Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Grupos Nilpotentes y Funciones Zeta

Autor: Alberto Martínez Díez

Tutor/es: Antonio Campillo

Índice general

Introducción

En este trabajo vamos a centrarnos en comprender qué es un grupo nilpotente y las utilidades matemáticas que nos ofrece. Este concepto se le atribuye a Sergei Chernikov en la década de 1930, que tendra gran relevancia a posteriori tanto en la clasificación de grupos, teoría de Galois y para los τ-grupos, que tienen gran relevancia en la función Zeta de grupos. Esta función Zeta ha sido impulsada por el desarrollo de D. Segal, F. Grunewald y M. du Satoy.

Para entender qué es un grupo nilpotente desarrollaremos la teoría de grupos necesaria, añadiendo los teoremas de Sylow. Buscando información sobre este tema, llegué a la teoría de Polya. Decidí introducirla porque es otro claro ejemplo de la utilidad del concepto de acción de grupo.

Las utilidad del concepto de grupo nilpotente se va a ir viendo durante este trabajo. El teorema de estructura de grupos nilpotentes finitos muestra explícitamente las propiedades importantes que tienen estos grupos, de los que se puede decir que son la clase de grupos más sencillos de comprender después de los abelianos. En particular la propiedad de que los grupos de Sylow son normales y que es producto directo de sus subgrupos de Sylow es especialmente relevante. El teorema de la estructura de los grupos finitos abelianos que he incluido en este trabajo, lo demostraremos utilizando este concepto.

También hablaremos de la hipótesis de Rienmann, de su función Zeta de Rienmann y de la hipótesis de Rienmann generalizada. Nosotros la trataremos un poco fuera del punto de vista del análisis complejo y más cercano al algebraico, ya que cualquier desarrollo de las funciones zeta a este nivel excede el contenido de este trabajo. Hablaremos de la función Zeta de un grupo y aquí veremos otra de las utilidades de los grupos nilpotentes: Sabemos que si el grupo es uno de los llamados τ-grupo cumple muchas propiedades deseables que nos facilitan el trabajo con su función Zeta de grupo. Utilizaremos esta noción de función zeta más bien como curiosidad y motivación para la selección de los contenidos de teoría de grupos para el trabajo.

Capítulo 1

Acciones de grupos sobre conjuntos

1.1. Conceptos previos

Vamos a empezar desde lo más básico de este trabajo, hablando de la noción de grupo.

Definición 1.1. *Dado G un conjunto no vacío y $\cdot$ una operación binaria definida en G, G es un* ***grupo*** *si se cumple:*

1. *La operación $\cdot$ es una* ***operación interna****, es decir, toma dos elementos de G y los lleva a otro elemento también de G. Es decir $\cdot$ tiene esta forma:*

$$\cdot : G \times G \to G \tag{1.1}$$

2. *La operación toma la* ***propiedad asociativa****, es decir, dado tres elementos g,h y k en G se cumple que:*

$$(g \cdot h) \cdot k = g \cdot (h \cdot k) \tag{1.2}$$

3. *G tiene un único elemento llamado* ***elemento neutro o identidad*** *denotado como e, con la siguiente propiedad: para todo g en G:*

$$e \cdot g = g \cdot e = g \tag{1.3}$$

4. *Todo elemento de g en G tiene un* ***elemento inverso*** *en el mismo G, que se denota por g^{-1} y se lee ïnverso de gçon la propiedad de que:*

$$g \cdot g^{-1} = g^{-1} \cdot g = e \tag{1.4}$$

Observación 1.2. Si nos fijamos,la operación no tiene por que ser conmutativa, es decir que $g \cdot h = h \cdot g$ no se cumple en principio. Si se cumpliera para todo g y h $g \cdot h = h \cdot g$ lo llamariamos **grupo abeliano o conmutativo**.

Aunque en general este trabajo hable de grupos sin ninguna restricción, nos centraremos sobre todo en la parte de grupos finitos, es decir, en los que el conjunto G sea finito. Sobre todo, cuando profundicemos sobre el concepto de p-grupo, necesitaremos resultados que necesitan la condición de grupo finito.

Hay otro concepto que es el de **grupo de generación finita** que no hay que confundir con grupo finito.

Definición 1.3. *Un **grupo de generación finita** G es un grupo que tiene un conjunto S finito tal que cada elemento de G se puede escribir como una combinación (bajo la operación del grupo) de elementos de S o de elementos inversos de S*

Todo grupo finito G es un grupo de generación finita ya que el conjunto G es finito y se genera a él mismo. Pero el recíproco es falso. Por ejemplo los números enteros $\mathbb{Z}$ es un grupo infinito con la suma, pero esta generado por {1}, ya que para cualquier n positivo es sumar n veces el 1. Y para un n negativo es sumar n veces el inverso de 1 (en el caso de la suma se llama opuesto).

Vamos a definir cuando dos grupos son equivalentes, para ello necesitamos la siguiente definición:

Definición 1.4. *Dados dos grupos (G,·) y (H,+), un **homomorfismo de grupos** es una aplicación ϕ:G $\rightarrow$ H que verifica:*

$$\phi(g') = \phi(g) + \phi(g) \text{ para todo g,g' de } G$$

Se dice que el homomorfismo mantiene la estructura algebraica, y si la aplicación ϕ es una biyección, se dice que existe un isomorfismo de grupos y la única diferencia entre ellos es la notación que hemos utilizado para denotarlos.

Vamos a dar una relación de equivalencia muy importante en la teoría de grupos y que más adelante veremos su utilidad.

Definición 1.5. *Dos elementos g y g' de un grupo G se dice que estan conjugados si y solo si:*

$$g' = h^{-1} \cdot g \cdot h \text{ para algun } h \text{ en } G.$$

Esta relación es una relación de equivalencia, y por ello se puede hacer una partición de G en clases. La clase de un elemento g la denotaremos la clase de conjugación de g.

Vamos a definir uno de los grupos más importantes en nuestra teoría:

Definición 1.6. *El **grupo simétrico** o S_n es un grupo cuyos elementos son las biyecciones de n elementos y su operación es la composición de funciones.*

Aunque sea un tema importante vamos a dar unos resultados sobre el grupo simétrico sin probarlos, ya que no es el tema central del trabajo pero si los necesitamos.

Observación 1.7.

1. Sabemos que el cardinal las biyecciones de n elementos es n! por lo que $|S_n| = n!$

2. Todo elemento de S_n se escribe de manera única (salvo orden de factores) como un producto de ciclos disjuntos.

3. El grupo simétrico S_n está generado por n-1 trasposiciones simples

4. Las clases de conjugación de S_n corresponden a la estructura de ciclos disjuntos, es decir, dos elementos son conjugados si y solo si tienen el mismo número de ciclos disjuntos y del mismo tamaño

Aunque no es estrictamente necesario hablar de acciones de grupo para abarcar lo que queremos ver, me gusta incluirlo en el trabajo ya que es una herramienta muy útil, muchas veces bastante visual y ofrece demostraciones muy bonitas, que veremos a lo largo del trabajo. Además simplifica muchas demostraciones posteriores.

1.2. Acciones de grupo

Definición 1.8. *Una **acción de un grupo** G, con operación $\cdot$ sobre un conjunto X, es una aplicación $\phi : G \times X \longrightarrow X$ que cumple:*

$$\textit{para todo } x \in X \ \phi(e, x) = x$$

$$\textit{para todo } x \in X \ g, h \in G, \ \phi(g \cdot h, x) = \phi(g, \phi(h, x))$$

En este caso, se dice que G actúa sobre X.

Observación 1.9. Para simplificar la notación en vez de denotra ϕ la función, la denotaremos mediante un punto o sin añadir nada: $\phi(g, x) = g \cdot x = gx$ y se lee "g actuando sobre x".

También hay otra definición de acción equivalente que nos da otra manera de ver lo que es una acción de grupo: Para todo g en G la biyección $\phi_g = \phi(g, \cdot) : X \longrightarrow X$ podemos verla como un elemento de S_X.

Una aplicación ϕ: $G \times X \to X$ es una acción de un grupo G sobre X si la aplicación ψ que a cada g de G le asocia un elemento del grupo de permutaciones de X es un homomorfismo de grupos.

$$\psi : G \to S_X$$

Es claro que si se cumple la primera definición se cumple que ψ es un homomorfismo de grupos, por las dos propiedades dadas. Y al revés también es fácil ver que por ser homomorfismo se cumple las dos propiedades.

Vamos a dar un par de ejemplos para clarificar y visualizar que significa exactamente una acción sobre un grupo:

Ejemplo 1.10. Cada elemento de nuestro conjunto X va a ser los vértices de un triángulo equilátero (ver figura 1.1) X={1,2,3} siendo 1 el vértice de color azul. Nuestro conjunto G va a ser el grupo diedral o grupo de rotaciones y simetrías que dejan al triangulo invariante (pero no tiene porque dejar los vértices invariantes) denotado D_3. Este grupo está generado por r, podemos verlo como una rotación de 120^{o} y por s, podemos verlo como una simetría respecto de un eje de simetría. Lo podemos definir mediante sus generadores y sus restricciones:

$$D_n =< r, s \quad | \quad r^n = 1, s^2 = 1, srs^{-1} = r^{-1} >$$

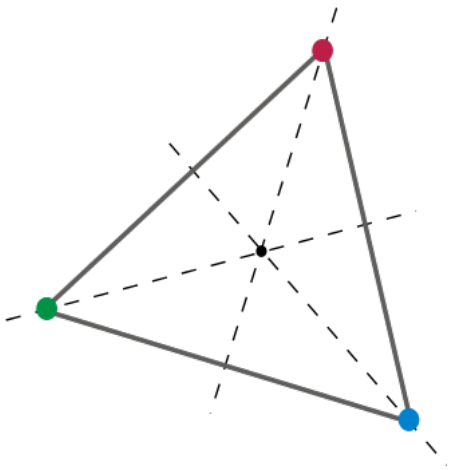

Figura 1.1: Acciones sobre el triangulo.

Intuitivamente lo que va a ser la acción podemos resumirlo en: si aplicamos r vamos a rotar los vértices en sentido contrarios a la aguja del reloj, es decir cada vértice se tralada al siguiente teniendo en cuenta el orden del sentido contrario de las agujas del reloj. Si aplicamos s queremos realizar la simetría respecto al vértice 1 que en la figura es el coloreado azul. Es decir el rojo y el verde se intercambiarían pero el azul seguiría estable.

Podríamos definir la acción por:

$$\psi : D_3 \longrightarrow S_X$$

$$\psi(r) = (123) \quad \psi(s) = (23)$$

Vemos que $(\psi(r))^3 = 1$ y que $(\psi(s))^2 = 1$. Con estas igualdades ya sabemos la imagen de todo D_3 ya que ψ es un homomorfismo de grupos.

Podemos repetir este ejemplo con cualquier polígono y con el grupo D_n siendo n el número de lados.

Las dos formas de ver una acción de un grupo, nos va a dar una demostración muy bella del teorema de Cayley. El teorema de Cayley dice que todos los grupos son isomorfos a un subgrupo de un grupo de permutaciones.

Demostración. Tomemos un grupo G cualquiera, y como conjunto X tomamos el mismo G. La aplicación que vamos a dar a esta acción es la multiplicación por la derecha en el propio grupo . Se comprueba facilmente que es una acción gracias a las propiedades de grupo. Con esto tenemos un homomorfismo de G hacia el grupo de permutaciones de G. El núcleo de este homomorfismo es el elemento neutro de G, por las propiedades de grupo.Si restringimos la llegada a la imagen de nuestro homomorfismo llegamos a que es un isomorfismo, es decir, que el grupo G es isomorfo a la imagen de nuestro homomorfismo, que es un subgrupo del grupo de permutaciones de G. □

Observación 1.11. Volvemos a tomar un grupo G cualquiera, y de nuevo como conjunto X tomamos el mismo G. Ahora como aplicación definimos $x \cdot g = g^{-1}xg$ llamado conjugado de x por g. Si buscamos el núcleo del homomorfismo de G hacia el grupo de permutaciones de G : g $\in G$ tal que $g^{-1}xg = x$ que son los mismo que $xg = gx$. El núcleo por lo tanto, son los elementos del grupo que conmutan con todo el grupo, es el conocido centro del grupo G denotado Z(G).

Lo que buscamos de las acciones es que nos permitan poder contar cosas, para ello vamos a dar varias definiciones que nos permitirá llegar a fórmulas muy interesantes como: la ecuación de clases o la fórmula de Burnside.

Definición 1.12. *Estabilizador de un punto $x \in X$, $Estab_G(x)$ es el conjunto de los elementos de G tal que para el x fijado se cumpla $g \cdot x = x$*

Es fácil ver que para cada punto de X , $Estab_G(x)$ es un subgrupo de G. En la acción de la demostración 1.2 , cuando tomamos X=G, vemos que para todo x $\in G$ $Estab_G(x)$ es el grupo trivial, ya que si existiese un elemento que no fuera el trivial en $Estab_G(x)$ se incumplirían las propiedades de grupo.

Pero en la acción de la observación 1.5, la de la conjugación, $Estab_G(x) = C_G(x)$

que es el centralizador de x (que es el subgrupo de G cuyos elementos conmutan con x).

En nuestro ejemplo del triángulo, el único elemento no trivial que nos fija un vértice V es la simetría respecto a la altura de V. Por lo que es el subgrupo de dos elementos.

Definición 1.13. *Dada una acción de G en X, la* ***órbita*** *de x está definida por:*

$$O_x = \{g \cdot x \text{ tal que } g \in G\} \tag{1.5}$$

El conjunto de órbitas lo denotamos X/G

Es obvio que cada punto está en al menos una órbita, y es fácil ver que las órbitas son iguales o disjuntas. Por lo que las órbitas son una partición de X.

Definición 1.14. *Los* ***puntos fijos*** *en X, o $Fix_G(X)$, son los siguientes:*

$$Fix_G(X) = \{x \in X \text{ tal que } g \cdot x = x \text{ para todo } g \in G\} \tag{1.6}$$

De manera análoga podemos definir $Fix_g(X) = Fix(g) = \{x \in X \text{ tal que } g \cdot x = x\}$

Teniendo en cuenta que X tenga un número de elementos finitos podemos realizar el siguiente razonamiento:

Como sabemos X se particionan en las órbitas, podemos calcular $|X|$ de la siguiente manera: calcular cuántas órbitas tienen bajo la acción de G y luego calculamos el cardinal de cada órbita. Podemos ver que el conjunto de $Fix_G(X)$ es una órbita, y es la órbita formada por un único punto. Podemos verlo en una ecuación:

$$|X| = |Fix_G(X)| + \sum_{O_x \text{ no unipuntual}} |O_x| \tag{1.7}$$

Esta ecuación la podemos aplicar a un ejemplo concreto como es el de la observación 1.11 en la que los puntos fijos son el centro del grupo Z(G) y la ecuación se llama **ecuación de clase**:

$$|G| = |Z(G)| + \sum_{O_x \text{ no unipuntual}} |O_x| \tag{1.8}$$

Esta ecuación la utilizaremos para ver una demostración del Teorema de Cauchy más tarde.

Proposición 1.15. *(**Principio fundamental para contar**) Dado G actuando sobre X, y suponiendo que O es una de las órbitas. Tomamos $x \in O$ y tomamos H=$Estab_G(x)$,*

el estabilizador de x. Dado $G/H = \{gH \text{ tal que } g \in G\}$ sea el conjunto de las clases por la derecha de H en G. Entonces existen una biyección entre $\theta : G/H \to O$ tal que $\theta(gH) = g \cdot x$. En particular $|O| = |G : G_g|$

Demostración. Como H=G_x sabemos que para todo $h \in H$ se cumple que $h \cdot x = x$. Utilizando esto veamos qque si gH=kH, entonces $g \cdot x = k \cdot x$.

