Leandro Vendramin

Teoría de grupos

– Notas –

7 de abril de 2021

Índice general

Capítulo 1
El teorema de Jordan–Hölder

Definición 1.1. Sea G un grupo. Un subgrupo propio M de G se dice **maximal** si $M \subseteq H \subseteq G$ para algún subgrupo H de G entonces $M = H$ o $H = G$.

Ejercicio 1.2. Demuestre que $\mathbb{Q}$ no tiene subgrupos maximales.

Sea M un subgrupo maximal de $\mathbb{Q}$. Como $\mathbb{Q}$ es abeliano, M es normal en $\mathbb{Q}$. Luego $\mathbb{Q}/M \simeq C_p$ para algún primo p pues $\mathbb{Q}/M$ es un grupo abeliano simple, esto es una contradicción porque $\mathbb{Q}$ no tiene subgrupos de índice finito. En efecto, si H es un subgrupo de $\mathbb{Q}$ con $(\mathbb{Q} : H) = n$, entonces $nx \in H$ para todo $x \in \mathbb{Q}$, lo que implica que $H = \mathbb{Q}$.

Ejercicio 1.3. Demuestre que todo subgrupo propio de un grupo finito está contenido en algún subgrupo maximal.

Supongamos que existe un subgrupo $S \neq G$ de orden máximo que no está contenido en un subgrupo maximal. Como en particular S no es maximal, existe un subgrupo propio $T \neq S$ tal que $S \subseteq T \subseteq G$. Como $|S| < |T|$, el subgrupo T está contenido en algún subgrupo maximal de G. Luego S está contenido en algún subgrupo maximal, una contradicción.

Definición 1.4. Sea G un grupo. Un subgrupo M es **maximal-normal** si $M \neq G$ es normal en G y no existe $K \neq G$ normal en G tal que $M \subsetneq K$.

Ejercicio 1.5. Demuestre que M es maximal-normal en G si y sólo si G/M es simple.

Es consecuencia inmediata del teorema de la correspondencia.

Ejemplo 1.6. El grupo $\mathbb{S}_3$ posee cuatro subgrupos maximales:

$$M_1 = \langle (123) \rangle, \quad M_2 = \langle (12) \rangle, \quad M_3 = \langle (13) \rangle, \quad M_4 = \langle (23) \rangle.$$

El subgrupo M_1 es además el único maximal-normal de $\mathbb{S}_3$. El código para reproducir estos resultados es el siguiente:

```
gap> MaximalSubgroups(SymmetricGroup(3));
[ Group([ (1,2,3) ]),
  Group([ (1,2) ]),
  Group([ (2,3) ]),
  Group([ (1,3) ]) ]
gap> MaximalNormalSubgroups(SymmetricGroup(3));
[ Group([ (1,2,3) ]) ]
```

Ejemplo 1.7. El grupo $\mathbf{SL}_2(3)$ posee un único subgrupo maximal-normal isomorfo a Q_8. Posee además cinco subgrupos maximales:

$$Q_8, \quad C_6, \quad C_6, \quad C_6, \quad C_6.$$

Para reproducir estos resultados utilizamos el siguiente código:

```
gap> List(MaximalNormalSubgroups(SL(2,3)), \
StructureDescription);
[ "Q8" ]
gap> List(MaximalSubgroups(SL(2,3)), \
StructureDescription);
[ "Q8", "C6", "C6", "C6", "C6" ]
```

Ejemplo 1.8. Sea G un grupo. Si M es un subgrupo normal y maximal entonces M es maximal-normal. Sin embargo la recíproca no es cierta pues por ejemplo $1 \times C_2$ es un subgrupo maximal-normal de $\mathbb{A}_5 \times C_2$ pero no es maximal.

Definición 1.9. Una **filtración** de un grupo G es una sucesión $(G_k)_{0 \leq k \leq n}$ de grupos tal que

$$G_0 = G \supseteq G_1 \supseteq \cdots \supseteq G_k \supseteq \cdots \supseteq G_n = 1,$$

donde cada G_{k+1} es normal en G_k.

Una filtración $(G_k)_{0 \leq k \leq n}$ se dice de **Jordan–Hölder** (o **serie de composición**) si cada **factor** G_k/G_{k+1} es simple; en este caso, n es la **longitud** de la serie de composición.

Ejemplo 1.10. La sucesión $\mathbb{S}_5 \supseteq \mathbb{A}_5 \supseteq 1$ es una serie de composición de $\mathbb{S}_5$.

Ejemplo 1.11. La sucesión $\mathbb{A}_4 \supseteq \langle (12)(34), (13)(24) \rangle \supseteq \langle (12)(34) \rangle \supseteq 1$ es una serie de composición de $\mathbb{A}_4$.

Ejemplo 1.12. Sea p un número primo. El grupo cíclico C_{p^2} admite la serie de composición $C_{p^2} \supseteq C_p \supseteq 1$. El grupo no cíclico $C_p \times C_p$ admite la serie de composición $C_p \times C_p \supseteq C_p \supseteq 1$. Estas series de composición tienen factores isomorfos, pero $C_{p^2} \not\cong C_p \times C_p$.

Ejemplo 1.13. La sucesión

$$\mathbf{SL}_2(3) \supseteq Q_8 \supseteq C_4 \supseteq C_2 \supseteq 1$$

es una serie de composición para $\mathbf{SL}_2(3)$. El código es el siguiente:

```
gap> List(CompositionSeries(SL(2,3)), \
> StructureDescription);
[ "SL(2,3)", "Q8", "C4", "C2", "1" ]
```

Proposición 1.14. *Todo grupo finito G tiene una serie de composición.*

Demostración. Si $G = 1$ basta tomar $n = 0$. Si G es simple basta tomar $n = 1$. Si $G \neq 1$ no es simple, procederemos por inducción en el orden de G. Sea N un subgrupo maximal-normal de G. Como G/N es simple y $|N| < |G|$, por hipótesis inductiva existe una serie de composición $N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = 1$ para N. Luego $G \supseteq N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = 1$ es una serie de composición para G. □

Ejercicio 1.15. Sea G un grupo que admite una serie de composición. Demuestre que todo N normal en G también admite una serie de composición.

Supongamos que $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k = 1$ es una serie de composición de G. Para cada $j \in \{0, \ldots, k\}$ sea $N_j = N \cap G_j$.

Para cada j sea $\eta_j \colon G_j \to G_j/G_{j+1}$ el morfismo canónico. Cada N_{j+1} es normal en N_j. Como $N \cap G_{j+1} = (N \cap G_j) \cap G_{j+1}$,

$$N_j/N_{j+1} = \frac{N \cap G_j}{N \cap G_{j+1}} \simeq \frac{(N \cap G_j)G_{j+1}}{G_{j+1}} = \eta_j(N \cap G_j),$$

es isomorfo a un subgrupo normal del grupo simple $\eta_j(G_j) = G_j/G_{j+1}$. Luego $N_j = N_{j+1}$ o bien $N_j/N_{j+1} \simeq G_j/G_{j+1}$ es simple. El ejercicio queda resuelto al remover los factores repetidos de la serie $N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = 1$.

Ejemplo 1.16. Sea $G = \langle g \rangle \simeq C_{30}$. Consideremos las series de composición:

$$\begin{aligned}
\mathscr{S}_1 &\colon G = \langle g \rangle \supseteq \langle g^5 \rangle \supseteq \langle g^{10} \rangle \supseteq 1, \\
\mathscr{S}_2 &\colon G = \langle g \rangle \supseteq \langle g^2 \rangle \supseteq \langle g^6 \rangle \supseteq 1, \\
\mathscr{S}_3 &\colon G = \langle g \rangle \supseteq \langle g^2 \rangle \supseteq \langle g^{10} \rangle \supseteq 1.
\end{aligned}$$

Los factores de $\mathscr{S}_1$ son C_5, C_2 y C_3. Los factores de $\mathscr{S}_2$ son C_2, C_3 y C_5. Los factores de $\mathscr{S}_3$ son C_2, C_5 y C_3.

Ejemplo 1.17. No todo grupo admite una serie de composición. El ejemplo básico es $\mathbb{Z}$ pues si K es un subgrupo normal de $\mathbb{Z}$ entonces $K \simeq d\mathbb{Z} \simeq \mathbb{Z}$.

Definición 1.18. Un **refinamiento** de $\mathscr{S}$ es una filtración obtenida al insertar finitos subgrupos en la serie $\mathscr{S}$. Por ejemplo: si G_i es normal en N y N es normal en G_{i+1} entonces

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{i+1} \supseteq N \supseteq G_i \supseteq \cdots \supseteq G_n = 1,$$

es un refinamiento de $\mathscr{S}$.

Definición 1.19. Diremos que las filtraciones

$$\mathscr{S}_1 \colon G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_k = 1,$$
$$\mathscr{S}_2 \colon G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_k = 1,$$

de G son **equivalentes** si existe $\sigma \in \mathbb{S}_k$ tal que $G_{i-1}/G_i \simeq H_{\sigma(i)-1}/H_{\sigma(i)}$ para todo $i \in \{1,\ldots,k\}$.

Ejemplo 1.20. Sea $G = \langle g \rangle \simeq C_{30}$. Las filtraciones

$$G \supseteq \langle g^5 \rangle \supseteq 1, \quad G \supseteq \langle g^{10} \rangle \supseteq 1$$

no son equivalentes. La serie subnormal

$$G \supseteq \langle g^5 \rangle \supseteq \langle g^{10} \rangle \supseteq 1$$

es refinamiento de ambas.

exercise:HK=KH

Ejercicio 1.21. Sea G un grupo y sean H, K subgrupos. Demuestre que HK es subgrupo de G si y sólo si $HK = KH$.

Supongamos que HK es subgrupo de G. Sea $x = hk \in HK$. Como HK es subgrupo de G, $x^{-1} \in HK$ y luego $x^{-1} = h_1 k_1$ para algún $h_1 \in H$ y $k_1 \in K$. Esto implica que $x = k_1^{-1} h_1^{-1} \in KH$. Recíprocamente: si $x = kh \in KH$ entonces $x^{-1} = h^{-1}k^{-1} \in HK$ y luego $x \in HK$ por ser HK subgrupo de G.

Supongamos ahora que $HK = KH$. Sean $x = hk \in HK$, $x_1 = h_1 k_1 \in HK$. Como $k^{-1}h^{-1}h_1 \in KH = HK$, entonces $x^{-1}x_1 = k^{-1}h^{-1}h_1 k_1 \in HK$. Esto implica que HK es subgrupo pues $1 \in HK$.

exercise:H_normal

Ejercicio 1.22. Sea H y K subgrupos de G. Si H es normal en G entonces HK es un subgrupo de G.

Por el ejercicio 1.21 necesitamos ver que $HK = KH$. Si $hk \in HK$ entonces $hk = k(k^{-1}hk) \in KH$ pues H es normal en G. Recíprocamente, si $kh \in KH$ entonces $kh = (khk^{-1})k \in HK$ pues H es normal en G.

lemma:Zassenhaus

Lema 1.23 (Zassenhaus). *Sean H, H_1, K, K_1 subgrupos de un grupo G. Si K_1 es normal en K y H_1 es normal en H entonces:*

1. $H_1(H\cap K_1)$ *es normal en* $H_1(H\cap K)$.
2. $K_1(H_1\cap K)$ *es normal en* $K_1(H\cap K)$.
3. $H_1(H\cap K)/H_1(H\cap K_1)\simeq K_1(H\cap K)/K_1(H_1\cap K)$.

Demostración. Como H_1 es normal en H y $H\cap K_1$ es subgrupo de H, $H_1(H\cap K_1)$ es subgrupo de H por el ejercicio 1.22 y luego $H_1(H\cap K_1)=(H\cap K_1)H_1$ por el ejercicio 1.21.

Demostremos la primera afirmación (la segunda se hace en forma análoga). Sean $h_1\in H_1$, $x\in H\cap K$. Escribimos

$$(h_1x)H_1(H\cap K_1)(h_1x)^{-1}=h_1(xH_1x^{-1})xH\cap K_1x^{-1}h_1^{-1}$$

Como H_1 es normal en H, $h_1xH_1x^{-1}\subseteq H_1$. Además $x\in H\cap K$ y K_1 es normal en K, entonces $xH\cap K_1x^{-1}\in H\cap K_1$. Luego

$$\begin{aligned}(h_1x)H_1(H\cap K_1)(h_1x)^{-1}\in H_1(H\cap K_1)h_1^{-1}&=(H\cap K_1)H_1h_1^{-1}\\&=(H\cap K_1)H_1=H_1(H\cap K_1).\end{aligned}$$

Demostremos ahora la tercera afirmación. Sean $A=H_1(H\cap K_1)$ y $B=H\cap K$.

Como $K_1\subseteq K$ es evidente que $AB=H_1(H\cap K)$.

Veamos ahora que $A\cap B=(H\cap K_1)(H_1\cap K)$. Como $H_1\subseteq H$ y $K_1\subseteq K$, tenemos $(H\cap K_1)(H_1\cap K)\subseteq H\cap K=B$. Además

$$(H\cap K_1)(H_1\cap K)\subseteq(H\cap K_1)H_1=H_1(H\cap K_1)=A.$$

Luego $(H\cap K_1)(H_1\cap K)\subseteq A\cap B$. Recíprocamente, si $a\in A\cap B$ entonces $a=xh_1$ para algún $x\in H\cap K_1$ y $h_1\in H_1$. Como $x^{-1}a=h_1\in H_1\cap K$, obtenemos inmediatamente que $a=xh_1\in(H\cap K_1)(H_1\cap K)$.

Vimos que A es un subgrupo normal de AB. Por el teorema de isomorfismo, $AB/A\simeq B/A\cap B$, es decir:

$$H_1(H\cap K)/H_1(H\cap K_1)\simeq H\cap K/(H\cap K_1)(H_1\cap K).$$

Análogamente se demuestra que $K_1(H\cap K)/K_1(H_1\cap K)\simeq H\cap K/(H\cap K_1)(H_1\cap K)$. □

theorem:Schreier

Teorema 1.24 (Schreier). *Dos filtraciones de un grupo G admiten refinamientos equivalentes.*

Demostración. Sean

$$\begin{aligned}\mathscr{S}_1&\colon G=G_0\supseteq G_1\supseteq\cdots\supseteq G_n=1,\\ \mathscr{S}_2&\colon G=H_0\supseteq H_1\supseteq\cdots\supseteq H_m=1\end{aligned}$$

filtraciones de G. Refinamos $\mathscr{S}_1$ de la siguiente forma: para cada i agrego los subgrupos $G_{i+1}(G_i\cap H_j)$, $j\in\{0,\dots,m\}$, entre G_i y G_{i+1}:

$$G_i=G_{i+1}(G_i\cap H_0)\supseteq G_{i+1}(G_i\cap H_1)\supseteq\cdots\supseteq G_{i+1}(G_i\cap H_m)=G_{i+1}.$$

Por el lema de Zassenhaus 1.23, $G_{i+1}(G_i \cap H_{j+1})$ es normal en $G_{i+1}(G_i \cap H_j)$ y tenemos un refinamiento de $\mathscr{S}_1$.

Para $\mathscr{S}_2$ hacemos algo similar. Para cada j agregamos entre H_j y H_{j+1} los subgrupos $H_{j+1}(G_i \cap H_j)$, $i \in \{0,\dots,n\}$:

$$H_j = H_{j+1}(G_0 \cap H_j) \supseteq H_{j+1}(G_1 \cap H_1) \supseteq \cdots \supseteq H_{j+1}(G_n \cap H_j) = H_{j+1}.$$

El lema de Zassenhaus implica que se tiene refinamiento de $\mathscr{S}_2$. Como además

$$\frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \simeq \frac{H_{j+1}(G_i \cap H_j)}{H_{j+1}(G_{i+1} \cap H_j)},$$

gracias al lema de Zassenhaus, los refinamientos obtenidos son equivalentes. □

theorem:JordanHolder

Teorema 1.25 (Jordan–Hölder). *Todas las series de composición de un grupo G son equivalentes.*

Demostración. Toda serie de composición es una filtración, y dos filtraciones admiten refinamientos equivalentes por el teorema de Schreier 1.24. Pero todo refinamiento de una serie de composición $\mathscr{S}$ es equivalente a $\mathscr{S}$. Luego todas las series de composición de G son equivalentes. □

Capítulo 2
El teorema de Itô

Definición 2.1. Un grupo G se dice **metabeliano** si $[G,G]$ es abeliano.

Ejercicio 2.2. Demuestre que un grupo G es metabeliano si y sólo si existe un subgrupo normal K de G tal que K y G/K son abelianos.

Ejercicio 2.3. Sea G un grupo metabeliano.

1. Si H es un subgrupo de G entonces H es metabeliano.
2. Si $f\colon G \to H$ es un morfismo entonces $f(H)$ es metabeliano.

Lema 2.4. *En un grupo valen las siguientes fórmulas:*

1. $[a,bc] = [a,b]b[a,c]b^{-1}$.
2. $[ab,c] = a[b,c]a^{-1}[a,c]$.

Demostración. Es un cálculo directo:

$$[a,b]b[a,c]b^{-1} = aba^{-1}b^{-1}baca^{-1}c^{-1}b^{-1} = abca^{-1}c^{-1}b^{-1} = [a,bc],$$
$$a[b,c]a^{-1}[a,c] = abcb^{-1}c^{-1}a^{-1}aca^{-1}c^{-1} = abcb^{-1}a^{-1}c^{-1} = [ab,c]. \qquad \square$$

Ejemplo 2.5. El grupo $\mathbb{S}_3$ es metabeliano pues $\mathbb{A}_3 \simeq C_3$ es un subgrupo normal de $\mathbb{S}_3$ tal que $\mathbb{S}_3/\mathbb{A}_3 \simeq C_2$ es abeliano.

Ejemplo 2.6. El grupo $\mathbb{A}_4$ es metabeliano pues el subgrupo

$$K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

es abeliano y normal en $\mathbb{A}_4$ y el cociente $\mathbb{A}_4/K \simeq C_3$ es abeliano.

Ejemplo 2.7. El grupo $\mathbf{SL}_2(3)$ no es metabeliano pues $[\mathbf{SL}_2(3), \mathbf{SL}_2(3)] \simeq Q_8$ no es un grupo abeliano. En efecto:

```
gap> IsAbelian(DerivedSubgroup(SL(2,3)));
false
gap> StructureDescription(DerivedSubgroup(SL(2,3)));
"Q8"
```

theorem:Ito

Teorema 2.8 (Itô). *Sea $G = AB$ una factorización de G con A y B subgrupos de G abelianos. Entonces G es metabeliano.*

Demostración. Como $G = AB$ entonces $AB = BA$. Veamos primero que $[A,B]$ es un subgrupo normal de G. Sean $a, \alpha \in A$, $b, \beta \in B$. Sean $a_1, a_2 \in A$, $b_1, b_2 \in B$ tales que $\alpha b \alpha^{-1} = b_1 a_1$, $\beta a \beta^{-1} = a_2 b_2$. Entonces, como

$$\alpha[a,b]\alpha^{-1} = a(\alpha b \alpha^{-1})a^{-1}(\alpha b^{-1}\alpha^{-1}) = ab_1a_1a^{-1}a_1^{-1}b_1^{-1} = [a,b_1] \in [A,B]$$
$$\beta[a,b]\beta^{-1} = (\beta a \beta^{-1})\beta b \beta^{-1}(\beta a^{-1}\beta^{-1})b^{-1} = a_2b_2bb_2^{-1}a_2^{-1}b^{-1} = [a_2,b] \in [A,B],$$

se concluye que $[A,B]$ es normal en G.

Veamos ahora que $[A,B]$ es abeliano. Como

$$\beta\alpha[a,b]\alpha^{-1}\beta^{-1} = \beta[a,b_1]\beta^{-1} = (\beta a \beta^{-1})b_1(\beta a^{-1}\beta^{-1})b_1^{-1} = [a_2,b_1],$$
$$\alpha\beta[a,b]\beta^{-1}\alpha^{-1} = \alpha[a_2,b]\alpha^{-1} = a_2(\alpha b \alpha^{-1})a_2^{-1}(\alpha b \alpha^{-1}) = [a_2,b_1],$$

un cálculo directo muestra que

$$[\alpha^{-1},\beta^{-1}][a,b][\alpha^{-1},\beta^{-1}]^{-1} = [a,b].$$

Como dos generadores arbitrarios de $[A,B]$ conmutan, el grupo $[A,B]$ es abeliano.

Para completar la demostración observamos $[G,G] = [A,B]$ pues

$$[a_1b_1,a_2b_2] = a_1[a_2,b_1]^{-1}a_1^{-1}a_2[a_1,b_2]a_2^{-1} \subseteq [A,B],$$

ya que $[A,B]$ es normal en G. □

Capítulo 3
El teorema del matrimonio de Hall

Supongamos que tenemos un conjunto finito de personas $p_1, p_2, \ldots, p_n$ y cada uno de esas personas, digamos la persona p_i, se postuló en varios trabajos, digamos T_i. Nos interesa saber bajo qué condiciones todas las personas podrán obtener un trabajo al que se postularon.

Teorema 3.1 (Hall). *El problema tiene solución si y sólo si para cada $k \in \{1, \ldots, n\}$ cada conjunto de k personas se postula en al menos k trabajos.*

Demostración. Demostremos primero la implicación fácil. Si existe un conjunto de k personas que se postuló a menos de k trabajos, entonces alguna de esas personas no podrá conseguir trabajo.

Para demostrar la afirmación recíproca procederemos por inducción en n, la cantidad de personas. El caso $n = 1$ es trivial. Supongamos entonces que el teorema es válido si hay $< n$ personas. Si hay n personas, hay dos casos a considerar.

Si todo conjunto de k personas, $k < n$, se postula colectivamente al menos a $k+1$ trabajos, entonces la condición de Hall se verifica (y sobrará un trabajo). Elegimos cualquier persona para que trabaje donde se haya postulado. Como la condición de Hall vale para las $n-1$ personas restantes, esas personas conseguirán un trabajo al que se postularon gracias a la hipótesis inductiva.

