea $G \leq S_\Omega, \Delta \subseteq \Omega$. Entonces $G_\Delta = \{\alpha \in G \mid i^\alpha = i, \forall i \in \Delta\}$ es un grupo, compuesto por permutaciones que fijan cada punto de Δ. A G_Δ se le llama **estabilizador** de Δ en G. Será importante el estabilizador de un punto $i \in \Omega$, al cual denotaremos G_i.

Observación 4. Sean $i, j \in \Omega$, $\Delta, \Gamma \subseteq \Omega$.

1) $G_\emptyset = G$
2) $G_\Omega = \langle 1 \rangle$
3) $G_{\{i,j\}} = (G_i)_j = (G_j)_i$
4) $G_{\Gamma \cup \Delta} = G_\Gamma \cap G_\Delta = (G_\Gamma)_\Delta$
5) $G_\Delta = \cap_{i \in \Delta} G_i$

Proposición 1.12. *$\forall \alpha \in G, \Delta \subseteq \Omega$, se tiene que $\alpha^{-1} G_\Delta \alpha = G_{\Delta^\alpha}$. En particular, si Δ es un bloque fijo por G, entonces $|G^\Delta| = |G|/|G_\Delta|$. Si $i^G = j^G$, entonces G_i y G_j son conjugados en G.*

Demostración. Veamos que $\alpha^{-1} G_\Delta \alpha = G_{\Delta^\alpha}$ por doble contenido:

$\subseteq$) Sea $\beta \in \alpha^{-1} G_\Delta \alpha \Rightarrow \exists \gamma \in G_\Delta$ t.q. $\beta = \alpha^{-1}\gamma\alpha$. Sea $i \in \Delta^G$. Entonces $i = j^\alpha$ con $j \in \Delta$.
Veamos ahora que $i^\beta = i : i^\beta = (j^\alpha)^\beta = j^{\alpha\alpha^{-1}\gamma\alpha} = j^{\gamma\alpha} = j^\alpha = i$, ya que $j^\gamma = j$.

$\supseteq$) Sea $\beta \in G_{\Delta^\alpha} \Rightarrow i^\beta = i$ para todo $i \in \Delta^\alpha \Rightarrow j^{\alpha\beta} = j^\alpha$ para todo $j \in \Delta \Rightarrow j^{\beta^{\alpha^{-1}}} = j \Rightarrow \beta^{\alpha^{-1}} \in G_\Delta \Rightarrow \beta = \beta^{\alpha^{-1}\alpha} \in G_\Delta^\alpha$.

Ahora, como Δ es un bloque fijo, consideremos el homomorfismo $\varphi : G \to G^\Delta$ dado por $\alpha \mapsto \alpha\Delta$. Veamos cual es su núcleo:

Sea $\alpha \in G$ t.q. $\alpha^\Delta = 1$. Es decir $i^\alpha = i^{\alpha^\Delta} = i^1 = i \ \ \forall i \in \Delta$. Así, tenemos que $\alpha \in G_\Delta$. Por otra parte, sea $\beta \in G_\Delta$, tenemos que $\varphi(\beta) = \beta^\Delta = 1$, ya que fija todos los puntos de Δ. Luego tenemos que $Ker(\varphi) = G_\Delta$.

Además, notemos también que $\varphi(G) = G^{\Delta}$. Luego por la proposición 1.6, tenemos que hay una biyección entre los elementos de G^{Δ} y las coclases módulo G_{Δ}, es decir, $|G^{\Delta}| = |G : G_{\Delta}| = |G|/|G_{\Delta}|$.

Finalmente veamos que si dos elementos i y j tienen las mismas órbitas, los subgrupos G_i y G_j son conjugados. Tenemos que $i = j^{\alpha}$, con $\alpha \in G$. Sea $\beta \in G_i \Rightarrow i^{\beta} = i \Rightarrow (j^{\alpha})^{\beta} = j^{\alpha} \Rightarrow j^{\alpha\beta\alpha^{-1}} = j \Rightarrow \alpha\beta\alpha^{-1} \in G_j$. Así obtenemos que $\alpha G_i \alpha^{-1} \subseteq G_j$. El otro contenido se obtiene de forma análoga, con lo que se obtiene la igualdad y finalizamos la demostración. □

Teorema 1.13. $|G_i||i^G| = |G|$.

Demostración. $i^{\alpha} = i^{\beta} \Leftrightarrow \alpha\beta^{-1} \in G_i \Leftrightarrow \alpha \in G_i\beta$. Luego hay tantos puntos i^{α} en la órbita de i como coclases a derecha $G_i\beta$, es decir: $|i^G| = |G : G_i| = |G|/|G_i|$ □

Proposición 1.14. $|G : G_{i,j}| = |i^G||j^{G_i}| = |j^G||i^{G_j}|$

Demostración. Por el teorema 1.13 $|G_{i,j}||i^G||j^{G_i}| = |G_i||i^G| = |G| = |G_j||j^G| = |G_{i,j}||j^G||i^{G_j}|$. □

Teorema 1.15. *Sea p un número primo, p^m divisor de $|i^G|$, P un p-subgrupo de Sylow de G. Entonces, se tiene que p^m también es divisor de $|i^P|$.*

Demostración. Tenemos que p^m divide a

$$|i^G||G_i : P_i| = |G : G_i||G_i : P_i| = |G : P_i| = |G : P||P : P_i| = |G : P||i^P|$$

Sin embargo, tenemos que p no divide a $|G : P|$, con lo que p^m divide a $|i^p|$. □

Teorema 1.16. *Todas las órbitas más cortas ψ de P en i^G tienen longitud p^m, siendo m la mayor potencia de p que divide a $|i^G|$.*

Demostración. Por el teorema 1.13, cada órbita de P tiene longitud potencia de p. Ahora bien, p^m divide a $|\psi|$ por el teorema 1.15, y p^{m+1} no divide a $|\psi|$, ya que sino también dividiría a $|i^G|$. Luego $|\psi| = p^m$. □

Teorema 1.17. *Sea un subgrupo $H \leq G_i$ t.q. es conjugado en G_i a todo subgrupo $K \leq G_i$ que sea conjugado a H en G. Sea N el normalizador de H en G. Si G es transitivo en Ω, tenemos que N es transitivo en Φ el conjunto de todos los puntos fijados por H.*

Demostración. Primero veamos que $\Phi^N = \Phi$.

Como H es normal en N, se tiene que para todos $\alpha \in N, \beta \in H$, se tiene que $\alpha\beta\alpha^{-1} \in H$. Sea $j \in \Phi$. Entonces $j = j^{\alpha\beta\alpha^{-1}} \Rightarrow j^{\alpha} = j^{\alpha\beta} \Rightarrow j^{\alpha} \in \Phi$. Así, tenemos que $\Phi^N \subseteq \Phi$, y como son del mismo tamaño se da también la igualdad.

Sean ahora $i, j \in \Phi$ cualquiera. Como G es transitivo, $\exists \alpha \in G$ t.q. $i = j^{\alpha}$. Sea $H^{\alpha} \leq G$. Por hipótesis, como es conjugado en G, lo es en G_i, es decir $\exists \beta \in G_i$ t.q. $H = \beta^{-1}H^{\alpha}\beta = H^{\alpha\beta}$.

Con la igualdad anterior tenemos que $\alpha\beta \in N$.

Así, como $j^{\alpha\beta} = i^{\beta} = i$, tenemos que N es transitivo en Φ. □

Notamos que en particular, el propio G_i y los subgrupos de Sylow de este, cumplen las condiciones de U del teorema anterior, lo cual nos proporciona los siguientes resultados.

Teorema 1.18. *En un grupo transitivo G, el normalizador de G_i es transitivo en los puntos fijos por G_i.*

Teorema 1.19. *En un grupo transitivo G, el normalizador de todo subgrupo de Sylow P de G_i es transitivo en los puntos fijos por P.*

Finalmente, mencionar que, relacionados con los estabilizadores G_{Δ} definimos dos tipos de grupos, de gran importancia, los grupos regulares y los grupos de Frobenius.

Definición. Un grupo de permutaciones G en Ω se dice **semirregular** si $\forall i \in \Omega, G_i = 1$. Además, si G es transitivo, se dice que es **regular**.

Definición. Se dice **grupo de Frobenius** a un grupo de permutaciones transitivo, de grado n, que tiene grado mínimo n-1. Es decir, un grupo que mueve los n puntos del conjunto, cuyas permutaciones mueven siempre al menos n-1 puntos (y hay alguna en particular que mueve solo n-1 puntos y no más). Luego son los grupos no regulares G con $G_{i,j} = 1 \ \ \forall i \neq j$. No estudiaremos estos grupos en este trabajo pero los mencionamos por su importancia.

Capítulo 2

Bloques y grupos primitivos

2.1. Bloques

Definición. Sea G un grupo de permutaciones sobre Ω. $\Psi \subseteq \Omega$ se dice **bloque** si $\forall \alpha \in G$, se tiene que Ψ^α coincide con Ψ o no tiene ningún punto en común.

El propio Ω, $\emptyset$, y los conjuntos $\{i\}$ de un solo punto son trivialmente bloques de cualquier G en Ω. Estos son los bloques triviales. Además, los bloques fijos, son en particular bloques, y si tenemos $H \leq G$, entonces todo bloque de G, es también un bloque de H.