Por gH=kH podemos escribir $k = gh$ para algún h de H. Entonces:

$$k \cdot x = gh \cdot x = g \cdot (h \cdot x) = g \cdot x \tag{1.9}$$

Dada una clase lateral gH $\in G/H$, el punto $g \cdot x$ se mantiene en O, y no depende del elemento de gH. Por lo que la aplicación θ está bien definida. Ahora probaremos que es inyectiva y sobreyectiva.

Ver que es sobreyectiva es fácil. Si $y \in O$ entonces por definición de órbita existe un g $\in G$ tal que $y = g \cdot x$. Entonces gH $\in G/H$ satisface $\theta(gH) = g \cdot x = y$.

Para probar que es inyectiva, supongamos $\theta(gh) = \theta(kH)$ tenemos $g \cdot x = k \cdot x$ entonces :

$$x = 1 \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (k \cdot x) = g^{-1}k \cdot x \tag{1.10}$$

Entonces $g^{-1}k$ fija x por lo que $g^{-1}k$ pertenece a H. Por lo que k $\in gH$ y se finaliza gH=kH. Y prueba que θ es inyectiva.

□

Ahora vamos a ver una forma de calcular el número de órbitas de una acción.

Proposición 1.16. ***Formula de Burnside*** *Sea G un grupo finito que actúa sobre un conjunto X. Siendo X/G el conjunto de órbitas y $Fix_g(X)$ los elementos fijos de X por la acción de g. Se cumple que:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |Fix_G(X)| \tag{1.11}$$

Demostración. Utilizando $\delta_{g \cdot x, x}$, el símbolo de Kronecker, vamos a llegar al resultado desarrollando el siguiente sumatorio.

$$\sum_{(g,x)\in G\times X} \delta_{g\cdot x,x} = \sum_{g\in G}\sum_{x\in X} \delta_{g\cdot x,x} = \tag{1.12}$$

$$= \sum_{g\in G} |Fix_G(X)| \tag{1.13}$$

Pero si desarrollamos de otra manera llegamos a:

$$\sum_{(g,x)\in G\times X} \delta_{g\cdot x,x} = \sum_{x\in X}\sum_{g\in G} \delta_{g\cdot x,x} = \tag{1.14}$$

$$= \sum_{x\in X} |Estab_G(x)| \tag{1.15}$$

Utilizando la partición de X en órbitas O_1 ,... , O_r donde r=|X/G|, y el hecho de que para x en la órbita O_i, el estabilizador tiene por orden:

$$|Estab_G(x)| = \frac{|G|}{|G\cdot x|} = \frac{|G|}{|O_i|} \tag{1.16}$$

$$\sum_{(g,x)\in G\times X} \delta_{g\cdot x,x} = \sum_{i=1}^{r}\sum_{x\in O_i} |Estab_G(x)| = \sum_{i=1}^{r}\sum_{x\in O_i|} \frac{|G|}{|O_i|} = \sum_{i=1}^{r} |G| = r|G| \tag{1.17}$$

Uniendo los dos desarrollos llegamos a la fórmula de Burnside. □

1.3. Aplicaciones del lema de Burnside

Para ver la utilidad de la fórmula de Burnside, usésmolo para resolver el siguiente problema: ¿Cuántas formas hay de colorear con tres colores los vértices de un cubo esencialmente diferentes*? (*Tendremos en cuenta que si tenemos un cubo con los vértices coloreados y hacemos un giro sobre el cubo es el mismo cubo)

La idea va a ser buscar una acción que represente el conjunto de colorear los vértices del cubo y luego buscar el grupo rotaciones o isometrías directas. Después lo que queremos ver es el número de órbitas, ya que cada órbita va a contar solo 1 coloración. Ya que un tipo de coloración si le aplicamos un giro va a ser la misma coloración, por lo que tenemos que contar el numero de órbitas.

Para empezar este problema debemos de saber cuál es el grupo G de isometrías directas del cubo. Para facilitar el ejemplo, vamos a suponer que sabemos que es S_4, y los elementos que variamos son las 4 diagonales del cubo. Ahora tenemos que ver cual es el conjunto X. Vamos a denotar Y=1,2,3,4,5,6,7,8 los vértices del cubo y C=R,A,V los 3 colores que vamos a dar. El conjunto X es el conjunto de funciones que van de Y hacia C, $X = C^Y$.

Cada función define una única manera de colorear los vértices, y cada manera de de colorear los vértices define una función. Por lo que estamos haciendo una buena modelación.

El grupo S_4 actúa sobre C^Y así:

$$\text{para todo } g \in S_4, \text{ para todo } f \in X, \text{ para todo } k \in Y,\ g \cdot f(k) = f(g^{-1} \cdot k). \quad (1.18)$$

En palabras: el color del vértice $g^{-1} \cdot k$ va a ser el color del vértice k despues de la isometría directa. Veremos que esta acción esta bien definida en el siguiente capítulo.

Necesitamos calcular para cada g los puntos fijos $|Fix_G(X)|$. Podemos ver que para todo $g \in S_4$ f es un punto fijo si se cumple $f(k) = f(g^{-1} \cdot k)$. Lo que es equivalente a decir que f es constante en las órbitas de g, es decir en las órbitas del grupo <g>=H sobre Y. Esto quiere decir que el numero de puntos fijos $|Fix_G(X)|$ es igual al nombre de colores a la potencia del número de órbitas del grupo <g>=H sobre Y. Es decir:

$$|X^g| = 3^{|\frac{Y}{H}|} \quad (1.19)$$

Ahora vamos a ver que $|Fix_G(X)|$ solo depende de la clase de conjugación, es decir, que g y hgh^{-1} tienen los mismo elementos:

$$X^{hgh^{-1}} = \{x \in X \ tal\ que\ (hgh^{-1}) \cdot x = x\} = \quad (1.20)$$

$$= \{x \in X \ tal\ que\ g(h^{-1} \cdot x) = h^{-1} \cdot x\} = \{x \in X \ tal\ que\ h^{-1} \cdot x \in X^g\} = h \cdot X^g \quad (1.21)$$

Sabemos que la aplicación h· sobre X es una permutación por lo que:

$$|X^{hgh^{-1}}| = |X^g| \quad (1.22)$$

Donde Id es la identidad, 1/2 centro es el medio giro entorno a 2 puntos opuestos que estan en un centro de una cara, 1/3 diag es un tercio de giro fijando dos puntos diagonalmente opuestos, 1/2 aristas contrarias es un medio giro fijando un punto en medio de una ariste y el otro es el punto opuesto (que también esta en el centro de una

g	()	(..)(..)	(...)	(..)	(....)
Naturaleza geomética de S_4	Id	1/2 centro	1/3 diag	1/2 aristas contrarias	1/4 centros
Cardinal de la clase de conjugación	1	3	8	6	6
Número de óbitas de <g>	8	4	4	4	2
Coloreaciones invariantes por g	3^8	3^4	3^4	3^4	3^2

arista), 1/4 centros es un cuarto de giro fijando dos puntos opuestos que esta en el centro de una cara.

Por la fórmula de Burnside

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |Fix_G(X)| \tag{1.23}$$

$$|X/G| = 1/24(1 \times 3^8 + (3 + 8 + 6) \times 3^4 + 6 \times 3^2) = 333 \tag{1.24}$$

Capítulo 2

Teorema de Polya

Este capítulo va a estar centrado en 2 cosas: generalizar el ejemplo de la coloración de los vértices de un cubo con un teorema famoso y resolver un problema histórico que responde a la pregunta de cuantos circuitos "distintos"hay con 4 interroptures. Para todo ello necesitaremos empezar por la teoría

2.1. Teoría de Polya

Definición 2.1. *Dado un grupo G que actúa sobre un conjunto |D|=n, y la acción la denotamos por ρ. Por lo visto en una de las definiciones de acciones de grupo, a cada g ∈ G le corresponde por la acción ρ un α ∈ S_n, y sabemos que se puede expresar de manera única como producto de ciclos disjuntos.*

1. ***Tipo de permutación*** *α se le asocia a $(j_1, j_2, ..., j_n)$ si α como producto de ciclos tiene j_k ciclos de longitud k. Cabe destacar que como dos elementos conjugados tienen el mismo número de ciclos disjuntos y de la misma longitud, tiene el mismo tipo de permutación.*

2. ***Monomial*** *de g: Mon(g)=$x_1^{j_1} x_2^{j_2} ... x_n^{j_n}$ donde $x_1, ..., x_n$ son distintas variables.*

3. ***Polinomio indicador de la acción ρ de G sobre D****: es el siguiente polinomio en $\mathbb{Q}$:*

$$P_\rho = \frac{\sum\{Mon(g) : g \in G\}}{|G|} \tag{2.1}$$

Observación 2.2. Por la asociación de α a $(j_1, j_2, ..., j_n)$ tenemos que darnos cuenta de que:

$$1 \cdot j_1 + 2 \cdot j_2 + ... + n \cdot j_n = n \tag{2.2}$$

Para comprender esta definición vamos a ver un ejemplo sencillo para ver como se calcula el polinomio indicador de la acción.

Ejemplo 2.3. G=S_3 y D={1,2,3}. Concretando más G={e,(12),(13),(23),(123),(132)}. Por lo tanto, ahora solo tenemos que ver el monomio de cada elemento y sumarlos. El elemento e es el unico de la forma (3,0,0) por lo que su monomial es x_1^3. Los 2-ciclos, (12) (13) y (23) su tipo de ciclo es (1,1,0) por lo que su monomial es x_1x_2. Y los 3-ciclos (123) y (132) tienen monomial x_3. Con lo que:

$$P_\rho = \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3) \tag{2.3}$$

Sabiendo lo que es el polinomio indicador de una acción, ahora ya podemos resolver un problema de corolación. Llamemos D al conjunto que vamos a colorear y R a los colores. R^D es el conjunto de coloraciones, que es el conjunto de aplicaciones de D en R: $R^D = \{f : D \to R\}$. También hay que considerar que un grupo G que actúa sobre D hace indistinguibles algunas coloraciones, que hacen que sean esecialmente iguales.

Ejemplo 2.4. Podriamos volver al ejemplo 1.3 donde D son los vértices de un cubo, R son los tres colores elegidos, y los elementos que eran indistinguibles eran las coloreaciones que eran iguales salvo una rotación.

Ayudados del anterior ejemplo que la acción que modelizaba una coloración era:

$$\text{para todo } g \in S_n, \text{ para todo } f \in R^D, \text{ para todo } k \in D,\ g \cdot f(k) = f(g^{-1} \cdot k). \tag{2.4}$$

En esta acción podemos ver como hay una acción natural π, que luego va a ser útil, de S_n hacia D con la acción, siendo g $\in S_n$ se cumple:

$$g \cdot d = g(d) \tag{2.5}$$

Veamos ahora que es una acción:

Proposición 2.5. *Sea G un grupo que actúa sobre D y R un conjunto de colores finito. Sea R^D el conjunto de coloraciones. Se tiene que la aplicación $G \to S_{|R^D|}$ dada por g $\to (f \to f^g)$ donde f^g está definida por $f^g(d) = f(g^{-1} \cdot d)$ es una acción de G sobre R^D.*

Demostración. Primero vamos a ver que $f \to f^g$ pertenece al grupo simétrico, es decir, que es biyectiva. Como es una función que va de R^D a él mismo (finito), con probar que es inyectiva es suficiente.

Probemoslo por el contrarreciproco: si f $\neq$ f' entonces habrá algún d para el que $f(g^{-1} \cdot d) \neq f'(g^{-1} \cdot d)$ luego $f^g \neq f'^g$ por lo que es inyectiva.

Ahora tenemos que ver que $\phi : G \to S_{|R^D|}$ es homomorfismo de grupos. Para ello tenemos que ver que: $f^{gg'} = (f^g)^{g'}$

$$f^{gg'}(d) = f((gg')^{-1} \cdot d) = f((g'^{-1}g^{-1}) \cdot d) \tag{2.6}$$

$$(f^g)^{g'} = f^g(g'^{-1} \cdot d) = f(g^{-1} \cdot (g'^{-1} \cdot d)) = f((g'^{-1}g^{-1}) \cdot d) \tag{2.7}$$

Lo que termina la prueba. □

Ahora vamos a hablar de lo que realmente es dificil de calcular en estos problemas. Hablando más técnicamente, una coloración es **esencialmente diferente** de otra si no estan en la misma órbita de la acción de ρ. Es decir, nuestro objetivo va a ser contar las órbitas de nuestra acción.

Intuitivamente en el ejemplo 1.3, está claro que una coloración es esencialmente igual que otra si existe una rotación que las asocia. El hecho de que solo queramos contar las coloraciones esencialmente diferentes dificulta el problema pero el teorema de Polya soluciona el problema con una igualdad muy sencilla.

Teorema 2.6. ***Teorema de Polya*** *Se considera una acción ρ del grupo finito G sobre un conjunto D. Se consideran $r \geq 1$ colores y se colorean los puntos de D con dichos r colores. Entonces el número de coloraciones esencialmente diferentes posibles N(r,ρ) está dado por:*

$$N(r, \rho) = P_\rho(r, ..., r) \tag{2.8}$$

Donde P_ρ es el polinomio indicador de ciclos de la acción ρ.

Demostración. Como hemos dicho previamente $N(r, \rho)$ son las órbitas de la acción definida en la ecuación 2.4. Para ello vamos a utilizar la fórmula de Burnside, en la cual lo único que necesitamos saber es $|Fix(g)|$ para cada g.

Para ello vamos a utilizar la acción natural π que se define entre G y D gracias a ρ. Veamos que las coloraciones fijas son aquellas que dan un color a cada órbita de π. Está claro que si damos un color a cada órbita de π la coloracion va a mantenerse fija ya que cada elemento de D va a seguir teniendo el mismo color. Supongamos que una órbita tiene dos colores, está claro que un elemento de D va a cambiar de color por lo que no es una coloración fija. Por lo que cada coloración fija esta asociada a una coloración sobre las órbitas de π.

Esta claro que para una permutación de k ciclos, es decir, donde hay k órbitas, el número de coloraciones que hay es r^k ya que no tiene que cumplir ninguna condición. Por lo que si k es el número de ciclos de g, $|Fix(g)| = r^k$. Ahora bien si tomamos $j_1, j_2, ..., j_n$ los valores del vector de tipo de permutación de g, tenemos que:

$$M_\rho(g) = x_1^{j_1} x_2^{j^2} ... x_n^{j_n} \tag{2.9}$$

Pero como sabemos la suma de los j_i tiene que dar k (número de ciclos de g). Por lo que si evaluamos $M_\rho(g)$ en (r,r,...,r):

$$M_\rho(g)(r, r, ..., r) = r^{j_1} r^{j^2} ... r^{j_n} = r^{j_1 + ... + j_n} = r^k \tag{2.10}$$

Por lo que $|Fix(g)| = r^k = M_\rho(g)(r, r, ..., r)$ Y ahora utilizando la fórmula de Burnside podemos ver:

$$N(r, \rho) = \frac{1}{|G|} \sum_{g \in G} |Fix(g)| = \frac{1}{|G|} \sum_{g \in G} M_\rho(g)(r, r, ..., r) \tag{2.11}$$

Y viendo la definición de polinomio indicador de la acción:

$$N(r, \rho) = P_\rho(r, r, ..., r) \tag{2.12}$$

□

Teorema 2.7. ***Teorema Redfield-Polya*** *Se considera una coloración ρ de G sobre R^D, donde en R hay r ≥1 colores. Dados $s_1, s_2, ..., s_r \geq 0$ tales que la suma de los s_j es n, donde n es el cardinal de D. Entonces el número de coloraciones esencialmente diferentes $R(s_1, s_2, ..., s_r)$ que utilizan exactamente s_j veces el color j-ésimo color, es igual al coeficiente del monomio $(y_1^{s_1} ... y_r^{s_r})$ en el polinomio:*

$$Q_\rho(y_1, ..., y_r) = P_\rho(y_1 + ... + y_r, y_1^2 + ... + y_r^2, ..., y_1^n + y_r^n) \tag{2.13}$$

Demostración. Dado g en G y c una coloración de R^D entonces tanto c como $g \cdot c$ utilizan cada color el mismo número de veces. Ahora si definimos $Y_{s_1,...,s_r}$ el subconjunto de R^D formado por la coloraciones que utilizan s_j veces el color j, donde la suma de los s_j es n. Simplificaremos a Y la notación aunque sepamos que depende de $s_1, ..., s_r$. Por lo tanto tenemos un Y para cada sucesión de s_j. Y para cada Y tenemos que contar las órbitas (aplicar la fórmula de Burnside) a la acción G×Y $\to Y$ definida por la restricción de ρ.

