Grupos finitos

Notas de clase de
Eugenio Miranda Palacios
para el curso 2010/2011
Adaptadas por Manuel Bullejos
para el curso 2020/2021

Índice

4. Series de composición. Grupos resolubles

Definición 4.1. Sea G un grupo. Llamamos *factor de* G a cualquier grupo cociente H/H' donde $G > H \rhd H'$.

Nótese que ni H ni H' tienen que ser normales en G.

Definición 4.2. Dados dos factores H/H', K/K' de un grupo G, el cociente

$$\frac{K'(H \cap K)}{K'(H' \cap K)}$$

se llama *proyección de* H/H' *sobre* K/K'

(Comparar con el lema de Zassenhaus o de la mariposa).

Definición 4.3. Llamamos *serie* del grupo G a una cadena finita de subgrupos

$$G = G_0 > G_1 > \cdots > G_r = 1 \tag{4.1}$$

Al número natural r le llamamos *longitud* de la serie 4.1

Definición 4.4. Dadas dos series para el mismo grupo G:

$$G = G_0 > G_1 > \cdots > G_r = 1$$
$$G = G'_0 > G'_1 > \cdots > G'_s = 1$$

decimos que la primera es un *refinamiento* de la segunda si todo grupo de la segunda aparece en la primera. Si además en la primera hay grupos que no aparecen en la segunda diremos que es un *refinamiento propio*.

Definición 4.5. Una serie 4.1 se llama *normal* si para todo $i = 1, 1, \ldots, r$ se verifica que G_i es un subgrupo normal de G_{i-1}.

Una serie 4.1 se llama *propia* si todas las inclusiones son propias.

Para cada serie 4.1 normal los grupos cocientes G_{i-1}/G_i se llaman *factores de la serie*

Dadas dos series normales

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$$
$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = 1$$

del mismo grupo G diremos que son *isomorfas* si $r = s$ y existe una permutación $\sigma \in S_r$ tal que $G_{i-1}/G_i \cong H_{\sigma(i)-1}/H_{\sigma(i)}$ para todo $i = 1, 2, \ldots r$.

Definición 4.6. Una serie normal propia sin refinamientos normales propios se llama *serie de composición del grupo* G.

Para cada serie de composición de G los factores de la serie se llaman *factores de composición del grupo* G. Los órdenes de los factores de composición se llaman *índices de composición del grupo* G.

Definición 4.7. Un grupo G se llama *simple* si no es trivial y no admite subgrupos normales propios.

Lema 4.8. *Un grupo abeliano finito simple es cíclico de orden primo*

Demostración. En un grupo abeliano G todos los subgrupos son normales. Así que G será simple si y sólo si no tiene subgrupos propios. Sea $1 \neq x \in G$. El grupo cíclico $< x >$ es un subgrupo no trivial de G, luego $< x >= G$ es cíclico. Si $|G| = mn$ no es primo, $< x^m >$ sería un subgrupo propio de G, contradicción. □

Lema 4.9. *Los factores de composición de un grupo G son simples.*

Demostración. Sea 4.1 una serie de composición del grupo G. y sea H un subgrupo normal propio de G_{i-1}/G_i. Sea $p : G_{i-1} \to G_{i-1}/G_i$ la proyección y sea $H' = p^*(H)$. Entonces $G_{i-1} \rhd H' \rhd G_i$ y las inclusiones son propias. La serie $G = G_0 \rhd \cdots \rhd G_{i-1} \rhd H' \rhd G_i \rhd \cdots \rhd 1$ es un refinamiento propio de la dada, contradicción. □

No es cierto que todo grupo posea una serie de composición. De hecho $\mathbb{Z}$ no la tiene. Sin embargo tenemos:

Lema 4.10. *Todo grupo finito G posee una serie de composición.*

Demostración. Inducción sobre el orden de G. Para grupos de orden primo, $G \rhd 1$ es una serie de composición. Supongámoslo demostrado para todos los grupos de orden menor que $|G|$. Sea G_1 un subgrupo normal propio maximal de G (existe porque el conjunto de subgrupos de G es finito). Sea $G_1 \rhd \cdots \rhd G_r = 1$ una serie de composición de G_1 (existe porque el orden de G_1 es estrictamente menor que el orden de G). Entonces $G \rhd G_1 \rhd \cdots \rhd G_r = 1$ es una serie de composición de G. □