Si, en cambio, existe un conjunto de k personas que se postula colectivamente a exactamente k trabajos, estas k personas, por hipótesis inductiva, podrán conseguir trabajo. Quedan ahora $n-k$ personas sin trabajo. Para cada $l \leq n-k$, toda colección de l de estas personas se postula al menos a l trabajos (pues de lo contrario, estas l personas junto con las k personas anteriores se hubieran postulado colectivamente a $< l+k$ trabajos, una contradicción). Podemos aplicar entonces la hipótesis inductiva a esas $n-k$ personas y vemos que también podrán conseguir trabajo. □

El teorema fue demostrado por Hall en 1935, aunque con una prueba distinta. La demostración que presentamos es básicamente la de Halmos y Vaughan [5], aunque allí el teorema se presenta en términos de hombres, mujeres y matrimonios.

Teorema 3.2 (Hall). *Sea G un grupo finito y $H \leq G$ tal que $(G : H) = n$. Existen $g_1, \ldots, g_n \in G$ tales que $\{g_1H, \ldots, g_nH\} = \{Hg_1, \ldots, Hg_n\}$.*

Demostración. Supongamos que $\{x_1,\dots,x_n\}$ es un sistema completo de representantes de coclases de H a derecha y $\{y_1,\dots,y_n\}$ es un sistema completo de representantes de coclases de H a izquierda. Para cada $i \in \{1,\dots,n\}$ sea

$$T_i = \{j : y_j H \cap Hx_i \neq \emptyset\}.$$

Si $I \subseteq \{1,\dots,n\}$ es un subconjunto no vacío, sea $J = \cup_{i\in I} T_i$. Si $i \in I$ y $g \in Hx_i$, entonces $y \in y_j H$ para algún $j \in \{1,\dots,n\}$. En particular, $j \in A_i$ y además

$$\bigcup_{i\in I} Hx_i \subseteq \bigcup_{j\in J} y_j H.$$

Como las uniones son disjuntas, al tomar cardinalidad en esta última inclusión y observar que $|H| = |Hx_i| = |y_j H|$ para todo i, j, se concluye que $|I| \leq |J|$.

Por el teorema de Hall, existen elementos distintos $t_1 \in T_1,\dots,t_n \in T_n$ tales que $Hx_i \cap y_{t_i} H \neq \emptyset$. Para cada $i \in \{1,\dots,n\}$ sea $g_i \in Hx_i \cap y_{t_i} H$. Entonces $g_1,\dots,g_n$ es un sistema completo de representantes de coclases de H a derecha y a izquierda. □

Para poder demostrar el teorema de Weiss necesitamos unos resultados auxiliares sobre coclases dobles.

Lema 3.3. *Sean G un grupo finito, H y K subgrupos de G del mismo índice y $x \in G$. Si $\alpha_1,\dots,\alpha_m$ es un sistema completo de representantes de $H/(xKx^{-1}\cap H)$, entonces*

$$HxK = \bigcup_{i=1}^{m} \alpha_i xK \quad (\textit{unión disjunta}). \tag{3.1}$$

eq:Weiss

En particular,

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

Demostración. Sea $L = xKx^{-1} \cap H$. Primero observemos que la unión es disjunta. Si $\alpha_i xK = \alpha_j xK$, entonces

$$x^{-1}\alpha_j^{-1}\alpha_i x = (\alpha_j x)^{-1}(\alpha_i x) \in K.$$

Luego $\alpha_j^{-1}\alpha_i \in xKx \cap H = L$, es decir $\alpha_i L = \alpha_j L$, lo que implica $i = j$.

Veamos ahora que $HxK \subseteq \cup_{i=1}^{m} \alpha_i xK$, ya que la otra inclusión es trivial. Como $H = \cup_{i=1}^{m} \alpha_i L$, entonces

$$HxK \subseteq \bigcup_{i=1}^{m} \alpha_i LxK = \bigcup_{i=1}^{m} \alpha_i xK,$$

pues $LxK = xK$.

El tomar cardinalidad en (3.1) obtenemos $|HxK| = m|K|$. □

Lema 3.4. *Sean G un grupo finito y $x \in G$. Si H y K son subgrupos de G, entonces*

$$\#\{yK : yK \subseteq HxK\} = (H : xKx^{-1} \cap H).$$

Demostración. Sea $L = xKx^{-1} \cap H$. Consideremos la función

$$\varphi\colon H/L \to \{yK : yK \subseteq HxK\}, \quad hL \mapsto hxK.$$

Veamos primero que φ está bien definida. Si $hL = h_1L$ para $h, h_1 \in H$, entonces $h_1^{-1}h \in L = xKx^{-1} \cap H$, es decir $h_1^{-1}h = xkx^{-1}$ para algún $k \in K$. Como entonces $(h_1x)^{-1}(hx) = x^{-1}h_1^{-1}hx \in K$, se concluye que $(hx)K = (h_1x)K$.

Claramente, φ es sobreyectiva, pues $hxK = \varphi(hL)$ para todo $h \in H$ y $k \in K$. Veamos entonces que φ es inyectiva. Si $hxK = h_1xK$, entonces $x^{-1}h_1^{-1}hx \in K$. Luego $h_1^{-1}h \in xKx^{-1} \cap H = L$, es decir $h_1L = hL$. □

Análogamente puede demostrarse que bajo las hipótesis del lema, también se tiene que $\#\{Hz : Hz \subseteq HxK\} = (K : x^{-1}Hx \cap K)$.

Teorema 3.5 (Weiss). *Sea G un grupo finito y sean H y K subgrupos de G del mismo índice. Entonces existe un sistema común de representantes de coclases a izquierda de H en G y de coclases a derecha de K en G.*

Demostración. Primero observamos que las coclases Hy y zK tienen un representante en común si y sólo si $Hy \cap zK \neq \emptyset$ pues

$$Hx = Hy \text{ y } zK = xK \iff xy^{-1} \in H \text{ y } z^{-1}x \in K \iff x \in Hy \cap zK.$$

Sabemos que G es unión disjunta de (H,K)-coclases dobles.

Afirmación. Si

$$HxK = \bigcup_{i=1}^{k} Hy_i = \bigcup_{j=1}^{l} z_jK,$$

donde las uniones son disjuntas, entonces $k = l$ (pues H y K tienen el mismo orden) y para cada $i \in \{1,\dots,k\}$ se tiene que $Hy_i \cap z_jK \neq \emptyset$ para todo $j \in \{1,\dots,l\}$.

Fijemos $i_0 \in \{1,\dots,k\}$. Sin perder generalidad (reordenando, si fuera necesario) podemos suponer que $Hy_{i_0} \cap z_jK \neq \emptyset$ para todo $j \in \{1,\dots,m\}$. Como

$$Hy_{i_0} \subseteq \bigcup_{i=1}^{k} Hy_i = HxK = \bigcup_{j=1}^{l} z_jK,$$

entonces, en particular, $k = \#\{Hy_i : Hy_i \subseteq HxK\} = (H : xHx^{-1} \cap K)$. Como además $Hy_{i_0}K \subseteq \cup_{j=1}^{m} z_jK$, entonces

$$\frac{|H||K|}{|H \cap xKx^{-1}|} = |Hy_{i_0}K| \leq m|K|.$$

Luego se concluye que $k = m$, pues $k = (H : L) \leq m \leq k$. □

Capítulo 4
Resolubilidad

resolubles

Definición 4.1. Una **filtración resoluble** (o **serie resoluble**) es una filtración con factores abelianos.

Definición 4.2. Un grupo se dice **resoluble** si posee una filtración resoluble.

Ejemplo 4.3. Todo grupo abeliano es resoluble.

Ejemplo 4.4. $\mathbb{S}_3$ es resoluble pues $\mathbb{S}_3 \supseteq \mathbb{A}_3 \supseteq 1$ es una filtración resoluble.

Ejemplo 4.5. El grupo dihedral $\mathbb{D}_{2n} = \langle r, s : r^n = s^2 = 1, srs = r^{-1} \rangle$ de orden $2n$ es resoluble pues $\mathbb{D}_{2n} \supseteq \langle r \rangle \supseteq 1$ una filtración resoluble.

Si p y q son números primos, entonces todo grupo finito de orden $p^a q^b$ es resoluble. Este resultado fue demostrado por Burnside y fue uno de los primeros éxitos de la teoría de caracteres. El famoso **teorema de Feit–Thompson** afirma que todo grupo finito de orden impar de resoluble. La demostración es muy difícil y ocupa un volumen completo del *Pacific Journal of Mathematics* [4].

exercise:conmutador

Ejercicio 4.6. Demuestre las siguientes afirmaciones:

1. El conmutador $[G,G]$ de un grupo G es normal en G.
2. Sea H es normal en G. Entonces G/H es abeliano si y sólo si $[G,G] \subseteq H$.

Si G es un grupo se define

$$G^{(0)} = G, \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad i \geq 0.$$

La **serie derivada** de G se define entonces como

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

Ejercicio 4.7. Demuestre que cada $G^{(i)}$ es un subgrupo característico de G.

Ejemplo 4.8. El grupo $\mathbf{SL}_2(3)$ es resoluble. La serie derivada de $\mathbf{SL}_2(3)$ es $\mathbf{SL}_2(3) \supseteq Q_8 \supseteq C_4 \supseteq C_2 \supseteq 1$. Veamos el código:

```
gap> IsSolvable(SL(2,3));
true
gap> List(DerivedSeries(SL(2,3)),StructureDescription);
[ "SL(2,3)", "Q8", "C2", "1" ]
```

lemma:serie_derivada

Lema 4.9. *Sea $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ una filtración resoluble para G. Entonces $G_i \supseteq G^{(i)}$ para todo $i \geq 0$.*

Demostración. Procederemos por inducción en i. El caso $i = 0$ es trivial pues por definición $G_0 = G = G^{(0)}$. Si suponemos que el resultado es válido para $i \geq 0$ entonces, como G_i/G_{i+1} es abeliano, $[G_i, G_i] \subseteq G_{i+1}$ (ejercicio 4.6). Luego, gracias a la hipótesis inductiva,

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}. \qquad \square$$

lemma:G^n=1

Lema 4.10. *Un grupo G es resoluble si y sólo si existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$.*

Demostración. Supongamos que G es resoluble. Entonces G tiene una filtración resoluble $G = G_0 \supseteq G_1 \supseteq \cdots \subseteq G_n = 1$. Luego $G^{(n)} \subseteq G_n = 1$ por el lema 4.9. Recíprocamente si existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$ entonces, por el ejercicio 4.6, G posee una filtración resoluble $G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(n)} = 1$. $\square$

Ejemplo 4.11. Si G es un grupo simple no abeliano, entonces G no es resoluble pues $[G, G] = G$.

theorem:resoluble

Teorema 4.12. *Sea G un grupo.*

1. *Todo subgrupo H de G es resoluble.*
2. *Sea K es un subgrupo normal de G. Entonces G es resoluble si y sólo si K y G/K son resolubles.*

Demostración. La primera afirmación es fácil: como $H^{(i)} \subseteq G^{(i)}$ para todo $i \geq 0$, el resultado se obtiene inmediatamente del lema 4.10.

Demostremos la segunda afirmación. Sean $Q = G/K$ y $\pi\colon G \to Q$ el morfismo canónico. Demostramos por inducción que $\pi(G^{(i)}) = Q^{(i)}$ para todo $i \geq 0$. El caso $i = 0$ es trivial pues π es sobreyectiva. Si el resultado es válido para algún $i \geq 0$ entonces

$$\pi(G^{(i+1)}) = \pi([G^{(i)}, G^{(i)}]) = [\pi(G^{(i)}), \pi(G^{(i)})] = [Q^{(i)}, Q^{(i)}] = Q^{(i+1)}.$$

Supongamos que Q y K son resolubles. Como Q es resoluble, existe n tal que $Q^{(n)} = 1$. Como $\pi(G^{(n)}) = Q^{(n)} = 1$, se tiene que $G^{(n)} \subseteq K$. Como K es resoluble, existe m tal que

$$G^{(n+m)} \subseteq (G^{(n)})^{(m)} \subseteq K^{(m)} = 1,$$

y luego G es resoluble.

Supongamos ahora que G es resoluble. Existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$. Luego Q es resoluble pues $Q^n = f(G^{(n)}) = f(1) = 1$. Además K es resoluble por ser un subgrupo de G. $\square$

Como corolario inmediato tenemos que si H y K son grupos resolubles, entonces $H \times K$ es resoluble.

Ejemplo 4.13. Sea $n \geq 5$. El grupo $\mathbb{S}_n$ no es resoluble pues $\mathbb{A}_n$ no es resoluble.

Ejercicio 4.14. Sea p un número primo y sea P un p-grupo finito. Demuestre que $Z(P) \neq 1$.

Proposición 4.15. *Sea p un número primo y sea G un p-grupo finito. Entonces G es resoluble.*

Demostración. Procederemos por inducción en $|G|$. Supongamos que el resultado es válido para todos los p-grupos de orden $< |G|$. Como $Z(G) \neq 1$, por hipótesis inductvia $G/Z(G)$ es un p-grupo resoluble. Como $Z(G)$ es resoluble por ser un grupo abeliano, G es resoluble por el teorema 4.12. □

Ejercicio 4.16. Sea G un grupo finito. Demuestre que G es resoluble si y sólo si G admite una serie de composición con factores cíclicos de orden primo.

Definición 4.17. Sea p un número primo. Un p-grupo P se dice **elemental abeliano** si $x^p = 1$ para todo $x \in P$.

Definición 4.18. Un subgrupo M de G se dice **minimal-normal** si $M \neq 1$, M es normal en G y el único subgrupo normal de G contenido propiamente en M es el trivial.

Ejemplo 4.19. Si un subgrupo normal M es minimal (con respecto a la inclusión), entonces es minimal-normal. Sin embargo, la recíproca no es cierta. El subgrupo de $\mathbb{A}_4$ generado por $(12)(34)$, $(13)(24)$ y $(14)(23)$ es normal-minimal en $\mathbb{A}_4$ pero no es minimal.

Ejercicio 4.20. Demuestre que todo grupo finito contiene un subgrupo minimal-normal.

Ejemplo 4.21. Sea $G = \mathbb{D}_{12} = \langle r, s : r^6 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diedral de doce elementos. Los subgrupos $S = \langle r^2 \rangle$ y $T = \langle r^3 \rangle$ son minimal-normales en G.

Ejemplo 4.22. Sea $G = \mathbf{SL}_2(3)$. No es difícil demostrar que el único subgrupo minimal-normal de G es el centro $Z(\mathbf{SL}_2(3)) \simeq C_2$:

```
gap> List(MinimalNormalSubgroups(SL(2,3)), \
StructureDescription);
[ "C2" ]
```

lemma:minimal_normal

Lema 4.23. *Sea M un subgrupo minimal-normal de G. Si M es resoluble y finito entonces M es un p-grupo elemental abeliano para algún primo p.*

Demostración. Como M es resoluble, $[M,M] \subsetneq M$. Además $[M,M]$ es normal en G pues $[M,M]$ es característico en M y M es normal en G. Por minimalidad, $[M,M] = 1$ y luego M es abeliano.

Si M es finito, existe un primo p tal que $1 \neq P = \{x \in M : x^p = 1\} \subseteq M$. Como P es característico en M, P es normal en G. Por minimalidad $P = M$. □

Teorema 4.24. *Sea G un grupo finito no trivial resoluble.*

1. *Todo subgrupo maximal tiene índice p^α para algún primo p.*
2. *Existe un primo p tal que G contiene un p-subgrupo minimal-normal.*

Demostración. Para demostrar la primera afirmación procederemos por inducción en $|G|$. Si $|G|$ es una potencia de un primo no hay nada para demostrar. Supongamos entonces que $|G| \geq 6$ y sea M un subgrupo maximal de G. Sea N un subgrupo minimal-normal de G y sea $\pi\colon G \to G/N$ el morfismo canónico. Como $[G,G] \neq G$, $N \neq G$. Como $M \subseteq NM \subseteq G$, se tiene que $M = NM$ o bien $NM = G$ (por maximalidad de M). Si $M = NM \supseteq N$, entonces $\pi(M)$ es un subgrupo maximal de $\pi(G) = G/N$ y luego

$$(G : M) = (\pi(G) : \pi(M))$$

es una potencia de un primo por hipótesis inductiva. Si en cambio $NM = G$ entonces

$$(G : M) = \frac{|G|}{|M|} = \frac{|NM|}{|N|} = \frac{|N|}{|N \cap M|}$$

es una potencia de un primo pues N es un p-grupo por el lema 4.23. La segunda afirmación es consecuencia inmediata de la primera. □

Ejemplo 4.25. Sea $G = \mathbb{S}_4$. El 2-subgrupo

$$K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$$

es minimal-normal. Sin embargo, G no posee 3-subgrupos minimal-normales.

Teorema 4.26. *Sea G un grupo finito no trivial. Entonces G es resoluble si y sólo si todo cociente no trivial de G contiene un subgrupo normal abeliano no trivial.*

Demostración. Todo cociente de G es resoluble y por lo tanto contiene un subgrupo minimal-normal, que resulta abeliano. Para demostrar la recíproca procederemos por inducción en $|G|$. Sea N un subgrupo normal abeliano de G. Si $N = G$ entonces G es resoluble por ser abeliano. Si $N \neq G$, entonces $|G/N| < |G|$. Como todo cociente de G/N es un cociente de G, el grupo G/N satisface las hipótesis del teorema. Luego G/N es resoluble por hipótesis inductiva y entonces, como N y G/N son resolubles, G es resoluble. □

Como aplicación del teorema 13.4 de Schur–Zassenhaus, en el capítulo 12, teorema 13.7, demostraremos que si G es un grupo finito resoluble no trivial y p es un primo que divide al orden de G, existe un subgrupo maximal de índice una potencia de p. Otra aplicación del teorema de Schur–Zassenhaus: la teoría de Hall, una generalización de la teoría de Sylow para grupos resolubles.

exercise:resoluble

Ejercicio 4.27. Sea G un grupo. Demuestre que G es resoluble si y sólo si existe una sucesión de subgrupos normales

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = G$$

tales que cada cociente N_i/N_{i-1} es abeliano.

Si existe una sucesión de subgrupos normales $1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = G$ tales que cada cociente N_i/N_{i-1} es abeliano, entonces $[N_i, N_i] \subseteq N_{i-1}$ para cada i. Demostremos por inducción que $G^{(m)} \subseteq N_{n-m}$ para todo $m \leq n$. El caso $m = 0$ es trivial pues $G^{(0)} = G \subseteq N_n = G$; si suponemos que el resultado vale para m entonces, por hipótesis inductiva,

$$G^{(m+1)} = [G^{(m)}, G^{(m)}] \subseteq [N_{n-m}, N_{n-m}] \subseteq N_{n-m-1}.$$

Luego $G^{(n)} \subseteq N_0 = 1$ y G es resoluble.

Supongamos ahora que G es resoluble. Entonces existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$. Como cada $G^{(i)}$ es característico en G, en particular cada $G^{(i)}$ es normal en G. Además

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

Capítulo 5
Los teoremas de Hall y Wielandt

lemma:Frattini_argument

Lema 5.1 (Argumento de Frattini). *Sea G un grupo finito y sea K un subgrupo normal de G. Si $P \in \mathrm{Syl}_p(K)$ para algún primo p, entonces $G = KN_G(P)$.*

Demostración. Sea $g \in G$. Como $gPg^{-1} \subseteq gKg^{-1} = K$ pues K es normal en G y además $gPg^{-1} \in \mathrm{Syl}_p(K)$, existe $k \in K$ tal que $kPk^{-1} = gPg^{-1}$. Luego $k^{-1}g \in N_G(P)$ pues $P = (k^{-1}g)P(k^{-1}g)^{-1}$. Tenemos entonces que $g = k(k^{-1}g) \in KN_G(P)$. □

theorem:Hall

Teorema 5.2 (Hall). *Sea G un grupo finito tal que todo subgrupo maximal de G tiene índice primo o el cuadrado de un primo. Entonces G es resoluble.*

Demostración. Procederemos por inducción en $|G|$. Sea N un subgrupo minimal-normal de G y sea p el mayor divisor primo de $|N|$. Sean $P \in \mathrm{Syl}_p(N)$ y $L = N_G(P)$. Si $L = G$ entonces P es normal en G y luego, como P y G/P son resoluble por hipótesis inductiva, G es resoluble. Supongamos entonces que $L \neq G$ y sea M un subgrupo maximal que contiene a L. Por el argumento de Frattini (lemma 5.1), $G = NL = NM$. Como M es maximal, existe un primo q tal que

$$(N : N \cap M) = (G : M) \in \{q, q^2\}$$

pues $(G:M) = |G|/|M| = |NM|/|M| = |N|/|N \cap M|$. Luego q divide a $|N|$ y entonces $q \leq p$; en particular $q \not\equiv 1 \pmod{p}$. Si $g \in G$ entonces

$$gPg^{-1} \subseteq gNg^{-1} = N$$

y luego $gPg^{-1} \in \mathrm{Syl}_p(N)$. Al hacer actuar a G por conjugación en $\mathrm{Syl}_p(P)$, vemos que la cantidad de p-subgrupos de N es entonces igual a

$$(G : N_G(P)) = (G : L) \equiv 1 \pmod{p}.$$

Como $L \subseteq M$ se tiene que $L = N_M(P)$.

Supongamos que $|P| = p^\alpha$. Como $P \subseteq M$, podemos hacer actuar a P en el conjunto $X = \{mPm^{-1} : m \in M\}$. Veamos que $\{P\}$ es la única órbita que contiene un único elemento. Si $\{P_1\}$ es una órbita con un único elemento, P_1 es un subgrupo normal de

$\langle P, P_1\rangle$ y luego P_1P es un subgrupo de M de orden p^β con $\beta \leq \alpha$. Como $P \subseteq P_1P$, se concluye que $P_1P = P$ y luego $P = P_1$. Podemos descomponer al conjunto X como unión disjunta de órbitas

$$X = \{P\} \cup O(P_1) \cup \cdots \cup O(P_k),$$

donde $\{P\}$ es la única órbita que contiene solamente un elemento y cada $O(P_j)$ tiene cardinal divisible por p. Luego

$$(M : N_M(P)) = (M : L) = |X| \equiv 1 \text{ mód } p.$$

De la igualdad $(G : L) = (G : M)(M : L)$ se concluye que $(G : M) \equiv 1$ mód p. Luego $(G : M) = q^2 \equiv 1$ mód p. Como esto implica que $q \equiv -1$ mód p, se concluye que $q = 2$ y $p = q + 1 = 3$.