Lo primero que tenemos que fijarnos es que Q_ρ es un polinomio homogéneo y de grado n. Repasando la observación 2.2 nos damos cuenta de que P_ρ es homogéneo si le damos peso i a x_i. Por definición $Q_\rho(y_1, ..., y_r) = P_\rho(y_1 + ... + y_r, y_1^2 + ... + y_r^2, ..., y_1^n + y_r^n)$ que a cada variable en P eleva al orden del término y hace la suma de todas las variables. Por lo que para que Q_ρ sea homogéneo no tenemos que variar los pesos como en P, simplemente

los pesos valen 1. Por lo tanto todos los términos monomiales son de la forma:

$$Ry_1^{s_1}...y_r^{s_r} \quad \text{Mientras se cumple que } s_1 + ... + s_r = n \tag{2.14}$$

Lo que queremos ver ahora es que R=R$(s_1, s_2, ..., s_r)$, es decir, el número de órbitas de la acción sobre Y. Para cada g en G con $M_\rho = x_1^{i_1}x_2^{i_2}...x_n^{i_n}$ las coloraciones c de de Y que están fijas en Fix(g) para la acción sobre Y, son aquellas que utilizan el mismo color para los elementos de cada ciclo de la descomposición de $\rho(g)$ y además utilizan en total s_j veces el color j para cada j.

Si una coloración de Fix(g) tiene pintados los elementos de uno de sus ciclos d, de longitud m, con el color j,entonces el monomio y_j^m que aparece en el factor $x_m = y_1^m + ... + y_r^m$ es el representante del ciclo d en:

$$M_\rho(g) = x_1^{i_1}x_2^{i_2}...x_n^{i_n} = (y_1 + ... + y_r)^{i_1}(y_1^2 + ... + y_r^2)^{i_2}...(y_1^n + ... + y_r^n)^{i_n}$$

La sustitucion de $x_m = y_1^m + ... + y_r^m$ lo que representa es el cambio de x_m que representa un ciclo de orden m, a $y_1^m + ... + y_r^m$ que son las r formas de colorear el ciclo de orden m. Ahora utilizando la ecuación 2.14 le damos el sentido de que el monomio $y_1^{s_1}...y_r^{s_r}$ representa una coloración donde el color 1 se utiliza s_1 veces.

Al tener $\rho(g)$ descompuesto en ciclos, cada elección del color j de cada ciclo d de longitud m lo asociamos a elegir dentro de $(y_1^m + ... + y_r^m)$ el color j para multiplicarlo con los demás términos de Q_ρ. Está claro que si elegimos el color de cada ciclo fijamos un término de Q_ρ, pero si fijamos un término de Q_ρ, por ejemplo $y_1^{s_1}...y_r^{s_r}$, existen todas las posibilidades de colorear cada ciclo tal que la suma de los elementos coloreados del color j sean s_j. Es decir, si vemos el polinomio como suma de términos de la forma 2.14 el coeficiente R es el que estamos buscando.

□

2.2. ¿Cuántos circuitos formados por n interruptores existen?

Este es un problema histórico en el cual podemos ver el potencial de cálculo que nos da el teorema de Polya. Para resolver esta pregunta se necesito un ordenador gigante en 1951 cuando se pudo resolver utilizando la teoria de Polya descubierta en 1937 (en 1927 por Redfield aunque Polya lo descubrió independientemente). Veremos que la resolución utilizando los teoremas previamente vistos, es bastante directa mientras que con comprobarlo con un ordenador además en el 1951 es un procedimiento muy lento.

En este caso no es tan fácil ver la coloración ya que, ¿qué significa que 2 interruptores sean esencialmente distintos? Lo que queremos ver es la "forma"del circuito, es decir, en

el caso que tuvieramos 2 interruptores está claro que no es lo mismo si están en serie o están en paralelo. Pero si que tendrían la misma forma (serian esencialmente iguales) dos circuitos en paralelo ,el cual uno de ellos tenga los interruptores cerrados(no pasa la electricidad) y el otro abiertos(pasa la electricidad). Es decir, aunque en uno al final si que llegase la electricidad al final del circuito y en el otro no, tiene sentido denotarles como el mismo circuito, ya que tienen la misma "forma". Ahora que podemos visualizar un poco lo que nos referimos intuitivamente, vamos a ver que es matemáticamente un interruptor, y luego analizar que es ser esencialmente iguales.

Comenzamos definiendo el conjunto D=$\{0,1\}^n$ y va a representar la agrupación de interruptores y R=$\{0,1\}$ va a representar si por todo el circuito pasa la electricidad o no. Es decir, D representa la posición de los n interruptores (si cada interruptor deja o no deja pasar la electricidad) y R representa si al final del circuito llega o no llega la electricidad.

Ahora definimos el conjunto de los circuitos como:

$$R^D = \{f | f : \{0,1\}^n \to \{0,1\}\} \tag{2.15}$$

Vamos a ver intuitivamente lo que es un circuito para n=2. Queremos ver que función sería un circuito en paralelo. Lo que cumple un circuito en paralelo es que con que un interruptor este abierto (pasa la electricidad) la electricidad llega al final. Es decir, la función que represente un circuito en paralelo para n=2 es:

$$f(0,0) = 0 \quad f(1,0) = 1 \quad f(0,1) = 1 \quad f(1,1) = 1 \tag{2.16}$$

Mientras que un circuito en serie, necesitariamos que los 2 interruptores estuviesen abiertos, es decir, tiene la forma:

$$f(0,0) = 0 \quad f(1,0) = 0 \quad f(0,1) = 0 \quad f(1,1) = 1 \tag{2.17}$$

Queremos ver que estos dos circuitos son esencialmente diferentes, para ello decimos que f_1, f_2 son esencialmente iguales si con un reordenamiento $(i_1, ..., i_n)$ de (1,...,n) se tiene que $f_1(b_1, ..., b_n) = f_2(b_{i_1}, ..., b_{i_n})$ para todo $(b_1, ..., b_n) \in \{0,1\}^n$. Esta claro que el circuito que no existe ninguna permutación para que el circuito en serie y en paralelo sean esencialemente iguales, por lo que son esencialmente diferentes.

Ahora podemos entender porque con un ordenador este problema es muy difícil de abarcar: $|R^D|$ que es el conjunto donde tenemos que comprobar cual son esencialemente iguales es enorme. Para n=4 el cardinal es $2^{2^4} = 65536$, un numero absurdamente grande para n=4. Vamos a resolverlo con nuestra teoría. Lo primero que tenemos que buscar es el polinomio indicador de la acción de S_4 sobre $\{0,1\}^4$:

Observación 2.8. Estamos enviando un elemento g de S_4 hacia un elemento de S_{16} ,es decir, a un elemento que permuta los elementos de $\{0,1\}^4$. Por lo que nuestros j_i tienen

que sumar 16.

También vamos a utilizar que sabemos que los conjugados tienen el mismo monomial, por lo que tomaremos un ciclo concreto y al monomio restante lo multiplicaremos por el número elementos conjugados del mismo que haya en S_4.

1. La identidad fija las 16 combinaciones (b_1, b_2, b_3, b_4) dando el monomio t_1^{16}

2. Hay seis 2-ciclos en S_4: {(12),(13),(14),(23),(24),(34)}.(12) en S_{16} da lugar a ocho 1-ciclos que quedan fijos de la forma (0,0,$b_3, b, 4$) y (1,1,$b_3, b, 4$) y a cuatro 2-ciclos fijos de la forma: ((1,0,$b_3, b, 4$),(0,1,$b_3, b, 4$)). Por lo que el monomio es $6t_1^8t_2^4$.

3. Hay tres productos de 2-ciclos en S_4: {(12)(34),(13)(24),(14)(23)}. (12)(34) en S_{16} da lugar a cuatro 1-ciclos que quedan fijos de la forma $(b_1, b_2$,$b_3, b, 4)$ y (1,1,$b_3, b, 4$) y a seis 2-ciclos fijos de la forma: $((b_1, b_2$,$b_3, b, 4)$,$(b_2, b_1$,$b_4, b, 3))$ donde $b_1 \neq b_2$ o $b_3 \neq b_4$. Por lo que el monomio es $3t_1^4t_2^6$.

4. Hay ocho 3-ciclos en S_4: {(123),(124),(134),(132),(142),(143),(234),(243)}. (123) en S_{16} da lugar a cuatro 1-ciclos que quedan fijos de la forma $(b_1, b_1$,$b_1, b, 4)$ y a cuatro 3-ciclos fijos de la forma: $((b_1, b_2$,$b_3, b, 4)$,$(b_3, b_1$,$b_2, b, 4)$,$(b_2, b_3$,$b_1, b, 4))$. Por lo que el monomio es $8t_1^4t_3^4$.

5. Hay seis 4-ciclos en S_4: {(1234),(1342),(1243),(1324),(1423),(1432)}.(1234) en S_{16} da lugar a dos 1-ciclos que quedan fijos de la forma (b_1,b_1,b_1,b_1), un 2-ciclos fijos de la forma: $((b_1$,b_2,$b_1, b, 2)$,$(b_2$,b_1,$b_2, b, 1))$. Y el resto esta en 4-ciclos de la forma $((b_1, b_2, b_3, b_4)$,(b_4, b_1, b_2, b_3),(b_3, b_4, b_1, b_2),(b_2, b_3, b_4, b_1),) Por lo que el monomio es $6t_1^2t_2^1t_4^3$.

Con todo esto llegamos a que el polinimo indicador es:

$$\frac{1}{24}(t_1^{16} + 6t_1^8t_2^4 + 3t_1^4t_2^6 + 8t_1^4t_3^4 + 6t_1^2t_2^1t_4^3) \tag{2.18}$$

Lo único que tenemos que hacer ahora es sustituir por $|R| = 2$ es decir sustituir todas las variables en el polinomio anterior por 2:

$$\frac{1}{24}(2^{16} + 62^82^4 + 32^42^6 + 82^42^4 + 62^22^12^3) = 3984 \tag{2.19}$$

Lo que nos resuelve el problema, hay 3984 circuitos formados por 4 interruptores.

Capítulo 3

Teoremas de Sylow

En esta sección vamos a recalcar que vamos trabajar solo con grupos finitos, aunque sería posible hablar en términos de grupos infinitos. Esta restricción de grupos finitos tiene un sentido y es aprovechar la definición de **p-grupo**, siendo p un primo.

Definición 3.1. *Un p-grupo es un grupo G en el que cada elemento de G tiene orden una potencia de p siendo p primo.*

Como es un grupo finito, podemos ver la equivalencia entre: G es p-grupo y el cardinal de G es una potencia de p.

Si el cardinal es una potencia de p, por el teorema de Lagrange, el orden de cada elemento divide al cardinal de G. Como p es primo cada elemento tiene orden una potencia de p (p-grupo)

Para probar la otra implicación, primero veremos el Teorema de Cauchy:

Teorema 3.2. ***Teorema de Cauchy*** *Si G es un grupo finito de orden n y p (numero primo) divide a n, entonces existe al menos un elemento de orden p.*

Demostración. Tomemos el subgrupo $<\gamma>$de S_p engendrado por $<\gamma>$=(1 2 ... p). Vamos a crear una acción de $<\gamma>$sobre el conjunto de G^p definida por:

$$\sigma \cdot (g_1, ..., g_p) = (g_{\sigma(1)}, ..., g_{\sigma(p)}) \tag{3.1}$$

Tomemos

$$X = \{(g_1, ..., g_p) \in G^p \ tal \ que \ g_1 \cdot ... \cdot g_p = e\} \tag{3.2}$$

Vamos a ver que X es estable sobre la acción de $<\gamma>$. Tomemos un elemento de X y

apliquemosle γ

$$\gamma \cdot (g_1, ..., g_p) = (g_2, ..., g_p, g_1) \tag{3.3}$$

Además sabemos que $g_1 \cdot ... \cdot g_p = e$ por lo que:

$$g_2...g_pg_1 = g_1^{-1}(g_1...g_p)g_1 = g_1^{-1}g_1 = e \tag{3.4}$$

Es decir, es un elemento de X otra vez. Para cualquier elemento de $<\gamma>$por ejemplo γ^r para cada vez que aplicamos γ sigue siendo estable, por lo que si se lo aplicamos r veces también lo es.

El cardinal de la órbita de un elemento es igual al indice del estabilizador de ese elemento en el grupo $<\gamma>$, por ser cíclico de orden p, el indice solo puede valer 1 o p. También podemos calcular el cardinal de X. Cada elección de un elemento de X corresponde con la elección de p-1 elementos de G y añadir el último gracias a la relación de X. Por lo que |X|=$|G^{p-1}|$=n^{p-1}. Y como p divide a n, también divide a |X|.

Sabemos que las órbitas forman una partición de X, como solo son de talla 1 o p y que |X| es divisible por p, utilizando la ecuación de clase **(1.4)** para concluir con que el número de órbitas de talla 1 es divisible por p. Al menos existen p-1 (el minimo primo es 2 por lo que existe) elementos diferentes del neutro que tienen órbita 1. Por lo que

$$\gamma \cdot (g_1, ..., g_p) = (g_2, ..., g_p, g_1) = (g_1, ..., g_p) \tag{3.5}$$

Lo que implica que $g_1 = g_2 = ... = g_p$ y llegamos a $g_1^p = e$. Como p es primo, podemos concluir que g_1 es de orden p. □

Ahora utilizando el contrarreciproco del teorema que acabamos de probar, podemos ver que si no existe ningún elemento de orden q diferente de p, q nunca divide a |G|. Por lo que si solo lo divide p, |G| es una potencia de p.

Definición 3.3. ***Sylow p-subgrupo*** *Fijado p primo, un subgrupo H de un grupo finito G, es un Sylow p-subgrupo de G si /H/ es una potencia de p y el indice de /G : H/ no es divisible por p.*

Observación 3.4. Sabemos que cada entero positivo puede factorizarse de forma única como potencia de p multiplicado por un entero no divisible por p. Una forma alternativa de formular la definición de Sylow p-subgrupo es utilizando esta observación: Si |G|=p^am donde a≥0 y p no dividen a m≥1, entonces un subgrupo H de G es un Sylow p-subgrupo de G si |S|=p^a

El objetivo de los teoremas de Sylow es "probar el recíproco del teorema de Lagrange". Abro comillas porque sabemos que el recíproco es falso. El teorema de Lagrange dice: Si G es un grupo y H un subgrupo, entonces $|G| = |H||G : H|$ siendo $|G : H|$ el número de clases laterales. En particular que el cardinal de H divide al cardinal de G. El reciproco afirmaría que para cualquier divisor r de $|G|$ existe un grupo H de G con r elementos.