Proposición 2.1. *Si Ψ y Ψ' son bloques de G, entonces $\Psi \cap \Psi'$ también es un bloque de G.*

Demostración. Sea $\alpha \in G$. Supongamos que $\exists i \in \Omega$ t.q. $i \in \Psi \cap \Psi'$ e $i \in (\Psi \cap \Psi')^\alpha = \Psi^\alpha \cap (\Psi')^\alpha$ (por ser α una permutación, biyectiva). En particular tenemos que $i \in \Psi, \Psi', \Psi^\alpha, (\Psi')^\alpha$. Pero, como Ψ y Ψ' son bloques de G, tenemos que $\Psi = \Psi^\alpha$ y $\Psi' = (\Psi')^\alpha$, pues sus intersecciones no son disjuntas. Con lo cual $\Psi \cap \Psi' = \Psi^\alpha \cap (\Psi')^\alpha = (\Psi \cap \Psi')^\alpha$. Finalmente, notamos que si no existiera tal punto i, eso quiere decir que $(\Psi \cap \Psi') \cap (\Psi \cap \Psi')^\alpha = \emptyset$. Con lo cual obtenemos que $\Psi \cap \Psi'$ es un bloque de G. □

Proposición 2.2. *Si $\alpha \in G, H \leq G$, y Ψ es un bloque de H, entonces Ψ^α es un bloque $\alpha^{-1} H \alpha$.*

Demostración. Sea $\beta \in H$. Entonces $\Psi^\alpha \cap (\Psi^\alpha)^{\alpha^{-1}\beta\alpha} = \Psi^\alpha \cap \Psi^{\beta\alpha} = (\Psi \cap \Psi^\beta)^\alpha$. Pero como Ψ es un bloque de H y $\beta \in H$, entonces $\Psi = \Psi^\beta$ o son disjuntos. Con lo que obtenemos que $(\Psi^\alpha)^{\alpha^{-1}\beta\alpha} = \Psi^\alpha$ o son disjuntos. □

Entonces, si Ψ es un bloque de G, tenemos que $\forall \alpha \in G, \Psi^\alpha$ es un bloque de G. Dos tales bloques son llamados conjugados. Cualquier par de bloques conjugados distintos son disjuntos. Además, todos los bloques conjugados a un bloque Ψ, forman un sistema completo de bloques. Todos los bloques de un sistema completo de bloques tienen la misma longitud, y si G es transitivo, la union de todos estos bloques es el propio Ω. De esto obtenemos el siguiente resultado:

Proposición 2.3. *La longitud de un bloque de un grupo transitivo G divide al grado de G.*

Proposición 2.4. *Sea Ψ un bloque del grupo transitivo G. Entonces $H = \{\alpha \in G \mid \Psi^\alpha = \Psi\}$ es un subgrupo de G. Además, tenemos que H es transitivo en Ψ.*

Demostración. Sean $\alpha, \beta \in H$. Entonces $\Psi^{\alpha\beta} = (\Psi^\alpha)^\beta = \Psi^\beta = \Psi$, luego $\alpha\beta \in H$ y tenemos que H es un subgrupo de G. Ahora sean $i, j \in \Psi$, veamos que $\exists \alpha \in H$ t.q. $i^\alpha = j$. Como G es transitivo, tenemos que $\exists \alpha \in G$ t.q. $i^\alpha = j$, luego $\Psi \cap \Psi^\alpha \neq \emptyset$, y como Ψ es un bloque, tenemos que $\Psi = \Psi^\alpha$ y $\alpha \in H$. □

2.2. Grupos imprimitivos

Definición. Un grupo transitivo es llamado **imprimitivo** si tiene al menos un bloque no trivial. Este bloque se dice conjunto de imprimitividad.

Proposición 2.5. *(condición suficiente). Si el grupo transitivo G contiene un subgrupo intransitivo normal N diferente de 1, entonces G es imprimitivo. Las órbitas de N forman un sistema de bloques completo de G.*

Demostración. Si Ψ es una órbita de N, entonces Ψ^α por 1.11 es una órbita de $\alpha^{-1}N\alpha = N$. Luego G solo puede permutar órbitas disjuntas una sobre otra. Es decir, estas órbitas son bloques de G. Como $N \neq 1$, estas órbitas tienen más de un punto. Como N es intransitivo, estos son subconjuntos propios de Ω, y por la transitividad de G son conjugados. □

Observación 5. Sea $\overline{\Omega} = \{\Psi_1, \cdots \Psi_n\}$ un sistema completo de bloques no triviales del grupo imprimitivo G, y sea $\overline{\alpha}$ la permutación en $\overline{\Omega}$ inducida por α, esto es, $\overline{\alpha}(\Psi_k) = \Psi_k^\alpha$. Estas $\overline{\alpha}$ forman un grupo $\overline{G}$ de permutaciones sobre $\overline{\Omega}$ y tenemos un homomorfismo $\varphi : G \to \overline{G}, \alpha \mapsto \overline{\alpha}$.

El núcleo N de este homomorfismo son las permutaciones que fijan todos los bloques de $\overline{\Omega}$. $\overline{G}$ es transitivo en $\overline{\Omega}$. Los bloques Ψ_k son bloques fijos por N, pero no necesariamente órbitas de N.

De igual manera, por proposicion 2.4, podemos considerar los subgrupos $H_k = \{\alpha \in G \mid \Psi_k^\alpha = \Psi_k\}$, transitivos en Ψ_k, de los cuales Ψ_k son bloques fijos. Así, aún siendo H_k intransitivo en Ω, podemos proceder como en la observación 3, y podemos construir los homomorfismos $\varphi_k : H_k \to H_k^{\Psi_k}$, para estudiar como funcionan las permutaciones dentro de cada bloque. Estos grupos $H_k^{\Psi_k}$ serán también transitivos.

De esta forma, podemos construir a partir de grupos imprimitivos transitivos, otros grupos transitivos de menor grado, esto es, un grupo que nos define como se permutan los bloques entre si, y grupos que nos definen, dentro de cada bloque, como funciona cada permutación que fija ese bloque.

Teorema 2.6. *Sea $\Delta \subseteq \Omega, i \in \Omega$. Entonces $\Psi = \cap_{i \in \Delta^\alpha} \Delta^\alpha$ es un bloque del grupo transitivo G.*

Demostración. Notar que $i \in \Psi$, ya que G es transitivo. Sea $\beta \in G$ t.q. $\Psi \cap \Psi^\beta \neq \emptyset$.

$\Psi^\beta = \cap_{i \in \Delta^\alpha} \Delta^{\alpha\beta}$.

Supongamos que $i \in \Psi^\beta$. Entonces $i \in \Delta^{\alpha\beta}$, luego $\Psi^\beta \subseteq \Psi$, pero como $|\Psi| = |\Psi^\beta|$, tenemos que $\Psi = \Psi^\beta$.

Sea ahora un $j \in \Psi \cap \Psi^\beta$. Como G es transitivo, tenemos que existen un $\gamma \in G$ t.q. $i^\gamma = j$. Entonces, tenemos que i está en $\Psi^{\gamma^{-1}}$, $\Psi^{\beta\gamma^{-1}}$ y Ψ. Razonando como antes, obtenemos que $\Psi = \Psi^{\gamma^{-1}} = \Psi^{\beta\gamma^{-1}}$, y aplicando γ, tenemos que $\Psi^\gamma = \Psi = \Psi^\beta$, con lo que obtenemos que Ψ es un bloque de G. □

Teorema 2.7. *Sea $i \in \Omega$. Un grupo transitivo G sobre S_Ω es imprimitivo si y solo si hay un grupo Z, propiamente contenido entre G y G_i, esto es $G_i < Z < G$.*

Demostración.

⇒) Sea G imprimitivo. Esto quiere decir que hay algún bloque Ψ no trivial de G. Entonces, consideremos $Z = \{\beta \in G \mid \Psi = \Psi^\beta\}$. Z es claramente un subgrupo de G. Además $Z \neq G$, ya que G es transitivo y $\Psi \neq \Omega$, es decir, que existe $\beta \in G$ t.q. $\Psi \neq \Psi^\beta$. Consideremos $i \in \Psi$. Podemos hacer esto ya que no solo disponemos del bloque Ψ, disponemos de un sistema completo de bloques, compuesto por los conjugados de los bloques, luego siempre podemos considerar un bloque en el que está i. Si $i^\alpha = i$, entonces $\Psi^\alpha = \Psi$, luego $G_i \leq Z$. Como $|\Psi| > 1$, tomemos $j \neq i$ t.q. $j \in \Psi$. Como G es transitivo, existe un $\gamma \in G$ de forma que $i^\gamma = j$. Este $\gamma \in Z$, pero no está en G_i, luego $G_i \neq Z$. Con lo que finalmente tenemos que $G_i < Z < G$.

⇐) Sea Z t.q. $G_i < Z < G$. Denotemos $\Psi = i^Z$. Sea $\alpha \in G$ t.q. $\Psi \cap \Psi^\alpha \neq \emptyset$. Para ver que Ψ es un bloque, tenemos que ver que $\Psi = \Psi^\alpha$. Sea $j \in \Psi \cap \Psi^\alpha$. Entonces, existen $\gamma, \gamma' \in Z$ de forma que $i^\gamma = j = i^{\gamma'\alpha}$. Luego $\gamma'\alpha\gamma^{-1} \in G_i < Z$, luego $\alpha \in Z$. Así, $\Psi = i^Z = i^{Z\alpha} = \Psi^\alpha$, y Ψ es un

bloque. Finalmente, veamos que es un bloque no trivial. Como $Z \neq G_i$, entonces Ψ no tiene un único punto. Además, como $Z \neq G$, y $\Psi = \Psi^\alpha$ si y solo si $\alpha \in Z$, entonces $\exists \alpha \in G$ t.q. $\Psi \neq \Psi^\alpha$, luego Ψ tampoco es el conjunto total Ω. Con todo esto, obtenemos que Ψ es un conjunto de imprimitividad, es decir, que G es imprimitivo.