Como $(N : N \cap M) = 4$, al hacer actuar a N en $N/N \cap M$ por multiplicación a izquierda tenemos un morfismo no trivial $\rho : N \to \mathbb{S}_4$. Como $[N,N]$ es característico en N y N es normal en G, por la minimalidad de N hay dos posibilidades: $[N,N] = 1$ o $[N,N] = N$. Si $[N,N] = N$ entonces

$$\rho(N) = \rho([N,N]) = [\rho(N), \rho(N)].$$

Como $\mathbb{S}_4$ es resoluble, $\rho(N)$ es resoluble y luego $\rho(N) = 1$, una contradicción. Luego $[N,N] = 1$. Como N es resoluble por ser abeliano y G/N es resoluble por hipótesis inductiva, G es resoluble. □

Para terminar esta sección veremos dos resultados que permiten detectar resolubilidad. Primero necesitamos un lema.

lemma:4Wielandt

Lema 5.3. *Sea G un grupo finito. Sean H y K subgrupos de G tales que de índices coprimos. Entonces $G = HK$ y $(H : H \cap K) = (G : K)$.*

Demostración. Sea $D = H \cap K$. Como

$$(G : D) = \frac{|G|}{|H \cap K|} = (G : H)(H : H \cap K),$$

$(G : H)$ divide a $(G : D)$. Similarmente obtenemos que $(G : K)$ divide a $(G : D)$. Como $(G : H)$ y $(G : K)$ son coprimos, se concluye que $(G : H)(G : K)$ divide a $(G : D)$. En particular,

$$\frac{|G|}{|H|}\frac{|G|}{|K|} = (G : H)(G : K) \leq (G : D) = \frac{|G|}{|H \cap K|},$$

que implica $|G| = |HK|$. Como entonces $|G| = |HK| = |H||K|/|H \cap K|$, se concluye que $(G : K) = (H : H \cap K)$. □

Recordemos que si H es un subgrupo de G, la **clausura normal** H^G de H en G se define como el subgrupo

$$H^G = \langle xHx^{-1} : x \in G \rangle.$$

Ejercicio 5.4. Sea G un grupo y H un subgrupo. Demuestre que H^G es normal en G y que H^G es el (único) menor subgrupo normal de G que contiene a H.

Es trivial demostrar que H^G es normal en G. Sea N un subgrupo normal de G tal que $H \subseteq N$. Como $xHx^{-1} \subseteq xNx^{-1} = N$ para todo $x \in G$, $H \subseteq H^G \subseteq N$.

Ejemplo 5.5. Sea $G = \mathbb{A}_4$ y sea $H = \{\mathrm{id}, (12)(34)\}$. La clausura normal de H en G es el grupo $H^G = \{id, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$. El código:

```
gap> G := AlternatingGroup(4);;
gap> NormalClosure(G, Subgroup(G, [(1,2)(3,4)]));
Group([ (1,2)(3,4), (1,3)(2,4) ])
gap> StructureDescription(last);
"C2 x C2"
```

heorem:Wielandt:solvable

Teorema 5.6 (Wielandt). *Sea G un grupo finito y sean H, K, L subgrupos de G con índices coprimos dos a dos. Si H, K, L son resolubles, entonces G es resoluble.*

Demostración. Podemos suponer que $G \neq 1$. Procederemos por inducción en $|G|$. Sea N un subgrupo de G minimal-normal y sea $\pi\colon G \to G/N$ el morfismo canónico. Los subgrupos $\pi(H)$, $\pi(K)$, $\pi(L)$ de $\pi(G) = G/N$ son resolubles. Los índices de $\pi(H)$, $\pi(K)$ y $\pi(L)$ en $\pi(G)$ son coprimos dos a dos pues por ejemplo[1]

$$(\pi(G) : \pi(H)) = (G/N : H/N \cap H) = (G : NH)$$

divide a $(G : N)$. Por hipótesis inductiva, $\pi(G)$ es resoluble. Si $H = 1$ entonces $|G| = (G : H)$ es coprimo con $(G : K)$ y luego $G = K$ es resoluble. Si $H \neq 1$ sea M un subgrupo minimal-normal de H. Por el lema 4.23, M es un p-grupo para algún primo p. Sin pérdida de generalidad podemos suponer que el primo p no divide a $(G : K)$. Existe entonces $P \in \mathrm{Syl}_p(G)$ tal que $P \subseteq K$. Como los subgrupos de Sylow son conjugados, existe $g \in G$ tal que $M \subseteq gKg^{-1}$. Como $(G : gKg^{-1}) = (G : K)$ es coprimo con $(G : H)$, el lema 5.3 implica que $G = (gKg^{-1})H$.

Veamos que todos los conjugados de M están en gKg^{-1}. Si $x \in G$ escribimos $x = uv$ con $u \in gKg^{-1}$, $v \in H$ y luego, como M es normal en H,

$$xMx^{-1} = (uv)M(uv)^{-1} = uMu^{-1} \subseteq gKg^{-1}.$$

En particular, $1 \neq M^G \subseteq gKg^{-1}$ es resoluble pues gKg^{-1} es resoluble. Como por hipótesis inductiva G/M^G es resoluble, se concluye que G es resoluble al aplicar el teorema 4.12. □

Definición 5.7. Sea G un grupo finito de orden $p^\alpha m$ con p coprimo con m. Un subgrupo H de G se dice un **p-complemento** si $|H| = m$.

[1] El núcleo de la restricción $\ker(\pi|_H) = \ker\pi \cap N$ y entonces $\pi(H) \simeq H/N \cap H$.

Ejemplo 5.8. Sea $G = \mathbb{S}_3$. El subgrupo $H = \langle (123) \rangle$ es un 2-complemento y el subgrupo $K = \langle (12) \rangle$ es un 3-complemento.

Recordemos que un teorema de Burnside afirma que todo grupo finito G de orden divisible por exactamente dos números primos es resoluble. Este resultado es necesario para demostrar el siguiente teorema de Hall:

theorem:Hall:solvable

Teorema 5.9 (Hall). *Sea G un grupo finito tal que admite un p-complemento para todo primo que divide al orden de G. Entonces G es resoluble.*

Demostración. Sea $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ con los p_j primos distintos. Procederemos por inducción en k. Si $k = 1$ el resultado es cierto pues G es un p-grupo. Si $k = 2$ el resultado es válido gracias al teorema de Burnside. Supongamos entonces que $k \geq 3$. Para cada $j \in \{1,2,3\}$ sea H_j un p_j-complemento en G. Como $|H_j| = |G|/p_j^{\alpha_j}$, los H_j tienen índices coprimos.

Veamos que H_1 es resoluble. Observemos que $|H_1| = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Sea p un primo que divide a $|H_1|$ y sea Q un p-complemento en G. Como $(G : H_1)$ y $(G : Q)$ son coprimos, el lema 5.3 implica que

$$(H_1 : H_1 \cap Q) = (G : Q)$$

y luego $H_1 \cap Q$ es un p-complemento en H_1. Luego H_1 es resoluble por hipótesis inductiva. De la misma forma se demuestra que H_2 y H_3 son resolubles.

Como H_1, H_2 y H_3 son resolubles y tiene índices coprimos, el resultado se obtiene al aplicar el teorema de Wielandt 5.6. □

Capítulo 6
Nilpotencia

Primero comenzaremos repasando algunas nociones básicas sobre conmutadores y subgrupos generados por conmutadores.

Notación 6.1. Si G es un grupo y $x,y,z \in G$, denotaremos la conjugación (como acción a izquierda) de la siguiente forma: ${}^{x}y = xyx^{-1}$. Luego, el conmutador entre x e y se escribirá como $[x,y] = xyx^{-1}y^{-1} = ({}^{x}y)y^{-1}$. Además $[x,y,z] = [x,[y,z]]$. Si X,Y,Z son subgruops de G escribimos $[X,Y,Z] = [X,[Y,Z]]$. Observemos que $[X,Y] = [Y,X]$.

exercise:HallWitt

Ejercicio 6.2 (La identidad de Hall–Witt). Sea G un grupo y $x,y,z \in G$. Demuestre que

$$\left({}^{y}[x,y^{-1},z]\right)\left({}^{z}[y,z^{-1},x]\right)\left({}^{x}[z,x^{-1},y]\right) = 1. \tag{6.1}$$

eq:HallWitt

Es interesante observar que si G es un grupo tal que $[G,G]$ es central, entonces la identidad de Hall-Witt se transforma en la identidad de Jacobi.

lemma:3subgrupos

Lema 6.3 (de los tres subgrupos de Hall). *Sean X,Y,Z subgrupos de un grupo G tales que $[X,Y,Z] = [Y,Z,X] = 1$. Entonces $[Z,X,Y] = 1$.*

Demostración. Alcanza con ver que $[z,x^{-1},y] = 1$ para todo $x \in X$, $y \in Y$, $z \in Z$ (pues si $[x,y] \in C_G(z)$ entonces $[X,Y] \in C_G(z)$ y luego $[X,Y] \subseteq C_G(Z)$). Como $[y^{-1},z] \in [Y,Z]$, entonces $[x,y^{-1},z] \in [X,Y,Z] = 1$; luego ${}^{y}[x,y^{-1},z] = 1$. Similarmente, ${}^{z}[y,z^{-1},x] = 1$. Entonces, al usar la identidad de Hall–Witt 6.2, se concluye que $[z,x^{-1},y] = 1$. □

lemma:3subgrupos_general

Lema 6.4. *Sea N un subgrupo normal de un grupo G y sean $X,Y,Z \subseteq N$ subgrupos. Si $[X,Y,Z] \subseteq N$ y $[Y,Z,X] \subseteq N$. Entonces $[Z,X,Y] \subseteq N$.*

Demostración. Sea $\pi\colon G \to G/N$ el morfismo canónico. Como $[X,Y,Z] \subseteq N$,

$$\begin{aligned} 1 &= \pi([X,Y,Z]) = \pi([X,[Y,Z]]) \\ &= [\pi(X),\pi([Y,Z])] = [\pi(X),[\pi(Y),\pi(Z)]] = [\pi(X),\pi(Y),\pi(Z)]. \end{aligned}$$

Similarmente $[\pi(Y),\pi(Z),\pi(X)] = 1$. Entonces, gracias al lema de los tres subgrupos 6.3, $[\pi(Z),\pi(X),\pi(Y)] = 1$, es decir $[Z,X,Y] \subseteq N$. □

Recordemos que un grupo G se dice **perfecto** si $[G,G] = G$.

theorem:Grun

Teorema 6.5 (Grün). *Si G es un grupo perfecto, entonces $Z(G/Z(G)) = 1$.*

Demostración. Si usamos el lema de Hall 6.3 con $X = Y = G$ y $Z = \zeta_2(G)$, $1 = [\zeta_2(G), G, G] = [\zeta_2(G), [G,G]] = [\zeta_2(G), G]$. Luego $\zeta_2(G) \subseteq Z(G)$ y entonces $\zeta_2(G) = Z(G/Z(G)) = 1$. □

theorem:gamma

Teorema 6.6. *Si G es un grupo, $[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G)$ para todo $i, j \geq 1$.*

Demostración. Procederemos por inducción en j. El caso $j = 1$ es trivial pues $[G, \gamma_j(G)] = \gamma_{j+1}(G)$ por definición. Supongamos entonces que el resultado vale para algún $j \geq 1$ y para todo $i \geq 1$.

Primero observemos que

$$[G, \gamma_i(G), \gamma_j(G)] = [\gamma_i(G), G, \gamma_j(G)] = [\gamma_{i+1}(G), \gamma_j(G)] \subseteq \gamma_{i+j+1}(G)$$

por hipótesis inductiva. Además, también por hipótesis inductiva,

$$[\gamma_i(G), \gamma_j(G), G] \subseteq [\gamma_{i+j}(G), G] = \gamma_{i+j+1}(G).$$

El lema 6.4 implica entonces que $[\gamma_j(G), G, \gamma_i(G)] \subseteq \gamma_{i+j+1}(G)$. Luego

$$[\gamma_i(G), \gamma_{j+1}(G)] = [\gamma_{j+1}(G), \gamma_i(G)] = [\gamma_j(G), G, \gamma_i(G)] \subseteq \gamma_{i+j+1}(G)$$

y el teorema queda demostrado. □

Podríamos considerar conmutadores arbitrarios donde no necesariamente se asocia siempre hacia la izquierda. Por ejemplo $[G,G,G] = [[G,G],G]$ y $[G,[G,G]]$ son ambos conmutadores de peso tres.

Corolario 6.7. *Sea G un grupo. Entonces todo conmutador de peso n está contenido en $\gamma_n(G)$.*

Demostración. Procederemos por inducción en n. El caso $n = 1$ es trivial. Supongamos entonces que el resultado es válido para algún $n \geq 1$. Tenemos entonces un conmutador de la forma $[A,B]$, donde A es un conmutador de peso k, B es un conjuntador de peso l y $n = k + l$. Como $k < n$ y $l < n$, la hipótesis inductiva implica que $A \subseteq \gamma_k(G)$ y $B \subseteq \gamma_l(G)$. Luego $[A,B] \subseteq [\gamma_k(G), \gamma_l(G)] \subseteq \gamma_{k+l}(G)$ por el teorema 6.6. □

Si H y K son subgrupos de G se define

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

Definición 6.8. Sea G un grupo. Se dice que un subgrupo K de G **normaliza** a H si $K \subseteq N_G(H)$.

Definición 6.9. Sea G un grupo. Se dice que un subgrupo K de G **centraliza** a H si $K \subseteq C_G(H)$, es decir si y sólo si $[H,K] = 1$.

Ejercicio 6.10. Sean K y H subgrupos de G con $K \subseteq H$ y K normal en G. Demuestre que $[H,G] \subseteq K$ si y sólo si $H/K \subseteq Z(G/K)$.

Sean $h \in H$ y $g \in G$. $hKgK = gKhK$ si y sólo si $[h,g] \in K$.

Definición 6.11. Sea G un grupo. La **serie central descendente** es la sucesión de subgrupos $\gamma_k(G)$ definida inductivamente como

$$\gamma_1(G) = G, \quad \gamma_{i+1}(G) = [G, \gamma_i(G)] \quad i \geq 0.$$

Definición 6.12. Un grupo G se dice **nilpotente** si existe c tal que $\gamma_{c+1}(G) = 1$. El menor de los c tales que $\gamma_{c+1}(G) = 1$ será el **índice de nilpotencia** de G.

Ejercicio 6.13. Demuestre que todo grupo nilpotente es resoluble.

Por inducción se demuestra que $G^{(i)} \subseteq \gamma_i(G)$ para todo $i \geq 1$. Luego si existe c tal que $\gamma_{c+1}(G)$ entonces G es resoluble pues $G^{(c+1)} = 1$.

Ejemplo 6.14. Un grupo es nilpotente de clase uno si y sólo si es abeliano.

Ejemplo 6.15. $\mathbb{S}_3$ es resoluble pues $\mathbb{S}_3 \supseteq \mathbb{A}_3 \supseteq 1$ es una serie de composición con factores abelianos pero $\mathbb{S}_3$ no es nilpotente pues

$$\gamma_1(\mathbb{S}_3) = \mathbb{A}_3, \quad \gamma_2(\mathbb{S}_3) = [\mathbb{A}_3, \mathbb{S}_3] = \mathbb{A}_3.$$

Luego $\gamma_i(\mathbb{S}_3) \neq 1$ para todo $i \geq 1$.

Ejemplo 6.16. El grupo $G = \mathbb{A}_4$ no es nilpotente pues

$$\gamma_1(G) = G, \quad \gamma_j(G) = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$$

para todo $j \geq 2$. Podemos usar la función `LowerCentralSeries` para calcular la sucesión $\gamma_j(G)$:

```
gap> List(LowerCentralSeries(AlternatingGroup(4)),\
StructureDescription);
[ "A4", "C2 x C2" ]
```

Alternativamente, podemos calcular a mano la sucesión $\gamma_j(G)$:

```
gap> G := AlternatingGroup(4);;
gap> gamma_1 := G;;
gap> gamma_2 := DerivedSubgroup(G);;
gap> gamma_3 := CommutatorSubgroup(gamma_2,G);;
gap> StructureDescription(gamma_1);
"A4"
gap> StructureDescription(gamma_2);
```

```
"C2 x C2"
gap> StructureDescription(gamma_3);
"C2 x C2"
```

Ejemplo 6.17. El grupo $G = \mathbf{SL}_2(3)$ no es nilpotente:

```
gap> IsNilpotent(SL(2,3));
false
```

exercise:gamma

Ejercicio 6.18. Sea G un grupo. Demuestre las siguientes afirmaciones:

1. Cada $\gamma_i(G)$ es un subgrupo característico de G.
2. $\gamma_i(G) \supseteq \gamma_{i+1}(G)$ para todo $i \geq 1$.
3. Si $f\colon G \to H$ es un morfismo sobreyectivo, $f(\gamma_i(G)) = \gamma_i(H)$ para todo $i \geq 1$.

Todas las afirmaciones se demuestran fácilmente por inducción. El paso inductivo para la primera es el siguiente: si $f \in \mathrm{Aut}(G)$ entonces

$$f(\gamma_{i+1}(G)) = f([G,\gamma_i(G)]) = [f(G), f(\gamma_i(G))] \subseteq [G,\gamma_i(G)] = \gamma_{i+1}(G).$$

Para la segunda:

$$\gamma_{i+1}(G) = [G,\gamma_i(G)] \subseteq [G,\gamma_{i-1}(G)] = \gamma_i(G).$$

Similarmente, el paso inductivo para demostrar la tercera afirmación:

$$f(\gamma_{i+1}(G)) = f([G,\gamma_i(G)]) = [f(G), f(\gamma_i(G))] = [H,\gamma_i(H)] = \gamma_{i+1}(H).$$

exercise:HxK_nilpotente

Ejercicio 6.19. Demuestre que si H y K son nilpotentes entonces $H \times K$ es nilpotente.

Por inducción se demuestra fácilmente que $\gamma_i(H \times K) \subseteq \gamma_i(H) \times \gamma_i(K)$ para todo $i \geq 1$.

theorem:nilpotente

Teorema 6.20. *Sea G un grupo nilpotente.*

1. *Si H es un subgrupo de G entonces H es nilpotente.*
2. *Si $f\colon G \to H$ es un morfismo sobreyectivo, entonces H es nilpotente.*

Demostración. La primera afirmación es cierta pues $\gamma_i(H) \subseteq \gamma_i(G)$ para todo $i \geq 1$. La segunda afirmación se deduce del ejercicio 6.18: si existe c tal que $\gamma_{c+1}(G) = 1$ entonces $\gamma_{c+1}(H) = f(\gamma_{c+1}(G)) = f(1) = 1$. □

Ejemplo 6.21. A diferencia de lo que pasa con grupos resolubles, podríamos tener un grupo G no nilpotente con un subgrupo normal K tal que K y G/K son nilpotentes. Por ejemplo: Sea $G = \mathbb{S}_3$ y sea $K = \mathbb{A}_3$. Entonces G no es nilpotente a pesar de que K y $G/K \simeq C_2$ sean nilpotentes.

sition:pgrupo_nilpotente

Proposición 6.22. *Todo p-grupo finito es nilpotente.*

Demostración. Procederemos por inducción en $|G|$. El caso $G = 1$ es trivial. Si suponemos que el resultado es válido para p-grupos de orden $< |G|$, entonces, como G es un p-grupo, $Z(G) \neq 1$. Esto implica que $G/Z(G)$ es un p-grupo nilpotente (por hipótesis inductiva) y luego existe c tal que $\gamma_{c+1}(G/Z(G)) = 1$. Sea $\pi\colon G \to G/Z(G)$ el morfismo canónico. Por el ejercicio 6.18, $\pi(\gamma_{c+1}(G)) = \gamma_{c+1}(G/Z(G)) = 1$ y entonces $\gamma_{c+1}(G) \subseteq \ker \pi = Z(G)$. Luego G es nilpotente pues

$$\gamma_{c+2}(G) = [\gamma_{c+1}(G), G] = [Z(G), G] = 1.$$

□

En el siguiente lema veremos que los grupos nilpotentes satisfacen la **condición normalizadora**.

lemma:normalizadora

Lema 6.23. *Sea G un grupo nilpotente. Si H es un subgrupo propio de G entonces* $H \subsetneq N_G(H)$.

Demostración. Sabemos que existe c tal que $G = \gamma_1(G) \supseteq \cdots \supseteq \gamma_{c+1}(G) = 1$. Como $1 = \gamma_{c+1}(G) \subseteq H$ y $\gamma_1(G) \not\subseteq H$, podemos tomar el mínimo k tal que $\gamma_k(G) \subseteq H$. Como

$$[\gamma_{k-1}(G), H] \subseteq [\gamma_{k-1}(G), G] = \gamma_k(G) \subseteq H,$$

se tiene que $xHx^{-1} \subseteq H$ para todo $x \in \gamma_{k-1}(G)$, es decir: $\gamma_{k-1}(G) \subseteq N_G(H)$. Si $N_G(H) = H$ entonces $\gamma_{k-1}(G) \subseteq H$, que contradice la minimalidad de k. □

Si G es un grupo se define sucesión $\zeta_0(G), \zeta_1(G), \ldots$ inductivamente de la siguiente forma:

$$\zeta_0(G) = 1, \quad \zeta_{i+1}(G) = \{g \in G : [g,x] \in \zeta_i(G) \text{ para todo } x \in G\}, \quad i \geq 0.$$

Por ejemplo: $\zeta_1(G) = Z(G)$.

lemma:central_ascendente

Lema 6.24. *Sea G un grupo. Para todo* $i \geq 0$ *el conjunto* $\zeta_i(G)$ *es un subgrupo normal de* $\zeta_{i+1}(G)$.

Demostración. Procederemos por inducción en i. El caso $i = 0$ es trivial pues $\zeta_0(G) = 1$. Supongamos entonces que el resultado es válido para i. Veamos primero que $\zeta_{i+1}(G)$ es un subgrupo de G. Sean $g, h \in \zeta_{i+1}(G)$ y sea $x \in G$. Por hipótesis inductiva,

$$[g^{-1}, x] = (xg^{-1})[g, x^{-1}](xg^{-1})^{-1} \in (xg^{-1})\zeta_i(G)(xg^{-1})^{-1} = \zeta_i(G),$$
$$[gh, x] = [g, hxh^{-1}][h, x] \in \zeta_i(G).$$

Como $1 \in \zeta_{i+1}(G)$, se concluye que todos los $\zeta_i(G)$ son subgrupos de G. La normalidad también se demuestra por inducción en i: si $g \in \zeta_{i+1}(G)$, $x \in G$ entonces $xgx^{-1} \in \zeta_{i+1}(G)$ pues

$$[xgx^{-1}, y] = x[g, xyx^{-1}]x^{-1} \in \zeta_i(G)$$

para todo $y \in G$. □

Definición 6.25. Sea G un grupo. Se define la **serie central ascendente** de G como la sucesión

$$1 = \zeta_0(G) \subseteq \zeta_1(G) \subseteq \zeta_2(G) \subseteq \cdots$$

lemma:gamma_zeta

Lema 6.26. *Sea G un grupo. Existe c tal que $\zeta_c(G) = G$ si y sólo si $\gamma_{c+1}(G) = 1$. Más aún, en ese caso*

$$\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$$

para todo $i \in \{0, 1, \ldots, c\}$.