Vamos a ver que el grupo simétrico A_4 tiene orden 12 y no tiene ningún subgrupo de orden 6. Tenemos que

$$A_4 = \{id, (123), (124), (132), (142), (143), (134), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

Supongamos que tiene un grupo de 6 elementos. Sabemos por el Teorema de Lagrange que 6 es el subgrupo propio más grande que puede haber en A_4. Tenemos ocho 3-ciclos y tres productos de 2-ciclos. Para tomar 6 elementos, sabiendo que tenemos ya la identidad existen las siguientes posibilidades:

1. Tener dos 3-ciclos que no son inversos entre ellos, y que por ser un subgrupo sus potencias también estarían y ya generarían 6 elementos. Vamos a ver que hay otro elemento diferente, lo que implicaría que hay al menos 7 elementos, y como el máximo de elementos que puede tener un subgrupo propio es 6, concluiriamos que nuestro subgrupo es A_4, contradiciendo que tiene 6 elementos.

   $$(abc)(abd) = (ad)(bc)$$

   Por lo que tiene un elemento diferente (ya que no tenemos ningún producto de 2-ciclos) y concluimos que este subgrupo es A_4

2. Tener los tres productos de dos ciclos y dos 3-ciclos (que serían inversos entre ellos), por lo que ya tendríamos 6 elementos. Repitiendo el argumento, vamos a buscar otro elemento diferente. Por tener todos los productos de 2-ciclos siempre vamos a encontra el elemento:

   $$(abc)(ab)(cd) = (bdc)$$

   Que es un elemento diferente a los que tenemos ya que, los únicos 3-ciclos que tenemos son (abc) y (acb) ya que son inversos.

Por lo que A_4 no tiene ningún subgrupo de 6 elementos.

3.1. Primer Teorema de Sylow

Teorema 3.5. ***Primer Teorema de Sylow***

Para cualquier factor primo p con multiplicidad a en el orden del grupo finito G, existe un p-subgrupo de Sylow de G, con orden p^a

Con la hipótesis de que el número sea primo, si que se cumple el reciproco del teorema de Lagrange, para demostrar necesitaremos el siguiente lema

Lema 3.6. *Dado un primo p, y a ≥ 0 and m ≥ 1 enteros:*

$$\binom{p^a m}{p^a} \equiv m \ mod\ p \tag{3.6}$$

Demostración. Consideremos el polinomio $(1+X)^p$. Como p es primo es fácil ver que los coeficientes $\binom{p}{i}$ son divisibles por p para i entre 1 y p-1. Por lo que los coeficientes del polinomio $(1+X)^p$ que no son 1 y X^p son 0 en módulo p. Por lo que $(1+X)^p \equiv 1+X^p$. Podemos volver aplicar esto mismo a : $(1+X)^{p^2} \equiv (1+X^p)^p$ mod p. Podemos finalizar con:

$$(1+X)^{p^a m} \equiv (1+X^{p^a})^m \ mod\ p \tag{3.7}$$

Como estos polinomios son congruentes, los coeficientes de cada X^i son congruentes, en concreto el coeficiente de X^{p^a} en ambos lados: en el primero es $\binom{p^a m}{p^a}$ y en el segundo es $\binom{m}{1} = m$ lo que finaliza la prueba.

□

Ahora probaremos el primer teorema de Sylow con la demostracion de Wielandt

Demostración. Como sabemos que p divide a |G| y p es primo podemos escribir |G|=$p^a m$ donde a≥ 1 y p no divide a m. Tomemos Ω el conjunto de todos los subconjuntos de G de cardinal p^a. Ahora observamos que G actúa con la multiplicación a la derecha sobre Ω.La operación va a ser, para todo g inG y todo H∈ Ω con H=$\{a_1, \ldots, a_{p^a}\}$:

$$g \cdot H = \{g \cdot a_1 \ , \ \ldots \ , \ g \cdot a_{p^a}\} \tag{3.8}$$

Es fácil ver que la aplicación esta bien definida y es una acción. Como hay una acción sabemos que Ω esta particionado en órbitas, por lo que |Ω| es la suma del tamaño de las órbitas, pero:

$$|\Omega| = \binom{p^a m}{p^a} \equiv m \not\equiv 0 \ mod\ p \tag{3.9}$$

Por lo que |Ω| no es divisible por p. Por lo que existe alguna órbita denotemosle O que $|O|$ no es divisible por p. Lo que queremos ver ahora es que si tomamos X ∈ O y H=G_X el estabilizador de X en G es un grupo de orden p^a que es lo que buscamos.

Ya sabemos que H es un grupo lo que nos hace falta es ver que tiene cardinal p^a. Utilizando el principio fundamental para contar, $|O|$=|G|/|H|. Como p no divide a $|O|$ pero p^a si divide a |G|, p^a también divide a |H| en particular $p^a \leq$ |H|.

Como H estabiliza a X, podemos ver que si x ∈ X, entonces xH ⊆ X por lo que |H|=|xH| ≤ |X|=p^a, donde la primera igualdad surge por la biyección evidente, la desigualdad por la primera contención y la última igualdad porque X pertenece a Ω. Lo que nos finaliza la prueba.

□

Observación 3.7. Utilizando el primer teorema de Sylow podemos afirmar muy facilmente que A_5 tiene subgrupos de ordenes 2,3,4 y 5. Lo que no sabemos es cuantos subgrupos hay de cada orden o cómo estan relacionados. Esta información nos la va a aportar los otros 2 teoremas de Sylow

3.2. Segundo Teorema de Sylow

Definición 3.8. *$Syl_p(G)$ es el conjunto de todos los grupos p-Sylow de G.*

El primer teorema de Sylow dice que $Syl_p(G)$ es no vacío para todos los grupos finitos G y p primos.

Teorema 3.9. ***Segundo Teorema de Sylow***

Dado un grupo finito G y un número primo p que divide al orden de G, entonces todos los p-subgrupos de Sylow son conjugados entre sí. Es decir, si P y S son p-subgrupos de Sylow entonces existe un elemento g en G tal que $g^{-1}Sg$=P.

También se puede escribir este teorema como: Para todo P,S ∈ $Syl_p(G)$. Entonces existe un g ∈ G tal que P ⊆ S^g. Siendo S^g la conjugacion de S con g.

Como |P|=|S|=|S^g| porque pertenecen a $Syl_p(G)$ la con que haya una contención nos sirve para afirmar la igualdad.

Demostración. Tomemos Ω ={ Sx : x ∈ G } el conjunto de clases laterales de S en G. Sabemos que |Ω|=|G:S| no es divisible por p porque S pertenece a $Syl_p(G)$. Sabemos que G actúa por la multiplicación a la derecha sobre Ω y por lo tanto P también actúa. Por lo que la acción de P particiona a Ω en P-órbitas. Como |Ω| no es divisible por p, al menos existe una P-órbita O tal que |O| no es divisible por p.

Por el principio fundamental para contar, |O| es el índice en P de algún subgrupo. Sigue que |O| divide a |P|, que es una potencia de p. Por lo que |O| es también una potencia de p pero no divisible por p, asi que la única opción es que |O|=1. Recordamos

que todos los elementos de Ω son clases laterales de S en G, podemos suponer que el único miembro de O es Sg.

Como Sg es el solo una P-órbita, se ve que es un elemento fijado por la acción de P y Sgu=Sg para todo u ∈ P. Por lo que gu ∈ Sg, y por lo tanto u ∈ $g^{-1}Sg = S^g$. Por lo que P ⊆ S^g como buscabamos.

□

3.3. Tercer Teorema de Sylow

Definición 3.10. *Denotemos el numero de p-subgrupos de Sylow de G como* $n_p(G)$=$|Syl_p(G)|$

Definición 3.11. *El conjunto:*

$$N(H) = \{g \in G : gHg^{-1} = H\} \tag{3.10}$$

es un subgrupo de G llamado normalizador de H en G.

Se puede observar que H es un subgrupo normal de N(H), de hecho se podria probar que N(H) es el mayor subgrupo de G en el que H es normal.

Antes de empezar el tercer teorema de Sylow vamos a demostrar un lema que nos hara falta:

Lema 3.12. *Dado un p-grupo finito H, dado Ω un conjunto finito y una acción de H sobre Ω. Denotamos X como el conjunto de los puntos fijos. Entonces:*

$$|\Omega| \equiv |X|(modp) \tag{3.11}$$

Demostración. Dado x ∈ Ω que no está fijado por H, está en una órbita de tamaño |H|/$|H_x|$ (donde H_x denota el estabilizador) que es un múltiplo de p por hipótesis de p-grupo. Por lo que si escribimos $|\omega|$ como suma del tamaño de sus órbitas módulo p solo quedarían los puntos fijos ya que las demás son múltiplos de p. □

Teorema 3.13. ***Tercer Teorema de Sylow*** *Dado p primo y un grupo finito G tal que* |G|=$p^a m$ *donde* $n \leq 0$ *y p no divide a m. Tenemos los siguientes resultados:*

1. n_p *divide a m, que es el índice de p-subgrupos de Sylow de G*
2. $n_p \equiv 1$ *mod p*

Demostración. Dado el conjunto de los p-subgrupos de Sylow vamos a hacerlos actuar con G bajo la acción de la conjugación:

$$x \in G, \quad K \in Syl_p(G) \quad x \cdot K = xKx^{-1} \tag{3.12}$$

Por se la acción de la conjugación esta claro que la imagen de la acción está contenida en $Syl_p(G)$. Dado P $\in Syl_p(G)$ por el segundo Teorema de Sylow sabemos que su órbita tiene tamaño n_p, así que n_p=$|G : G_p|$, siendo G_p=$\{g \in G \quad | \quad gPg^{-1} = P\}$=$N_G(P)$ que es el estabilizador para esta acción. Sabemos que P es un subgrupo de $N_G(P)$, por lo que podemos deducir que n_p divide a $|G : P| = m$.

Ahora dado P $\in Syl_p(G)$ vamos a hacer actuar $Syl_p(G)$ con P con la acción de conjugación. Denotemos X el conjunto de los puntos fijos de la acción. Dado Q $\in X$ cumple que Q=xQx^{-1} para todo x de P por lo que P $\leq N_G(Q)$. Por el segundo teorema de Sylow P y Q son conjugados en $N_G(Q)$, y sabemos que Q es normal por lo que Q=P. Es decir el único elemento de X es P. Y con el lema anterior podemos finalizar que $n_p = |Syl_p(G)| \equiv |X|$=1 (mod p). □

3.4. Ejemplos prácticos

Siguiendo con la observación 1.18, nos vamos a fijar en el número de 5-subgrupos de A_5. Sabemos que ese número divide a 60 y es congruente a 1 (mod 5). Por lo que puede haber o un 5-subgrupo o 6. Ahora utilizamos el detalle de que si solo hubiera uno, este sería conjugado de si mismo, es decir seria normal. Pero A_5 no tiene subgrupos normales luego es imposible. Es decir, hay 6 5-subgrupos de Sylow en A_5

Hay muchísimos ejemplos de utilidad de los Teoremas de Sylow pero enseñar en un caso práctico como podemos utilizarlo. Una de las grandes proezas de las matemáticas actuales es la clasificación de los grupos simples finitos.Un **grupo simple** significa que sus únicos subgrupos normales son el trivial y el mismo grupo. Esta elección es porque un grupo no simple se puede dividir en dos grupos más pequeños: un subgrupo normal no trivial y su cociente. Nuestro objetivo va a ser ver todos los grupos de orden 99. Aqui vamos a ver el potencial de la ecuación de clases y los teoremas de Sylow.

Antes de clasificar los grupos de orden 99 vamos a ver 2 resultados muy importantes:

Teorema 3.14. *Sea G un grupo de orden p^n donde p es primo. Entonces G tiene centro no trivial.*

Demostración. Utilizando la ecuacion de clase:

$$|G| = |Z(G)| + \sum_{i=k}^{n} |O_{x_i}| \tag{3.13}$$

Como cada órbita tiene orden estrictamente mayor que 1, y divide a |G| concluimos que p divide a cada $|O_{x_i}|$, luego p divide a |Z(G)|. Como el elemento neutro siempre está en el centro, |Z(G)|≥1. Por lo tanto, |Z(G)|≥p y concluimos.

□

Corolario 3.15. *Sea G un grupo de orden p^2 donde p es primo. Entonces G es abeliano*

Demostración. Por el teorema anterior sabemos que |Z(G)|=p o p^2. Si |Z(G)|=p^2 estaria probado nuestro corolario. Supongamos que |Z(G)|=p. Entonces Z(G) y G/Z(G) ambos tendrian orden p y por lo tanto serían ambos grupos cíclicos. Elegimos un generador aZ(G) para G/Z(G), por ser cíclico podemos escribir cualquier elemento gZ(G) en el cociente como $a^m Z(G)$ para algun entero, luego g=$a^m x$ para algún x en el centro de G. Podemos hacer lo mismo con hZ(G) ∈ G/Z(G), entonces existe un y tal que h=$a^n y$ para algún entero n. Como x e y estan en el centro, conmutan con todos los elementos y tenemos:

$$gh = a^m x a^n y = a^{m+n} xy = a^{m+n} yx = a^n y a^m x = hg \tag{3.14}$$

Como g y h son dos elementos de G cualesquiera, finalizamos con que G es abeliano.

□

Empecemos a clasificar los grupos de orden 99=$3^2 \cdot 11$ salvo isomorfismo. Primero veremos que todo grupo G de orden 99 es abeliano. Por el Tercer teorema de Sylow hay 1+3k 3-subgrupos, cada uno de orden 9. Además 1+3k divide a 11, luego solo puede haber un 3-subgrupo de sylow H en G y este es normal. Procedemos con el mismo argumento con los 11-subgrupos y obtenemos que solo puede haber un 11-subgrupo de sylow K en G.

Por el corolario, cualquier grupo de orden 3^2 es abeliano, luego H es isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$ o $\mathbb{Z}_9$. Como K tiene orden 11, debe de ser isomorfo a $\mathbb{Z}_{11}$. Por lo tanto los únicos grupos de orden 99 son $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ y $\mathbb{Z}_9 \times \mathbb{Z}_{11}$

Capítulo 4

Grupos Nilpotentes.

4.1. Definición y ejemplos de grupos nilpotentes

Empezaremos dando la definición de grupos nilpotentes y avanzaremos dando grandes resultados sobre este tipo tan concreto de grupos, que después nos facilitaran la teoría.

Definición 4.1. *Una colección finita de* ***subgrupos normales*** N_i *de un grupo G es una* ***serie normal*** *de G si:*

$$1 = N_0 \subseteq N_1 \subseteq ... \subseteq N_r = G \tag{4.1}$$

Además si tenemos $N_i/N_{i-1} \subseteq Z(G/N_{i-1})$ *para* $1 \leq i \leq r$ *es una* ***serie central***

Por último un ***grupo nilpotente*** *es un grupo que tiene una serie central.*

Ahora vamos a ver varios ejemplos para identificarnos a como son y como funcionan los grupos nilpotentes:

Observación 4.2.

1. Es fácil ver que cada N_i de la serie central de un grupo nilpotente, también es un grupo nilpotente.

2. Cualquier grupo abeliano G es nilpotente ya que $1 \to G$ es una serie central, ya que tanto como 1 y G son subgrupos normales de G y G/1=G=Z(G) cumple las condiciones que requerimos.