□

Esta demostración, nos establece una conexión directa entre cada uno de los grupos contenidos entre G y G_i, y los bloques que contienen a i. En base a esto, se obtiene la demostración al siguiente teorema:

Teorema 2.8. *El retículo de grupos contenidos entre G y G_i es isomorfo al retículo de bloques de G que contiene a i.*

Ejemplo 4. Consideremos el grupo diédrico de 12 elementos, este es:

$$D_{12} = \langle \alpha = (1,2,3,4,5,6), \beta = (1,6)(2,5)(3,4) \rangle \leq S_6$$

Consideremos $A = \{1,4\}$, $B = \{2,5\}$, $C = \{3,6\}$, los conjuntos de vértices opuestos de un hexágono regular. Notar que por cualquier movimiento que hagamos, cualquier par de vértices opuestos, se colocarán en otro o el mismo par de vértices opuestos, con lo cual obtenemos A,B,C son bloques no triviales de D_{12}, y así D_{12} será imprimitivo. Si estudiaramos los estabilizadores de cada punto, obtendríamos que $G_1 = G_4 = \langle \alpha^5\beta \rangle$, $G_2 = G_5 = \langle \alpha^3\beta \rangle$, y $G_3 = G_6 = \langle \alpha\beta \rangle$, es decir, el estabilizador de cada par de vértices opuestos es la simetría que pasa por ellos. Consideremos ahora

$$H = \langle \alpha^2, \alpha\beta \rangle = \{1, \alpha^2, \alpha^4, \alpha\beta, \alpha^3\beta, \alpha^5\beta\}$$

Notar que este es un subgrupo propiamente contenido entre los estabilizadores de un punto y D_{12}. Luego tenemos otra forma de comprobar que efectivamente este es un grupo imprimitivo.

2.3. Grupos primitivos

Definición. Un grupo transitivo se dice **primitivo** si todos sus bloques son triviales.

Notar que para hablar de grupos imprimitivos y primitivos, hemos considerado los grupos transitivos porque no tiene sentido hablar de primitividad de grupos intransitivos, ya que estos, por definición, tienen bloques no triviales, que en particular son bloques fijos, las distintas órbitas, luego nunca podrían ser primitivos, y no tiene interés. Por eso, solo podríamos hablar de la primitividad de sus componentes transitivas.

Ahora, usando 2.6, tenemos que si $\Delta \subset \Omega, i \in \Omega$, entonces $i = \cap_{i \in \Delta^\alpha} \Delta^\alpha$. De esto se deduce el siguiente resultado:

Teorema 2.9. *Sea $\emptyset \subset \Delta \subset \Omega$. Si G es primitivo en Ω, entonces para todos $i, j \in \Omega$ distintos, se tiene que $\exists \alpha \in G$ t.q. $i \in \Delta^\alpha$ y $j \notin \Delta^\alpha$.*

Teorema 2.10. *Sea $i \in \Omega, |\Omega| > 1$. Un grupo transitivo G sobre S_Ω es primitivo si y solo si G_i es un subgrupo maximal de G.*

Demostración. Inmediato por el teorema 2.7. □

Teorema 2.11. *Un grupo transitivo de grado primo es primitivo.*

Demostración. Por 2.3, la longitud de cada bloque de un grupo transitivo, divide al grado, luego en este caso cada bloque es trivial. □

Ejemplo 5. Consideremos el grupo diédrico de 10 elementos, este es:

$$D_{10} = \langle \alpha = (1,2,3,4,5), \beta = (1,5)(2,4) \rangle \leq S_5$$

Esta vez, a diferencia de con el diédrico de 10 elementos, no hay simetrías que pasen a través de 2 puntos, ni simetrías que no pasan a través de ningún punto. Asi, los estabilizadores de cada punto será el grupo generado por la única simetría que pasa por dicho punto, y todos serán disjuntos. Esto es, $G_1 = \langle \alpha^4\beta \rangle$, $G_2 = \langle \alpha^2\beta \rangle$, $G_3 = \langle \beta \rangle$, $G_4 = \langle \alpha^3\beta \rangle$ y $G_5 = \langle \alpha\beta \rangle$. Ahora bien, notar que todos los giros se obtienen a partir de uno cualquiera, debido a que 5 es primo, es decir $\langle \alpha \rangle = \langle \alpha^2 \rangle = \langle \alpha^3 \rangle = \langle \alpha^4 \rangle$, luego si consideramos un subgrupo generado por un giro y una simetría, obtendremos todas los giros y todas las simetrías tambíen por lo tanto, es decir, $\langle \alpha^i, \alpha^j\beta \rangle = D_{10}$. De la misma forma, cualquier subgrupo generado por dos simetrías, como su producto será un giro, también contendrán a todos los giros y simetrías, es decir, $\langle \alpha^i\beta, \alpha^j\beta \rangle = D_{10}$. Con lo cual, obtenemos que los estabilizadores de cada punto son maximales, pues no hay ningún subgrupo propiamente contenido entre ellos y D_{10}, y así obtenemos que el diédrico de orden 10 es un grupo primitivo. Esto se debe, a que los únicos bloques que tiene esta vez, son vértices del pentágono regular individuales, triviales, en vez de parejas de vértices opuestos, como en el diédrico de orden 12. En general, el grupo diédrico D_{2n} será primitivo si y solo si n es primo.

Observación 6. Notar que, como vimos en la sección de grupos imprimitivos, si $\overline{\Omega} = \{\Psi_1, \cdots \Psi_k\}$ un sistema completo de bloques no triviales, podremos construir otros grupos transitivos a partir de este, todos de menor grado. Como esto podemos hacerlo mientras obtengamos grupos primitivos, podemos reiterar las veces que haga falta en los grupos imprimitivos que obtengamos, de forma que los grupos que obtenemos son cada vez de menor tamaño. De esta forma, llegará un punto en que todos los grupos que hayamos obtenido sean primitivos, ya que, como estamos obteniendo grupos de menor grado, este proceso tendrá un límite de veces las cuales podamos hacerlo, y este solo terminará cuando todos los grupos que hayamos obtenido sean primitivos. De ahí la importancia que tendrá el estudio de los grupos primitivos.

Ejemplo 6. Sigamos con el ejemplo 4 del diédrico de 12 elementos. Recordar que este era:

$$D_{12} = \langle \alpha, \beta \rangle \leq S_6 \ \ con \ \ \alpha = (1,2,3,4,5,6), \beta = (1,6)(2,5)(3,4)$$

Este, era imprimitivo, y teníamos el siguiente sistema completo de bloques:

$$\overline{\Omega} = \{A,B,C\} \ \ con \ \ A = \{1,4\}, B = \{2,5\}, C = \{3,6\}$$

Así, podemos seguir lo visto en la observación 5 para construir grupos primitivos a partir de él.

Así, podemos considerar $\overline{\alpha} = (A,B,C)$ y $\overline{\beta} = (A,C)$ permutaciones de $\overline{\Omega}$. Con esto podemos crear un grupo $\overline{G} = \langle \overline{\alpha}, \overline{\beta} \rangle \leq S_{\overline{\Omega}}$, el cual es isomorfo a S_3, y es primitivo. Notar que si consideramos $\varphi : G \to \overline{G}$, tenemos que su núcleo N es $N = \langle \alpha^3 \rangle$, estas son las simetrías que fijan a todos los bloques, un giro de π y la identidad.

Ahora bien, consideremos los subgrupos que dejan fijo a cada bloque. Estos son:

$$H_A = \{1, \alpha^3, \alpha^2\beta, \alpha^5\beta\} \quad H_B = \{1, \alpha^3, \beta, \alpha^3\beta\} \quad H_C = \{1, \alpha^3, \alpha\beta, \alpha^4\beta\}$$

En cada grupo tenemos la identidad, un giro de π, que intercambia a los puntos del bloque, la simetría que pasa por ambos puntos, que fija a ambos puntos del bloque, y la simetría que intercambia ambos puntos del bloque.

Así, finalmente consideremos los homomorfismos:

$$\varphi_A : H_A \to (H_A)^A \quad \varphi_B : H_B \to (H_B)^B \quad \varphi_C : H_C \to (H_C)^C$$

Cada grupo de la forma $(H_\Delta)^\Delta$ es isomorfo S_2, que es primitivo.

Así, hemos derivado el estudio de nuestro D_{12} imprimitivo, al estudio de los grupos S_3 y S_2, todos primitivos.