Demostración. Supongamos primero que $\zeta_c(G) = G$. Por inducción vamos a demostrar que $\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$. Como el caso $i = 0$ es trivial, supongamos que el resultado es válido para un cierto $i \geq 0$. Si $g \in \gamma_{i+2}(G) = [\gamma_{i+1}(G), G]$, podemos escribir

$$g = \prod_{k=1}^{N} [g_k, x_k],$$

donde $g_1, \ldots, g_N \in \gamma_{i+1}(G)$ y $x_1, \ldots, x_N \in G$. Por hipótesis inductiva

$$g_j \in \gamma_j(G) \subseteq \zeta_{c-j}(G)$$

y entonces $[g_j, x_j] \in \zeta_{c-i-1}(G)$ para todo j. Luego $g \in \zeta_{c-(i+1)}(G)$. La implicación que queremos queda demostrada al tomar $i = c$.

Supongamos ahora que $\gamma_{c+1}(G) = 1$. Demostremos por inducción en $c - i$ que $\gamma_{c+1-i}(G) \subseteq \zeta_{c-i}(G)$. El caso $c - i = 0$ es trivial. Si el resultado es válido para algún $c - i \geq 0$, sea $g \in \gamma_{c+2-i}(G) = [\gamma_{c+1-i}(G), G]$. Escribimos

$$g = \prod_{k=1}^{N} [g_k, x_k]$$

con $g_1, \ldots, g_N \in \gamma_{c+1-i}(G) \subseteq \zeta_i(G)$ por hipótesis inductiva. Luego $g \in \zeta_{c-(i+1)}(G)$ pues cada $[g_j, x_j] \in \zeta_{i-1}(G)$. Al tomar $i = 0$ se obtiene la implicación buscada. □

Ejemplo 6.27. Sea $G = \mathbb{S}_3$. Entonces $\zeta_j(G) = 1$ para todo $j \geq 0$:

```
gap> UpperCentralSeries(SymmetricGroup(3));
[ Group(()) ]
```

Definición 6.28. Sea G un grupo. Una **serie central** para G es una sucesión

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$$

de subgrupos normales de G tal que para cada $i \in \{1,\dots,n\}$, $\pi_i(G_{i-1})$ es un subgrupo de $Z(G/G_i)$, donde $\pi_i\colon G \to G/G_i$ es el morfismo canónico.

lemma:serie_central

Lema 6.29. *Sea G un grupo y sea $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ una serie central para G. Entonces $\gamma_{i+1}(G) \subseteq G_i$ para todo i.*

Demostración. Procederemos por inducción en i. El caso $i = 0$ es trivial. Supongamos que el resultado es válido para algún $i \geq 0$. Entonces

$$\gamma_{i+1}(G) = [G, \gamma_i(G)] \subseteq [G, G_{i-1}] \subseteq G_i$$

pues, como $\pi_i(G_{i-1}) \subseteq Z(G/G_i)$, entonces $\pi([G,G_{i-1}]) = [\pi(G), \pi(G_{i-1})] = 1$ y luego $[G,G_{i-1}] \subseteq G_i$. □

Teorema 6.30. *Un grupo es nilpotente si y sólo si admite una serie central.*

Demostración. Si el grupo G es nilpotente, entonces los $\gamma_j(G)$ forman una serie central para G. Recíprocamente, si $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ es una serie central para G, entonces, por el lema 6.29 G es nilpotente pues $\gamma_{n+1}(G) \subseteq G_n = 1$. □

Ejercicio 6.31. Sea G un grupo. Demuestre que si K es un subgrupo de $Z(G)$ tal que G/K es nilpotente, entonces G es nilpotente.

theorem:Z(nilpotent)

Teorema 6.32 (Hirsch). *Sea G un grupo nilpotente. Si H es un subgrupo normal no trivial de G entonces $H \cap Z(G) \neq 1$. En particular, $Z(G) \neq 1$.*

Demostración. Como $\zeta_0(G) = 1$ y existe c tal que $\zeta_c(G) = G$, existe

$$m = \min\{k : H \cap \zeta_k(G) \neq 1\}.$$

Como H es normal,

$$[H \cap \zeta_m(G), G] \subseteq H \cap [\zeta_m(G), G] \subseteq H \cap \zeta_{m-1}(G) = 1.$$

Luego $1 \neq H \cap \zeta_m(G) \subseteq H \cap Z(G)$. Si $H = G$ entonces $Z(G) \neq 1$. □

Ejercicio 6.33. Sea G un grupo nilpotente y sea M un subgrupo minimal-normal de G. Demuestre que $M \subseteq Z(G)$.

Como $M \cap Z(G)$ es normal en G, la minimalidad de M implica que hay dos posibilidades: $M \cap Z(G)$ es trivial o bien $M = M \cap Z(G) \subseteq Z(G)$. Por el teorema 6.32, $M \cap Z(G) \neq 1$.

Corolario 6.34. *Sea G un grupo nilpotente no abeliano y sea A un subgrupo maximal-normal y abeliano de G. Entonces $A = C_G(A)$.*

Demostración. Como A es abeliano, $A \subseteq C_G(A)$. Supongamos que $A \neq C_G(A)$. El centralizador $C_G(A)$ es normal en G pues, como A es normal en G,

$$gC_G(A)g^{-1} = C_G(g^{-1}Ag) = C_G(A).$$

para todo $g \in G$. Sea $\pi\colon G \to G/A$ el morfismo canónico. Entonces $\pi(C_G(A))$ es un subgrupo normal no trivial de $\pi(G)$. Como G es nilpotente, $\pi(G)$ es nilpotente y, por el teorema 6.32, $\pi(C_G(A)) \cap Z(\pi(G)) \neq 1$. Sea $x \in C_G(A) \setminus A$ tal que $\pi(x)$ es central en $\pi(G)$. El grupo $\langle A, x\rangle$ es abeliano pues $x \in C_G(A)$. Además $\langle A, x\rangle$ es normal en G pues A es normal en G y si $g \in G$ entonces $gxg^{-1}x^{-1} \in A$ porque $\pi(x)$ es central y luego $gxg^{-1} \in \langle A, x\rangle$. $A \subsetneq \langle A, x\rangle \subsetneq G$, una contradicción. □

Teorema 6.35. *Sea G un grupo nilpotente. Valen las siguientes afirmaciones:*

1. *Todo subgrupo minimal-normal tiene orden primo y es central.*
2. *Todo subgrupo maximal es normal de índice primo y contiene a $[G,G]$.*

Demostración. Demostremos la primera afirmación. Sea N un subgrupo minimal-normal. Como $N \cap Z(G) \neq 1$ por el teorema 6.32, $N \cap Z(G)$ es un subgrupo normal de G contenido en N. Luego $N = N \cap Z(G) \subseteq Z(G)$ por la minimalidad de N. En particular, N es abeliano. Además, como todo subgrupo de N es normal en G, N es simple y luego $N \simeq C_p$ para algún primo p.

Demostremos ahora la segunda afirmación. Si M es un subgrupo maximal, M es normal en G por el ejercicio 6.48. La maximalidad de M implica que G/M no contiene subgrupos propios no triviales. Luego $G/M \simeq C_p$ para algún primo p. Como en particular G/M es abeliano, $[G,G] \subseteq M$. □

proposition:g^n

Proposición 6.36. *Sea G un grupo nilpotente y sea H un subgrupo de G de índice n. Si $g \in G$ entonces $g^n \in H$.*

Demostración. El resultado es obvio en el caso en que H sea un subgrupo normal. Sea $H_0 = H$ y $H_{i+1} = N_G(H_i)$ para $i \geq 0$. Por definición, H_i es normal en H_{i+1} y además, como G es nilpotente, si $H_i \neq G$ entonces $H_i \subsetneq H_{i+1}$ por el lema 6.23. Como $(G : H)$ es finito, existe k tal que $H_k = G$. Veamos que

$$g^{(G:H)} = g^{(H_k:H_{k-1})(H_{k-1}:H_{k-2})\cdots(H_1:H_0)} \in H.$$

Observemos que $g^{(H_k:H_{k-1})} \in H_{k-1}$ pues H_{k-1} es normal en $H_k = G$, y que, como $g^{(H_k:H_{k-1})} \in H_k$, entonces

$$g^{(H_k:H_{k-2})} = g^{(H_k:H_{k-1})(H_{k-1}:H_{k-2})} = \left(g^{(H_k:H_{k-1})}\right)^{(H_{k-1}:H_{k-2})} \in H_{k-2}$$

pues H_{k-2} es normal en H_{k-1}. Al repetir este argumento se concluye que $g^{(G:H)} \in H$. □

Ejemplo 6.37. La proposición 6.36 no vale si el grupo G no es nilpotente. Sea $G = \mathbb{S}_3$ y sea $H = \{\mathrm{id}, (12)\}$ de índice tres. Si $g = (13)$ entonces $g^3 = (13) \notin H$.

lemma:a[GG]

Lema 6.38. *Sea G un grupo nilpotente de clase $c \geq 2$. Si $x \in G$ entonces el subgrupo $\langle x, [G,G] \rangle$ es nilpotente de clase $< c$.*

Demostración. Sea $H = \langle x, [G,G] \rangle$. Si $x \in [G,G]$, el resultado es cierto. Supongamos entonces que $x \notin H$. Observemos que

$$H = \{x^n c : n \in \mathbb{Z}, c \in [G,G]\}.$$

Basta demostrar que $[H,H] \subseteq \gamma_3(G)$. Sean $h = x^n c, k = x^m d \in H$ con $c,d \in [G,G]$. Como

$$[h,x^m] = [x^n,[c,x^m]][c,x^m] \in \gamma_4(G)\gamma_3(G) \subseteq \gamma_3(G),$$

entonces

$$\begin{aligned}[h,k] &= [h,x^m][x^m,[h,d]][h,d] \\ &= [x^n,[c,x^m]][c,x^m][x^m,[h,d]][h,d] \in \gamma_3(G).\end{aligned}$$

□

Ejemplo 6.39. Sea $G = \mathbb{D}_{16} = \langle r,s : r^8 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diedral de orden 16. El grupo G es nilpotente de clase tres y $[G,G] = \{1, r^2, r^4, r^6\} \simeq C_4$. El subgrupo $\langle s, [G,G] \rangle \simeq \mathbb{D}_8$ es nilpotente de clase dos.

```
gap> G := DihedralGroup(IsPermGroup,16);;
gap> gens := GeneratorsOfGroup(G);;
gap> r := gens[1];;
gap> s := gens[2];;
gap> D := DerivedSubgroup(G);;
gap> S := Subgroup(G, Concatenation(Elements(D), [s]));;
gap> StructureDescription(S);
"D8"
gap> NilpotencyClassOfGroup(G);
3
gap> NilpotencyClassOfGroup(S);
2
```

theorem:T(nilpotent)

Teorema 6.40. *Si G es un grupo nilpotente, entonces*

$$T(G) = \{g \in G : g^n = 1 \text{ para algún } n \in \mathbb{N}\}$$

es un subgrupo de G.

Demostración. Sean $a,b \in T(G)$ y sean

$$A = \langle a, [G,G] \rangle, \quad B = \langle b, [G,G] \rangle.$$

Como A y B son nilpotentes por el lema 6.38, por hipótesis inductiva, $T(A)$ es un subgrupo de A y $T(B)$ es un subgrupo de B. Como $T(A)$ es característico en A y A es normal en G, $T(A)$ es normal en G. Similarmente se demuestra que $T(B)$ es

normal en B. Veamos ahora que todo elemento de $T(A)T(B)$ tiene orden finito: si $x \in T(A)T(B)$, digamos $x = a_1b_1$ con a_1 de orden m, entonces x tiene orden finito pues

$$\begin{aligned} x^m = (a_1b_1)^m &= (a_1b_1a_1^{-1})(a_1^2b_1a_1^{-2})\cdots(a^mba^{-m}) \\ &= (a_1b_1a_1^{-1})(a_1^2b_1a_1^{-2})\cdots(a^{m-1}ba^{-m+1})b \in T(B). \end{aligned}$$

En particular, ab y a^{-1} tienen orden finito. Luego $T(G)$ es un subgrupo de G. □

theorem:a=b **Teorema 6.41.** *Sea G un grupo nilpotente y sin torsión y sean $a,b \in G$. Si existe $n \neq 0$ tal que $a^n = b^n$ entonces $a = b$.*

Demostración. Procederemos por inducción en el orden de nilpotencia c de G. El resultado es trivialmente cierto si G es abeliano. Supongamos entonces que G es nilpotente de índice $c > 1$. Como $\langle a, [G,G]\rangle$ es un subgrupo de G nilpotente de índice $< c$, y $bab^{-1} = [b,a]a \in \langle a, [G,G]\rangle$, por hipótesis inductiva, $ba = ab$ pues

$$a^n = (bab^{-1})^n = b^n.$$

Luego $(ab^{-1})^n = a^nb^{-n} = 1$ y por lo tanto, como G no tiene torsión, se concluye que $a = b$. □

Corolario 6.42. *Sea G un grupo nilpotente sin torsión. Sean $x,y \in G$ tales que $x^ny^m = y^mx^n$ para algún $n,m \neq 0$, entonces $xy = yx$.*

Demostración. Sean $a = x$ y $b = y^nxy^{-n}$. Como $a^m = b^m$, el teorema 6.41 implica que $a = b$ y luego $xy^n = y^nx$. Al usar nuevamente el teorema 6.41, esta vez con con $a = y$ y $b = xyx^{-1}$, se concluye que $xy = yx$. □

lemma:fg **Lema 6.43.** *Sea G un grupo finitamente generado y sea H un subgrupo de índice finito. Entonces H es finitamente generado.*

Demostración. Supongamos que G está generado por $\{g_1,\ldots,g_m\}$ y supongamos que para cada i existe k tal que $g_i^{-1} = g_k$. Sea $t_1,\ldots,t_n$ un conjunto de representantes de G/H. Para $i \in \{1,\ldots,n\}$, $j \in \{1,\ldots,m\}$, escribimos

$$t_ig_j = h(i,j)t_{k(i,j)}.$$

Vamos a demostrar que H está generado por los $h(i,j)$. Sea $x \in H$. Escribamos

$$\begin{aligned} x &= g_{i_1}\cdots g_{i_s} \\ &= (t_1g_{i_1})g_{i_2}\cdots g_{i_s} \\ &= h(1,i_1)t_{k_1}g_{i_2}\cdots g_{i_s} \\ &= h(1,i_1)h(k_1,i_2)t_{k_2}g_{i_3}\cdots g_{i_s} \\ &= h(1,i_1)h(k_1,i_2)\cdots h(k_{s-1},g_{i_s})t_{k_s}, \end{aligned}$$

donde $k_1,\ldots,k_{s-1} \in \{1,\ldots,n\}$. Como $t_{k_s} \in H$, $t_{k_s} = t_1 \in H$ y luego $x \in H$. □

theorem:T(G)finito

Teorema 6.44. *Sea G un grupo finitamente generado, de torsión y nilpotente. Entonces G es finito.*

Demostración. Procederemos por inducción en la clase de nilpotencia c. El caso $c = 1$ es verdadero pues G es abeliano. Supongamos entonces que el resultado es válido para $c \geq 1$. Como $[G,G]$ y $G/[G,G]$ son nilpotentes de clase $< c$, finitamente generados (por el lema 6.43) y de torsión, por hipótesis inductiva se tiene que $[G,G]$ y $G/[G,G]$ son finitos. Luego G es también finito de orden $|[G,G]|(G : [G,G])$. □

lemma:normalizador

Lema 6.45. *Sean G un grupo finito, p un primo que divide a $|G|$ y $P \in \mathrm{Syl}_p(G)$. Entonces*

$$N_G(N_G(P)) = N_G(P).$$

Demostración. Sea $H = N_G(P)$. Como P es normal en H, P es el único p-subgrupo de Sylow de H. Para ver que $N_G(H) = H$ basta demostrar que $N_G(H) \subseteq H$. Sea $g \in N_G(H)$. Como

$$gPg^{-1} \subseteq gHg^{-1} = H,$$

$gPg^{-1} \in \mathrm{Syl}_p(H)$ y H tiene un único p-subgrupo de Sylow, $P = gPg^{-1}$. Luego $g \in N_G(P) = H$. □

theorem:nilpotente:eq

Teorema 6.46. *Sea G un grupo finito. Son equivalentes:*

1. *G es nilpotente.*
2. *Todo subgrupo de Sylow de G es normal.*
3. *G es producto directo de sus subgrupos de Sylow.*

Demostración. Veamos que $(1) \implies (2)$. Sea $P \in \mathrm{Syl}_p(G)$. Queremos ver que P es normal en G, es decir $N_G(P) = G$. Por el lema 6.45, $N_G(N_G(P)) = N_G(P)$. La condición normalizadora del lema 6.23 implica entonces que $N_G(P) = G$.

Veamos ahora que $(2) \implies (3)$. Sean $p_1, \cdots, p_k$ los factores primos de $|G|$ y para cada $i \in \{1, \ldots, k\}$ sea $P_i \in \mathrm{Syl}_{p_i}(G)$. Por hipótesis, cada P_j es normal en G.

Vamos a demostrar que $P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$ para todo j. El caso $j = 1$ es trivial. Supongamos entonces que el resultado vale para algún $j \geq 1$. Como

$$N = P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$$

es normal en G y tiene orden coprimo con $|P_{j+1}|$, $N \cap P_{j+1} = 1$. Luego

$$NP_{j+1} \simeq N \times P_{j+1} \simeq P_1 \times \cdots \times P_j \times P_{j+1}$$

pues P_{j+1} es también normal en G.

Ahora que sabemos que $P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k$ es un subgrupo de orden $|G|$, se concluye que $G = P_1 \times \cdots \times P_k$.

Para ver que $(3) \implies (1)$ simplemente hace falta observar que todo p-grupo es nilpotente (proposición 6.22) y que el producto directo de finitos nilpotentes es nilpotente (ejercicio 6.19). □

exercise:truco

Ejercicio 6.47. Sea G un grupo finito. Demuestre que si $P \in \mathrm{Syl}_p(G)$ y M es un subgrupo de G tal que $N_G(P) \subseteq M$ entonces $M = N_G(M)$.

Sea $x \in N_G(M)$. Como $P \subseteq M$ y M es normal en $N_G(M)$, $xPx^{-1} \subseteq M$. Como P y xPx^{-1} son p-subgrupos de Sylow de M, existe $m \in M$ tal que

$$mPm^{-1} = xPx^{-1}.$$

Luego $x \in M$ pues $m^{-1}x \in N_G(P) \subseteq M$.

exercise:normalizadora

Ejercicio 6.48. Sea G un grupo finito. Son equivalentes:

1. G es nilpotente.
2. Si $H \subsetneq G$ es un subgrupo entonces $H \subsetneq N_G(H)$.
3. Todo subgrupo maximal de G es normal en G.

Para demostrar que $(1) \implies (2)$ simplemente usamos el lema 6.23. Para demostrar que $(2) \implies (3)$ hacemos lo siguiente: si M es un subgrupo maximal, como $M \subsetneq N_G(M)$ por hipótesis, $N_G(M) = G$ por maximalidad. Finalmente demostremos que $(3) \implies (1)$. Sea $P \in \mathrm{Syl}_p(G)$. Si P no es normal en G, $N_G(P) \neq G$ y entonces existe un subgrupo maximal M tal que $N_G(P) \subseteq M$. Como M es normal en G, el ejercicio 6.47 implica que $M = N_G(M) = G$, una contradicción. Luego P es normal en G y entonces G es nilpotente por el teorema 6.46.

Teorema 6.49. *Sea G un grupo finito nilpotente. Si p es un primo que divide al orden de G, existe un subgrupo minimal-normal de orden p y existe un subgrupo maximal de índice p.*

Demostración. Supongamos que $|G| = p^\alpha m$, donde p es un primo coprimo con m. Escribamos $G = P \times H$, donde $P \in \mathrm{Syl}_p(G)$. Como $Z(P)$ es un subgrupo normal no trivial de P, cualquier subgrupo de $Z(G)$ de orden p es minimal-normal en G. Por otro lado, como P contiene un subgrupo de índice p, que resulta maximal. Luego $P \times H$ también contiene un subgrupo maximal de índice p. □

exercise:pgrupos

Ejercicio 6.50. Sea p un primo y sea G un grupo no trivial de orden p^n. Demuestre las siguientes afirmaciones:

1. G tiene un subgrupo normal de orden p.
2. Para todo $j \in \{0, \ldots, n\}$ existe un subgrupo normal de G de orden p^j.

1. Sabemos que $Z(G) \neq 1$. Sea $g \in Z(G)$ tal que $g \neq 1$. Supongamos que el orden de g es p^k para algún $k \geq 1$. Entonces $g^{p^{k-1}}$ tiene orden p y luego genera un subgrupo central de orden p.
2. Procederemos por inducción en n. Si $n = 1$ el resultado es trivial. Supongamos entonces que el resultado vale para un cierto $n \geq 2$. Por el punto anterior, G posee un subgrupo normal N de orden p. Luego G/N tiene orden p^{n-1}. Sea $\pi\colon G \to G/N$ el morfismo canónico. Por hipótesis inductiva, para cada $j \in \{0,\dots,n-1\}$. Por el teorema de la correspondecia, cada subgrupo normal S_j de G/N de orden p^j se corresponde con un subgrupo $\pi^{-1}(S_j)$ de G de orden p^{j+1} pues, como π es sobreyectiva, se tiene $\pi(\pi^{-1}(S_j)) = S_j$, y luego

$$p^j = |S_j| = |\pi(\pi^{-1}(S_j))| = \frac{|\pi^{-1}(S_j)|}{|\pi^{-1}(S_j) \cap N|} = \frac{|\pi^{-1}(S_j)|}{|N|} = \frac{|\pi^{-1}(S_j)|}{p}.$$

Ejercicio 6.51. Sea G un grupo finito. Demuestre que las siguientes afirmaciones son equivalentes:

1. G es nilpotente.
2. Cualesquiera dos elementos de órdenes coprimos conmutan.
3. Todo cociente no trivial de G tiene centro no trivial.
4. Si d divide al orden de G, existe un subgrupo normal de G de orden d.