3. Siendo H y K dos grupos, utilizando que Z(H × K)=Z(H) × Z(K) se podría probar que el grupo directo de 2 grupos nilpotentes es nilpotente

Ejemplo 4.3. Vamos a ver si el grupo de los cuaterniones o $\mathcal{Q}_8$ es nilpotente. Para

empezar, el grupo consta de :

$$\mathcal{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\} \tag{4.2}$$

Y la regla de la multiplicación a excepción de incluir los opuestos (-1, -i, -j, -k) que los omitiremos ya que si sabemos como se multiplican 1,i,j,k también sabemos los otros 4.

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Como podemos ver, tiene orden 8=2^3 por lo que el orden posible de los subgrupos propios es 2 o 4. Pero viendo la tabla vemos que el único elemento que tiene orden 2 es el -1, los demás tienen orden 4. Sabemos que su centro era no trivial por ser un 2-grupo y es fácil comprobar que es Z($\mathcal{Q}_8$)={1,-1}

Veamos que $1 \to \{1,-1\} \to \mathcal{Q}_8$ es una serie central. Tenemos que comprobar que $\mathcal{Q}_8$ / {1,-1} $\leq$ Z($\mathcal{Q}_8$) / {1,-1}) y {1,-1} $\leq$ Z($\mathcal{Q}_8$). Por ser abeliano sabemos que {1,-1} es normal.

Respecto a la primera podemos decir que $|\mathcal{Q}_8$ / {1,-1}|=4 y como los únicos grupos de 4 elementos son $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ que son abelianos por lo que su centro es el total. Por lo que la primera contención es correcta.

Sabemos que Z($\mathcal{Q}_8$)={1,-1} por lo que la segunda contención también es correcta y concluimos que $\mathcal{Q}_8$ es un grupo nilpotente.

Vemos que ver a mano que un grupo cumple la condición de nilpotente es díficil porque tenemos que proponer una serie central, además ¿cómo podemos ver que un grupo **no** es nilpotente? Vamos a ver que podemos simplificar la búsqueda, además de ver equivalencias para comprobar la no existencia de ninguna serie central. Para ello necesitaremos más teoria para solucionar este problema.

Definición 4.4. *Sean g y h elementos de un grupo G. El* ***conmutador*** *de g y h, denotado como* $[g, h]$ *es:*

$$[g, h] = g^{-1}h^{-1}gh = g^{-1}g^h \tag{4.3}$$

Donde g^h *es g conjugado por h.*

Observación 4.5. 1. Si g y h conmutan [g,h]=e

2. Si [g,h]=e implica que g y h conmutan: $g^{-1}h^{-1}gh = e$ y pasando los elementos al

otro lado vemos que conmutan.

3. Podemos ver el centro de otra manera:

$$Z(G) = \{g \in G \quad | \quad [g,h] = e \quad \text{para todo } h \in G\} \tag{4.4}$$

4. También podemos definir un subgrupo conmutador de X_1 y X_2:

$$[X_1, X_2] =< \{[x_1, x_2] \quad x_1 \in X_1, x_2 \in X_2\} > \tag{4.5}$$

5. Podemos ver que si G es abeliano [G,G]={e}

Ahora vamos a utilizar un lema para amplificarnos la vista de lo que significa el grupo conmutador:

Lema 4.6. *Si tomamos G un grupo tenemos las siguientes propiedades:*

1. *Si $H \leq G$ y $[G,G] \leq H$, entonces $H \trianglelefteq G$ y G/H es abeliano. En particular podemos utilizar: $[G,G] \trianglelefteq G$ y G/[G,G] es abeliano.*

2. *Si $N \trianglelefteq G$ y G/N es abelinano entonces $[G,G] \trianglelefteq N$.*

Demostración. 1. Sea g ∈ G y h ∈ H. Tenemos la siguiente igualdad:

$$\text{para todo } h \quad \text{para todo } g \quad h^g = g^{-1}hg = hh^{-1}g^{-1}hg = h[h,g] \in H \tag{4.6}$$

Las igualdades son simplemente operaciones y la pertenencia se debe a la hipótesis que [G,G] ≤ H por lo que para todo h y para todo g [h,g] ∈ H. Se concluye diciendo que h^g ∈ H para todo h luego H ⊴ G.

Sean g_1H y g_2H elementos de G/H podemos ver que:

$$[g_1H, g_2H] = [g_1, g_2]H = H \tag{4.7}$$

Teniendo en cuenta en la primera igualdad la multiplicación de dos elementos en G/H y en la segunda que [G,G] ≤ H. Utilizando que si el conmutador de dos elementos es el elemento nulo, esos dos elementos conmutan, como hemos tomado g_1H y g_2H cualesquiera sabemos que G/H es abeliano.

2. Si gN y hN ∈ G/N para g,h ∈ G. Utilizando el hecho de que G/N es abeliano tenemos que [gN,hN]=N además de [gN,hN]=[g,h]N. Lo que podemos concluir que [g,h] ∈ N para todo h y g. Por lo que [G,G] ≤ N.

Ahora tenemos la siguiente igualdad:

$$[x,y]^z = z^{-1}(x^{-1}y^{-1}xy)z = (z^{-1}xz)^{-1}(z{-}1yz)^{-1}(z^{-1}xz)(z^{-1}yz) = [x^z, y^z] \quad (4.8)$$

Por lo que sea z ∈ N, $[g,h]^z = [g^z, h^z]$ que pertenece a [G,G], por lo que es un grupo normal de N y concluimos.

□

En la prueba vemos que $[g,h]^z = [g^z, h^z]$ pero el z no utilizamos que este en N para esa igualdad, es decir podemos hacer que z pertenezca a G y seguiría siendo verdad. Por lo que [G,G] ⊴ G,

Este lema nos dice que el subgrupo conmutador de un grupo es el subgrupo normal más pequeño que induce un cociente abeliano.

Vamos a dar un ejemplo para ver como podemos calcular [G,G] o **grupo derivado**:

Ejemplo 4.7. Vamos a calcular el grupo derivado del grupo alternado A_n sobre el conjunto S= {1,2,...,n}. Sabemos que para n=1,2,3 el grupo alternado es abeliano por lo que podemos concluir que $[A_n, A_n]$={e}.

Para n=4 notemos que A_4 contiene un único subgrupo normal no trivial (podemos utilizar los argumentos del segundo y tercer teoremas de Sylow):

$$K = \{e, (12)(34), (13)(24), (14)(23)\} \quad (4.9)$$

Como $[A_4$:K]=3, y sabiendo que salvo isomorfismos el único grupo de 3 elementos es $\mathbb{Z}_3$ deducimos que A_4/K es abeliano.

Juntando la existencia de un único grupo normal y por el lema que acabamos de ver que $[A_4, A_4]$⊴ K. Sabemos que $[A_4, A_4]$ es diferente de el elemento unidad ya que A_4 no es abeliano, entonces $[A_4, A_4]$=K.

Evitaremos demostrar el siguiente resultado muy importante: El grupo alternado para n ≤ 5 no tiene ningún subgrupo normal propio. Esta situado en el apéndice.

Considereamos ahora el caso n ≥ 5. En este caso A_n es simple: no tiene subgrupos normales propios. Por lo que como A_n no es abeliano, se sigue que $[A_n, A_n]$=A_n

Ejemplo 4.8. Calcularemos ahora el grupo derivado del grupo simétrico S_n sobre el conjunto S= {1,2,...,n}. Para n=1,2 S_n es abeliano asi que [S_n,S_n]={e}.

Evitaremos demostrar el siguiente resultado muy importante: El grupo simétrico para n ≤ 5 **solo** tiene A_n como subgrupo normal propio.

Ahora vamos a utilizar que A_n es un subgrupo normal de índice 2 en S_n por lo que S_n/A_n es un grupo abeliano. Para n $\geq$ 5 como sabemos que S_n no es abeliano y S_n/A_n es un grupo abeliano podemos concluir que $[S_n,S_n]=A_n$.

Veamos ahora para n=3, seguimos sabiendo que $[S_3,S_3] \trianglelefteq A_3$. Vamos a ver ahora que A_3 está contenido en $[S_3,S_3]$. Por ejemplo:

$$(123) = [(23), (132)] \quad (132) = [(23), (123)] \tag{4.10}$$

Por lo que $[S_3,S_3]=A_3$

Podemos hacer lo mismo con A_4 para ver que $[S_4,S_4]=A_4$

4.2. Series centrales ascendentes y descendentes

Definición 4.9. *Una **serie central descendente** de un grupo G es la secuencia de subgrupos:*

$$G = G_1 \trianglerighteq G_2 \trianglerighteq ... \trianglerighteq G_i \trianglerighteq ... \tag{4.11}$$

donde para cada n:

$$G_{n+1} = [G_n, G] \tag{4.12}$$

Comenzando por $G_2 = [G, G]$ el derivado de G.

Veamos que está definición tiene sentido y que esta serie definida cumple las condiciones de serie central quitando la restricción que acabe en el elemento unidad. Para ello tenemos que ver que cada G_i es normal y que G_{i-1}/G_i este contenido en Z(G/G_i).

Vamos a utilizar la propiedad ya probada $[g, h]^z = [g^z, h^z]$ para ver que cada G_i es normal. Es fácil ver que el grupo derivado, es normal ya que como G es normal sobre G, $[G, G]^z = [G^z, G^z] = [G, G]$ que concluye que es normal.

Fijemonos ahora en la sucesion de G_i, siguen la siguiente sucesión:

$$G \quad [G, G] \quad [[G, G], G] \quad [[[G, G], G], G]... \tag{4.13}$$

Como ya hemos dicho G y [G,G] son normales, ahora volviendo a utilizar la propiedad $[g, h]^z = [g^z, h^z]$ por inducción podemos ver que todos los G_i son normales.

Para ver que G_{i-1}/G_i este contenido en Z(G/G_i) utilizaremos el siguiente lema que es la razón de porque hemos definido así la serie:

Lema 4.10. *Sea G un grupo y supongamos que $N \trianglelefteq G$ y $H \leq G$. Entonces [H,G] $\leq N$ si y solo si $HN/N \leq Z(G/N)$.*

Demostración. Supongamos que [H,G] $\leq$ N y sea sN $\in$ HN/N con s $\in$ HN, por lo que s=hn con h $\in$ H y n $\in$ N. Teniendo en cuenta que s=hnN=hN, y tomando un elemento gN de G/N, podemos ver:

$$[sN, gN] = [hnN, gN] = [hN, gN] = [h, g]N = N \tag{4.14}$$

Donde la última ecuación es por nuestra hipótesis. Por la equivalencia entre dos elementos conmutan si y solo si su conmutador es el elemento unidad, podemos concluir que cualquier elemento de HN/N está en Z(G/N).

Ahora suponemos que HN/N $\leq$ Z(G/N), sea h $\in$ H h=he $\in$ HN por lo que hN $\in$ HN/N $\leq$ Z(G/N). Por lo que para todo g $\in$ G [hN,gN]=N ya que conmuta. Es decir [h,g]N=N y terminamos viendo que [h,g] $\in$ N. □

Sabiendo que cada $G_{n+1} = [G_n, G]$ es facil ver que cumple la primera condición del lema, además cada G_n está contenido en el anterior podemos concluir que $G_nG_{n-1}/G_n = G_{n-1}/G_n$, y terminamos con G_{n-1}/G_n está contenido en Z(G/G_n). Por lo que nuestra serie cumple las condiciones.

Ahora tenemos una manera de encontrar una serie central de un grupo, podemos ver en el ejemplo de los cuaterniones que la serie que dimos coincide con la serie central descendiente. Probemos que pasa con los ejemplos del grupo alternado y el grupo simétrico.

Ejemplo 4.11. Calcularemos la serie central descendiente del grupo alternado: Tanto para n=1,2,3 el segundo término ya es $[A_n, A_n]$={e} y como [e,A_n]={e} a partir del segundo término todos van a ser el grupo trivial. Por lo que para n=1,2,3 el grupo alternado es un grupo nilpotente, ya que su serie central descendiente acaba llegando al grupo trivial.

Para n=4 sabemos que $[A_4, A_4]$=K siendo K el grupo de Klein, que por tener 4 elementos es abeliano, asi que los términos son: $A_4 \trianglerighteq$ K $\trianglerighteq$ $\trianglerighteq$ AAAA $\trianglerighteq$ ...

Para n$\geq$5 sabemos que $[A_n, A_n]$=A_n por lo que todos los términos van a ser A_n y la serie central descendiente nunca llega al grupo trivial. Con este ejemplo vemos que hemos encontrado una manera buena de encontrar series centrales pero no hemos resuelto el problema de la no existencia de una serie central por lo que vamos a ver una equivalencia muy importante, pero antes demos otra definición.

Si tomamos G un grupo, podemos denotar $Z_0(G)$={e} y $Z_1(G)$=Z(G), también lo simplificaremos a Z_i si sabemos a que G nos referimos. Ahora tomando:

$$\pi_1 : G \to G/Z_1(G) \tag{4.15}$$

Sabemos que es un homomorfismo por ser el centro de G normal. Definimos

$$Z_2(G) = \pi_1^{-1}(Z(G/Z_1(G)) \tag{4.16}$$

Que son los elementos de G tal que pasados al cociente de Z_1 son el centro de G/Z_1. Así $Z_2/Z_1 \trianglelefteq G/Z_1$ por ser el centro, y concluimos utilizando el teorema de la correspondencia podemos decir que $Z_2 \trianglelefteq$ G. Podemos utilizar el mismo argumento para ver que $Z_i \trianglelefteq$ G.

Si ahora tenemos π_i: G$\rightarrow G/Z_i(G)$ homomorfismo, entonces tenemos que:

$$Z_{i+1} = \pi_i^{-1}(Z(G/Z_i(G)) = \tag{4.17}$$

$$= \{g \in G \quad | \quad gZ_i \textit{ pertence al centro de } G/Z_i\} \tag{4.18}$$

$$= \{g \in G \quad | \quad (gZ_i)(hZ_i) = (hZ_i)(gZ_i) \quad \text{para todo } h \in G\} \tag{4.19}$$

$$= \{g \in G \quad | \quad [g,h] \in Z_i \textit{ para todo } h \ \in G\} \tag{4.20}$$

Ayudandonos del lema 2.10 tenemos que $[Z_{i+1}, G] \leq Z_i$

Definición 4.12. *Una **serie central ascendente** de un grupo G es la secuencia de subgrupos:*

$$1 = Z_0 \lhd Z_1 \lhd ... \lhd Z_i \lhd ... \tag{4.21}$$

Donde cada grupo es definido como:

$$Z_{i+1} = \{x \in G \quad | \quad \textit{para todo } y \in G : [x,y] \in Z_i\} \tag{4.22}$$

y Z_0 es {e}.

Vemos que Z_1 es el centro de G y que se cumple que $Z_{i+1}/Z_i \subseteq$ Z(G/Z_i). Es decir, si esta serie alcanza en algún i finito a G, tendriamos una serie central por lo que G sería nilpotente.

Aparte de probar una equivalencia con las series centrales ascendentes vamos a probar un resultado que nos ayudara a ver que todos los p-subgrupos son grupos nilpotentes. Para ello vamos a necesitar del teorema 1.24 que dice que un p-subgrupo no tiene centro trivial y de los siguientes resultados:

Proposición 4.13. *Sean G y H grupos, y sean N_1 y N_2 subgrupos de G. Si $\theta \in$ Hom(G,H), entonces $\theta([N_1, N_2])$=$[\theta(N_1), \theta(N_2)]$.*

Proposición 4.14. *Sean G y K grupos. Si $\phi : G \to K$ es un homomorfismo, entonces $\phi(G_i(G)) = G_i(\phi(G))$ para cada $i \in \mathbb{N}$*

Demostración. Lo demostraremos ayudandonos de inducción sobre i. Para i=1 vemos que $\phi(G_1(G)) = \phi(G) = G_1(\phi(G))$ ya que $G_1(K) = K$ para todo subgrupo K.