Teorema 4.11 (Teorema de refinamiento de Schreier)**.** *Dos series normales arbitrarias de un grupo G tienen refinamientos isomorfos.*

Demostración. Sean las series normales

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1 \tag{4.2}$$

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = 1 \tag{4.3}$$

Llamamos $G_{ij} = G_i(H_j \cap G_{i-1})$, $i = 1, \ldots, r$, $j = 1, \ldots s$. Entonces $G_{i-1} = G_{i0} \rhd G_{i1} \rhd \cdots G_{is} = G_i$ es una cadena normal de G_{i-1} a G_i. Uniendo estas cadenas obtenemos un refinamiento de 4.2:

$$G = G_{10} \rhd G_{11} \rhd \cdots \rhd G_{1s}(= G_{20}) \rhd G_{21} \rhd \cdots \rhd G_{r-1,s} \\ (= G_{r0}) \rhd \cdots \rhd G_{rs} = 1 \tag{4.4}$$

Similarmente los grupos $H_{ij} = H_j(G_i \cap H_{j-1})$, $i = 1, \ldots, r$, $j = 1, \ldots s$ forman un refinamiento de 4.3:

$$G = H_{01} \triangleright H_{11} \triangleright \cdots \triangleright H_{r1} (= H_{02}) \triangleright H_{12} \triangleright \cdots \triangleright H_{s-1,r} (= H_{s0}) \triangleright \cdots \triangleright H_{sr} = 1 \quad (4.5)$$

Por el lema de Zassenhaus, $G_{i,j-1}/G_{ij} \cong H_{j.i-1}/H_{ji}$, lo que demuestra que los refinamientos anteriores son isomorfos. Si omitimos todas las repeticiones en 4.4 y 4.5 (correspondientes a factores triviales), las series que quedan siguen siendo isomorfas. □

Teorema 4.12 (Teorema de Jordan-Hölder)**.** *Si un grupo admite una serie de composición, cualquier serie normal propia puede refinarse a una serie de composición.*

Dos series de composición de un grupo G son isomorfos.

Demostración. Sea G un grupo que admite una serie de composición. Cualquier refinamiento de tal serie coincide con ella misma. Tomemos cualquier serie normal de G y construimos los refinamientos isomorfos de esta serie y la serie de composición dada que existen por el teorema de refinamiento de Schreier. Deben ser series de composición isomorfas a la dada. □

4.1. El programa de Hölder

Sea G un grupo y N un subgrupo normal de G. El primer teorema de isomorfismo nos dice que el grupo cociente G/N describe la estructura de G "sobre" N (es decir, los retículos de subgrupo son isomorfos). Esto plantea el problema de hasta que punto el conocimiento de N y G/N fuerza cómo tiene que ser G.

El teorema de Jordan-Hölder nos dice que todo grupo finito tiene una serie de composición y aunque la serie en sí no tiene que ser única, su longitud y los tipos de isomorfismo de los factores sí son únicos. Además está claro que grupos isomorfos tienen los mismos factores de composición, aunque grupos no isomorfos también pueden tener los mismos factores (por ejemplo, $\mathbb{Z}_6$ y S_3).

Esta situación motiva un programa de dos partes para clasificar todos los grupos finitos salvo isomorfismo, expuesto por Hölder en un artículo de 1893:

1. Clasificar todos los grupos finitos simples.
2. Hallar las técnicas para construir grupos a partir de otros mas sencillos.

Estos dos problemas son una motivación importante para gran parte del desarrollo de la teoría de grupos. Problemas análogos se encuentran recurrentemente a través de toda la matemática. Vamos a comentar un poco los dos problemas del programa de Hölder:

La clasificación de los grupos simples finitos se completó en 1980. Los esfuerzos de unos 100 matemáticos repartidos entre 300 y 500 artículos que cubren entre 5,000 y 10,000 páginas de revistas demostraron el siguiente teorema:

Teorema 4.13. *Existe una lista consistente en 18 familias infinitas de grupos simples y 26 grupos simples no pertenecientes a estas familias (los* grupos simples esporádicos*) tal que todo grupo simple finito es isomorfo a uno de los grupos de esta lista.*

Tres ejemplos de familias infinitas: $\mathbb{Z}_p$ para p primo, A_n para $n \geq 5$ y $PSL_n(F)$ para $n \geq 2$ excepto $PSL_2(\mathbb{Z}_2)$ y $PSL_2(\mathbb{Z}_3)$.