Veamos que $(1) \implies (2)$. Sabemos que G es producto directo de sus subgrupos de Sylow, digamos $G = \prod_{i=1}^{k} S_i$, donde los S_i son los distintos subgrupos de Sylow de G. Sean $x = (x_1,\dots,x_k), y = (y_1,\dots,y_k) \in G$. Como $|x|$ y $|y|$ son coprimos, para cada $i \in \{1,\dots,k\}$ se tiene $x_i = 1$ o $y_i = 1$. Luego

$$[x,y] = ([x_1,y_1],[x_2,y_2],\dots,[x_k,y_k]) = 1.$$

Demostremos ahora que $(2) \implies (1)$. Supongamos que $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, donde los p_j son primos distintos y para cada j sea $P_j \in \mathrm{Syl}_{p_j}(G)$. Como elementos de órdenes coprimos conmutan, la función $P_1 \times \cdots \times P_k \to G$, $(x_1,\dots,x_k) \mapsto x_1 \cdots x_k$, es un morfismo inyectivo de grupos. Como entonces $G \simeq P_1 \times \cdots P_k$, y cada P_j es nilpotente, G es nilpotente.

Para demostrar que $(1) \implies (3)$ simplemente hay que observar que todo cociente de G es nilpotente y luego utilizar el teorema 6.32. Demostremos que $(3) \implies (1)$. Como todo cociente no trivial de G tiene centro no trivial, en particular $Z_1 = Z(G)$ es no trivial. Si $Z_1 = G$ entonces G es abeliano y no hay nada para demostrar. Si $Z_1 \neq G$ entonces $G/Z_1 \neq 1$; luego $Z(G/Z_1) \neq 1$. Si $\pi_1\colon G \to G/Z_1$ es el morfismo canónico, $Z_2 = \pi_1^{-1}(Z(G/Z_1))$. Inductivamente, si tenemos construido el subgrupo Z_i, $Z_i \neq G$ y $\pi_i\colon G \to G/Z_i$ es el

morfismo canónico, se define el subgrupo $Z_{i+1} = \pi_i^{-1}(Z(G/Z_i))$. Por construcción, $Z_i \subseteq Z_{i+1}$ para todo i. Como G es finito, existe k tal que $Z_k = G$ y luego G es nilpotente.

Demostremos que (1) $\implies$ (4). Esta implicación es consecuencia inmediata del ejercicio 6.50. Como G es nilpotente, G producto directo de sus p-grupos de Sylow. Si $d = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ es un divisor del orden de G, basta tomar $H = H_1 \times \cdots \times H_k$, donde cada H_j es un subgrupo normal del p_j-subgrupo de Sylow de G de orden $p_j^{\alpha_j}$. Para demostrar que (4) $\implies$ (1) simplemente se aplica la hipótesis a cada p-subgrupo de G de orden maximal.

El siguiente resultado, que puede demostrarse en forma completamente elemental, fue descubierto en 2014.

Teorema 6.52 (Baumslag–Wiegold). *Sea G un grupo finito tal que $|xy| = |x||y|$ si x e y son elementos de órdenes coprimos. Entonces G es nilpotente.*

Demostración. Sean $p_1, \ldots, p_n$ los primos que dividen al orden de G son Para cada $i \in \{1, \ldots, n\}$ sea $P_i \in \mathrm{Syl}_{p_i}(G)$. Primero vamos a demostrar que $G = P_1 \cdots P_n$. Para demostrar la inclusión no trivial basta con demostrar que la función

$$\psi \colon P_1 \times \cdots \times P_n \to G, \quad (x_1, \ldots, x_n) \mapsto x_1 \cdots x_n$$

La función ψ es inyectiva pues si $\psi(x_1, \ldots, x_n) = \psi(y_1, \ldots, y_n)$, entonces

$$x_1 \cdots x_n = y_1 \cdots y_n.$$

Si $y_n \neq x_n$, entonces $x_1 \cdots x_{n-1} = (y_1 \cdots y_{n-1}) y_n x_n^{-1}$. Pero $x_1 \cdots x_{n-1}$ es un elemento de orden coprimo con p y $y_1 \cdots y_{n-1} y_n x_n^{-1}$ es un elemento de orden múltiplo de p, una contradicción. Entonces $x_n = y_n$ y luego, el mismo argumento, prueba que ψ es inyectiva. Como $|P_1 \times \cdots \times P_n| = |G|$, se concluye que ψ es biyectiva.

Veamos ahora que cada P_j es normal en G. Sea $j \in \{1, \ldots, n\}$ y sea $x_j \in P_j$. Sea $g \in G$ y sea $y_j = g x_j g^{-1}$. Como $y_j \in G$, podemos escribir $y_j = z_1 \cdots z_n$ con $z_k \in P_k$ para todo k. Como el orden de y_j es una potencia del primo p_j, el elemento $z_1 \cdots z_n$ tiene orden una potencia de p_j y luego $z_k = 1$ para todo $k \neq j$ y además $y_j = z_j \in P_j$. Como cada subgrupo de Sylow es normal en G, se concluye que G es nilpotente. □

lemma:commutador

Lema 6.53. *Si $x, y \in G$ son tales que $[x,y] \in C_G(x) \cap C_G(y)$, entonces*

$$[x,y]^n = [x^n, y] = [x, y^n]$$

para todo $n \in \mathbb{Z}$.

Demostración. Procederemos por inducción en $n \geq 0$. El caso $n = 0$ es trivial. Supongamos entonces que el resultado vale para algún $n \geq 0$. Entonces, como $[x,y] \in C_G(x)$,

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

Para demostrar el lema en el caso $n < 0$ basta observar que, como $[x,y]^{-1} = [x^{-1},y]$, $[x,y]^{-n} = [x^{-1},y]^n = [x^{-n},y]$. □

lemma:Hall **Lema 6.54 (Hall).** *Sea G un grupo nilpotente de clase dos y $x,y \in G$. Entonces*

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

para todo $n \in \mathbb{N}$.

Demostración. Procederemos por inducción en n. Como el caso $n = 1$ es trivial, supongamos que el resultado es válido para algún $n \geq 1$. Entonces, gracias al lema 6.53,

$$\begin{aligned}(xy)^{n+1} &= (xy)^n(xy) = [y,x]^{n(n-1)/2}x^n y^{n-1}(yx)y \\ &= [y,x]^{n(n-1)/2}x^n[y^n,x]xy^{n+1} = [y,x]^{n(n-1)/2}[y,x]^n x^{n+1}y^{n+1}.\end{aligned}$$

□

lemma:class2 **Lema 6.55.** *Sea $p > 2$ un número primo y sea P un p-grupo de clase de nilpotencia ≤ 2. Si $[y,x]^p = 1$ para todo $x,y \in P$ entonces $P \to [P,P]$, $x \mapsto x^p$, es un morfismo de grupos.*

Demostración. Por lema 6.54, $(xy)^p = [y,x]^{p(p-1)/2}x^p y^p = x^p y^p$. □

thm:class2 **Teorema 6.56.** *Sea $p > 2$ un número primo y sea P un p-grupo de clase de nilpotencia ≤ 2. Entonces $\{x \in P : x^p = 1\}$ es un subgrupo de P.*

Demostración. Como P tiene clase de nilpotencia dos, los conmutadores son centrales. Para cada $x \in G$, la función $g \mapsto [g,x]$ es un morfismo de grupos pues

$$[gh,x] = ghxh^{-1}g^{-1}x^{-1} = g[h,x]xg^{-1}x^{-1} = [g,x][h,x].$$

En particular, si $x,y \in P$ con $x^p = y^p = 1$, entonces

$$[x,y]^p = [x^p,y] = [1,y] = 1.$$

Luego, al usar el lema 6.54, se concluye qye $(xy)^p = [y,x]^{p(p-1)/2}x^p y^p = 1$. □

Capítulo 7
Grupos A-nilpotentes

7. Grupos con Sylows abelianos

Un grupo finito se denomina A-grupo si todos sus subgrupos de Sylow son abelianos.

Teorema 7.1 (Hall). *Si G es un grupo resoluble cuyos subgrupos de Sylow son abelianos, entonces $[G,G] \cap Z(G) = 1$.*

Demostración. Si G es un p-grupo, el resultado es cierto pues en este caso G es abeliano. Supongamos entonces que el teorema no vale y sea G un contraejemplo minimal. Entonces $H = [G,G] \cap Z(G)$ es un subgrupo normal no trivial de G.

Veamos que $H \subseteq N$ para todo subgrupo normal no trivial N de G. En particular, H es el único subgrupo minimal-normal de G. Si N es un subgrupo normal no trivial de G y $\pi\colon G \to G/N$ es el morfismo canónico, $\pi(G)$ es también un grupo cuyos subgrupos de Sylow son abelianos. Por la minimalidad de G, entonces, como $|\pi(G)| < |G|$, $[\pi(G),\pi(G)] \cap Z(\pi(G)) = 1$. Esto implica que $H \subseteq N$ pues si $h \in H$, entonces, como $\pi(h) \in [\pi(G),\pi(G)] = \pi([G,G])$ y además $\pi(h) \in \pi(Z(G)) \subseteq Z(\pi(G))$ pues $h \in Z(G)$.

Claramente H es abeliano pues $H \subseteq Z(G)$. Veamos que H es el único subgrupo minimal-normal de $Z(G)$. En efecto, si $N \subseteq Z(G)$, entonces N es normal en G y luego $H \subseteq N$. En particular, $|H| = p$ para algún primo p y $Z(G)$ es cíclico de orden p^β para algún β. En efecto, si $x \in Z(G)$ es un elemento no trivial, entonces $H \subseteq \langle x \rangle$ y luego $H = \langle x \rangle$ tiene orden p para algún primo p. Como entonces $Z(G)$ es un p-grupo y solamente tiene un único subgrupo de orden una potencia de p, $Z(G)$ tiene que ser cíclico.

Como G es resoluble, $G^{(1)} = [G,G] \neq G$. Si $1 \neq G^{(2)} = [G^{(1)},G^{(1)}]$, entonces, como $G^{(2)}$ es normal en G, se tiene que $H = G^{(1)} \cap Z(G) \subseteq Z(G^{(1)})$ y luego $H \subseteq Z(G^{(1)}) \cap G^{(2)} = 1$ por la minimalidad de G, una contradicción. Esto implica que $G^{(2)} = 1$ y entonces $G^{(1)}$ es un grupo abeliano. Como los Sylows de $G^{(1)}$ son característicos en $G^{(1)}$, también son característicos en G (si $f \in Aut(G)$ y $Q \in \mathrm{Syl}_q(G^{(1)})$, entonces $f(Q)$ es un Sylow de $G^{(1)}$ y luego $f(Q) = Q$). Por lo que

demostramos antes, todo Sylow de $G^{(1)}$ contiene entonces a H y luego $|G^{(1)}| = p^\gamma$ para algún γ pues $|H| = p$. Si $Q \in \mathrm{Syl}_p(G)$ sabemos que existe $g \in G$ tal que $gQg^{-1} \cap G^{(1)} \in \mathrm{Syl}_q(G^{(1)})$ y luego $H \subseteq gQg^{-1} \cap G^{(1)}$. Esto implica que G es un p-grupo, una contradicción. □

7. Grupos A-nilpotentes

Sean A y G dos grupos tales que A actúa por automorfismos en G. Podemos pensar que A y G son subgrupos del producto semidirecto $\Gamma = G \rtimes A$. Dados $a \in A$ y $g \in G$ se define

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

Definimos además

$$[A,G] = \langle [a,g] : a \in A,\, g \in G \rangle.$$

Podemos entonces definir inductivamente $[A,G]_1 = [A,G]$, $[A,G]_{m+1} = [A,[A,G]_m]$ para $m \geq 1$.

El **núcleo** de la acción de A en G es el subgrupo

$$C_A(G) = \{a \in A : a \cdot g = g \text{ para todo } g \in G.$$

Ejercicio 7.1. Demuestre que el subgrupo $[A,G]$ es normal en G y A-invariante.

Si $H \leq G$ es un subgrupo A-invariante, A permuta las coclases de H en G. En el caso particular en que H sea normal en G, A actúa por automorfismos en G/H. Esta acción es la **acción inducida** de A en G/H. Si $\pi\colon G \to G/H$ es el morfismo canónico,

$$\pi([A,G]) = [A,\pi(G)]$$

pues $\pi([a,g]) = \pi((a \cdot g)g^{-1}) = \pi(a \cdot g)\pi(g)^{-1} = (a \cdot \pi(g))\pi(g)^{-1} = [a,\pi(g)]$ para todo $a \in A$ y $g \in G$.

Lema 7.2. *Si A actúa por automorfismos en G entonces $[A,G]$ es el menor subgrupo normal de G tal que la acción inducida en $G/[A,G]$ es trivial.*

Demostración. Sea N un subgrupo normal de G tal que N es A-invariante. Sea $\pi\colon G \to G/N$ el morfismo canónico. El grupo A actúa trivialmente en G/N si y sólo si $\pi([A,G]) = [A,\pi(G)] = 1$ (pues $a \cdot (Ng) = Ng$ si y sólo si $(a \cdot g)g^{-1} \in N$), es decir si y sólo si $[A,G] \subseteq N$. □

oposition:trivial_action

Proposición 7.3. *Sea A un grupo que actúa por automorfismos en G y sea H un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

1. *Toda coclase Hg es A-invariante.*
2. *Toda coclase gH es A-invariante.*
3. $[A,G] \subseteq H$.

Demostración. Sea ι es la funcion $x \mapsto x^{-1}$. Como A actúa por automorfismos, $a \cdot \iota(x) = a \cdot x^{-1} = (a \cdot x)^{-1} = \iota(a \cdot x)$. Como $\iota(Hg) = g^{-1}H$ y además $\iota(gH) = Hg^{-1}$, obtenemos la equivalencia entre la primera y la segunda afirmación.

Para demostrar que $(1) \implies (3)$ basta observar que si $a \in A$ y $g \in G$ son tales que $a \cdot (Hg) = Hg$, entonces $(a \cdot g)g^{-1} \in H$.

Veamos entonces que $(3) \implies (1)$. Como $[A,G] \subseteq H$, entonces Hg es unión de coclases de $[A,G]$ en G. Luego Hg es A-invariante pues lo es toda coclase de $[A,G]$ en G. □

Definición 7.4. Sea A un grupo que actúa por automorfismos en un grupo G. El grupo G se dice A-nilpotente si $[A,G]_m = 1$ para algún m.

:Anilpotente=>Aresoluble

Teorema 7.5. *Sea A un grupo que actúa por automorfismos en G. Supongamos que $[A,G]_m = 1$ para algún m. Entonces $A^{(m-1)} \subseteq C_A(G)$. En particular, si la acción de A en G es fiel, A es resoluble y la longitud de su serie derivada es $\leq m-1$.*

Demostración. Primero demostraremos que $A^{(m-1)} \subseteq C_A(G)$ para todo m. El caso $m = 1$ es fácil: si $[A,G] = 1$ entonces $A = C_A(G)$ y no hay nada para demostrar. Supongamos entonces que el resultado es válido para algún $m \geq 1$. Si $H = [A,G]$ entonces $[A,H]_{m-1} = [A,G]_m = 1$. Por hipótesis inductiva, $A^{(m-2)} \subseteq C_A(H)$, y luego

$$1 = [A^{(m-2)}, H] = [A^{(m-2)}, [A,G]] = [A,G,A^{(m-2)}].$$

Como $A^{(m-2)} \subseteq A$, $[A^{(m-2)}, G, A^{(m-2)}] = 1$. Además $[G, A^{(m-2)}, A^{(m-2)}] = 1$. Luego, por el lema de los tres subgrupos 6.3 con $X = A^{(m-2)}$, $Y = G$ y $Z = A^{(m-2)}$, se tiene que

$$1 = [A^{(m-2)}, A^{(m-2)}, G] = [A^{(m-1)}, G].$$

□

Corolario 7.6. *Si A actúa fielmente por automorfismos en G y $[A,A,G] = 1$, entonces A es abeliano.*

Demostración. Es el teorema 7.5 con $m = 2$. □

Teorema 7.7. *Sean A y G grupos finitos tales que A actúa por automorfismos en G. Supongamos que $[A,G]_m = 1$ para algún m. Entonces $A^\infty \subseteq C_A(G)$. En particular, si la acción es fiel, A es nilpotente.*

Demostración. Vamos a demostrar que A^∞ actúa trivialmente en G. Supongamos que el teorema no es válido y sea G un contraejemplo minimal. Como G es A-nilpotente, $[A,G] \neq G$, y luego A^∞ actúa trivialmente en $[A,G]$, es decir:

$$[A,G,A^\infty] = 1$$

por la proposición 7.3

Veamos que $[G, A^\infty, A] = 1$. □

Capítulo 8
Acciones coprimas

8. Acciones de grupos

Supongamos que un grupo A actúa por automorfismos en un grupo G. Si $U \subseteq G$ y $B \subseteq A$ consideramos los siguientes subgrupos

$$N_B(U) = \{b \in B : b \cdot U = U\}, \tag{8.1}$$
$$C_B(U) = \{b \in B : b \cdot u = u \text{ para todo } u \in U\}, \tag{8.2}$$
$$C_U(a) = \{u \in U : a \cdot u = u\}, \quad a \in A, \tag{8.3}$$
$$C_U(B) = \bigcap_{b \in B} C_U(b). \tag{8.4}$$

El **conjunto de puntos fijos** de A en G es

$$C_G(A) = \{g \in G : a \cdot g = g \text{ para todo } a \in A\}$$

y el núcleo de la acción de A en G es

$$C_A(G) = \{a \in A : a \cdot g = g \text{ para todo } g \in G\}.$$

Para $a \in A$ y $g \in G$ definimos el conmutador $[a,g] = (a \cdot g)g^{-1}$ y los conjuntos de conmutadores

$$[a,U] = \langle [a,u] : u \in U \rangle, \tag{8.5}$$
$$[B,U] = \langle [b,U] : b \in B \rangle. \tag{8.6}$$

Similarmente $[g,a] = g(a \cdot g)^{-1}$ y se tienen las siguientes fórmulas

$$a \cdot [B,U] = [aBa^{-1}, a \cdot U], \tag{8.7}$$
$$[G,A] = [A,G], \tag{8.8}$$
$$\tag{8.9}$$

Lema 8.1. *$U \leq C_G(A)$ si y sólo si $[A,U] = 1$.*

Demostración. □

Proposición 8.2. *Sea N un subgrupo normal de G que es A-invariante. Valen las siguientes afirmaciones:*

1. *Si A actúa trivialmente en G/N, entonces $[A,G] \subseteq N$.*
2. *Si A actúa trivialmente en N, entonces A actúa trivialmente en $G/C_G(N)$.*
3. *Si A actúa trivialmente en N y en G/N, entonces $[A,G] \subseteq Z(N)$ y $[A,A] \subseteq C_A(G)$.*

Demostración. La primera afirmación es fácil: si $a \cdot (gN) = gN$, entonces $[A,G] \subseteq N$ por el lema anterior.

Demostremos ahora la segunda afirmación. Si $a \cdot n = n$ para todo $a \in A$ y $n \in N$, entonces $[a,n] = (a \cdot n)n^{-1} = 1$ y luego $[A,N] = 1$. Como entonces $[G,[A,N]] = [A,[N,G]] = 1$, el lema de los tres subgrupos implica que $[N,[G,A]] = 1$. Luego

$$[G,A] = [A,G] \subseteq C_G(N).$$

Veamos que $C_G(N)$ es A-invariante: si $a \in A$ y $g \in G$, entonces

$$(a \cdot g)n(a \cdot g^{-1}) = (a \cdot g)(a \cdot n)(a \cdot g)^{-1} = a \cdot (gng^{-1}) = a \cdot n = n,$$

y luego $a \cdot C_G(N) = C_G(N)$. Como sabemos que $[A,G] \subseteq C_G(N)$ y además $C_G(N)$ es A-invariante, el lema anterior implica que A actúa trivialmente en $G/C_G(N)$.

Por último demostremos la tercera afirmación. Como A actúa trivialmente en N, $[A,G] \subseteq C_G(N)$. Además $[A,G] \subseteq N$ pues A actúa trivialmente en G/N. Luego $[A,G] \subseteq N \cap C_G(N) = Z(N)$. Como A actúa trivialmente en N, $[A,N] = 1$ y entonces $[A,[A,G]] = [A,[G,A]] = 1$. Entonces el lema de los tres subgrupos implica que $[G,[A,A]] = 1$ y luego $[A,A] \subseteq C_A(G)$. □

Si un grupo A actúa por automorfismos en un grupo G, nos interesá estudiar este contexto cuando A y G sean finitos de órdenes coprimos y al menos uno de los grupos involucrados sea resoluble. En este caso diremos que la acción de A en G es una **acción coprima**. En realidad, no es necesario suponer que A o G son resolubles ya que como A y G son de orden coprimo, alguno de los dos tiene orden impar y luego es resoluble por el teorema de Feit–Thompson. Se agrega esta hipótesis adicional para hacer una presentación autocontenida que no requiera apelar al uso del teorema de Feit-Thompson.

Teorema 8.3. *Supongamos que A actúa en G coprimamente. Si U es un subgrupo A-invariante de G y $A \cdot (gU) = gU$ para algún $g \in G$, entonces existe $c \in C_G(A)$ tal que $cU = gU$.*

Demostración. Sea $a \in A$. Como $a \cdot g \in A \cdot (gU) = gU$, entonces $g^{-1}(a \cdot g) \in U$. Sea Γ el producto semidirecto $\Gamma = G \rtimes A = GA$. Como en el grupo Γ sabemos que $g^{-1}aga^{-1} = g^{-1}(a \cdot g) \in U$, entonces $g^{-1}Ag \subseteq UA$ pues

$$g^{-1}ag = (g^{-1}aga^{-1})a \in UA.$$

Como entonces A y $g^{-1}Ag$ son ambos complementos para U en UA, el teorema de Schur–Zassenhaus nos dice que A y $g^{-1}Ag$ son conjugados en UA, es decir que existe $u \in U$ tal que $uAu^{-1} = g^{-1}Ag$. Si $c = gu$, entonces obviamente $c \in G$ y además $cAc^{-1} = A$. Luego $c \in N_{GA}(A) \cap gU$ y en consecuencia, $[A,c] \subseteq A \cap G = 1$. Esto implica que $c \in C_G(A)$. □

Veamos algunos corolarios:

Corolario 8.4. *Sea A es un grupo que actúa por automorfismos en G y supongamos que A y G son finitos y de órdenes coprimos. Si N es un subgrupo normal A-invariante de G y $\pi\colon G \to G/N$ es el morfismo canónico, entonces*

$$C_{\pi(G)}(A) = \pi(G_G(A)).$$

En particular, si A actúa trivialmente en N y en G/N, entonces A también actúa trivialmente en G.