Utilizando la proposición 4.13 tenemos que:

$$\phi(G_{k+1}(G)) = \phi([G_k(G), G]) = [\phi(G_k(G)), \phi(G)] = \tag{4.23}$$

$$= [(G_k(\phi(G)), \phi(G)] = G_{k+1}(\phi(G)) \tag{4.24}$$

□

Proposición 4.15. *La imagen de un homomorfismo de un grupo nilpotente G es nilpotente*

Demostración. Sea K un grupo y $\phi \in$ Hom(G,K) por la proposición 4.14 sabemos que $\phi(G_i(G)) = G_i(\phi(G))$ para cada i $\in \mathbb{N}$. Como G es nilpotente, existe un c tal que $G_c(G) = \{e\}$ y como ϕ es homomorfismo tenemos:

$$\{e\} = \phi(G_c(G)) = G_c(\phi(G)) \tag{4.25}$$

Luego $\phi(G)$ es nilpotente. □

Teorema 4.16. *Si G es un grupo finito, las siguientes condiciones son equivalentes*

1. *G es nilpotente*
2. *Cualquier imagen de un homomorfismo no trivial de G no tiene centro trivial*
3. *G aparece como miembro de su serie central ascendente*

Demostración. 1. 1 implica 2. Por definición de grupo nilpotente, el primer subgrupo (sin tener en cuenta del grupo trivial) cumple que está contenido en el centro de G. Ahora solo hay que fijarse que la imagen por un homomorfismo de un grupo nilpotente, también es nilpotente (si ϕ es el homomorfismo y la serie central de G es N_i, la serie central de $\phi(G)$ estaría compuesta de $\phi(N_i)$). Juntando estos dos hechos deducimos 2.

2. 2 implica 3 . Si Z_i<G donde Z_i es un término de la serie central ascendente, entonces tenemos que $Z_{i+1}/Z_i = Z(G/Z_i)$. Pero por hipótesis no es trivial, por lo que $Z_i < Z_{i+1}$ estrictamente. Como estamos partiendo de que G es finito, esta claro que en algún momento G aparecerá en la serie central ascendente.

3. 3 implica 1. Ya hemos comprobado que si la serie central ascendente contiene a G es una serie central por lo que G sería nilpotente.

□

Todos los p-subgrupos son nilpotentes.

Demostración. Si tenemos a G p-subgrupo, H un grupo cualquiera y ϕ: G →H . Gracias al primer teorema fundamental de isomorfía tenemos un isomorfismo de grupos entre G/kerϕ y H. Sabemos que el kerϕ (|kerϕ|>1 por ser un homomorfismo no trivial) es un subgrupo de G por lo que por ser p primo y el teorema de Lagrange concluimos que también es un p-grupo. Como hay un homomorfismo con H, H también es un p-grupo. Utilizando que todos los p-grupos no tienen centro trivial, hemos llegado a que cualquier imagen de un homomorfismo no trivial de un p-grupo no tiene centro trivial por lo que teniendo en cuenta la proposición anterior los p-grupos son nilpotentes. □

EL siguiente teorema funciona para grupos sin necesidad de reducirlos a los finitos aunque nosotros trabajemos solo con los finitos.

Proposición 4.17. *Dado G un grupo nilpotente con serie central:*

$$1 = N_0 \subseteq N_1 \subseteq ... \subseteq N_r = G \tag{4.26}$$

y la serie central ascendente:

$$1 = Z_0 \subseteq Z_1 \subseteq ... \subseteq Z_i \subseteq ... \tag{4.27}$$

Entonces $N_i \subseteq Z_i$ para 0≤ $i \leq r$ y en particular $Z_r = G$

Demostración. Vamos a probarlo utilizando inducción, para n=0 $Z_0 = \{e\} = N_0$. Ahora vamos a probarlo para i>0 suponiendo que es cierto para i-1 ($N_{i-1} \subseteq Z_{i-1}$, para simplificar $N_{i-1} = N \quad Z_{i-1} = Z$).

Como $N \subseteq Z$ existe un homomorfismo subyectivo: $\theta : G/N \to$ G/Z, definido por $\theta(gN)$=gZ para todo elemento g ∈ G. Está bien definido ya si tomamos g' un elemento de gN diferente de g, sabemos que cumple $g' = gn$. Por lo que $g'Z = \theta(g'N) = \theta(gnN) = \theta(gN) = gZ$.

Por ser θ subyectiva y homomorfismo veamos que θ envia elementos del centro de

G/N al centro de G/Z. Si tomamos g ∈ Z(G/N) sabemos que gh=hg para todo h ∈ G/N. Ahora:

$$\phi(g)\phi(h) = \phi(gh) = \phi(hg) = \phi(h)\phi(g) \quad \text{para todo } h \in G/N \tag{4.28}$$

Sabiendo que θ es subyectiva $\phi(h)$ recorre todos los elementos de G/Z y concluimos que $\phi(g)$ pertenece al centro de G/N.

Ahora como N_i/N está contenido en el centro de G/N, la imagen por ϕ va a parar a Z(G/Z)=Z_i/Z. Ahora si x ∈ N_i, sabemos que su imagen por ϕ es xZ que por lo anterior sabemos que pertence Z(G/Z)=Z_i/Z. Por lo que x ∈ Z_i □

El siguiente resultado nos motiva una definición: ¿cuál es la serie central con menor número de factores? Viendo el anterior teorema como cualquier serie central va a contener más elementos que la serie central ascendente, si el grupo es nilpotente, la serie central ascendente es la que menor número de factores tiene, antes de ello veamos la relación entre la serie central ascendente y descendente

Proposición 4.18. *Sea* $1 = N_0 \subseteq N_1 \subseteq ... \subseteq N_r = G$ *una serie central de un grupo nilpotente G, y* G_i *los factores de la serie central descendente:*

$$G_i \leq N_{n-i+1} \quad para 1 \leq i \leq n+1 \tag{4.29}$$

Demostración. Utilizaremos la inducción para n=1 se cumple. Supongamos que $G_{i-1} \leq N_{n-(i-1)+1} = N_{n-i+2}$. Para i>1, sabemos que $N_{n-i+1}/N_{n-i} \leq Z(G/N_{n-i})$ entonces sabemos que $[N_{n-i+1}, G] \leq G_{n-i}$.

Por hipótesis de inducción, tenemos que G_i=$[G_{i-1}$,G] ≤ $[N_{n-i+2}, G] \leq N_{n-i+1}$ para todo 1 ≤ i ≤ n+1 □

Teorema 4.19. *Sea G un grupo. Entonces, son equivalentes:*

1. *G es nilpotente*
2. *Existe* $n \in \mathbb{N}$ *tal que* $Z_n(G) = G$
3. *Existe* $m \in \mathbb{N}$ *tal que* $G_n(G) = \{e\}$

Demostración. Notemos por las anteriores propiedades:

$$G_{n-k+1} \leq N_k \leq Z_k \tag{4.30}$$

1. 1 implica 2.Ya hemos visto esta equivalencia en la proposición 4.16

2. 2 implica 3. Tomando $N_k = Z_k$ y utilizando 4.30 para k=0, tenemos que $G_{n+1} \leq Z_0 = \{e\}$

3. 3 implica 1. Está claro que si la serie central descendiente llega al elemento unidad, G es nilpotente.

□

Y ahora hemos visto que la çonvergencia"de alguna serie es equivalente a ser un grupo nilpotente, lo que nos facilita mucho el trabajo para ver que es y que no es un grupo nilpotente.

Ejemplo 4.20. Volviendo con el ejemplo 4.11 de la serie central descendiente del grupo alternado para n≥5. Vimos que nunca alcanzaba el grupo trivial para la serie central descendiente. Utilizando la anterior equivalencia concluimos que no es nilpotente

Observación 4.21. Veamos que n=min{ i ∈ ℕ tal que $Z_i = G$}=min{i ∈ ℕ tal que $G_{i+1} = \{e\}$ }=m Volvemos a necesitar la ecuación 4.30 y nos quedaremos con que $G_{n-k+1} \leq Z_k$. Si k=0 $G_{n+1} = \{e\}$ y como m es el mínimo que satisface esa condición, vemos que m ≤ n.

Ahora si utilizamos la ecuación 4.30 tenemos $G_{m-k+1} \leq Z_k$, y tomamos k=m vemos que G=$G_1 \leq Z_m$ y como n es el menor número que lo cumple, se satisface que n ≤ m. Con lo que n=m.

Definición 4.22. *Sea G un grupo nilpotente, definimos* ***clase de nilpotencia*** *de g denotado cl(G) por:*

$$cl(G) = min\{i \in \mathbb{N} \text{ tal que } Z_i = G\} = min\{i \in \mathbb{N} \text{ tal que } G_{i+1} = \{e\} \quad \} \tag{4.31}$$

4.3. Propiedades grupo nilpotente

Antes de llegar a un teorema muy importante ,el cual nos relaciona un grupo nilpotente con sus grupos de Sylow, necesitamos un poco de teoría para comprenderlo. Comenzaremos con varias definiciones y aclaraciones:

Definición 4.23. *El **normalizador** de un subconjunto S de un grupo G, esta definido por:*

$$N(S) = \{g \in G \text{ tal que } gSg^{-1} = S\} \tag{4.32}$$

En particular si S es un subgrupo, entonces N(S) es el mayor subgrupo de G en el cual S es un subgrupo normal.

Ahora vamos a dar otro teorema simple pero muy util para el teorema de caracterización de los grupos nilpotentes:

Teorema 4.24. *Si $G_1, ..., G_n$ son grupos nilpotentes entonces $G_1 \times ... \times G_n$ es nilpotentes*

Demostración. Con probarlo para n=2 nos sirve ya que luego para n=3 podriamos hacer el siguiente razonamiento: Como $(G_1 \times G_2) \times G_3$ es isomorfo a $G_1 \times G_2 \times G_3$ veriamos primero que $(G_1 \times G_2)$ es nilpotente y luego que el total es nilpotente. Y procederiamos de esta manera para cualquier n.

Sea G=H × K, con H,K nilpotentes por lo que existen series centrales:

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_m = H \tag{4.33}$$

$$\{e\} = K_0 \trianglelefteq K_1 \trianglelefteq ... \trianglelefteq K_m = K \tag{4.34}$$

Ahora utilizando el lema 4.10 sabemos que $[H, H_i] \leq H_{i-1}$ y $[K, K_i] \leq K_{i-1}$. Ahora repitiendo término podemos hacer que n=m y tenemos que:

$$\{e\} = H_0 \times K_0 \trianglelefteq H_1 \times K_1 \trianglelefteq ... \trianglelefteq H_m \times K_m = H \times K \tag{4.35}$$

$$[H \times K, H_i \times K_i] = [H, H_i] \times [K, K_i] \leq H_{i-1} \times K_{i-1} \tag{4.36}$$

Y volviendo a utilizar el lema 4.10 en la otra implicación concluimos que H×K es nilpotente. □

Observación 4.25. Vamos a incluir una nueva notación para simplificar y facilitar el trabajo con los cocientes. Aunque no hemos trabajado con esta notación es habitual utilizarla.

Dado N $\trianglelefteq$ G, escribimos $\bar{G}$ para denotar G/N. El efecto de la barra es enviar el elemento o subgrupo por la aplicación canónica del cociente, es decir: si π es la aplicación de paso al cociente $\bar{x} = \pi(x) = xN$.

Por el teorema de la correspondencia (o *correspondence theorem*) el homomorfismo barra define una biyección entre el conjunto de subgrupos que contienen a N en el conjunto de todos los subgrupos de $\bar{G}$. Cada subgrupo de $\bar{G}$, tiene la forma de un $\bar{H}$ para algún subgrupo H $\subseteq$ G.

Si $H \subseteq G$ arbitrario, vemos que $\bar{HN} = \bar{H}\bar{N} = \bar{H}$ ya que N es el núcleo del homomofismo de paso al cociente. Se sigue que HN es el unico subgrupo contenido en N cuya imagen en $\bar{G}$ es $\bar{H}$.

El teorema de la correspondencia también nos dice que si N $\subseteq H \subseteq K \subseteq G$ entonces $H \trianglelefteq K \iff \bar{H} \trianglelefteq \bar{K}$. En particular si N$\subseteq$H como H $\subseteq N_G(H)$ vemos que $\bar{H} \trianglelefteq \overline{N_G(H)}$ y tenemos que $\overline{N_G(H)} \subseteq N_{\bar{G}}(\bar{H})$. De hecho podemos ver más, si nos damos cuenta que $N_{\bar{G}}(\bar{H})$ es un subgrupo de $\bar{G}$, podemos escribirlo como $\bar{U}$ para algún subgrupo U con N $\subseteq U \subseteq G$. Entonces $\bar{H} \trianglelefteq \bar{U}$ y $H \trianglelefteq U$ y U $\subseteq N_G(H)$ y nos lleva a $N_{\bar{G}}(\bar{H}) = \bar{U} \subseteq \overline{N_G(H)}$ Y tenemos la igualdad entre $\overline{N_G(H)} = N_{\bar{G}}(\bar{H})$.

Teorema 4.26. *Dado un grupo G finito, entonces los siguientes enunciados son equivalentes*

1. *G es nilpotente.*
2. *$N_G(H) > H$ para cada subgrupo propio H.*
3. *Cada subgrupo propio maximal de G es normal.*
4. *Cada subgrupo de Sylow de G es normal.*
5. *G es el producto directo de sus subgrupos de Sylow.*
6. *Si a,b $\in$ G y $(|a|, |b|) = 1$ entonces a y b conmutan en G*

Demostración. 1. 1 implica 2. Como G es nilpotente tiene una serie central.

$$\{e\} = N_0 \subseteq N_1 \subseteq ... \subseteq N_r = G \tag{4.37}$$

Sea H un subgrupo propio tenemos: $N_0 \subseteq H$ y $N_r \not\subseteq H$. Tiene que exister un k tal que $N_k \subseteq H$ pero $N_{k+1} \not\subseteq H$. Vamos a demostrar que $N_{k+1} \subseteq N_G(H)$ y se seguirá que $N_G(H) > H$ buscado.

Escribimos $\bar{G} = G/N_k$ y utilizaremos la notación de barra. Como los subgrupos N_i forman una serie central tenemos que:

$$\bar{N_{k+1}} \subseteq Z(\bar{G}) \subseteq N_{\bar{G}}(\bar{H}) = \bar{N_G(H)} \tag{4.38}$$

donde las desigualdad se mantiene porque $N_k \subseteq H$, y porque $N_k \subseteq N_G(H)$ podemos quitar las barras y obtenemos $N_{k+1} \subseteq N_G(H)$.

2. 2 implica 3. Tomamos M un subgrupo propio maximal de G. Utilizando nuestra hipótesis M $<N_G(M)$ pero por ser M maximal, sabemos que $N_G(M)$=G. Y por definición de $N_G(M)$=G M es normal.