Capítulo 3

Grupos abstractos y acciones

3.1. Grupos abstractos

La definición habitual de grupo, es un conjunto G con una operación binaria interna asociativa, con elemento neutro, e inverso para cada elemento. Notar, que tenemos que todo grupo de permutaciones, se corresponde con la definición habitual de grupo, por la observación 1. Además, notemos que, en la mayoría de definiciones sobre conceptos de grupos de permutaciones, no interviene el conjunto Ω de puntos a permutar, solo las propias permutaciones. Así, toda definición de grupos de permutaciones, en la que no intervenga Ω, podrá ser extrapolada a grupos con elementos abstractos. Esto incluye las definiciones sobre subgrupos, coclases, normalidad y homomorfismos. Por su parte, las definiciones sobre órbitas, estabilizadores, bloques y por lo tanto primitividad, no pueden ser extrapolados de forma directa, por lo que tendremos que dar alguna herramienta para poder utilizar estos conceptos de alguna forma en grupos abstractos.

Empecemos dando algunos resultados que no vimos en grupos de permutaciones, por haber necesitado dar entonces un concepto más general de grupo.

Definición. Sea ahora $H \trianglelefteq G$. Entonces podemos definir el **subgrupo cociente** de G por H, G/H, el cual está formado por las coclases de G por H, indistintamente a derecha o a izquierda, puesto que son iguales, con la operación dada por (Hx)(Hy)=Hxy. Esta, tiene una estructura de grupo. Notar que en caso de que H no sea normal, también podemos considerar el conjunto de coclases a derecha(o izquierda), pero no podremos construir dicha estructura de grupo.

Observación 7. Notar que, en el caso de grupos de permutaciones, no podíamos estudiar el espacio cociente, ya que este dejaba de ser un grupo de permutaciones.

A continuación, daremos dos resultados sobre isomorfía, cuyas demostraciones podemos encontrar en el capítulo 1.3. de [3].

Teorema 3.1. *Teorema de isomorfía. Sea $\varphi : G \to H$ un homomorfismo. Entonces la aplicación*

$$\overline{\varphi} : G/Ker(\varphi) \to \varphi(G) \quad Ker(\varphi)\alpha \mapsto \varphi(\alpha)$$

está bien definida y es un isomorfismo.

Esto es una extensión de lo que veíamos en la proposición 1.6, cuando no habíamos establecido lo que era el subgrupo cociente, simplemente viéndolo como un conjunto de coclases, sin operación.

Teorema 3.2. *Segundo teorema de isomorfía. Sea $N \trianglelefteq G$, entonces:*

a) La aplicación $\varphi : G \to G/N$ dada por $\varphi(g) = Ng$ es un homomorfismo suprayectivo, y si $H \leq G$, entonces $\varphi(H) = HN/N$.

b) Si $H \leq G$, entonces $H \cap N \trianglelefteq H$ y $H/H \cap N \cong NH \cap N$.

Definición. Sean G,H dos grupos cualesquiera, entonces podemos definir una estructura de grupo en el conjunto $G \times H = \{(g,h) \mid g \in G, h \in H\}$, con la operación definida por las operaciones en G y H componente a componente, de forma que $(g_1,h_1) * (g_2,h_2) = (g_1 * g_2, h_1 * h_2)$.

Este grupo se denomina el **producto directo** de G y H. Notar que $G \times H$ tiene dos subgrupos normales, que son isomorfos a G y H, cuyo producto es $G \times H$, y cuya intersección es 1.

Así mismo, si tenemos $N_1, N_2 \trianglelefteq G$ tales que $N_1 N_2 = G$ y $N_1 \cap N_2 = 1$, entonces tenemos que $G \cong N_1 \times N_2$, y podemos llamar a G producto directo de N_1 y N_2.

Definición. Consideremos ahora N, H grupos cualesquiera, y $\varphi : H \to Aut(N)$ un homomorfismo de H en los automorfismos de N. Para cada $h \in H$, tenemos un automorfismo $\varphi(h) : N \to N$. Entonces llamaremos **producto semidirecto vía** φ a:

$$[N]_\varphi H = \{(n,h) \mid n \in N, h \in H\}$$

con la operación definida de la siguiente forma:

$$(n_1,h_1) * (n_2,h_2) = (n_1 n_2^{\varphi(h_1^{-1})}, h_1 h_2)$$

De la misma forma, si tenemos $N \trianglelefteq G$, y $H \leq G$, tales que $NH = G$ y $N \cap H = 1$, entonces cada elemento de g se define de forma única como g=nh, con $n \in N, h \in H$, y la operación en G se puede realizar a través de las operaciones en N y H, de forma que $g_1 g_2 = n_1 h_1 n_2 h_2 = n_1 n_2^{h_1^{-1}} h_1 h_2$. Esto, es lo mismo que considerar, $\forall g \in G$, el automorfismo dado por $\varphi(g)(h) = h^g$. Así, tenemos que $G \cong [N]_\varphi H$, y podemos llamar a G producto semidirecto de N con H vía φ.

Esto, es lo que sucede con los grupos diédricos, los cuales podemos verlos como $D_{2n} \cong [C_n]_\varphi C_2$, con el automorfismo dado por $\varphi(\beta)(\alpha) = \alpha^{-1}$, con $\alpha \in C_n$ y $C_2 = \langle \beta \rangle$.

Ejemplo 7. Consideremos en S_8 los siguientes elementos:

$$x = (1,2,3,4)(5,8,6,7), \quad y = (1,5,3,6)(2,7,4,8)$$

Operando, podemos ver que $x^2 = (1,3)(2,4)(5,6)(7,8) = y^2$, y que $x^y = (5,7,6,8)(3,2,1,4) = x^{-1}$. Así, tenemos que $\langle y \rangle \subseteq N_{S_8}(\langle x \rangle)$, luego $\langle x \rangle \langle y \rangle = \langle y \rangle \langle x \rangle$, y así este es un grupo de permutaciones. Este es el llamado grupo de los cuaternios, y lo escribiremos, $Q_8 = \langle x \rangle \langle y \rangle$.

Ahora, consideremos $z = xy = (1,7,3,8)(2,6,4,5)$. Con esto tenemos que:

$$x^2 = y^2 = z^2, \quad x^4 = y^4 = z^4 = 1$$

Así, tenemos que el grupo se podrá escribir de la siguiente forma:

$$Q_8 = \{1, x, x^2, x^3, y, y^3, z, z^3\}$$

Este grupo tiene 4 subgrupos, estos son $\langle x \rangle$, $\langle y \rangle$ y $\langle z \rangle$, todos ellos de orden 4, normales en Q_8, y todos ellos cortandose en $\langle x^2 \rangle$, de orden 2, también normal por ser $C_{Q_8}(Q_8) = \langle x^2 \rangle$.

Así, este grupo, es producto de cualquiera de sus subgrupos de orden 4, ambos siendo normales, pero siendo sus intersecciones no triviales. Así, este grupo no puede ser producto semidirecto de subgrupos propios.

Además, todo subgrupo tendrá core no trivial, a excepción de $1 \leq Q_8$, por lo que la única acción fiel que podemos considerar es la regular, y esta es la única forma de verlo como grupo de permutaciones.

3.2. Acciones de grupos

Definición. Tomemos ahora un conjunto cualquiera Ω. Una **acción** de G sobre Ω es un homomorfismo

$$\varphi : G \to S_\Omega$$

Ahora bien, las acciones son unas herramientas que nos relacionan los grupos abstractos con grupos de permutaciones. Por ello, las definiciones de grupos de permutaciones que no pudimos trasladar en la anterior sección, por necesitar del conjunto Ω, podrán ser trasladadas a grupos asbtractos, siempre y cuando consideremos una acción. Así, si G es un grupo abstracto, podemos hablar de las órbitas de G y de su transitividad, del estabilizador en G de un subconjunto de Ω, y de bloques de G, si consideramos alguna acción de G sobre Ω.

Se dice que G actúa fielmente sobre Ω, si φ es inyectiva. Notar que en este caso, G es isomorfo a un subgrupo de S_Ω. Si $i \in \Omega, g \in G$, escribiremos i^g en vez de $i^{\varphi(g)}$, mientras no haya lugar a error. Así, $(i^g)^h = i^{gh}$.

Observación 8. Si G no es fiel, podemos considerar $K = Ker(\varphi) = \{g \in G \mid \varphi(g) = 1\}$, y considerar la acción $\overline{\varphi} : G/K \to S_\Omega$, definida de forma que $Kg \mapsto \varphi(g)$, la cual está bien definida, de forma análoga a lo que veíamos en la proposición 1.6. Sin embargo, siempre podremos considerar alguna acción fiel.

Notar que, dado un grupo G, siempre podemos considerar las acciones dadas por $\varphi, \psi : G \to S_G$, entendiendo G como un conjunto de puntos a permutar, de forma que para todo $g \in G$, $\varphi(g) : G \to G$ y $\psi(g) : G \to G$, están definidas como $\varphi(g)(h) = hg$ y $\psi(g)(h) = g^{-1}h \quad \forall h \in G$, es decir, acciones que cada elemento de G permuta a los propios elementos de G. Estas acciones son fieles, por lo que siempre, podremos considerar G isomorfo a algún grupo de permutaciones.

Por ejemplo, consideremos la acción por multiplicación a derecha. Entonces tenemos que el grupo de permutaciones es transitivo y para cada $h \in G$ el estabilizador G_h solo tiene a la identidad. Por ello, estas son las llamadas representaciones regulares de G, ya que los grupos de permutaciones a los que obtenemos que G es isomorfo, son regulares.

También, notar que G puede ser isomorfo a grupos de permutaciones distintos.