Demostración. Siempre vale que $\pi(C_G(A)) \subseteq C_{\pi(G)}(A)$ pues si $g \in C_G(A)$, entonces para todo $a \in A$ se tiene que $a \cdot \pi(g) = \pi(a \cdot g) = \pi(g)$ pues π es A-invariante.

Veamos ahora que $\pi(C_G(A)) \supseteq C_{\pi(G)}(A)$. Si $g \in G$ es tal que $A \cdot \pi(g) = \pi(g)$, entonces $A \cdot (gN) = gN$. Al aplicar el teorema anterior con $U = N$ tenemos entonces que $\pi(g) = \pi(c)$ para algún $c \in C_G(A)$.

Para demostrar la última afirmación, sea $g \in G$. Como $\pi([a,g]) = [a,\pi(g)] = 1$ para todo $a \in A$, entonces $\pi(g) \in C_{\pi(G)}(A) = \pi(C_G(A))$. Luego $\pi(g) = \pi(c)$ para algún $c \in C_G(A)$ y en consecuencia $g = cn$ para algún $n \in N$. Como A actúa trivialmente en N y $c \in C_G(A)$,

$$[a,g] = (a \cdot g)g^{-1} = (a \cdot (cn))(cn)^{-1} = (a \cdot c)(a \cdot n)n^{-1}c^{-1} = (a \cdot c)c^{-1} = 1.$$

□

pro:G=[AG]C_G(A)

Proposición 8.5. *Sea A un grupo que actúa por automorfismos en un grupo G. Supongamos que A y G son finitos y de órdenes coprimos. Entonces $G = [A,G]C_G(A)$.*

Demostración. Observemos que $[A,G]$ es un subgrupo normal A-invariante de G. Si $\pi\colon G \to G/[A,G]$ es el morfismo canónico, entonces $C_{\pi(G)}(A) = \pi(C_G(A))$ por el corolario anterior. Sea $g \in G$. Como $\ker\pi = [A,G]$, sabemos que $a \cdot \pi(g) = \pi(g)$ para todo $a \in A$, es decir

$$\pi(g) \in C_{\pi(G)}(A) = \pi(C_G(A)).$$

Pero entonces $\pi(g) = \pi(c)$ para algún $c \in C_G(A)$ y luego existe $x \in [A,G] = \ker\pi$ tal que $g = cx$. □

8. Teoremas de Sylow

Tal como dice Isaacs tener una acción coprima de A en G es como tener un par de anteojos que nos permiten ver solamente las cosas que son invariantes por la acción de A en G. Naturalmente surge entonces la siguiente pregunta: ¿qué teoremas podemos ver si utilizamos los anteojos de Isaacs? En esta sección demostraremos que los teoremas de Sylow son válidos si utilizamos los anteojos.

lem:Glauberman

Lema 8.1 (Glauberman). *Supongamos que A actúa coprimamente en G. Si A actúa en un conjunto X, G actúa en X transitivamente y vale*

$$a \cdot (g \cdot x) = (a \cdot g) \cdot (a \cdot x) \tag{8.10}$$

eq:Glauberman

para todo $a \in A$, $g \in G$ y $x \in X$, entonces valen las siguientes afirmaciones:

1. *Existe un elemento $x \in X$ que es A-invariante.*
2. *Si $x, y \in X$ son A-invariantes, entonces existe $c \in C_G(A)$ tal que $c \cdot x = y$.*

Demostración. Vamos a demostrar la primera afirmación. Consideremos el producto semidirecto $\Gamma = G \rtimes A$, donde identificaremos a los grupos G y A con ciertos subgrupos de Γ. Todo elemento de Γ es de la forma $\gamma = ga$ para algún $g \in G$ y $a \in A$. El producto en Γ es

$$(ga)(hb) = (g(a \cdot h))(ab)$$

Hagamos actuar a Γ en X por

$$(ga) \cdot x = g \cdot (a \cdot x).$$

La condición de compatibilidad del enunciado garantiza que esto define una acción de Γ en X:

$$\begin{aligned}(ga) \cdot ((hb) \cdot x) &= (ga) \cdot (h \cdot (b \cdot x)) = g \cdot (a \cdot (h \cdot (b \cdot x)) \\ &= g \cdot ((a \cdot h) \cdot ((ab) \cdot x)) = (g(a \cdot h)) \cdot ((ab) \cdot x)) = (g(a \cdot h)(ab)) \cdot x.\end{aligned}$$

Fijemos $x \in X$ y sea $\Gamma_x = \{\gamma \in \Gamma : \gamma \cdot x = x\}$ el estabilizador de x en Γ. Vamos a demostrar que $\Gamma = G\Gamma_x$. Basta con demostrar que que $\Gamma \subseteq G\Gamma_x$. Como G actúa transitivamente en X, si $\gamma \in \Gamma$, existe $g \in G$ tal que $\gamma \cdot x = g \cdot x$. Luego $g^{-1}\gamma \in \Gamma_x$ y en consecuencia $\gamma \in G\Gamma_x$.

Como G es normal en Γ, el subgrupo $\Gamma_x \cap G$ es normal en Γ_x. Además

$$(\Gamma_x : \Gamma_x \cap G) = (G\Gamma_x : G) = (\Gamma : G) = |A|$$

es coprimo con $|\Gamma_x \cap G|$ pues $|A|$ y $|G|$ son coprimos. Por el teorema de Schur–Zassenhaus existe entonces un complemento H para Γ_x con respecto al subgrupo normal $\Gamma_x \cap G$. En particular, $|H| = (\Gamma_x : \Gamma_x \cap G) = |A|$ y entonces H es también un complemento normal para G en Γ. Como A también lo es, el teorema de Schur–Zassenhaus implica que existe $\gamma \in \Gamma$ tal que $\gamma H \gamma^{-1} = A$. Como $H \subseteq \Gamma_x$, $H \cdot x = x$ y

entnoces el elemento $\gamma \cdot x$ es A-invariante:

$$A \cdot (\gamma \cdot x) = (\gamma H \gamma^{-1}) \cdot (\gamma \cdot x) = (\gamma H) \cdot x = \gamma \cdot (H \cdot x) = \gamma \cdot x.$$

Demostremos ahora la segunda afirmación. Sean $x, y \in X$ dos elementos A-invariantes. Como G actúa transitivamente en X, el conjunto

$$S = \{g \in G : g \cdot x = y\}$$

es no vacío. Nuestro objetivo es encontrar un elemento del conjunto S que sea A-invariante. Primero observamos que A actúa en S. En efecto, si $s \in S$ y $a \in A$, entonces, como vale la condición de compatibilidad (8.10) y x e y son A-invariantes,

$$(a \cdot s) \cdot x = (a \cdot s) \cdot (a \cdot x) = a \cdot (g \cdot x) = a \cdot y = y.$$

Sea $H = G_y$. El argumento anterior con y en lugar de x y H en lugar de S nos dice que A actúa por automorfismos en H. Además la acción de A en H es una acción coprima (pues H es un subgrupo de G). Veamos que H actúa en S por multiplicación a izquierda: si $s \in S$ y $h \in H$, entonces

$$(hs) \cdot x = h \cdot (s \cdot x) = h \cdot y = y.$$

Además, la acción es transitiva: si $s, t \in S$, entonces $ts^{-1} \in H$ pues

$$ts^{-1} \cdot y = t \cdot (s^{-1} \cdot y) = t \cdot x = y$$

y luego $(ts^{-1})s = t$. Veamos que vale la condición (8.10) de compatilibdad. Si $a \in A$, $h \in H$ y $s \in S$, entonces, como A actúa por automorfismos,

$$a \cdot (h \cdot s) = a \cdot (hs) = (a \cdot h)(a \cdot s).$$

Luego la primera parte del lema puede aplicarse y nos dice que S contiene un elemento A-invariante, es decir que existe $c \in C_G(A)$ tal que $c \cdot x = y$. □

Estamos en condiciones de probar la versión A-invariante de los teoremas de Sylow. ¿Cuál serían los teoremas de Sylow que los anteojos mágicos de Isaacs nos dejan ver? Para el primer teorema la respuesta es fácil: tenemos que poder demostrar que existe un subgrupo de Sylow A-invariante. El segundo teorema nos dice que si vemos dos subgrupos de Sylow (recordemos que nuestros anteojos solamente nos dejan ver cosas A-invariantes), estos resultarán ser conjugados por un elemento que podamos ver (es decir, por un elemento A-invariante).

Teorema 8.2. *Supongamos que A actúa coprimamente en G. Para cada primo p, valen las siguientes afirmaciones:*

1. *Existe un p-subgrupo de Sylow de G que es A-invariante.*
2. *Si S y T son p-subgrupos de Sylow de G A-invariantes, entonces $cSc^{-1} = T$ para algún $c \in C_G(A)$.*

Demostración. Sea $X = \mathrm{Syl}_p(G)$ el conjunto de subgrupos de Sylow de G. Por los teoremas de Sylow sabemos que X es un conjunto no vacío y que G actúa transitivamente en X por conjugación. Como A actúa por automorfismos en G, A actúa también en X (todo $a \in A$ induce un automorfismo de G que permuta a los subgrupos de Sylow de G). Verifiquemos la condición (8.10) de compatibilidad: como A actúa por automorfismos,

$$a \cdot (gPg^{-1}) = (a \cdot g)(a \cdot P)(a \cdot g)^{-1} = (a \cdot g) \cdot (a \cdot P).$$

La primera parte del lema de Glauberman implica entonces que existe un elemento A-invariante $P \in X = \mathrm{Syl}_p(G)$.

Si $P_1, P_2 \in X$ son A-invariantes, la segunda parte del lema de Glauberman nos dice que existe $c \in C_G(A)$ tal que $c \cdot P_1 = cP_1c^{-1} = P_2$. □

Para otro análogo de un teorema importante de la teoría de Sylow necesitamos unos lemas. Si G es un grupo finito y $p \in \pi(G)$, consideramos el subgrupo

$$O_p(G) = \cap_{P \in \mathrm{Syl}_p(G)} P.$$

Como los automorfismos de G permutan a los elementos de $\mathrm{Syl}_p(G)$, este subgrupo resulta ser característico en G. Más generalmente:

lem:O_p(G)

Lema 8.3. *Sea G un grupo finito. Si N es un p-subgrupo normal de G, entonces $N \subseteq O_p(G)$.*

Demostración. Supongamos que $|G| = p^\alpha m$, donde p no divide a m. Supongamos además que $|N| = p^\beta$. Si $P \in \mathrm{Syl}_p(G)$, entonces, como N es normal en G, PN es un subgrupo de G tal que $P \subseteq PN$. En particular, $|PN| = p^\alpha n$ para algún n no divisible por p. Como además $P \cap N$ es un p-subgrupo de N,

$$p^\alpha n = |PN| = \frac{|P||N|}{|P \cap N|} = \frac{p^\alpha p^\beta}{p^\gamma},$$

para algún γ. Luego $n = p^\beta / p^\gamma$ no es divisible por p y en consecuencia $\beta = \gamma$, es decir $N = P \cap N \subseteq P$. □

lem:normalizador_crece

Lema 8.4. *Sea G un grupo finito. Si P es un p-subgrupo de G tal que p divide a $(G : P)$, entonces $P \subsetneq N_G(P)$.*

Demostración. Sea X el conjunto de coclases a izquierda de P en G. Si hacemos actuar a P en X por multiplicación a izquierda: $x \cdot (gP) = (xg)P$ para $x \in P$ y $g \in G$. Como p divide a $(G : P) = |X|$, si miramos módulo p a la ecuación de clases vemos que $|X_0| \equiv 0$ mód p. Pero $|X_0| > 1$ pues $P \in X_0$, y luego existe $g \in G \setminus P$ pues existe una coclase gP tal que $gP \neq P$. Como $P(gP) = gP$, entonces $g^{-1}PgP = P$ y luego $g^{-1}Pg = P$, es decir $g \in N_G(P) \setminus P$. □

Teorema 8.5. *Sea p un número primo. Supongamos que A actúa coprimamente en G. Si $P \subseteq G$ es un p-subgrupo A-invariante, entonces P está contenido en algún p-subgrupo de Sylow A-invariante.*

Demostración. Sin perder generalidad podemos suponer que P no está contenido en algún p-subgrupo A-invariante. Vamos a demostrar que entonces $P \in \mathrm{Syl}_p(G)$. Sea $N = N_G(P)$. Primero observamos que N es A-invariante pues si $a \in A$ y $n \in N$, entonces

$$(a \cdot n)P(a \cdot n)^{-1} = a \cdot (nPn^{-1}) = a \cdot P = P.$$

Sea $S \in \mathrm{Syl}_p(N)$ tal que S es A-invariante. Como $P \subseteq N$, algún conjugado de P en N está contenido en S, y entonces

$$P = nPn^{-1} \subseteq S, \quad n \in N,$$

pues P es normal en N. completar □

8. El teorema de Fitting

Teorema 8.1 (Fitting). *Sea A un grupo finito que actúa por automorfismos en un grupo abeliano G. Si $(|G| : |A|) = 1$, entonces $G = C_G(A) \times [A,G]$.*

Demostración. Como G es abeliano, $C_G(A)$ y $[A,G]$ son subgrupos normales de G. Tenemos que demostrar entonces que $C = C_G(A)[A,G]$ y que $C_G(A) \cap [A,G] = 1$.

Sabemos que $C = C_G(A)[A,G]$ por la proposición 8.5.

Sea $\theta\colon G \to G$, $\theta(g) = \prod_{b \in A}(b \cdot g)$. Como G es abeliano, θ está bien definida. Además, como G es abeliano, θ es un morfismo de grupos:

$$\theta(xy) = \prod_{b \in A} b \cdot (xy) = \prod_{b \in A}(b \cdot x)(b \cdot y) = \prod_{b \in A} b \cdot x \prod_{b \in A} b \cdot y = \theta(x)\theta(y).$$

Vamos a demostrar que $C_G(A) \cap [A,G] = 1$. Primero vamos a demostrar que $C_G(A) \cap \ker\theta = 1$: Si $g \in C_G(A) \cap \ker\theta$, entonces, como $g \cdot b = b$ para todo $b \in A$, $1 = \theta(g) = g^{|A|}$ y luego $g = 1$ pues $(|G| : |A|) = 1$. Demostramos ahora que $[A,G] \subseteq \ker\theta$: Si $a \in a$ y $g \in G$, entonces

$$\theta(a \cdot g) = \prod_{b \in A} a \cdot (b \cdot g) = \prod_{b \in A}(ab) \cdot g = \theta(g).$$

Luego $\theta([a,g]) = \theta((a \cdot g)g^{-1}) = 1$. □

Corolario 8.2. *Sea A un grupo finito que actúa por automorfismos en un p-grupo abeliano G. Si $|A|$ no es divisible por p y A fija todo elemento de orden p de G, entonces A actúa trivialmente en G.*

Demostración. Por el teorema de Fitting, $G = C_G(A) \times [A,G]$. Si $g \in C_G(A)$ es un elemento de orden p, entonces, por hipótesis, $A \cdot g = g$ y luego $g \in C_G(A)$. Como además $C_G(A) \cap [A,G] = 1$, entonces $[A,G]$ no tiene elementos de orden p. Pero entonces, como $[A,G]$ es un subgrupo del p-grupo G, se concluye que $[A,G] = 1$. □

8. El teorema de Thompson

Lema 8.1. *Sea P un p-grupo que actúa por automorfismos en un p-grupo G no trivial. Entonces $[P,G] \neq 1$ y $C_G(P) \neq 1$.*

Demostración. Como el grupo $\Gamma = G \rtimes P$ es un p-grupo, es nilpotente. □

Capítulo 9
Super resolubilidad

super

Definición 9.1. Un grupo G se dice **superresoluble** si existe una sucesión de subgrupos normales

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$$

tales que cada cociente G_{i-1}/G_i es cíclico.

Ejemplo 9.2. El grupo $\mathbb{D}_{2n}$ es superresoluble pues $\mathbb{D}_{2n} \supseteq \langle r \rangle \supseteq 1$ es una sucesión de subgrupos normales con factores cíclicos.

Observación 9.3. Todo grupo superresoluble es resoluble, ver ejercicio 4.27.

Ejemplo 9.4. El grupo $\mathbb{A}_4$ es resoluble pero no es superresoluble. El único subgrupo propio no trivial normal de $\mathbb{A}_4$ es

$$\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2.$$

Luego $\mathbb{A}_4$ no posee una sucesión de subgrupos normales con factores cíclicos.

Ejemplo 9.5. El grupo $\mathbf{SL}_2(3)$ es resoluble pero no es superresoluble:

```
gap> IsSolvable(SL(2,3));
true
gap> IsSupersolvable(SL(2,3));
false
```

exercise:super

Ejercicio 9.6. Demuestre las siguientes afirmaciones:

1. Todo subgrupo de un grupo superresoluble es superresoluble.
2. Todo cociente de un grupo superresoluble es superresoluble.

Sea G un grupo superresoluble y sea

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$$

una sucesión de subgrupos normales donde cada cociente G_{i-1}/G_i es cíclico.

1. Sea H un subgrupo de G. Como G es superresoluble, Sea
$$H = H \cap G_0 \supseteq H \cap G_1 \supseteq \cdots \supseteq H \cap G_n = 1$$
una sucesión de subgrupos de H. Cada $H \cap G_i$ es normal en H pues G_i es normal en G. Fijemos $i \in \{1, \ldots, n\}$ y sea $\pi_{i-1} \colon G_{i-1} \to G_{i-1}/G_i$ el morfismo canónico. La restricción de π_{i-1} al subgrupo $H \cap G_{i-1}$ es un morfismo con núcleo $G_i \cap H$. Al usar el teorema de isomorfismos vemos que
$$\frac{H \cap G_{i-1}}{H \cap G_i} \simeq \pi_{i-1}(H \cap G_i) \subseteq G_{i-1}/G_i$$
es un grupo cíclico por ser subgrupo de un grupo cíclico.
2. Sea K un subgrupo normal de G y sea $\pi \colon G \to G/K$ el morfismo canónico. Para cada i sea $Q_i = \pi(G_i)$. Cada Q_i es normal en $Q_n = \pi(G_n) = G/K$ pues G_i es normal en G. Como $G_{i-1}K = G_{i-1}(G_iK)$ para todo i, el grupo
$$\begin{aligned} Q_{i-1}/Q_i &\simeq \frac{G_{i-1}/G_{i-1} \cap K}{G_i/G_i \cap K} \simeq \frac{G_{i-1}K/K}{G_iK/K} \\ &\simeq \frac{G_{i-1}K}{G_iK} \simeq \frac{G_{i-1}(G_iK)}{G_iK} \simeq \frac{G_{i-1}}{G_iK \cap G_{i-1}} \simeq \frac{G_{i-1}/G_i}{G_iK \cap G_{i-1}/G_i} \end{aligned}$$
es cíclico por ser un cociente de un grupo cíclico.

exercise:directosuper

Ejercicio 9.7. Demuestre que el producto directo de grupos superresolubles es superresoluble.

Supongamos que G admite una sucesión $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ de de subgrupos normales tales que cada cociente G_{i-1}/G_i es cíclico, y que H admite una sucesión $H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = 1$ de subgrupos normales donde cada H_{i-1}/H_i es cíclico. Consideramos la sucesión

$$1 = G_0 \times H_0 \supseteq G_1 \times H_0 \supseteq \cdots \supseteq G_n \times H_0 \supseteq G_n \times H_1 \supseteq \cdots \supseteq G_n \times H_m = G \times H$$

tiene factores cíclicos pues cada $G_{i-1} \times H_0/G_i \times H_0 \simeq G_{i-1}/G_i$ es cíclico y cada $G_n \times H_{j-1}/G_n \times H_j$ también pues

$$G_n \times H_{j-1}/G_n \times H_j \simeq \frac{GH_{j-1}/G}{GH_j/G} \simeq \frac{H_{j-1}/H_{j-1} \cap G}{H_j/H_j \cap G} \simeq H_{j-1}/H_j.$$

Ejercicio 9.8. Sean H y K subgrupos normales de un grupo G tales que G/K y G/H son superresolubles. Demuestre que $G/H \cap K$ es superresoluble.

El producto directo $G/H \times G/K$ es superresoluble. Sea $\partial\colon G \to G/H \times G/K$, $g \mapsto (gH, gK)$. Como $\ker\partial = H \cap K$, se tiene que $G/H \cap K \simeq \partial(G)$, que es superresoluble por ser un subgrupo de un grupo superresoluble.

proposition:Nciclico

Proposición 9.9. *Sea N un subgrupo normal cíclico de un grupo G. Si G/N es superresoluble entonces G es superresoluble.*

Demostración. Sea $\pi\colon G \to G/N$ el morfismo canónico y sea $Q = G/N$. Como Q es superresoluble, tenemos una sucesión

$$Q = Q_0 \supseteq Q_1 \supseteq \cdots \supseteq Q_n = 1$$

de subgrupos normales de Q tales que cada cociente Q_{i-1}/Q_i es cíclico. Cada elemento de la sucesión

$$G = \pi^{-1}(Q) \supseteq \pi^{-1}(Q_1) \supseteq \cdots \supseteq \pi^{-1}(Q_n) = N \supseteq 1$$

es normal en G (por la correspondencia) cada cociente es cíclico N es cíclico y cada

$$\frac{\pi^{-1}(Q_j)}{\pi^{-1}(Q_{j+1})} = \frac{Q_j N}{Q_{j+1}N} \simeq \frac{Q_j N/N}{Q_{j+1}N/N} \simeq \frac{Q_j(Q_{j+1}N)}{Q_{j+1}N} \simeq \frac{Q_j/Q_{j+1}}{Q_{j+1}N \cap Q_j}$$

es cíclico por ser cociente de un grupo cíclico. □

theorem:ZorCp

Teorema 9.10. *Sea G un grupo superresoluble no trivial. Entonces G posee una sucesión de subgrupos $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ de subgrupos normales tales que cada cociente G_{i-1}/G_i es cíclico de orden primo o isomorfo a $\mathbb{Z}$.*

Demostración. Sea $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ una sucesión de subgrupos normales tal que cada cociente G_{i-1}/G_i es cíclico. Sea $i \in \{1, \ldots, n\}$ tal que el cociente $G_{i-1}/G_i \simeq C_n$ para algún n que no es primo y sea $\pi\colon G_{i-1} \to G_{i-1}/G_i$ el morfismo canónico. Sea p un primo que divide a n y sea H un subgrupo de G tal que $\pi(H)$ es un subgrupo de G_{i-1}/G_i de orden p. Por el teorema de la correspondencia, $G_i \subseteq H \subseteq G_{i-1}$.