3. 3 implica 4. Vamos a razonar por reducción al absurdo. Supongamos que para algún divisor primo de |G| existe un P p-subgrupo de sylow de G que no es normal en G, equivalentemente que $N_G(P) \neq G$. Tomemos ahora M el subgrupo maximal de G que contiene a $N_G(P)$:

$$P \leq N_G(P) \leq M < G \tag{4.39}$$

Utilizando la hipótesis, sabemos que M es normal. Sea g un elemento de arbitrario de G, tenemos que $P^g \subseteq M^g \subseteq M$. Tenemos que P y P^g son p-subgrupos de Sylow de G contenidos en M entonces son p-subgrupos de Sylow de M. Luego por el segundo teorema de Sylow, exite x ∈ M tal que:

$$P^g = P^x \iff g^{-1}Pg = x^{-1}Px \iff (gx^{-1})^{-1}Pgx^{-1} = P \tag{4.40}$$

Por lo que $gx^{-1} \in N_G(P)$ y también lo podemos ver como g ∈ $N_G(P)x \subseteq N_G(P)M$. Como g fue tomado arbitrario, se sigue que G ⊆ $N_G(P)M$ pero está claro que $N_G(P)MG$. Entonces $N_G(P)M = G$. Obviamente tenemos que $N_G(P)M \leq M$, pero $N_G(P)M = G$ por lo que G≤M. En contradicción con que M sea grupo propio

4. 4 implica 5. Gracias a los teoremas de Sylow sabemos que si P es un p-subgrupo de Sylow de un grupo finito G, entonces P ⊴ G $\iff$ P es el único p-subgrupo de Sylow de G.

Supongamos ahora que G tiene orden $p_1^{r_1}p_2^{r_2}p_3^{r_3}...p_n^{r_n}$ donde los p_i son primos distintos y $r_i \in \mathbb{N}$. Ahora tomemos P_i como los p_i-subgrupos de Sylow. Utilizando la hipótesis y la observación que hemos visto en el párrafo anterior, los subgrupos de Sylow son únicos y de orden $p_i^{r_i}$ para cada p_i. Entonces para P_i, P_j para i≠j, tienen intersección trivial

Como P_i, P_j son normales, para i≠j vemos que $g_j^{-1}g_ig_j$ pertenece a P_i entonces si multiplicamos por un elemento de P_i seguirá en P_i, concretamente tenemos que $g_i^{-1}g_j^{-1}g_ig_j$. Podemos repetir el argumento y ver que $g_j^{-1}g_j^{-1}g_jg_i$ pertenece a P_j. Y ver que este es el inverso del anterior elemento. Obviamente por ser grupo el inverso pertenece también al grupo y tenemos que:

$$g_i^{-1}g_j^{-1}g_ig_j = [g_i, g_j] \in P_i \cap P_j = \{e\} \tag{4.41}$$

Acabamos de ver que los elementos de P_i conmutan con los elementos de P_j para i≠j.

Ahora definimos la aplicaciónn :

$$\phi : P_1 \times ... \times P_n \to G \tag{4.42}$$

$$\phi(g_1, ..., g_n) = g_1...g_n \tag{4.43}$$

Veamos ahora que ϕ es un isomorfismo de grupos. Para ello primero vamos a probar que es un homomorfismo, depués que es inyectiva y como tienen el mismo cardinal pues terminariamos con que es un isomorfismo.

Ahora vamos a utilizar la propiedad de que cada elemento de P_i conmuta con cada elemento de P_j para $i \neq j$ para ver que ϕ es un homomorfismo:

$$\phi((g_1, ..., g_n)(h_1, ..., h_n)) = \phi(g_1h_1, ..., g_nh_n) = g_1h_1...g_nh_n = \tag{4.44}$$

$$= g_1...g_nh_1...h_n = \phi(g_1, ..., g_n)\phi(h_1, ..., h_n) \tag{4.45}$$

Lo que confirma que ϕ es homomorfismo.

Veamos que ϕ es inyectivo, tengamos:

$$\phi(h_1, ..., h_n) = h_1...h_n = e \tag{4.46}$$

Como cada h_i y h_j conmutan y tienen orden coprimo (ya que pertenecen a grupos de Sylow de orden primo diferente) tenemos que:

$$|h_1...h_n| = |h_1|...|h_n| = 1 \tag{4.47}$$

El orden por ser un número natural nos lleva a que $|h_1| = ... = |h_n| = 1$ por lo que $h_1 = ... = h_n = e$. Entonces el kerϕ es trivial. Por lo que como hemos comentado antes, un homomorfismo inyectivo entre dos grupos del mismo orden, es un isomorfismo.

5. 5 implica 6. Partiendo de que G=$P_1 \times ... \times P_n$ donde los P_i son p_i-subgrupos de Sylow, correspondientes a p_i primos diferentes. Sea g=$g_1...g_n$ y h=$h_1...h_n$ elementos de orden coprimo en G, además para cada $i \neq j$ se tiene:

$$[g_i, g_j] = [h_i, h_j] = \{e\} \tag{4.48}$$

Luego $|g| = |g_1|...|g_n|$ y $|h| = |h_1|...|h_n|$. Como cada g_i y h_i tiene que ser una potencia de p_i, si para algún i $h_i \neq e \neq g_i$ tendríamos que p_i dividiria a g y a h por lo que no serían coprimos. Entonces si $|g|$ y $|h|$ son coprimos, solo si $|g_i|$ o $|h_i|$ es

igual a 1 para cada i. Por lo que g_i o h_i son elementos triviales para cada i.

Por lo que ahora g_i sabemos que conmuta con cualquier elemento fuera de P_i y como en el producto gh solo puede haber un elemento de P_i (o g_i es el elemento unidad y ya conmutaria con todos los demás elementos o g_i es el único elemento de P_i) podemos concluir que g_i conmuta con todos los elementos del producto gh. Podemos generar el mismo argumento con h_i y concluimos que gh=hg.

6. 6 implica 1. Primero vamos a ver que 6 implica 5 y con ello vamos a probar que 6 implica 1. **6 implica 5.** Supongamos que los elementos de orden coprimo conmutan. Sean $p_1, ..., p_n$ primos distintos divisores de G, y sean $P_1, ..., P_n$ los correspondientes subgrupos de Sylow asociados.

   Si vemos ahora que los P_i subgrupos de Sylow son normales utilizando 4 implica 5 tendriamos el resultado.

   Sean g ∈ G y h ∈ P_i para algun i. Si g ∈ P_i esta claro que la conjugación está en P_i. Pero si g no pertenece a P_i, entonces pertenece a P_j para algún j ≠ i. Entonces tiene orden coprimo, y por hipótesis conmutan por lo que el conjugado también pertenece a P_i. Por tanto $P_i \trianglelefteq G$.

   6 implica 1. Como 6 implica 5 sabemos que G es el producto directo de subgrupos de Sylow. Por ser subgrupos de Sylow tienen orden potencia prima y ya hemos visto que los p-grupos son nilpotentes. Luego por el teorema 4.24 G es un grupo nilpotente finito.

□

4.4. Teorema de la estructura de los grupos finitos abelianos

Este resultado es muy importante por dos cosas, hemos visto una çualidad"muy importante de los grupos nilpotente, y es que son "muy conmutativo", que cumplen la 6 condición del anterior teorema, y también que si sabemos que es nilpotente podemos ver de una manera más sencilla ese grupo (utlizando los grupos de Sylow).

Observación 4.27. Sabemos que todo grupo abeliano es nilpotente, por lo que todo grupo abeliano es el producto directo de sus grupos de Sylow pero de hecho podemos saber más sobre la estructura de los grupos abelianos. Antes del resultado importante necesitamos esta proposición:

Proposición 4.28. *Si G es un p-grupo finito abeliano y C es un subgrupo de G cíclico del orden mayor posible, existe un subgrupo B de G de forma que G=C × B*

Demostración. Vamos a probar por inducción sobre el número de elementos de G, es decir si para p es cierto lo será para p^2, y así sucesivamente. Es claro que para n=p G es un grupo cíclico.

Podemos suponer que C<G porque si C=G el resultado sería trivial. Ahora cogemos x ∈ G-C de orden lo menor posible. Como x≠1 el orden de x^p <que el orden de x. Como x era del menor orden posible x^p pertenece a C. Si $<x^p>$=C podríamos ver que |<x>|=p|c| lo que no es posible ya que por hipótesis C es el subgrupo cíclico más grande. Si C=<c>, existe un m tal que $x^p = c^m$ y sabemos que p|m ya que $<x^p>$es un subgrupo propio de C=<c>, y si p no dividiese a m generaria C.

Sea m=m'p. Se tiene que $x^p = (c^{m'})^p$. Llamemos y=$c^{m'}$, y pertenece a C por ser una potencia de c. Como x no pertenece a C $xy^{-1} \neq 1$ y $xy^{-1} \notin C$. Pero podemos ver que teniendo en cuenta la conmutatividad $(xy^{-1})^p = x^p(y^p)^{-1} = 1$ por la elección de y. Utilizando que x es el elemento que no pertenece a C con menor orden, sabemos que el orden de x es menor al de xy^{-1} que por lo que acabamos de ver es p. Como p (quitando 1) es el menor orden posible en un p grupo, el orden de x es p.

Sea X=<x>y consideremos el homomorfismo ϕ de g sobre G/X=. Sabiendo que C es máximo y que x no pertenece a c sabemos que X∪C={e}. Además $\phi(C) = \bar{C} = CX/X \cong C$, luego $\bar{C}$ es cíclico y del mismo orden que C. Si $\bar{G}$ tuviera un subgrupo cíclico $<\bar{g}>$ de orden mayor se tendría que:

$$| < g > | = orden(g) \geq orden(\bar{g}) = | < Barg > | > |\bar{C}| = |C| \tag{4.49}$$

Lo que es una contradicción. Por lo que $\bar{C}$ es un subgrupo cíclico de orden máximo. Ahora es cuando vamos a utilizar la hipótesis de inducción, como ||<|G| se concluye que $\bar{C}$ es un factor directo de $\bar{G}$ es decir, que existe $\bar{B} \leq \bar{G}$ tal que $\bar{G} = \bar{C} \times \bar{B}$ siendo $\bar{B} = B/X$. Así G=CB, CX∪B=X(C∪B)=X, luego $C \cup B \leq X \cup C = 1$ y G=C×B □

Teorema 4.29. ***Teorema de la estructura de los grupos finitos abelianos*** *Si G es un grupo finito abeliano, G es producto directo de grupos cíclicos.*

Demostración. Por inducción sobre el orden de G, es obvio que para n=2 se cumple. Como G es nilpotente ya sabemos que G es producto directo de sus grupos de Sylow. Si el orden de G es divisible por al menos dos primos distintos, por hipótesis de inducción cada uno de los correspondientes subgrupos de Sylow se expresará como producto directo de cíclicos y por tanto tambien G. Ahora si G es un p-grupo para algún primo p, por el teorema anterior G=C×B, siendo C un subgrupo cíclico de orden maximal. Si B=1, G es cíclico pero sino B se expresará como producto directo de cíclicos y por tanto también G. □

Capítulo 5

Funciones Zeta

5.1. Introducción a las funciones Zeta

Antes de hablar de la función Zeta de Rienmann, todo empieza con dos preguntas a priori que no se conectan fácilmente: ¿cuál es la distribución de los numeros primos en los números naturales? ¿Cual es el valor de la siguiente serie?

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + ... + \frac{1}{n^2} + ...$$

Esta última pregunta se conoció como el problema de Basilea, y fue resuelto por Euler en el 1735 y la solución es $\frac{\pi^2}{6}$. Pero Leonhard Euler no se quedó solo ahí sino que definió las siguiente función:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \tag{5.1}$$

Además de calcular la función para s=2, también en esta función dió el valor a todos lo números pares:

$$\zeta(2m) = \frac{2^{2m-1}\pi^{2m}|B_{2m}|}{(2m)!}$$

Siendo B_m los numeros de Bernouilli.

Uno de los hechos más importantes por lo que está función es tan famosa es por su gran relación con los números primos. Veamos una prueba heurística la identidad del producto de Euler, ya que aunque el tuvo la intuición de este resultado, para su prueba necesitamos conceptos del análisis complejo que quedan fuera de este trabajo fin de grado.

Teorema 5.1. ***Identidad del producto de Euler***

$$\sum_{n=1}^{\infty} n^{-s} = \prod_{p\ primos} \frac{1}{1-p^{-s}} \tag{5.2}$$

Demostración. Sabemos que por el Teorema Fundamental de la Aritmética, para cada n≥1 existe una **única** expresión de la forma:

$$n = 2^{e_2}3^{e_3}5^{e_5}...p^{e_p}...$$

Teniendo en cuenta de que p es primo, que los e_i siempre son enteros no negativos y que excepto un número finito, todos ellos son 0. Ahora elevando a la -s, vemos que:

$$n = 2^{-se_2}3^{-se_3}5^{-se_5}...p^{-se_p}... \tag{5.3}$$

Lo que vamos a buscar ahora es ver que se verifica la igualdad siguiente:

$$\sum_{n=1}^{\infty} n^{-s} = (1+2^{-s}+2^{-2s}+...)(1+3^{-s}+3^{-2s}+...)(1+5^{-s}+5^{-2s}+...)...$$

Vamos a ver que cada término de la izquierda, está una vez en el producto de la derecha, y que cada término de la derecha está en la izquierda. Fijando un n^{-s}, lo podemos descomponer como 5.3. Y ahora tomamos de cada $(1+p^{-s}+p^{-2s}+...)$ el número e_p, Está claro que el producto de todos estos elementos es igual a n^{-s} por lo que el término n^{-s} está en la derecha, además de forma única, ya que el Teorema Fundamental de la Aritmética nos da una única descomposición. Tomando un término finito de la parte de la derecha, es fácil ver que siempre hay un n que es producto de números primos.

Ahora utilizamos que:

$$1+p^{-s}+p^{-2s}+... = \frac{1}{(1-p^{-s})}$$

Y llegamos a que:

$$\sum_{n=1}^{\infty} n^{-s} = \prod_{p\ primos} \frac{1}{1-p^{-s}}$$

□

5.2. Hipótesis de Rienmann

Bernhard Rienmann empezó a estudiar la función 5.1 como Euler $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ pero ahora siendo s una variable compleja. A priori solo esta definida para aquellos s $\in \mathbb{C}$ tales que Re(s)>1 que son aquellos valores para los que la serie converge. Pero a posteriori la función holomorfa que se define en esa región se puede prologar a una función meromorfa en todo $\mathbb{C}$, que tiene un polo en s=1 siendo este un polo simple. Dicha extensión satisface:

$$\zeta(s) = 2^s \pi^{s-1} sen(\frac{\pi s}{2}) \Gamma(1-s) \zeta(1-s)$$

Se puede ver que todos los numeros pares negativos anulan la función, a estos valores los llamaremos ceros triviales de la función ζ. Lo que dice la hipótesis de Rienmann es que los ceros no triviales de la función ζ tienen parte real 1/2.

5.3. Relación hipótesis de Rienmann y teorema de los numeros primos

Antes de hablar del teorema de los números primos necesitamos hablar de la función $\pi(x)$ también llamada función contador de números primos, denota la cantidad de primos que no exceden de x.

El teorema de los números primos dice que $\pi(x) \sim \frac{x}{ln(x)}$, que implica que el cociente de estas funciones cuando x tiende a infinito es 1.

Aunque hoy conocemos que la funcion Li(x)=$\int_2^x \frac{dy}{ln(y)}$ es una de las mejores aproximaciones que tenemos, y lo podemos ver en la siguiente gráfica:

Helge von Koch demostró en 1901 que la hipótesis de Rienmann es equivalente al considerable refinamiento del teorema de los números primos: Existe una constante C >0 tal que

$$|\pi(x) - \int_2^x \frac{dy}{ln(y)}| \leq C\sqrt{x} ln(x)$$

para todo x suficientemente grande.