Ejemplo 8. Sea G el grupo de movimientos rígidos (giros) del cubo. Podemos ver este grupo, como el grupo que actúa sobre el conjunto de los 8 vértices del cubo, sobre el conjunto de las 6 caras, o de las 4 diagonales que unen vértices opuestos, ya que estos movimientos, llevan todo vértice a un vértice, toda cara a una cara, y toda diagonal a toda diagonal. Sean las acciones:

$$\varphi_v : G \to S_8 \quad g \mapsto g_v$$

$$\varphi_c : G \to S_6 \quad g \mapsto g_c$$

$$\varphi_d : G \to S_4 \quad g \mapsto g_d$$

siendo g_v, g_c, g_d las permutaciones inducidas por el movimiento g sobre el conjunto de los vértices, las caras, o las diagonales, respectivamente.

Notar que estas acciones son fieles y transitivas, por lo que G puede considerarse isomorfo a subgrupos transitivos de S_8, S_6 y S_4.

Además, consideremos por ejemplo la acción sobre el conjunto de las caras. Entonces, por el teorema 1.13, tenemos que el orden de G es igual al producto del tamaño de la órbita de un punto, por el orden de su estabilizador. Como la acción es transitiva, tenemos que $|i^G| = 6$, es la única órbita, con 6 puntos. Ahora bien, consideremos los movimientos rígidos del cubo que fijan una cara. Estos son 4 giros de $\pi/2$ (incluido la identidad) sobre el eje trazado uniendo el centro de dicha cara y la opuesta a ella. Así, tenemos que $|G| = |G_i||i^G| = 4$ x $6 = 24$, y obtenemos que hay 24 movimientos rígidos que fijan al cubo. Podríamos obtener esto mismo considerando también las otras acciones.

Ahora bien, notemos que, como $|S_4|$=24, y G es isomorfo a un subgrupo suyo, tenemos en particular que $G \cong S_4$, con lo que no vamos a poder verlo como subgrupo de ningún S_n con n < 4.

Ejemplo 9. Sea $H \leq G$, y $\Omega = \{Hx \mid x \in G\}$. La aplicación $\varphi : G \to S_\Omega$ dada por

$$\varphi(g) : Hx \mapsto Hxg \quad \forall x \in G$$

es una acción de G sobre el conjunto de coclases a derecha.

El núcleo de esta aplicación son los $g \in G$ tales que:

$$Hxg = Hx \ \forall x \in G \Leftrightarrow x^{-1}Hxg = x^{-1}Hx \ \forall x \in G \Leftrightarrow g \in x^{-1}Hx = H^x \ \forall x \in G$$

Así, $Ker(\varphi) = \cap_{x \in G} H^x$.

Definición. La acción de un grupo G sobre un conjunto Ω se dice que es **equivalente** a la acción de G sobre un conjunto $\overline{\Omega}$, si existe una biyección $\Omega \to \overline{\Omega}$ de modo que si llamamos $\bar{i}$ a la imagen de $i \in \Omega$, se tiene para todo $i \in \Omega$ y $g \in G$,

$$\overline{i^g} = \bar{i}^g$$

Observar que si tenemos dos acciones equivalentes el estabilizador de i es exactamente el mismo que el estabilizador de su imagen $\bar{i}$.

Teorema 3.3. *Sea G un grupo que actúa transitivamente sobre un conjunto Ω y sea $i \in \Omega$.*

La acción de G sobre Ω es equivalente a la acción de G sobre las coclases de G_i en G por multiplicación a derecha.

Demostración. Para cada $j \in \Omega$, existe $x \in G$ tal que $j = i^x$ por ser la acción transitiva. Veamos que la aplicación

$$\Omega \to \{G_i g \mid g \in G\} \qquad j \to G_i x$$

está bien definida y es biyectiva.

Si $j = i^x = i^y$, se tiene que $i^{xy^{-1}} = i$ luego $xy^{-1} \in G_i$, y así $G_i x = G_i y$, luego la aplicación está bien definida.

La aplicación es claramente suprayectiva y por ser la acción transitiva se tiene que el número de elementos de Ω que es la única órbita, es exactamente $|G|/|G_i| = |G : G_i| = |\{G_i g | g \in G\}|$, luego la aplicación es biyectiva.

Veamos ahora que las dos acciones son equivalentes. Para todo $j \in \Omega$ y $g \in G$, si $j = i^x$, la coclase que le corresponde a j es $G_i x = \overline{j}$ y la coclase que le corresponde a $j^g = i^{xg}$ es $G_i xg = \overline{j^g}$ que es exactamente $\overline{j}^g$.

□

Proposición 3.4. *Sea un grupo G y un subgrupo $H \leq G$, y consideremos la acción por multiplicación a derecha sobre las coclases a derecha de H. Entonces $H = G_H$.*

Observación 9. Notar que estamos considerando el estabilizador de H, entendido como elemento del conjunto de las coclases a derecha de H, es decir, como un punto.

Proposición 3.5. *Sean H, Y subgrupos de G. Las correspondientes acciones por multiplicación a derechas son equivalentes si y solo si H e Y son conjugados en G.*

Demostración.

$\Rightarrow$) Supongamos que las acciones son equivalentes. Sea entonces Hx la coclase que le corresponde a la coclase Y por la biyección entre conjuntos de puntos. Veamos cuales son sus estabilizadores:

$$g \in G_{Hx} \Leftrightarrow Hx = Hxg \Leftrightarrow xgx^{-1} \in H \Leftrightarrow g \in H^x$$

Además, el estabilizador de la coclase Y es el subgrupo Y, y como estos estabilizadores son iguales, tenemos que

$$Y = G_Y = G_{Hx} = H^x$$

y efectivamente H e Y son conjugados.

$\Leftarrow$) Sean ahora las acciones por multiplicación a derecha sobre las coclases de H y H^x. Veamos que son equivalentes.

Consideremos la aplicación dada por $Hg \mapsto H^x x^{-1} g$. Veamos que está bien definida:

$$Hg = Hy \Leftrightarrow gy^{-1} \in H \Leftrightarrow x^{-1}gy^{-1}x \in H^x \Leftrightarrow H^x x^{-1} g = H^x x^{-1} y$$

Sean Hy una coclase de H cualquiera, $g \in G$. Veamos por último que estas acciones son equivalentes:

$$\overline{(Hy)^g} = \overline{Hyg} = H^x x^{-1} yg = (H^x x^{-1} y)^g = (\overline{Hy})^g$$

□

Así, hemos obtenido que sea cual sea nuestra acción transitiva, esta es equivalente a la acción por multiplicación a derecha sobre las coclases de un estabilizador, y dado cualquier subgrupo H de G, la acción sobre las coclases de H tiene por estabilizador de un punto el propio H, es decir, también es una acción sobre las coclases de un estabilizador.

Es decir, estamos relacionando el estudio de cualquier acción transitiva que pueda tener un grupo G, con el estudio de sus subgrupos H, ya que toda acción será equivalente a una sobre las coclases de un subgrupo, y todo subgrupo define una acción.

Ahora bien, estas acciones no siempre serán fieles, para ser fieles se necesitará que el núcleo de estas acciones sea trivial, pero notar que como vimos en el ejemplo 9, el núcleo de la acción sobre las coclases de H por multiplicación a derecha es $\cap_{x \in G} H^x$. A este conjunto se le llamará Core de H en G, y lo denotaremos como

$$Core_G(H) = \cap_{x \in G} H^x$$

Así, si queremos estudiar las acciones que nos permiten relacionar un grupo asbtracto con un grupo de permutaciones por un isomorfismo, esto será lo mismo que estudiar los subgrupos de H de core trivial.

Recíprocamente, tenemos que el estudio de los grupos de permutaciones, será equivalente al estudio de pares de grupos (G,H) tales que $H \leq G$, y $Core_G(H) = 1$.

Proposición 3.6. *Sea $N \trianglelefteq G$ con $N \subseteq H$. Entonces $N \subseteq Core_G(H)$. Es decir, $Core_G(H)$ es el mayor subgrupo normal de G contenido en H.*

Demostración. Notar que $Core_G(H)$ es claramente un subgrupo normal de G, por ser el núcleo de una acción. Además, tenemos que $N = N^x \subseteq H^x \ \forall x \in G$. Luego $N \subseteq \cap_{x \in G} H^x = Core_G(H)$. □

Ejemplo 10. Siguiendo el grupos de los cuaternios del ejemplo 7, esto es Q_8, habíamos obtenido que este contenía a 4 subgrupos, todos normales. Así pues, si consideramos cualquier $1 \neq H \leq Q_8$, tenemos que $Core_{Q_8}(H) = H \neq 1$.

Así, la única acción fiel que va a tener este grupo, es la acción sobre las coclases de 1, esto es, la acción regular, con lo que no vamos a poder ver Q_8 como un subgrupo de S_n con n < 8.

Capítulo 4

Estructura y clasificación de los grupos primitivos

4.1. Grupos primitivos

Notar que ya poseemos una noción de grupos primitivos en el caso particular de los grupos de permutaciones. Para relacionar esta idea con grupos abstractos, nos ayudaremos de las acciones fieles.

Teorema 4.1. *Sea G un grupo. Las siguientes condiciones son equivalentes:*

1. *G es isomorfo a un grupo de permutaciones transitivo primitivo.*
2. *Existe un subgrupo maximal de G con core trivial.*

Demostración.