Veamos que H es normal en G. Sea $g \in G$. Como $\pi(gHg^{-1})$ es un subgrupo de orden p del cíclico G_{i-1}/G_i, $\pi(gHg^{-1}) = \pi(H)$. Luego $gHg^{-1} = G_iH$,

$$\frac{gHg^{-1}}{G_i} = \frac{G_iH}{G_i} \simeq \frac{H}{G_i \cap H} = \frac{H}{G_i}$$

y entonces $gHg^{-1} \subseteq H$. Observemos que H/G_i es cíclico de orden primo pues

$$H/G_i = H/H \cap G_i \simeq \pi(H) \simeq C_p$$

y que G_{i-1}/H también es cíclico pues

$$G_{i-1}/H \simeq \frac{G_{i-1}/G_i}{H/G_i}$$

es cociente de un grupo cíclico. Demostramos que al insertar H en la sucesión obtenemos una nueva sucesión con factores cíclicos y donde H/G_i es cíclico de orden primo. Al repetir este proceso se obtiene el resultado deseado. □

Corolario 9.11. *Un grupo finito superresoluble admite una sucesión de subgrupos $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ normales donde cada cociente G_{i-1}/G_i es cíclico de orden primo.*

Demostración. Es consecuencia inmediata del teorema 9.10. □

theorem:super_structure

Teorema 9.12. *Sea G un grupo superresoluble.*

1. *Si N es minimal-normal en G entonces $N \simeq C_p$ para algún primo p.*
2. *Si M es maximal en G entonces $(G : M) = p$ para algún primo p.*
3. *El conmutador $[G,G]$ es nilpotente.*
4. *Si G es no abeliano existe un subgrupo normal $N \neq G$ tal que $Z(G) \subsetneq N$.*

Demostración. Demostremos la primera afirmación. Como G es superresouble, existe una sucesión $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1$ de subgrupos normales con factores G_{i-1}/G_i cíclicos. Como cada $G_i \cap N \subseteq N$ es normal en G, cada $G_i \cap N$ es trivial o igual a N. Además $N \cap G_0 = 1$ y $N \cap G_n = N$. Sea j el máximo entero tal que $N \cap G_j = 1$. Como $N \subseteq G_{j+1}$ (pues $N \cap G_{j+1} = N$), la composición

$$N \hookrightarrow G_{j+1} \to G_{j+1}/G_j$$

es un monomorfismo pues tiene núcleo igual a $N \cap G_j = 1$. Luego N es cíclico por ser isomorfo a un subgrupo del cíclico G_{i+1}/G_i. Si $G_{i+1}/G_i \simeq \mathbb{Z}$ entonces $N \simeq \mathbb{Z}$ pero no sería minimal-normal ya que por ejemplo $2\mathbb{Z}$ es un subgrupo característico de $\mathbb{Z}$ y por lo tanto es normal en G. Luego N es cíclico y finito y entonces $N \simeq C_p$ por el lema 4.23.

Demostremos la segunda afirmación. Sea M un subgrupo maximal de G. Si M es normal en G entonces G/M no contiene subgrupos propios no triviales. Luego $G/M \simeq C_p$ para algún primo p. Supongamos entonces que M no es normal en G. Sea $H = \cap_{g \in G} gMg^{-1}$ y sea $\pi\colon G \to G/H$. Como $\pi(M)$ es maximal en $\pi(G) = G/H$ y además

$$(G : M) = (G/H : M/H) = (G/H : M/H \cap M) = (\pi(G) : \pi(M)),$$

podemos suponer que M es simple. Como G es superresoluble existe una sucesión $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ de subgrupos normales con factores isomorfos a $\mathbb{Z}$ o cíclicos de orden primo. Sea $N = G_1$. Como N es cíclico, todo subgrupo de N es característico en N y por lo tanto es normal en G. En particular, $M \cap N$ es normal en G y luego $M \cap N = 1$. Como $M \subseteq NM \subseteq G$, entonces, por la maximalidad de M, $M = NM$ o bien $G = NM$. Pero como $N \subseteq NM = M$ es una contradicción, se concluye que $G = NM$. Si $N \simeq C_p$ para algún primo p, entonces $(G : M) = p$ y la afirmación queda

demostrada. Si $N \simeq \mathbb{Z}$ sea H un subgrupo propio de N. Como H es característico en N, H es normal en G y luego, como $M \subseteq HM \subseteq NM = G$, la maximalidad de M implica que $HM = M$ o bien $HM = G$. Como el caso $HM = M$ implica que $H \subseteq M \cap N = 1$, podemos suponer que $HM = G$. Si $n \in N \setminus H$ entonces $n = hm$ para algún $h \in H$, $m \in M$. Luego $h = n$ pues $h^{-1}n \in N \cap M = 1$, una contradicción.

Demostremos ahora la tercera afirmación. Como G es superresoluble, existe una sucesión

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$$

de subgrupos normales tal que cada G_i/G_{i+1} es cíclico. Para cada $i \in \{0, \ldots, n\}$ sea $H_i = [G,G] \cap G_i$. Como $[G,G]$ y los G_i son normales en G, se tiene una sucesión

$$[G,G] = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = 1$$

de subgrupos normales de G. Como H_i y H_{i+1} es normal en G, el grupo G actúa por conjugación en H_i/H_{i+1}. Esto induce un morfismo $\gamma\colon G \to \mathrm{Aut}(H_i/H_{i+1})$. Como H_i/H_{i+1} es cíclico, $\mathrm{Aut}(H_i/H_{i+1})$ es abeliano y luego $[G,G] \subseteq \ker\gamma$. Luego $[G,G]$ actúa trivialmente por conjugación en H_i/H_{i+1} y entonces

$$H_i/H_{i+1} \subseteq Z([G,G]/H_{i+1}).$$

Por último demostremos la cuarta afirmación. Como G es no abeliano, $Z(G) \neq G$. Sea $\pi\colon G \to G/Z(G)$ el morfismo canónico. El cociente $G/Z(G)$ es superresoluble y la sucesión

$$G/Z(G) = \pi(G) \supseteq \pi(G_1) \supseteq \cdots \supseteq \pi(1) = 1$$

es una sucesión de subgrupos normales de $G/Z(G)$ con cocientes cíclicos. En particular, $1 \neq \pi(G_1)$ es propio y normal en $G/Z(G)$. Por el teorema de la correspondencia, $\pi^{-1}(\pi(G_1)) \neq G$ es un subgrupo normal de G que contiene propiamente a $Z(G)$. □

Ejemplo 9.13. Si G es resoluble no necesariamente $[G,G]$ es nilpotente. El grupo $\mathbb{S}_4$ es resoluble pero $[\mathbb{S}_4, \mathbb{S}_4] = \mathbb{A}_4$ no es nilpotente.

proposition:psuper

Proposición 9.14. *Sea p un número primo. Todo p-grupo finito es superresoluble.*

Demostración. Sea G un contraejemplo de orden minimal. Podemos suponer que $|G| = p^n$ con $n > 1$ (pues si $n = 1$ el grupo G es trivialmente superresoluble). Como G es un p-grupo, es nilpotente y existe un subgrupo normal N de orden p. El cociente G/N tiene orden p^{n-1} entonces es superresoluble pues $|G/N| < |G|$. Como N es cíclico y G/N es superresoluble, G es superresoluble por la proposición 9.9. □

Corolario 9.15. *Todo grupo finito nilpotente es superresoluble.*

Demostración. Todo grupo finito nilpotente es producto directo (finito) de subgrupos de Sylow. Como cada p-grupo es superresoluble por la proposición 9.14, el resultado se obtiene inmediatamente del ejercicio 9.7. □

Teorema 9.16. *Todo grupo superresoluble tiene subgrupos maximales.*

Demostración. Procederemos por inducción en la longitud de la sucesión de superresolubilidad. Si la longitud es uno, el teorema es cierto pues en este caso el grupo es cíclico. Supongamos entonces que G admite una sucesión

$$G = G_0 \supseteq \cdots \supseteq G_k = 1$$

y que la afirmación es cierta para grupos superresolubles con sucesiones de longitud $< k$. Como G_{k-1} es normal en G, sea $\pi\colon G \to G/G_{k-1}$ el morfismo canónico. Entonces la sucesión

$$G/G_{k-1} = \pi(G) \supseteq \pi(G_1) \supseteq \cdots \supseteq \pi(G_{k-1}) = 1$$

prueba la resolubilidad de $\pi(G)$ y tiene longitud $< k$. Por hipótesis inductiva, G/G_{k-1} admite subgrupos maximales y luego, por el teorema de la correspondencia, G también admite subgrupos maximales. □

Ejemplo 9.17. Los grupos resolubles o nilpotentes no siempre admiten subgrupos maximales, ver por ejemplo $\mathbb{Q}$.

Definición 9.18. Se dice que un grupo G satisface la **condición maximal para subgrupos** si todo subconjunto $\mathscr{S}$ no vacío de subgrupos tiene un subgrupo maximal (es decir, no contenido en ningún otro subgrupo de $\mathscr{S}$).

lemma:MAX=fg

Lema 9.19. *Sea G un grupo. Entonces G satisface la condición maximal para subgrupos si y sólo si todo subgrupo de G es finitamente generado.*

Demostración. Supongamos que G satisface la condición maximal para subgrupos y sea H un subgrupo de G. Sea $\mathscr{S}$ el conjunto de subgrupos de H finitamente generados. Como $\mathscr{S}$ es no vacío (pues $1 \in \mathscr{S}$), existe un elemento maximal $M \in \mathscr{S}$. Sea $x \in H$. Como $\langle M, x\rangle \in \mathscr{S}$, $M = \langle M, x\rangle$ y luego $x \in M$. Como entonces $H = M$, H es finitamente generado.

Supongamos ahora que todo subgrupo de G es finitamente generado. Si $\mathscr{S}$ es un subconjunto no vacío de subgrupos de G sin elemento maximal, podemos construir una sucesión de subgrupos $S_1 \subseteq S_2 \subseteq \cdots$ que no se estabiliza (acá necesitamos utilizar el axioma de elección). Como la unión

$$S = \bigcup_{j \geq 1} S_j$$

es un subgrupo de G, es finitamente generado y luego $S \subseteq S_k$ para algún k suficientemente grande, una contradicción. □

proposition:max:N

Proposición 9.20. *Sea G un grupo y sea H un subgrupo de G. Si G satisface la condición maximal para subgrupos entonces H también.*

Demostración. Es consecuencia inmediata del lemma 9.19. □

proposition:max:G/N

Proposición 9.21. *Sea G un grupo y sea N un subgrupo normal de G. Si G/N y N satisfacen la condición maximal para subgrupos entonces G también.*

Demostración. Sea $\pi\colon G \to G/N$ el morfismo canónico. Sea $\mathscr{S}$ un subconjunto no vacío de subgrupos de G. El conjunto $\{S\cap N : S \in \mathscr{S}\}$ tiene un elemento maximal A y el conjunto $\{\pi(S) : S \in \mathscr{S}, S\cap N = A\}$ tiene un elemento maximal B. Sea $S \in \mathscr{S}$ tal que $\pi(S) = B$ y $S\cap N = A$. Si S no es maximal en $\mathscr{S}$, existe $T \in \mathscr{S}$ tal que $S \subseteq T$, $N\cap T = A$ y $\pi(T) = B$. Sea $x \in T \setminus S$. Como $\pi(xN) = \pi(x) \in \pi(T) = B$, existe $y \in S$ tal que $xN = yN$. Luego $y^{-1}x \in N\cap T = A = N\cap S$, una contradicción pues $x \notin S$. □

proposition:superfg **Proposición 9.22.** *Todo grupo superresoluble satisface la condición maximal para subgrupos. En particular, todo grupo superresoluble es finitamente generado.*

Demostración. Procederemos por inducción en la longitud n de la sucesión de superresolubilidad. El caso $n = 1$ es trivial pues entonces G es cíclico. Supongamos entonces que el resultado vale para grupos superresolubles con serie de longitud $\leq n-1$. Sea G un grupo superresoluble no trivial y sea

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = 1$$

una sucesión de subgrupos normales de G con factores cíclicos. Como G_{n-1} es superresoluble por el ejercicio 9.6, G_{n-1} satisface la condición maximal para subgrupos por hipótesis inductiva. Luego, por la proposición 9.21, G satisface la condición maximal para subgrupos porque G/G_{n-1} es un grupo cíclico. □

Ejemplo 9.23. El grupo abeliano $\mathbb{Q}$ es nilpotente pero no es superresoluble porque no es finitamente generado.

Si G es un grupo y $x_1,\dots,x_{n+1} \in G$ se define

$$[x_1,\dots,x_{n+1}] = [[x_1,\dots,x_n],x_{n+1}], \quad n \geq 1.$$

lemma:G_n **Lema 9.24.** *Sea G un grupo finitamente generado, digamos $G = \langle X\rangle$ con X finito. Para cada $n \geq 2$ se define*

$$G_n = \langle g[x_1,\dots,x_n]g^{-1} : x_1,\dots,x_n \in X, g \in G\rangle.$$

Entonces $G_n = \gamma_n(G)$ para todo $n \geq 2$.

Demostración. Observemos que cada G_n es normal en G. Procederemos por inducción en n. El caso $n = 2$ es trivial. Supongamos entonces que $\gamma_{n-1}(G) = G_{n-1}$. Sean $x_1,\dots,x_n \in X$. Como $[x_1,\dots,x_n] \in \gamma_n(G)$, $G_{n-1} \subseteq \gamma_n(G)$. Sea $N = G_n$ y sea $\pi\colon G \to G/N$ el morfismo canónico. El grupo G/N es finitamente generado. Como

$$[\pi([x_1,\dots,x_{n-1}]),\pi(x_n)] = \pi([x_1,\dots,x_n]) = 1,$$

se tiene que $\pi([x_1,\dots,x_{n-1}]) \in Z(G/N)$. Luego $\pi(g[x_1,\dots,x_n]g^{-1}) = 1$ para todo $g \in G$ y, por hipótesis inductiva, se concluye que

$$\pi(\gamma_{n-1}(G)) = \pi(G_{n-1}) \subseteq Z(G/N).$$

Como entonces

$$\pi(\gamma_n(G)) = \pi([\gamma_{n-1}(G), G]) = [\pi(\gamma_{n-1}(G)), \pi(G)] = 1,$$

se concluye que $\gamma_n(G) \subseteq N = G_n$. □

lemma:gamma_n/gamma_n+1

Lema 9.25. *Sea G un grupo finitamente generado. Entonces $\gamma_n(G)/\gamma_{n+1}(G)$ es finitamente generado.*

Demostración. Supongamos que $G = \langle X \rangle$ con X finito. Al escribir

$$g[x_1, \ldots, x_n]g^{-1} = [g, [x_1, \ldots, x_n]][x_1, \ldots, x_n]$$

y usar el lema 9.24 para obtener que $[g, [x_1, \ldots, x_n]] \in \gamma_{n+1}(G) = G_{n+1}$,

$$g[x_1, \ldots, x_n]g^{-1} \equiv [x_1, \ldots, x_n] \text{ mód } \gamma_{n+1}(G).$$

Luego $\gamma_n(G)/\gamma_{n+1}(G)$ está generado por el conjunto finito

$$\{[x_1, \ldots, x_n]\gamma_{n+1}(G) : x_1, \ldots, x_n \in X\}.$$

□

theorem:super=fg

Teorema 9.26. *Sea G un grupo nilpotente. Entonces G es superresoluble si y sólo si G es finitamente generado.*

Demostración. Si G es superresoluble, es finitamente generado por la proposición 9.22. Supongamos que G es finitamente generado y nilpotente. Como por el lema 9.25 cada $\gamma_n(G)/\gamma_{n+1}(G)$ es finitamente generado, digamos por $y_1, \ldots, y_m$. Sea $\pi\colon G \to G/\gamma_{n+1}(G)$ el morfismo canónico. Para cada $j \in \{1, \ldots, m\}$ sea

$$K_j = \langle \gamma_{n+1}(G), y_1, \ldots, y_j \rangle.$$

Como $[K_j, G] \subseteq [\gamma_n(G), G] = \gamma_{n+1}(G)$, se tiene que $\pi(K_j)$ es central en $\pi(G)$. Luego $\pi(K_j)$ es normal en $\pi(G)$ y por lo tanto K_j es normal en G. Como cada K_j/K_{j-1} es cíclico generado por y_jK_{j-1}, entre $\gamma_n(G)$ y $\gamma_{n+1}(G)$ pudimos construir una sucesión de subgrupos normales de G con factores cíclicos. Como G es nilpotente, existe c tal que $\gamma_{c+1}(G) = 1$ y luego G es superresoluble. □

orollary:nilpotente=>max

Corolario 9.27. *Todo grupo nilpotente finitamente generado satisface la condición maximal en subgrupos.*

Demostración. Es consecuencia del teorema 9.26 y la proposición 9.22. □

Teorema 9.28. *Sea G un grupo nilpotente y finitamente generado. Entonces $T(G)$ es finito.*

Demostración. Como G es nilpotente, G satisface la condición maximal para subgrupos por el corolario 9.27 y entonces todo subgrupo de G es finitamente generado. Como $T(G)$ es un subgrupo por el teorema 6.40, es finitamente generado y de torsión. Luego $T(G)$ es finito por el teorema 6.44. □

Capítulo 10
Subgrupos característicos

10. El subgrupo de Chermak–Delgado

CD

Definición 10.1. Sea G un grupo finito y H un subgrupo de G. Se define la **medida de Chermak–Delgado** de H como

$$m_G(H) = |H||C_G(H)|.$$

Ejemplo 10.2. Si G es un grupo abeliano y H es un subgrupo de G entonces $m_G(H) = |H||G|$.

Ejemplo 10.3. Sea $G = \mathbb{S}_3$. Los subgrupos de G son:

$$H_0 = 1, \quad H_1 = \langle (23) \rangle, \quad H_2 = \langle (12) \rangle, \quad H_3 = \langle (13) \rangle, \quad H_4 = \langle (123) \rangle, \quad H_5 = \mathbb{S}_3.$$

Un cálculo directo muestra que

$$m_G(H_j) = \begin{cases} 6 & \text{si } j \in \{0,5\}, \\ 4 & \text{si } j \in \{1,2,3\}, \\ 9 & \text{si } j = 4. \end{cases}$$

lemma:CD1

Lema 10.4. *Sean G un grupo finito y H un subgrupo de G. Entonces*

$$m_G(H) \leq m_G(C_G(H)).$$

Si vale la igualdad, $H = C_G(C_G(H))$.

Demostración. Sea $C = C_G(H)$. Como $H \subseteq C_G(C)$,

$$m_G(C) = |C||C_G(C)| \geq |C||H| = m_G(H).$$

Si $m_G(H) = m_G(C_G(H))$ entonces $|H| = |C_G(C_G(H))|$ y luego $H = C_G(C_G(H))$ pues $H \subseteq C_G(C_G(H))$. □

Lema 10.5. *Sean G un grupo finito y H,K subgrupos de G. Sean $D = H \cap K$ y $J = \langle H,K\rangle$. Entonces*

$$m_G(H)m_G(K) \leq m_G(D)m_G(J).$$

lemma:CD2 *Si vale la igualdad, $J = HK$ y $C_G(D) = C_G(H)C_G(K)$.*

Demostración. Sean $C_H = C_G(H), C_K = C_G(K), C_D = C_G(D), C_J = C_G(J)$. Entonces $C_J = C_H \cap C_K$ y $C_H \cup C_K \subseteq C_D$. Como

$$|J| \geq |HK| = \frac{|H||K|}{|D|}, \quad |C_D| \geq |C_H C_K| = \frac{|C_H||C_K|}{|C_J|},$$

tenemos

$$m_G(D) = |D||C_D| \geq \frac{|H||K|}{|J|}\frac{|C_H||C_K|}{|C_J|} = \frac{m_G(H)m_G(K)}{m_G(J)}.$$

La segunda afirmación es evidente. □

Sea G un grupo finito y sea $\mathscr{L}$ una colección de subgrupos de G. Diremos que $\mathscr{L}$ es un **reticulado** si dados $H,K \in \mathscr{L}$ se tiene que $H \cap K \in \mathscr{L}$ y $\langle H,K\rangle \in \mathscr{L}$.

Como el grupo G es finito, tiene sentido considerar el conjunto $\mathscr{L}(G)$ de subgrupos de G donde la medida de Chermak–Delgado alcanza su máximo valor, digamos M_G.

exercise:M_S **Ejercicio 10.6.** Sea G un grupo finito y sea H un subgrupo de G. Demuestre que $M_H \leq M_G$.