Una idea de la complejidad de la clasificación de los grupos finitos simples la proporciona uno de los teoremas claves de la clasificación:

Teorema 4.14 (Feit-Thompson)**.** *Si G es un grupo simple de orden impar, entonces $G \cong \mathbb{Z}_p$ para algún primo impar p.*

La demostración de este teorema (publicado en 1963) ocupa 255 páginas de matemática dura.

La segunda parte del programa de Hölder se llama *problema de la extensión.* Vamos a describirla con más precisión: Dados dos grupos H y K, determinar (salvo isomorfismo) todos los grupos G que contienen un subgrupo normal N tal que $N \cong H$ y $G/N \cong K$ (se suele decir que G *es una extensión de K por H*). Por ejemplo si $H = K = \mathbb{Z}_2$ existen exactamente dos posibilidades: $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$. El programa de Hölder busca cómo pueden construirse los dos grupos de orden 4 a partir de los de orden 2 sin tener un conocimiento previo de la existencia de aquellos. Esta parte del programa de Hölder es extremadamente difícil aún cuando los subgrupos envueltos son de orden pequeño. Por ejemplos, si $|G| = 2^n$ todos los factores de composición tienen orden 2.

Sin embargo el número de grupos no isomorfos de orden 2^n crece exponencialmente como función de n:

Orden:	Número de Grupos:
2	1
4	2
8	5
16	14
32	51
64	267
128	2328
256	56092
512	10494213
1024	49487365422

Así que el número de extensiones de un 2-grupo por otro 2-grupo puede ser muy grande. Aún así existen unas cuantas técnicas interesantes y poderosas para revelar la estructura de amplias clases de grupos. Mas adelante expondremos un par de maneras de construir (en el sentido anterior) grupos grandes a partir de otros mas pequeños, y aún con una técnica muy limitada (el producto semidirecto) podremos construir numerosos ejemplos nuevos de grupos y clasificar totalmente los grupos de algún tipo particular.

No sería justo decir que la teoría de grupos finitos trata *solamente* del programa de Hölder, pero sí es justo decir que el programa de Hölder sugiere un gran número de problemas y motiva bastantes técnicas algebraicas. Por ejemplo, el estudio de las extensiones de K por H cuando H es abeliano nos lleva a clasificar las acciones (por automorfismos) de K sobre H.

4.2. Grupos resolubles

El teorema de Jordan-Hölder nos dice que cada grupo determina unívocamente a su serie de composición (salvo isomorfismo). Nos permite por tanto definir clases especiales de grupos mediante propiedades que satisfacen sus factores de composición. La más evidente de tales clases es la de los grupos resolubles, que además tiene un papel clave en la teoría de Galois.

Definición 4.15. Dado un grupo G y dos elementos $x, y \in G$ el conmutador de x e y se define como

$$[x, y] = xyx^{-1}y^{-1}.$$

Algunas propiedades del conmutador son:

1. $xy = [x, y]yx$.
2. Los elementos x e e conmutan si, y sólo si, su conmutador es trivial, $[x, y] = 1$.
3. El inverso de un conmutador es un conmutador, más concretamente:

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

4. Todo conjugado de un conmutador es un conmutador, más concretamente:

$$z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}].$$

Notemos que el producto de dos conmutadores no tiene porqué ser un conmutador.

Definición 4.16. Dado dos subgrupos $H, K \leq G$ se define $[H, K]$, el conmutador de H y K, como el subgrupo generado por los conmutadores $[h, k]$ con $h \in H$ y $k \in K$,

$$[H, K] = \langle [h, k];\ h \in H, k \in K \rangle.$$

Los elementos de $[H, K]$ serán producto de conmutadores y está claro (usando la propiedad 4 anterior) que si H y K son subgrupos normales de G entonces tambien lo es $[H, K]$,

$$H, K \trianglelefteq G \Rightarrow [H, K] \trianglelefteq G.$$

Definición 4.17. El primer derivado de un grupo G es el conmutador $G' = [G, G]$.