$\Rightarrow$) Tenemos que existe $\varphi : G \to S_\Omega$ acción fiel transitiva tal que $\varphi(G)$ es primitivo. Sea $i \in \Omega$. La acción es equivalente a la acción por multiplicación a derecha de las coclases de G_i. Además, $Core_G(G_i) = Ker(\varphi) = 1$, por ser φ fiel, y G_i será maximal por el teorema 2.10.

$\Leftarrow$) Sea U subgrupo maximal de G de Core trivial. Entonces consideremos la acción por multiplicación a derecha de las coclases de U. Esta acción es fiel, por ser $Core_G(U) = 1$, y transitiva, luego nuestro grupo es isomorfo a un grupo de permutaciones transitivo. Además, tenemos que $G_U = U$, que es maximal, y nuevamente por el teorema 2.10, tenemos que este grupo de permutaciones es primitivo.

□

Definición. Un **grupo primitivo** es un grupo isomorfo a un grupo de permutaciones primitivo. Equivalentemente, un grupo es primitivo si tiene un subgrupo maximal de core trivial.

Un **par primitivo** es un par (G, U), donde G es un grupo primitivo, y U es un subgrupo maximal de core trivial. Es más preciso hablar de pares primitivos, ya que cada clase de conjugación de un subgrupo maximal de core trivial nos dan acciones, equivalentes entre sí, fieles y transitivas, que nos darán isomorfismos a grupos de permutaciones sobre conjuntos distintos.

4.2. Teorema de Baer. Estructura de un grupo primitivo

A continuación daremos una clasificación de todos los grupos primitivos, debida a Reinhold Baer, según la estructura de sus grupos normales minimales, esto es, su socle.

Definición. El **zócalo o socle** de un grupo G, Soc(G), es el producto de todos sus subgrupos normales minimales.

Observación 10. Si tenemos dos subgrupos normales minimales distintos M y N, entonces $M \cap N = 1$, por ser $M \cap N$ normal, y además tanto M como N son normales en MN, por serlo en $G \supseteq MN$. Entonces $M \times N$ es isomorfo a MN. Así, en el caso del socle, es indistinto considerar el producto de grupos o el producto directo, es decir , si $N_1, N_2, \cdots, N_n$ son los subgrupos normales minimales de G, entonces:

$$Soc(G) = N_1 N_2 \cdots N_n \cong N_1 \times N_2 \times \cdots \times N_n$$

Proposición 4.2. *Sean $M, N \trianglelefteq G$ con $M \cap N = 1$. Entonces $M \leq C_G(N)$ y $N \leq C_G(M)$.*

Demostración. Para ello, veamos que para todo $m \in M$ y $n \in N$, se tiene que $nm = mn$.

Sean $m \in M, n \in N$ cualesquiera. Como M es normal, tenemos que $m^n \in M$, y así $m^{-1}m^n \in M$. Como N es normal, tenemos que $(n^{-1})^m \in N$, y así $(n^{-1})^m n \in N$. Pero como $m^{-1}m^n = (n^{-1})^m n$, y $M \cap N = 1$, se tiene que $m^{-1}n^{-1}mn = 1$, y así $mn = nm$. □

Teorema 4.3. *Teorema de Baer.*

1. *Un grupo G es primitivo si y solo si existe un subgrupo M de G tal que $G = NM$ para todos los subgrupos normales minimales N de G.*

2. *Sea G un grupo primitivo. Supongamos que U es un subgrupo maximal de core trivial de G y que N es un subgrupo normal minimal no trivial. Sea $C = C_G(N)$. Entonces $C \cap U = 1$, y además, o $C = 1$, o C es un subgrupo normal minimal de G.*

3. *Sea (G,U) un par primitivo. Entonces, se cumple una única de las siguientes condiciones:*

   a) *$Soc(G) = N$ es un subgrupo de G normal minimal abeliano autocentralizador, es decir, $N = C_G(N)$. Además, es complementado por U, es decir, $G = NU$ y $U \cap N = 1$.*

   b) *$Soc(G) = N$ es un subgrupo de G normal minimal no abeliano que es suplementado por U, es decir $G = NU$. En este caso $C_G(N) = 1$.*

   c) *$Soc(G) = N_1 \times N_2$, donde N_1 y N_2 son los dos únicos subgrupos normales minimales de G. Además, ambos son complementados por U, es decir, $G = N_1U = N_2U$ y $N_1 \cap U = N_2 \cap U = 1$. En este caso, $N_1 = C_G(N_2)$ y $N_2 = C_G(N_1)$, y N_1, N_2 y $N_1N_2 \cap U$ son grupos no abelianos isomorfos.*

Demostración.

1. $\Rightarrow$ Sea U un subgrupo maximal de G cuyo core es trivial. Sea N un subgrupo normal minimal de G. Entonces $N \nsubseteq U$, luego $U \neq UN$, pero como U es maximal y $U \subseteq UN$, entonces $NU = G$.

   $\Leftarrow$ Sea $M \leq G$ t.q. $G = NM \ \forall N \trianglelefteq G$. Sea U subgrupo maximal t.q. $M \leq U$. U no puede contener ningún subgrupo N normal minimal, ya que sino, si $M, N \leq U$, entonces $MN \leq U \neq G$. Así, U es un subgrupo maximal que no contiene ningún subgrupo normal de G, luego su core es trivial, y G es primitivo.

2. Sea $C = \{g \in G \mid n^g = n \ \forall n \in N\}$. Veamos que C es normal en G.

   Sea $g \in G, c \in C$. Tenemos que comprobar que $c^g \in C$. Sea $n \in N$, entonces

   $$(c^g)^{-1} n c^g = (n^{g^{-1}})^{cg} = n^{g^{-1}g} = n$$

   ya que $n^{g^{-1}} \in N$ por ser N normal. Así, C es normal en G, y por lo tanto $C \cap U$ es normal en U, es decir, $U \leq N_G(C \cap U)$.

   De igual forma tenemos que $C \cap U$ centraliza N, lo que significa que todos los elementos de $C \cap U$ conmutan con los de N, es decir, N centraliza también a $C \cap U$, $N \leq C_G(C \cap U) \leq N_G(C \cap U)$.

Pero, como $G = NU$, entonces $G \leq N_G(C \cap U)$, y también se da la igualdad, luego $C \cap U$ es normal en G.

Como $C \cap U$ es normal en G y $C \cap U \subseteq U$, tenemos $C \cap U = 1$.

Supongamos que $C \neq 1$. Sea entonces X un subgrupo normal minimal t.q. $X \leq C$. Entonces, por el apartado 1, tenemos que $G = XU$. Así, $C = C \cap XU = X(C \cap U) = X$, por la ley de Dedekind 1.5. Por lo tanto, tenemos que, o C=1, o C es un subgrupo normal minimal .

3. Supongamos que N_1, N_2 y N_3 son tres subgrupos normales minimales distintos. La intersección de dos subgrupos normales, es un subgrupo normal, pero como los N_i son normales minimales, entonces tenemos que $N_1 \cap N_2 = N_1 \cap N_3 = N_2 \cap N_3 = 1$. Así, por el lema, $N_2, N_3 \leq C_G(N_1)$, y por lo tanto $N_2N_3 \leq C_G(N_1)$, pero, como $N_2 \cap N_3 = 1$, entonces $N_2, N_3 \subsetneq N_2N_3$, pero por el apartado 2, $C_G(N_1)$ tendría que ser normal minimal. Luego, en un grupo primitivo, existen como mucho 2 subgrupos normales minimales.

   a) Supongamos que N es un subgrupo abeliano de G normal minimal no trivial. Entonces $N \leq C_G(N)$, pero como por el apartado 2, este es normal minimal, se tiene que $N = C_G(N)$, y así tenemos que N se autocentraliza, y por los apartados anteriores $G = NU$ y $N \cap U = C_G(N) \cap U = 1$.

      Además, si tiene un subgrupo abeliano normal minimal, no puede tener ningún otro subgrupo normal minimal, porque estaría contenido en $C_G(N) = N$.

   b) Si existe un único subgrupo N normal minimal no abeliano, entonces $G = NU$, y como $C_G(N) \neq N$, por no ser N abeliano, y $C_G(N)$ no puede ser un subgrupo normal minimal distinto de N tampoco, entonces $C_G(N) = 1$ por el apartado 2.

   c) Si existen dos subgrupos normales minimales N_1 y N_2, entonces $N_1 \cap N_2 = 1$, y así $N_1 \leq C_G(N_2)$, $N_2 \leq C_G(N_1)$ por la proposición 4.2, pero como estos son normales minimales por el apartado 2, tenemos que $N_1 = C_G(N_2)$ y $N_2 = C_G(N_1)$.

      Ahora, por los apartados anteriores, tenemos que $N_1 \cap U = C_{N_2} \cap U = 1$ y $N_2 \cap U = C_G(N_1) \cap U = 1$, y también $G = N_1U = N_2U$. Notar que como $N_1 = C_G(N_2)$, entonces $N_2 \nsubseteq C_G(N_2)$, y obtenemos tambien que N_2 no puede ser abeliano, y de forma análoga N_1 tampoco podría serlo, lo cual es coherente con la última observación en a).