Lowel Schoenfeld refinó la anterior equivalencia diciendo que C=$1/8\pi$. Está claro que la función ζ esta intimamente relacionada con los números primos y su distribución.

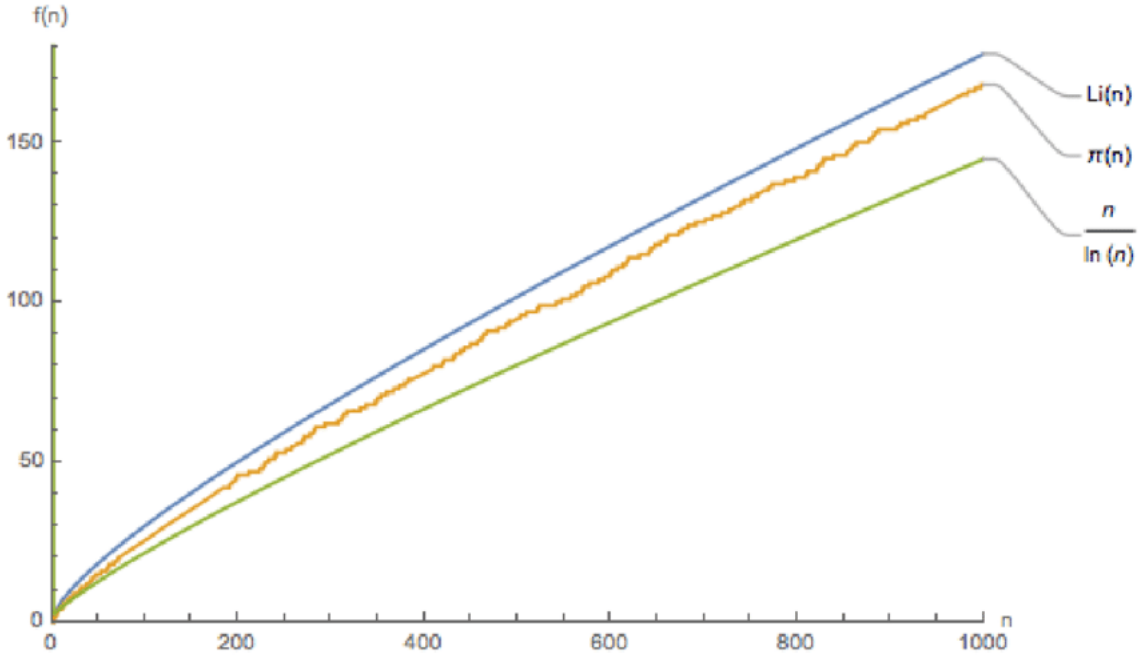

Figura 5.1: primos

5.4. Función Zeta de Dirichlet

La idea de Dirichlet fue darle una vuelta a la ecuación 5.1 y añadirle a cada término n^{-s} un coeficiente a_n bajo unas ciertas propiedades. Es decir, estudiar las funciones de variable compleja dadas por las series $\sum_{n=1}^{\infty} a_n n^{-s}$, que hoy llevan su nombre. En particular a estos a_n los ve como una función, los llama **Carácter de Dirichlet de periodo m** donde m>0 es un número entero y tienen las siguientes propiedades:

$$\chi : \mathbb{N} \to \mathbb{C}$$

1. $\chi(1)=1$
2. $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$ para todo $n_1, n_2 \in \mathbb{N}$
3. $\chi(m+n) = \chi(n)$ para todo $n \in \mathbb{N}$
4. $\chi(n) = 0$ si el máximo común divisor entre m y n es >1

En otras palabras los carácteres son esencialmente la misma forma que los homomorfismo de grupos multiplicativos $\mathbb{Z}/(m)* \to \mathbb{C}/\{0\}$ donde $\mathbb{Z}/(m)*$ es el grupo de unidades del grupo modular $\mathbb{Z}/(m)$ La L-función de Dirichlet de χ está definida por:

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} \tag{5.4}$$

Usando estas L-funciones, Dirichlet probó que si el máximo común divisor entre r y N es 1, la progresión aritmética r,r+N,r+2N,... contiene infinitos números primos. De hecho, en la prueba demuestra en cierto sentido que los primos están distribuidos uniformemente entre las clases de congruencia de enteros coprimos a N. En concreto define una medida de densidad a partir de la función Zeta de Rienmann.

La propiedad multiplicativa de los carácteres χ nos permiten probar un producto de Euler para las L-funciones de Dirichlet:

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}}$$

Nuevamente la seie que define L(s,χ) converge para Re(s)>1 y su suma en esa región se prolonga analíticamente a una función meromorfa sobre $\mathbb{C}$ que satisface una ecuación funcional. Para estas L-funciones existe su propia versión de hipótesis de Rienmann llamada Hipótesis Generalizada de Rienmann (HGR) la cual dice que: para todo carácter de Dirichlet χ y todo número complejo s con $L(s,\chi) = 0$, si la parte entera de s está comprendida entre 0 y 1, entonces la parte entera es 1/2. Los otros ceros, que son los triviales, son o bien los enteros negativos pares o bien los enteros negativos impares.

Las series de Dirichet convergentes son siempre en una región Re(s)>α para algún α que se llama abcisa de convergencia y diverge en Re(s)<α.

5.5. Función Zeta de Dedekind

Dedekind fue la primera persona que utilizó la función zeta para un objetivo algebraico. Para extensión K de los numeros racionales $\mathbb{Q}$, que se llama cuerpo de números, la función zeta de Dedekind en el cuerpo K esta definida para:

$$\zeta_K(s) = \sum_{a\ ideal} |O_K : a|^{-s}$$

Donde a es un ideal de O_K distinto de 0. Siendo O_K el anillo de enteros de K, que está definido por ser el anillo de todos los números enteros sobre $\mathbb{Z}$ contenidos en K. Un número algebraico α de K es aquel para el que existe un polinomio mónico con coeficientes en $\mathbb{Z}$ el cual posee a α como raíz.

Esta función es meromorfa sobre $\mathbb{C}$ con un polo único que es simple en s=1. El resultado más importante de las funciones zeta de Dedekind es la fórmula de número de clases, en la que podemos calcular el residuo en el polo s=1 de la función $\zeta_K(s)$ que depende de la siguiente información:

1. $\Delta(K)$ Es el discriminante del cuerpo K.

2. R_K el regulador de K.

3. u es el orden del grupo de raices de la unidad dentro del anillo de los enteros O_K

4. h_K es el número de clase de K

5. r_1 es el número de inmersiones de K en $\mathbb{R}$ y $r_2 = [K : \mathbb{Q}] - r_1$

$$Res_{s=1}(\zeta_K(s)) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{u\sqrt{|\Delta(K)|}}$$

Naturalmente la función Zeta de Dedekind satisface una ecuación funcional y tiene un producto de Euler gracias a la factorización única de ideales de O_K que fue probada por el propio Dedekind. La hipótesis de Rienmann se enuncia como las anteriores y se conoce como hipótesis de Rienmamnn extendida.

5.6. Función Zeta de grupos

Existen muchas funciones Zeta más alla de las que hemos nombrado. Para poder agruparlas existen 4 propiedades que una función Zeta debe satisfacer:

1. (ZF1) La función es meromorfa en todo el plano complejo (holomorfa menos en un punto).

2. (ZF2) La función tiene una expansión en serie de Dirichlet.

3. (ZF3) La función tiene una expansión en producto de Euler.

4. (ZF4) La función satisface una ecuación funcional.

Dado un grupo G, la definición de función Zeta de G es:

$$\zeta_G^{\leq}(s) = \sum_{H \leq G} |G : H|^{-s}.$$

Que está definida siempre que el grupo tenga una cantidad finita de subgrupos de índice n para todo n. Si el grupo es de generación finita eso sucede. Y el término que acompañaría a n^{-s} sería:

$$a_n^{\leq}(G) = |\{H : H \leq G \ y \ |G : H| = n\}|$$

Y podríamos escribir nuestra función Zeta de grupos como una serie de Dirichlet satisfaciendo ZF2:

$$\zeta_G^{\leq}(s) = \sum_{n=1}^{\infty} a_n^{\leq}(G) n^{-s}$$

Si el grupo además de ser de generación finita, es libre de torsión (si ningún elemento excepto la identidad tiene orden finito) y es un grupo nilpotente tenemos que la función zeta de grupos asociada satisface la condición ZF3:

$$\zeta^{\leq}_{G,p}(s) = \sum_{n=0}^{\infty} a^{\leq}_{p^n}(G)p^{-ns}$$

$$\zeta^{\leq}_{G}(s) = \prod_{p\ primo} \zeta^{\leq}_{G,p}(s)$$

Estos grupos de generación finita, libres de torsión y nilpotentes se llaman $\tau - grupos$ y tienen una gran importancia en la hipótesis generalizada de Rienmann. Bajo ciertas condiciones sofisticadas también se cumple ZF4.

Capítulo 6

Apéndice

6.1. Grupo alternado

En esta sección vamos a demostrar que para n $\geq$ 5 el grupo alternado A_n es simple (no contiene ningún grupo normal propio).

Lema 6.1. *El grupo alternante A_n es generado por 3-ciclos para n≥3*

Demostración. Como ya sabemos que A_n también está generado por transposiciones, si vemos que los 3-ciclos generan cualquier transposición estaría probado el lema. Como (ab)=(ba) todo par de transposiciones debe de ser uno de los siguientes:

$$(ab)(ab) = id \tag{6.1}$$

$$(ab)(cd) = (acb)(acd) \tag{6.2}$$

$$(ab)(ac) = (acb) \tag{6.3}$$

□

Lema 6.2. *Sea N un subgrupo normal de A_n donde n≥3. Si N contiene un 3-ciclo, entonces N=A_n*

Demostración. Primero vamos a demostrar que A_n es generado por 3-cicos de la forma específica (ijk) donde i y j están fijos en {1,2,...,n} pero hacemos variar k. ahora podemos ver que:

$$(iaj) = (ija)^2 \tag{6.4}$$

$$(iab) = (ijb)(ija)^2 \tag{6.5}$$

$$(jab) = (ijb)^2(ija) \tag{6.6}$$

$$(abc) = (ija)^2(ijc)(ijb)^2(ija) \tag{6.7}$$

Ahora tomamos N un subgrupo normal de A_n no trivial y que contiene un 3-ciclo de la forma (ija). Usando estas dos propiedades vemos:

$$[(ij)(ak)](ija)^2[(ij)(ak)]^{-1} = (ijk) \tag{6.8}$$

Por ser normal está en N, luego N debe de contener todos los 3-ciclos (ijk) para cualquier k. Por el anterior lema sabemos que $A_n = N$ □

Lema 6.3. *Para $n \geq 5$, todo subgrupo normal no trivial N de A_n contiene un 3-ciclo.*

Demostración. Sea σ un elemento arbitrario, distinto de la identidad, en un subgrupo normal N. Existen varias posibles estructuras de ciclos para σ

1. σ es un 3-ciclo
2. σ es el producto de ciclos disjuntos, σ=$\tau(a_1a_2...a_r) \in$ N, con r>3
3. σ es el producto de ciclos disjuntos, σ=$\tau(a_1a_2a_3)(a_4a_5a_6)$
4. σ= $\tau(a_1a_2a_3)$ donde τ es el producto de 2-ciclos disjuntos
5. σ=$\tau(a_1a_2)(a_3a_4)$ donde τ es el producto de un número par de 2-ciclos disjuntos

Ahora vamos a ver que cada una de estas opciones conduce a nuestro lema:

1. Si σ es un 3 ciclo tenemos el resultado
2. Si N contiene un producto de ciclos disjuntos y al menos uno de esos ciclos tiene r>3 es decir, $\sigma = \tau(a_1a_2a_3...a_r)$ entonces:

   $$(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \tag{6.9}$$

   Esta en N pues es normal y multiplicado por σ^{-1} sigue estando en N. Ahora desarrolemos:

   $$\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} = \sigma^{-1}(a_1a_2a_3)\sigma(a_1a_3a_2) \tag{6.10}$$

   $$(a_1a_2...a_r)^{-1}\tau^{-1}(a_1a_2a_3)\tau(a_1a_2...a_r)(a_1a_3a_2) = \tag{6.11}$$

   $$(a_1a_ra_{r-1}...a_2)(a_1a_2a_3)(a_1a_2...a_r)(a_1a_3a_2) = (a_1a_3a_r) \tag{6.12}$$

Luego N contiene un 3-ciclo.

3. Ahora supongamos que N contiene un producto disjunto de la forma $\sigma = \tau(a_1a_2a_3)(a_4a_5a_6)$. Repetimos el mismo argumento que en el anterior caso y vemos que:

$$\sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} = \tag{6.13}$$

$$[\tau(a_1a_2a_3)(a_4a_5a_6)]^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_2a_4)^{-1} = \tag{6.14}$$

$$(a_4a_6a_5)(a_1a_3a_2)\tau^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2) = \tag{6.15}$$

$$(a_4a_6a_5)(a_1a_3a_2)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2) = (a_1a_4a_2a_6a_3) \tag{6.16}$$

Así que N contiene un ciclo disjunto con r>3 por lo que podemos aplicar el caso anterior.

4. Si N es un producto disjunto de la forma $\sigma = \tau(a_1a_2a_3)$ donde τ es el producto de 2-ciclos disjuntos. Esta claro que σ^2 pertenece a N:

$$\sigma^2 = \tau(a_1a_2a_3)\tau(a_1a_2a_3) = (a_1a_3a_2) \tag{6.17}$$

Por lo que contiene un 3-ciclo

5. El último caso es $\sigma=\tau(a_1a_2)(a_3a_4)$ donde τ es el producto de un número par de 2-ciclos disjuntos. Volvemos a repetir el argumento utilizado varias veces para ver que $\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1}$ está en N.

$$\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} = \tag{6.18}$$

$$\tau^{-1}(a_1a_2)(a_3a_4)(a_1a_2a_3)\tau(a_1a_2)(a_3a_4)(a_1a_2a_3)^{-1} = \tag{6.19}$$

$$(a_1a_3)(a_2a_4) \tag{6.20}$$

utilizando nuestra hipótesis que n≥5 podemos coger b$\neq a_1, a_2, a_3, a_4$. Tomemos $\mu = (a_1a_3b)$, entonces $\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4)$ esta en N.

$$\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) = \tag{6.21}$$

$$(a_1ba_3)(a_1a_3)(a_2a_4)(a_1a_3b)(a_1a_3)(a_2a_4) = (a_1a_3b) \tag{6.22}$$

Por lo tanto N contiene un 3-ciclo.

□

Teorema 6.4. *El grupo alternado A_n es simple para n≥5*

Demostración. Sea N un subgrupo no trivial de A_n sabemos por el lema anterior que contiene un 3-ciclo. Tambíen sabemos que si contiene un 3-ciclo N=A_n por lo que A_n no

contiene ningún subgrupo normal que sea propio y no trivial para n$\geq$5 $\square$

Referencias

[1] I.Martin Isaacs (2008) *Finite Group Theory (Graduate Studies in Mathematics)*

[2] Anthony E. Clement, Stephen Majewicz, Marcos Zyman (2017) *The Theory of Nilpotents Groups*

[3] Thiago Feipe da Silva (2015) *Nilpotencia y p-nilpotencia de Grupos Finitos*

[4] Marcus du Satoy, Luke Woodward (1925) *Zeta Functions of Groups and Rings*

[5] Lidl, R y Pilz, G (1997), *Applied Abstract Algebra. EEUU: editorial Board (Springer)*