Es claro que G es abeliano si, y sólo si, su primer derivado es trivial. Además tenemos

Proposición 4.18 (Caracterización del primer derivado)**.**

Dado un grupo G el primer derivado es un subgrupo normal, $G' \trianglelefteq G$. Además el cociente $G_{ab} = G/G'$ es un grupo abeliano, que llamaremos el abelianizado de G. Y G' es el menor subgrupo normal de G tal que el cociente es abeliano.

Demostración. Ya que $G \trianglelefteq G$, tenemos que $G' = [G, G] \trianglelefteq G$. Además para cualquier conmutador en el cociente se tiene $[xG', yG'] = [x, y]G' = 1$ y por tanto $G_{ab} = G/G'$ es abeliano. Supongamos ahora que $K \trianglelefteq G$ es un subgrupo normal tal que el cociente G/K es abeliano, entonces el conmutador de cualquiera elementos de G/N ha de ser trivial, pero $[xK, yK] = [x, y]K = 1 \Rightarrow [x, y] \in K$; $\forall x, y \in G$ y por tatno $G' \leq K$. □

Definición 4.19. Dado un grupo G, los derivados de G están definidos de forma recursiva como

$$G^{(1} := G', \text{ y supuesto definido } G^{(i}, \text{ entonces } G^{(i+1} := [G^{(i}, G^{(i}].$$

La *serie derivada de G* se define como

$$G = G^{(0} \triangleright G^{(1} \triangleright G^{(2} \triangleright \cdots \triangleright G^{(i} \triangleright \cdots$$

En general esta serie no tiene porqué alcanzar el 1. De hecho tenemos:

Teorema 4.20. *Sea G un grupo finito. Las siguientes propiedades son equivalentes:*

1. *Los factores de composición de G son cíclicos de orden primo.*
2. *G tiene una serie normal con factores cíclicos.*
3. *G tiene una serie normal con factores abelianos.*
4. *Existe un $i \geq 1$ tal que $G^{(i} = 1$.*

Demostración.

Es inmediato que $1 \Rightarrow 2 \Rightarrow 3$.

Veamos que $3 \Rightarrow 1$:

Sea $G = H_0 \triangleright \cdots \triangleright H_s = 1$ una serie normal con factores abelianos. Por el teorema de Jordan-Hölder, esta serie se puede refinar a una serie de composición, cuyos factores serán cocientes de subgrupos de la serie dada y por tanto abelianos. Todo grupo simple abeliano es cíclico de orden primo y tenemos 1.

Por último, veamos que 3 y 4 son equivalentes.

Supongamos que la serie derivada alcanza el uno. Entonces es una serie con factores abelianos y ese es el enunciado 3. A la inversa, supongamos que G tiene la siguiente serie normal con factores abelianos:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$$

Como G_0/G_1 es abeliano, el grupo G_1 contiene al derivado de G_0 que es G'. Por inducción supongamos que $G_i \supseteq G^{(i}$. Como G_i/G_{i+1} es abeliano se verifica que $G_{i+1} \supseteq G_i' \supseteq (G^{(i)})' = G^{(i+1}$. Al final $1 = G_r \supseteq G^{(r}$ y la serie derivada alcanza el 1. □

Definición 4.21. Un grupo finito G se llama *resoluble* si verifica las propiedades del teorema 4.20.

El nombre de grupo resoluble proviene de una importante aplicación a la resolución de ecuaciones por radicales que se estudia en teoría de Galois.

La clase de los grupos resolubles se comporta bien respecto a subgrupos y cocientes:

Proposición 4.22.

1. *Todo subgrupo de un grupo resoluble es resoluble.*
2. *Todo grupo cociente de un grupo resoluble es resoluble.*
3. *Sea N un subgrupo normal de G. Si N y G/N son resolubles, también G es resoluble.*

Demostración. Sea $H < G$. Por inducción se ve que para todo $i \geq 0$ se cumple $H^{(i} < G^{(i}$. Si G es resoluble existe un r tal que $H^{(r} < G^{(r} = 1$, luego H es resoluble. Un argumento similar se aplica a los cocientes.

Supongamos que N es un subgrupo normal de G y que N y G/N son grupos solubles. Existe un s tal que $(G/N)^{(s} = 1$, luego $G^{(s} < N$. Existe ahora un r tal que $N^{(r} = 1$. Luego $G^{(r+s} < N^{(r} = 1$ y G es resoluble. □

Corolario 4.23. *Un producto finito de grupos es resoluble si, y sólo si, cada factor es resoluble.*