      Finalmente, como $N_1, N_2 \subseteq N_1N_2$, y $G = N_1U = N_2U$ se tiene, por la ley de Dedekind:

$$N_1(N_1N_2 \cap U) = N_1N_2 \cap N_1U = N_1N_2 = N_1N_2 \cap N_2U = N_2(N_1N_2 \cap U)$$

      y ahora, por el segundo teorema de isomorfía, y por la ley de Dedekind otra vez:

$$N_1 \cong N_1/(N_1 \cap N_2) \cong N_1N_2/N_2 = N_2(N_1N_2 \cap U)/N_2 \cong N_1N_2 \cap U$$

      y de forma análoga también $N_2 \cong N_1N_2 \cap U$.

□

Esto nos proporciona una clasificación de los grupos primitivos en 3 tipos distintos.

Definición. Sea G un grupo primitivo, este se dice:

1. un grupo primitivo de **tipo 1** si tiene un subgrupo normal minimal abeliano.
2. un grupo primitivo de **tipo 2** si tiene un único subgrupo normal minimal no abeliano.
3. un grupo primitivo de **tipo 3** si tiene dos subgrupos normales minimales no abelianos distintos.

4.3. Ejemplos

A continuación, daremos ejemplos de todos los tipos de grupos primitivos.

Ejemplo 11. Sea S un grupo simple no abeliano, y sea $M \leq S$ maximal cualquiera. Como S es simple, no contiene ningún subgrupo normal, y por extensión M tampoco, luego $Core_S(M) = 1$. Así, todo grupo simple será primitivo. Además, como S no contiene subgrupos normales, tenemos que el propio S será un subgrupo normal minimal en S, el único, el cual no es abeliano, luego todo grupo simple es primitivio de tipo 2. Finalmente notar que claramente S suplementa a M, ya que $SM = S$, y que el centralizador de S es 1, porque no es el propio S, al ser este no abeliano, y como $C_S(S) \trianglelefteq S$, entonces este tiene que ser 1, al ser S simple.

Ejemplo 12. Consideremos el diédrico de orden 10, $G = D_{10}$, que es primitivo. Los subgrupos de este grupo, son el subgrupo generado por cualquier giro, $\langle \alpha^i \rangle$, todos de orden 5, y los subgrupos generados por una simetría $\langle \alpha^i \beta \rangle$, de orden 2. Notar que si generamos un grupo con dos simetrías, obtenemos un giro y con ello el resto de giros y simetrías, y si lo generamos con una simetría y un giro, también obtenemos el diédrico D_{10}. Así, estos son los únicos subgrupos de D_{10}.

En este teníamos el estabilizador de un elemento, por ejemplo $G_3 = \langle \beta \rangle$, que es maximal, y además tenemos $Core_G(G_3) = \cap_{\gamma \in G} G_3^\gamma = 1$, ya que, por ejemplo $G_3^\alpha = \langle \alpha^3 \beta \rangle$, y este se corta trivialmente con $G_3 = \langle \beta \rangle$.

Todos los subgrupos propios de D_{10} son minimales, ya que no hay ninguno propiamente contenido en otro. Sin embargo, los estabilizadores, es decir, los generados por una simetría cualquiera, no son normales, puesto que son conjugados unos de otros, pero $\langle \alpha \rangle$ si que es un subgrupo normal, ya que es un subgrupo de índice 2. Así, tenemos que $Soc(D_{10}) = \langle \alpha \rangle$, y además como este es cíclico, tenemos que el socle es un subgrupo normal minimal abeliano. Es decir, este es un grupo primitivo de tipo 1.

Notar que $C_G(\langle \alpha \rangle) = \langle \alpha \rangle$, puesto que las simetrías no conmutan con los giros, y tenemos que se autocentraliza. Además, tenemos que $\langle \alpha \rangle G_3 = \langle \alpha \rangle \langle \beta \rangle = G$, y $\langle \alpha \rangle \cap G_3 = 1$. Así, $\langle \alpha \rangle$ complementa a G_3.

Para el siguiente ejemplo nos ayudaremos del siguiente resultado:

Lema 4.4. *Sea G un grupo. Consideremos $D = \{(g,g) \mid g \in G\} \leq G \times G$. Sea $D \leq H \leq G \times G$ un subgrupo contenido entre D y $G \times G$. Entonces existe $N \trianglelefteq G$ t.q. $H = \{(a,b) \in G \times G \mid ab^{-1} \in N\}$.*

Demostración. Sea $N = \{g \in G \mid (g,1) \in H\}$. Como H es un subgrupo, tenemos que N es también un subgrupo. Veamos que este es normal en G.

Si $g \in N$ y $h \in G$, entonces, como $(g,1) \in H$ y $(h,h), (h^{-1},h^{-1}) \in D \leq H$, tenemos que:

$$(h^{-1}gh, 1) = (h^{-1},h^{-1})(g,1)(h,h) \in H$$

y así $h^{-1}gh \in N$, y tenemos que N es un subgrupo normal de G.

Además, para todos $g,h \in G$, tenemos que $(gh^{-1},1)(h,h) = (g,h)$, luego $(g,h) \in H \Leftrightarrow gh^{-1} \in N$. Con esto, obtenemos una correspondencia biyectiva entre los subgrupos normales de G, y los subgrupos contenidos entre D y $G \times G$. □

Observación 11. En caso de que G sea simple, los únicos subgrupos normales que contiene son 1 y G, los cuales se corresponden con $H = D$ y $H = G \times G$, respectivamente. Luego en este caso, D será un subgrupo maximal de $G \times G$.

Ejemplo 13. Consideremos $G = S \times S$, siendo S un grupo simple no abeliano. Consideremos $D = \{(g,g) \mid g \in S\}$. Por la obervación 11, tenemos que D es maximal en G. Además, como D es isomorfo a S simple, tenemos que D también es simple, y no contiene ningún subgrupo normal en D, y por lo tanto tampoco en G. Finalmente, notemos que como S no es abeliano, el propio D tampoco será normal en G, y así, tenemos que $Core_G(D) = 1$, y tenemos que $S \times S$ es primitivo.

Ahora, veamos cuales son los subgrupos normales de G. Como G es un producto directo, está claro que tiene dos subgrupos normales, que son $N_1 = 1 \times S$ y $N_2 = S \times 1$, y como G es primitivo, estos serán los únicos. Es decir, $S \times S$ es un grupo primitivo de tipo 3.

Notar que $N_1 D = N_2 D = G$, ya que dado un $(g,h) \in G$, entonces:

$$(gh^{-1},1)(h,h) = (g,h) = (1,hg^{-1})(g,g)$$

También, tenemos que $N_1 \cap D = N_2 \cap D = N_1 \cap N_2 = 1$. Así, tenemos que los dos subgrupos normales minimales complementan al maximal.

Finalmente, notemos que $C_G(N_1) = N_2$ y $C_G(N_2) = N_1 S$, ya que, por lo que vimos en el ejemplo 11, no hay ningún elemento de un grupo simple que conmute con todos los demás, y así los únicos elementos que conmutan con todos los elementos de la forma (g,1) con $g \in S$, serán los (1,h) con $h \in S$.

Finalmente, notar que N_1 y N_2 son isomorfos, ya que son isomorfos a S, y $N_1 N_2 \cap D = D$, el cual también es isomorfo S, tomando por ejemplo el isomorfismo $\varphi : S \to D$ dado por $g \mapsto (g,g) \ \ \forall g \in S$.

A continuación, daremos un par de ejemplos de productos semidirectos de grupos. Para ayudarnos, daremos un resultado, acerca de determinados subgrupos de estos.

Lema 4.5. *Sea $G = [N]_\varphi H$ el producto semidirecto de los grupos N y H vía $\varphi : H \to Aut(N)$. Entonces, los subgrupos $M \leq G$ t.q. $H \leq M$, son grupos de la forma UH, con $U \leq N$.*

Demostración. Sea un subgrupo M de G t.q. $H \leq M$, entonces $M \cap N$ es un subgrupo de G normal en M. Veamos que $(M \cap N)H = M$.

Así, como $M \cap N \trianglelefteq M$ y $H \leq M$, entonces $(M \cap N)H \leq M$, y aplicando la ley de Dedekind 1.5, tenemos que $(M \cap N)H = M \cap NH = M \cap G = M$. □

Ejemplo 14. Sea $G = [A_5 \times A_5]_\varphi C_2$ con $C_2 = \langle \beta \rangle$ y $\varphi(\beta)(\gamma,\delta) = (\delta,\gamma)$ para todos $\gamma, \delta \in A_5$.

A diferencia de lo que pasaba en el grupo diédrico, aquí C_2 no nos servirá como subgrupo maximal, pero si que podremos considerar uno que lo contenga. Como vimos en el lema 4.5, los subgrupos que contengan a C_2, serán de la forma HC_2 con $H \leq A_5 \times A_5$, y para que estos sean un grupo, podemos considerar por ejemplo $H \leq C_G(C_2)$. Notar que $(\alpha,\alpha)^\beta = (\alpha,\alpha)$, es decir β está en el conmuta con los elementos diagonales, los elementos con la misma permutación en ambas componentes.

Así, consideremos $H = D = \{(\alpha,\alpha) \mid \alpha \in A_5\}$. Como vimos en el anterior ejemplo, D es maximal en $A_5 \times A_5$, por ser A_5 simple. Así, tenemos que DC_2 será un subgrupo, maximal en G.

Veamos ahora que no contiene ningún subgrupo normal.

Notemos primero, que el propio DC_2 no es normal, ya que si consideramos por ejemplo $\beta \in D_2$, y un $1 \neq \alpha \in A_5$ cualquiera de orden distinto de 2, entonces, como $\beta^{(\alpha,1)} = (\alpha^{-1},1)\beta(\alpha,1) = (\alpha^{-1},\alpha)\beta$ que no está en DC_2, tenemos que DC_2 no es normal en G.

Los subgrupos de DC_2 serán de la forma H o HC_2 con $H \leq C_2$, según esté o no el elemento β en ellos. Si consideramos H, como D es simple por ser isomorfo a A_5, entonces H no será normal en D, y por lo tanto tampoco lo será en G. Por su parte, $\beta \in HC_2$, y ya vimos que este al conjugarlo con algún elemento de G, no estaba en DC_2, y por tanto tampoco en HC_2, y así este tampoco podrá ser normal.

Con todo esto, vemos que no hay ningún subgrupo normal contenido en DC_2, y así $Core_G(DC_2) = 1$ y como es maximal, obtenemos que G es primitivo.

Notemos ahora que $A_5 \times A_5$ es normal en G trivialmente, por ser G producto semidirecto de él. Para ver si hubiera algún otro subgrupo normal en G, veamos como es su centralizador en G, el cual por el apartado 2 será un subgrupo normal, sea trivial o no, lo cual nos dirá así mismo de que tipo es el grupo primitivo G.

Notar que β solo conmuta con los elementos diagonales de $A_5 \times A_5$, y así mismo, no hay ningún elemento de $A_5 \times A_5$ que conmute con todos ellos. Así, no va a haber ningún elemento de G que conmute con todos los de $A_5 \times A_5$, y así tenemos que $C_G(A_5 \times A_5) = 1$, luego $A_5 \times A_5$ será el único subgrupo normal minimal, y deducimos que G es un grupo primitivo de tipo 2.

El único subgrupo normal minimal, $A_5 \times A_5$, no es abeliano, tiene centralizador trivial, y suplementa al maximal DC_2, ya que $(A_5 \times A_5)(DC_2) = G$ y $(A_5 \times A_5) \cap (DC_2) = D \neq 1$.

Ejemplo 15. Sea U un grupo primitivo de tipo 2, y sea N el único subgrupo normal minimal no abeliano que contiene. Consideremos $\varphi : U \to Aut(N)$ de forma que para todo $g \in U$, tenemos $\varphi(g) : N \to N$ dada por $n \mapsto n^g \ \ \forall n \in N$. Estos automorfismos están bien definidos, porque N es normal en U. Entonces, podemos considerar el producto semidirecto de N por U vía φ, esto es, $G = [N]_\varphi U$.

Veamos que U es maximal de G. Sea $U \leq M \leq G$, entonces, por el lema, tenemos que M se puede escribir de la forma VU, con algún $V \leq N$. Pero, para que VU sea un grupo, se tiene que dar que:

$$VU = UV = \{(1,u)(v,1) \mid (1,u) \in U, (v,1) \in V\}$$

Pero $(1,u)(v,1) = (v^{u^{-1}}, u)$, y así:

$$(1,u)(v,1) \in VU \Leftrightarrow v^{u^{-1}} \in V$$

Luego $UV = VU$ si y solo si V es normal en U, ya que de esta forma se da que $VU \supseteq UV$, y se tiene la igualdad porque son del mismo tamaño.

Ahora, veamos que $Core_G(U) = 1$. Notar que $U = \{(1,g) \mid g \in U\}$ si lo miramos como subgrupo de G. Para ello, estudiemos los conjuntos de la forma U^h con $h \in G$. En particular, tomemos $h = (n,1)$ con $n \in N$. Entonces los elementos de U^h son de la forma

$$(n,1)^{-1}(1,g)(n,1) = (n^{-1},1)(1,g)(n,1) = (n^{-1},g)(n,1) = (n^{-1}n^{g^{-1}},g) \quad con \quad g \in U$$

Para que tenga intersección no trivial con U, necesitamos elementos en los que la primera componente sea 1, esto es $n^{-1}n^{g^{-1}} = 1$, y esto solo ocurre si $n \in N$ conmuta con $g \in U$, pero como U es primitivo de tipo 2, tenemos que $C_U(N) = 1$. Así $U \cap U^{(h,1)} = 1$, luego $Core_G(U) = 1$ y tenemos la primitividad de G.

Veamos ahora cuales son sus subgrupos normales minimales. Por ser producto semidirecto, tenemos que $N_1 = \{(n,1) \mid n \in N\}$ es un subgrupo normal de G. Además, no contiene más subgrupos normales de G en él, ya que sino podríamos construir subgrupos propios de G que contuvieran a U por producto, y tenemos que N_1 es normal minimal.

Para ver cual si contiene algún otro subgrupo normal, estudiaremos el centralizador de N_1 en G. Si este fuera trivial, tendríamos que sería el único subgrupo normal minimal, y G sería de tipo 2, y si su centralizador es un subgrupo normal mininmal propio, tendremos que G será primitivo de tipo 3.

$C_G(N_1) = \{g \in G \mid gn = ng \ \forall n \in N_1\}$. Sea $g = (a,b)$ con $a \in N, b \in U$, $(n,1) \in N_1$ con $n \in N$. Entonces:

$$(a,b)(n,1) = (an^{b^{-1}},b) \quad y \quad (n,1)(a,b) = (na,b)$$

y así,

$$(a,b)(n,1) = (n,1)(a,b) \Leftrightarrow an^{b^{-1}} = na \Leftrightarrow n^{b^{-1}a^{-1}} = n$$

pero como $C_U(N) = 1$, esto se tiene si y solo si $a = b^{-1}$. Es decir, tenemos que $N_2 = \{(n,n^{-1}) \mid n \in N\}$ será nuestro segundo subgrupo normal minimal.

Para empezar, veamos como son los elementos inversos en G. Sea $(n,g) \in G$, entonces:

$$(n,g)(a,b) = (na^{g^{-1}},gb) = (1,1) \Leftrightarrow na^{g^{-1}} = 1 \ \ y \ \ gb = 1 \Leftrightarrow a = (n^{-1})^g \ \ y \ \ b = g^{-1}$$

Es decir $(n,g)^{-1} = ((n^{-1})^g, g^{-1})$.

Ahora comprobemos que N_2 es un subgrupo normal. Sean $(a,a^{-1}),(b,b^{-1}) \in N_2$. Entonces:

$$(a,a^{-1})(b,b^{-1}) = (ab^a, a^{-1}b^{-1}) = (ba, a^{-1}b^{-1}) \in N_2$$

$$(a,a^{-1})^{-1} = ((a^{-1})^{a^{-1}},a) = (a^{-1},a) \in N_2$$

Con lo que obtenemos que N_2 es un subgrupo de G.

Veamos que este es normal. Sean $(a,a^{-1}) \in N_2$, $(b,c) \in G$. Entonces:

$$(b,c)^{-1}(a,a^{-1})(b,c) = ((b^{-1})^c, c^{-1})(a,a^{-1})(b,c) = ((b^{-1})^c a^c, c^{-1}a^{-1})(b,c) =$$

$$= ((b^{-1})^c a^c b^{ac}, c^{-1}a^{-1}c) = ((b^{-1}ab^a)^c, (a^{-1})^c) = (a^c, (a^{-1})^c) = (a^c, (a^c)^{-1}) \in N_2$$

Con lo que obtenemos la normalidad de N_2.

Así mismo, tendremos que $C_G(N_2) = N_1$. Sea $(n,g) \in G$, $(a,a^{-1}) \in N_2$. Entonces:

$$(n,g)(a,a^{-1}) = (na^{g^{-1}}, ga^{-1}) \quad y \quad (a,a^{-1})(n,g) = (an^a, a^{-1}g)$$

y así,

$$(n,g)(a,a^{-1}) = (a,a^{-1})(n,g) \Leftrightarrow na^{g^{-1}} = an^a \;\; y \;\; ga^{-1} = a^{-1}g$$

Pero como $C_U(N) = 1$, entonces como $a^{-1} \in N$, tenemos que $g = 1$. Así, si $g = 1$, la primera condición se reduce a $na = an^a = na$, la cual se da para todo $n \in N$, con lo que obtenemos que efectivamente $C_G(N_2) = N_1$.

Veamos ahora que N_1 y N_2 complementan a U. Efectivamente $N_1U = G$, por la propia definición del producto semidirecto, además para cualquier $(n,h) \in G$ tenemos que $(n,h) = (n,n^{-1})(1,nh) \in N_2U$, y así $N_2U = G$. También tenemos que $N_1 \cap U = N_2 \cap U = N_1 \cap N_2 = 1$.

Finalmente para los isomorfismos, notemos que efectivamente, tanto N_1 como N_2 son isomorfos a N, y además $N_1N_2 \cong N \times N$, y $N_1N_2 \cap U \cong 1 \times N \cong N$.

Bibliografía

[1] ALLENBY, R. (1991). *Rings, Fields and Groups: An Introduction to Abstract Algebra*. Edward Arnold.

[2] BALLESTER-BOLINCHES, A., Y EZQUERRO L. M. (2006). *Classes of Finite Groups*. Springer.

[3] LANG, S. (1992). *Algebra*. Addison-Wesley.

[4] TIGNOL, J. (2001). *Galois' Theory of Algebraic Equations*. World Scientific Publishing Company.

[5] WIELANDT H. (1968). *Finite permutations groups*. Academic Paperbacks.