Sabemos que existe algún subgrupo K de H tal que $M_H = m_H(K)$. Como $C_H(K) \subseteq C_G(K)$,

$$M_H = m_H(K) = |H||C_H(K)| \leq |H||C_G(K)| \leq m_G(H) \leq M_G.$$

example:D8_CD **Ejemplo 10.7.** Sea $G = \mathbb{D}_8 = \langle r,s : r^4 = s^2 = 1, srs = r^{-1}\rangle$ el grupo diedral de ocho elementos. En los subgrupos

$$G, \quad Z(G) = \{1,r^2\}, \quad A = \{1,r,r^2,r^3\}, \quad B = \{1,s,sr^2,r^2\}, \quad C = \{1,sr,sr^3,r^2\},$$

la medida de Chermak–Deglado vale 16, y este es el mayor valor posible que puede tomar esta medida. Luego $\mathscr{L}(G) = \{G,Z(G),A,B,C\}$ y $M_G = 16$.

```
gap> ChermakDelgado := function(group, subgroup)
> return Size(subgroup)\
> *Size(Centralizer(group, subgroup));
> end;
function( group, subgroup ) ... end
gap> gr := DihedralGroup(IsPermGroup, 8);;
gap> r := gr.1;;
```

```
gap> s := gr.2;;
gap> ChermakDelgado(gr, Subgroup(gr, [r]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [s*r,s*r^3]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [s,s*r^2]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [r^2]));
16
gap> List(AllSubgroups(gr), x->ChermakDelgado(gr, x));
[ 8, 16, 8, 8, 8, 8, 16, 16, 16, 16 ]
```

Teorema 10.8. *Sea G un grupo finito. Valen las siguientes afirmaciones:*

1. *$\mathscr{L}(G)$ es un reticulado.*
2. *Si $H,K \in \mathscr{L}(G)$ entonces $\langle H,K\rangle = HK$.*
3. *Si $H \in \mathscr{L}(G)$ entonces $C_G(H) \in \mathscr{L}(G)$ y $C_G(C_G(H)) = H$.*

theorem:reticulado

Demostración. Si $H,K \in \mathscr{L}(G)$ entonces $m_G(H) = m_G(K) = M_G$. Sean $D = H \cap K$ y $J = \langle H,K\rangle$. Por el lema 10.5,

$$M_G^2 = m_G(H)m_G(K) \leq m_G(D)m_G(J).$$

Como $m_G(D) \leq M_G$ y $m_G(J) \leq M_G$ por ser M_G el máximo valor posible, se concluye que $m_G(D) = m_G(J) = M_G$. Luego $\mathscr{L}(G)$ es un reticulado.

En particular, como $m_G(H)m_G(K) = m_G(D)m_G(J) = M_G^2$, se obtiene que $J = HK$ al aplicar el el lema 10.5.

Por el lema 10.4,

$$M_G = m_G(H) \leq m_G(C_G(H)).$$

Como M_G es maximal, $m_G(C_G(H)) = M_G$ y luego $C_G(H) \in \mathscr{L}(G)$. Por el lema 10.4, $C_G(C_G(H)) = H$. □

Como aplicación del teorema 10.8, se demuestra la existencia del **subgrupo de Chermak–Delgado**:

corollary:ChermakDelgado

Corolario 10.9. *Sea G un grupo finito. Entonces existe un único subgrupo M minimal tal que $m_G(M)$ toma el mayor valor posible entre los subgrupos de G. Además M es característico, abeliano y $Z(G) \subseteq M$.*

Demostración. Por el teorema 10.8, $\mathscr{L}(G)$ es un reticulado. Sea

$$M = \bigcap_{H \in \mathscr{L}(G)} H \in \mathscr{L}(G).$$

Por el teorema 10.8 sabemos que $C_G(M) \in \mathscr{L}(G)$ y que $M = C_G(C_G(M)) \supseteq Z(G)$. Como $C_G(M) \in \mathscr{L}(G)$, $M \subseteq C_G(M)$ y luego M es abeliano. Además M es característico pues $f(M) \in \mathscr{L}(G)$ para todo $f \in \mathrm{Aut}(G)$. □

Ejemplo 10.10. Sea $G = \mathbb{D}_8$ el grupo diedral de ocho elementos. Por lo visto en el ejemplo 10.7, el subgrupo de Chermak–Delgado de G es $Z(G) \simeq C_2$.

Teorema 10.11 (Chermak–Delgado). *Sea G un grupo finito. Entonces G tiene un subgrupo abeliano característico M tal que $(G:M) \leq (G:A)^2$ para todo subgrupo abeliano A.*

theorem:ChermakDelgado

Demostración. Sea M el subgrupo de Chermak–Delgado del corolario 10.9 y sea A un subgrupo abeliano de G. Como A es abeliano, $A \subseteq C_G(A)$. Luego

$$m_G(M) \geq m_G(A) = |A||C_G(A)| \geq |A|^2,$$

y entonces

$$(G:A)^2 = \frac{|G|^2}{|A|^2} \geq \frac{|G|^2}{m_G(M)} = \frac{|G|}{|M|}\frac{|G|}{|C_G(M)|} = \frac{|G|}{|M|} = (G:M).$$

□

Corolario 10.12. *Sea G un grupo finito y sea H un subgrupo de G tal que*

$$|H||C_G(H)| > |G|.$$

Entonces G no es simple no abeliano.

Demostración. Sea M el subgrupo de Chermak–Delgado de G. Entonces

$$m_G(M) \geq m_G(H) > |G|. \tag{10.1}$$

equation:mG

Esta desigualdad implica que $M \neq 1$ pues $m_G(M) = m_G(1) = |G|$. Si G fuera simple, $M = G$ sería abeliano. □

Corolario 10.13. *Sea G un grupo finito no abeliano y sea $P \in \mathrm{Syl}_p(G)$ abeliano tal que $|P|^2 > |G|$. Entonces G no es simple.*

Demostración. Sea M el subgrupo de Chermak–Delgado. Como P es abeliano, por el teorema 10.11, $(G:M) \leq (G:P)^2 < |G|$, y luego $M > 1$. Si G fuera simple, entonces $M = G$ y luego G resultaría abeliano. □

10. El zócalo

Teorema 10.1. *Sea G un grupo finito sin subgrupos característicos distintos de 1 y G. Entonces G es simple o es producto directo de grupos simples isomorfos.*

theorem:caracteristico

Demostración. Supongamos que G no es simple y sea H un subgrupo minimal-normal de G. Sea $H_1 = H$ y sea M un subgrupo de G de orden maximal de la forma

$$H_1 \times \cdots \times H_n,$$

para algún $n \geq 1$ y donde cada H_i es normal en G e isomorfo a H.

Vamos a demostrar que M es un subgrupo característico de G. Basta ver que $f(H_i) \subseteq M$ para todo $i \in \{1,\ldots,n\}$ y todo $f \in \mathrm{Aut}(G)$. Si $f(H_i) \not\subseteq M$, entonces $f(H_i) \cap M \subsetneq f(H_i)$ y luego $|f(H_i) \cap M| < |f(H_i)| = |H|$. Como $f(H_i) \cap M$ es normal en G, la minimalidad de H implica que $f(H_i) \cap M = 1$. Como $f(H_i) \simeq H$, $f(H_i)$ es normal en G y $\langle f(H_i), M\rangle = f(H_i) \times M$ es un subgrupo de orden $> |M|$, la maximalidad del orden de M implica que $f(H_i) \subseteq M$.

Por hipótesis, $M = G$. Si H_1 es simple, no hay nada para demostrar. Si no, sea N un subgrupo normal de H_1. Como N es también normal en $M = H_1 \times \cdots \times H_n = G$, tenemos una contradicción a la minimalidad de H. □

corollary:minimal-normal

Corolario 10.2. *Un subgrupo minimal-normal de un grupo es simple o es producto directo de simples isomorfos.*

Demostración. Sea G un grupo y sea H un subgrupo minimal-normal. Si N es característico en H entonces, como N es normal en G, la minimalidad de H implica que $N = 1$ y $N = H$. El resultado se obtiene entonces inmediatamente del teorema 10.1. □

Corolario 10.3. *Sea G un grupo finito. Si K es minimal-normal en G entonces K es un p-grupo elemental abeliano para algún primo p o bien $Z(K) = 1$.*

Demostración. Si K es minimal-normal en G, K es simple o es producto directo de simples isomorfos por el corolario 10.2. Si K es no abeliano, $Z(K) = 1$. Si K es abeliano, existe $m \in \mathbb{N}$ y un primo p tal que $K \simeq C_p \times \cdots \times C_p$. □

ZÃşcalo

Definición 10.4. Sea G un grupo finito. El **zócalo** $\mathrm{Soc}(G)$ es el subgrupo generado por todos los subgrupos minimal-normales de G, es decir:

$$\mathrm{Soc}(G) = \langle S : S \text{ es subgrupo minimal-normal de } G\rangle.$$

Observación 10.5. Sea G un grupo finito. Si $N \neq 1$ es normal en G, N contiene un subgrupo minimal-normal de G. Luego $N \cap \mathrm{Soc}(G) \neq 1$. En particular, si G es no trivial entonces $\mathrm{Soc}(G) \neq 1$.

Ejercicio 10.6. Demuestre que $\mathrm{Soc}(G)$ es un subgrupo característico de G.

Pues todo automorfismo de G induce una permutación del conjunto de subgrupos minimal-normales.

Ejemplo 10.7. Sea $G = \mathbb{S}_3$. Un cálculo sencillo muestra que el único subgrupo minimal-normal de G es $H = \langle(123)\rangle$. Luego $\mathrm{Soc}(G) = \langle(123)\rangle$.

Ejemplo 10.8. Sea $G = \langle g\rangle \simeq C_{12}$. Como todo subgrupo de G es normal, los únicos minimal-normales son $\langle g^4\rangle \simeq C_3$ y $\langle g^6\rangle \simeq C_2$. Luego $\mathrm{Soc}(G) = \langle g^4, g^6\rangle = \langle g^6\rangle \simeq C_6$.

Ejemplo 10.9. El zócalo de $\mathbf{SL}(2,3)$ es isomorfo a C_2 y el zócalo de $\mathbb{S}_4$ es isomorfo a $C_2 \times C_2$.

```
gap> StructureDescription(Socle(SL(2,3)));
"C2"
gap> StructureDescription(Socle(SymmetricGroup(4)));
"C2 x C2"
```

lemma:KsubsetL

Lema 10.10. *Sea G un grupo finito no trivial. Si K es minimal-normal y L es normal en G entonces $K \subseteq L$ o bien $\langle K, L\rangle = K \times L$.*

Demostración. Como $K \cap L$ es normal en G, $K \subseteq L$ o $K \cap L = 1$. Si $K \cap L = 1$ entonces $\langle K, L\rangle = KL = K \times L$ pues K y L son normales en G. □

theorem:socle

Teorema 10.11. *Sea G un grupo finito no trivial. Existen subgrupos $K_1, \ldots, K_m$ minimal-normales de G tales que $\mathrm{Soc}(G) = K_1 \times \cdots \times K_m$. Más aún, si los K_j son no abelianos, los K_j son los únicos minimal-normales de G.*

Demostración. Como G es finito, existe un conjunto finito $\mathscr{S} = \{K_1, \ldots, K_m\}$ de subgrupos maximal-normales de G maximal con siguiente la propiedad:

$$\langle K_1, \ldots, K_m\rangle = K_1 \times \cdots \times K_m.$$

Sea $K = \langle K_1, \ldots, K_m\rangle$. Si N es minimal-normal en G entonces, como K es normal en G, el lema 10.10 implica que $N \subseteq K$ o $\langle N, K\rangle = N \times K$. Luego $N \subseteq K$ por la maximalidad del conjunto $\mathscr{S}$. Supongamos ahora que existe un subgrupo K minimal-normal de G tal que $K \notin \mathscr{S}$. Como $K \cap K_j = 1$ (pues si $K \cap K_j = K$ entonces $K \subseteq K_j$ y luego $K = K_j$), entonces

$$K \subseteq C_G(K_j)$$

para todo j, pues si $k \in K$ y $k_j \in K_j$ entonces $[k, k_j] = kk_jk^{-1}k_j^{-1} \in K \cap K_j = 1$. Entonces

$$K \subseteq Z(K_1 \cdots K_m) = Z(\mathrm{Soc}(G)) = Z(K_1) \times \cdots \times Z(K_m).$$

Si los K_j son no abelianos, entonces el corolario 10.2 implica que $Z(K_j) = 1$ para todo j. Luego $K = 1$, una contradicción. □

10. El subgrupo de Frattini

Definición 10.1. Sea G un grupo. Si G posee grupos maximales, se define el **subgrupo de Frattini** $\Phi(G)$ como la intersección de los subgrupos maximales de G. En caso contrario, se define $\Phi(G) = G$.

Ejercicio 10.2. Demuestre que $\Phi(G)$ es un subgrupo característico de G.

Si M es un subgrupo maximal de G y $f \in \mathrm{Aut}(G)$ entonces $f(M)$ es también un subgrupo maximal de G. La colección de subgrupos maximales de G es invariante por automorfismos de G y luego $f(\Phi(G)) \subseteq \Phi(G)$.

Ejemplo 10.3. Sea $G = \mathbb{S}_3$. Los subgrupos maximales de G son

$$M_1 = \langle (123) \rangle, \quad M_2 = \langle (12) \rangle, \quad M_3 = \langle (23) \rangle, \quad M_4 = \langle (13) \rangle.$$

Luego $\Phi(G) = 1$.

Ejemplo 10.4. Sea $G = \langle g \rangle \simeq C_{12}$. Como G es cíclico, los subgrupos de G son

$$1, \quad \langle g^6 \rangle \simeq C_2, \quad \langle g^4 \rangle \simeq C_3, \quad \langle g^3 \rangle \simeq C_4, \quad \langle g^2 \rangle \simeq C_6, \quad G.$$

Como los únicos subgrupos maximales son $\langle g^3 \rangle \simeq C_4$ y $\langle g^2 \rangle \simeq C_6$, obtenemos que $\Phi(G) = \langle g^3 \rangle \cap \langle g^2 \rangle = \langle g^6 \rangle \simeq C_2$.

Ejemplo 10.5. Sea $G = \mathbf{SL}_2(3)$. El siguiente código muestra que $\Phi(G) \simeq C_2$:

```
gap> StructureDescription(FrattiniSubgroup(SL(2,3)));
"C2"
```

lemma:Dedekind

Lema 10.6 (Dedekind). *Sean H, K, L subgrupos de G tales que $H \subseteq L \subseteq G$. Entonces $HK \cap L = H(K \cap L)$.*

Demostración. Demostraremos que $HK \cap L \subseteq H(K \cap L)$ pues la otra inclusión es trivial. Si $x = hk \in HK \cap L$, donde $x \in L$, $h \in H$, $k \in K$, entonces $k = h^{-1}x \in L \cap K$ pues $H \subseteq L$. Luego $x = hk \in H(L \cap K)$. □

lemma:G=HPhi(G)

Lema 10.7. *Sea G un grupo finito. Si H es un subgrupo de G tal que $G = H\Phi(G)$ entonces $H = G$.*

Demostración. Supongamos que $H \neq G$ y sea M un subgrupo maximal de G tal que $H \subseteq M$. Como $\Phi(G) \subseteq M$, $G = H\Phi(G) \subseteq M$, una contradicción. □

proposition:phi(N)phi(G)

Proposición 10.8. *Sea N un subgrupo normal de un grupo finito G. Entonces $\Phi(N) \subseteq \Phi(G)$.*

Demostración. Como $\Phi(N)$ es característico en N y N es normal en G, $\Phi(N)$ es normal en G. Sea M un subgrupo maximal de G tal que $\Phi(N) \not\subseteq M$. La maximalidad de M implica que $\Phi(N)M = G$ pues de lo contrario $M = \Phi(N)M \supseteq \Phi(N)$. Por el lema de Dedekind 10.6 (con $H = \Phi(N)$, $K = M$ y $L = N$),

$$N = G \cap N = (\Phi(N)M) \cap N = \Phi(N)(M \cap N).$$

Por el lema 10.7 esto implica que $\Phi(N) \subseteq N \subseteq M$, una contradicción. Luego todo subgrupo maximal de G contiene a $\Phi(N)$ y por lo tanto $\Phi(G) \supseteq \Phi(N)$. □

lemma:nongenerators

Lema 10.9. *Sea G un grupo finito. Entonces*

$$\Phi(G) = \{x \in G : \text{si } G = \langle x, Y\rangle \text{ para algún } Y \subseteq G \text{ entonces } G = \langle Y\rangle\}.$$

Demostración. Veamos primero la inclusión $\supseteq$. Sea $x \in G$ y sea M un subgrupo maximal de G. Si $x \notin M$ entonces, como $G = \langle x, M\rangle$, se tiene $G = \langle M\rangle = M$, absurdo. Luego $x \in M$ para todo subgrupo maximal M y entonces $x \in \Phi(G)$.

Veamos ahora la inclusión $\subseteq$. Sea $x \in \Phi(G)$ tal que $G = \langle x, Y\rangle$ para algún subconjunto Y de G. Si $G \neq \langle Y\rangle$, existe un subgrupo maximal M tal que $\langle Y\rangle \subseteq M$. Como $x \in M$, $G = \langle x, Y\rangle \subseteq M$, una contradicción. □

Ejemplo 10.10. Sea p un número primo. Sea G un p-grupo elemental abeliano, es decir $G \simeq C_p^m$ para algún $m \in \mathbb{N}$. Supongamos además que $G = \langle x_1\rangle \times \cdots \times \langle x_m\rangle$ con $\langle x_j\rangle \simeq C_p$. Veamos que $\Phi(G)$ es trivial. Sea $j \in \{1, \ldots, m\}$ y sea $n_j \in \{1, \ldots, p-1\}$. Como el conjunto

$$\{x_1, \ldots, x_{j-1}, x_j^{n_j}, x_{j+1}, \ldots, x_m\}$$

genera al grupo G y $\{x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m\}$ no lo hace, entonces $x_j^{n_j} \notin \Phi(G)$ por el lema 10.9. Luego $\Phi(G) = 1$.

theorem:Frattini

Teorema 10.11 (Frattini). *Sea G un grupo finito. Entonces $\Phi(G)$ es nilpotente.*

Demostración. Sea $P \in \mathrm{Syl}_p(\Phi(G))$ para algún primo p. Como $\Phi(G)$ es normal en G, gracias al argumento de Frattini, lema 5.1, podemos escribir $G = \Phi(G)N_G(P)$. Por el lema 10.7, $G = N_G(P)$. Como todo subgrupo de Sylow de $\Phi(G)$ es normal en G, $\Phi(G)$ es nilpotente. □

exercise:G/M

Ejercicio 10.12. Sea G un grupo y sea M un subgrupo normal de G maximal. Demuestre que G/M es cíclico de orden primo.

Por el teorema de la correspondencia, G/M no tiene subgrupos no trivales. Luego $G/M \simeq C_p$ para algún primo p.

theorem:Gaschutz

Teorema 10.13 (Gaschütz). *Si G es un grupo finito entonces*

$$[G,G] \cap Z(G) \subseteq \Phi(G).$$

Demostración. Sea $D = [G,G] \cap Z(G)$. Supongamos que D no está contenido en $\Phi(G)$. Como $\Phi(G)$ está contenido en todo subgrupo maximal de G, existe un subgrupo maximal M de G tal que D no está contenido en M. Esto implica que $G = MD$. Como $D \subseteq Z(G)$, M es normal en G pues si $g = md \in G = MD$ entonces

$$gMg^{-1} = (md)Md^{-1}m^{-1} = mMm^{-1} = M.$$

El ejercicio 10.12 implica que G/M es cíclico de orden primo. Como en particular G/M es abeliano, $[G,G] \subseteq M$. Luego $D \subseteq [G,G] \subseteq M$, una contradicción. □

lemma:N_G(H)=H

Lema 10.14. *Sea G un grupo finito y sea $P \in \mathrm{Syl}_p(G)$. Sea H un subgrupo de G tal que $N_G(P) \subseteq H$. Entonces $N_G(H) = H$.*

Demostración. Sea $x \in N_G(H)$. Como $P \in \mathrm{Syl}_p(H)$ y $Q = xPx^{-1} \in \mathrm{Syl}_p(H)$, existe $h \in H$ tal que $hQh^{-1} = (hx)P(hx)^{-1} = P$. Entonces $hx \in N_G(P) \subseteq H$ y luego $x \in H$. □

theorem:Wielandt

Teorema 10.15 (Wielandt). *Sea G un grupo finito. Entonces G es nilpotente si y sólo si $[G,G] \subseteq \Phi(G)$.*

Demostración. Supngamos que $[G,G] \subseteq \Phi(G)$. Sea $P \in \mathrm{Syl}_p(G)$. Si $N_G(P) \neq G$ entonces $N_G(P) \subseteq M$ para algún subgrupo maximal M de G. Si $g \in G$ y $m \in M$ entonces, como

$$gmg^{-1}m^{-1} = [g,m] \in [G,G] \subseteq \Phi(G) \subseteq M,$$

M es normal en G. Como además $N_G(P) \subseteq M$, el lema 10.14 implica que

$$G = N_G(M) = M,$$

una contradicción. Luego $N_G(P) = G$. Todo subgrupo de Sylow de G es normal en G y entonces G es nilpotente.

Supongamos ahora que G es nilpotente. Sea M un subgrupo maximal de G. Como M es normal en G y maximal, G/M no tiene subgrupos propios. Luego $G/M \simeq C_p$ para algún primo p. En particular G/M es abeliano y luego $[G,G] \subseteq M$. Como $[G,G]$ está contenido en todo subgrupo maximal de G, $[G,G] \subseteq \Phi(G)$. □

theorem:G/phi(G)

Teorema 10.16. *Sea G un grupo finito. Entonces G es nilpotente si y sólo si $G/\Phi(G)$ es nilpotente.*

Demostración. Si G es nilpotente, entonces $G/\Phi(G)$ es nilpotente por el teorema 6.20. Supongamos que $G/\Phi(G)$ es nilpotente. Sea $P \in \mathrm{Syl}_p(G)$. Como $\Phi(G)P/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$ y $G/\Phi(G)$ es nilpotente, $\Phi(G)P/\Phi(G)$ es un subgrupo normal de $G/\Phi(G)$. Luego, por el teorema de la correspondencia, $\Phi(G)P$ es un subgrupo normal de G. Como $P \in \mathrm{Syl}_p(\Phi(G)P)$, el argumento de Frattini del lemma 5.1 implica que

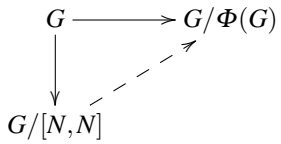
$$G = \Phi(G)PN_G(P) = \Phi(G)N_G(P)$$

pues $P \subseteq N_G(P)$. Luego $G = N_G(P)$ por el lema 10.9 y entonces P es normal en G. Esto implica que G es nilpotente. □

theorem:Hall_nilpotente

Teorema 10.17 (Hall). *Sea G un grupo finito y sea N un subgrupo normal de G. Si N y $G/[N,N]$ son nilpotentes, entonces G es nilpotente.*

Demostración. Como N es nilpotente, $[N,N] \subseteq \Phi(N)$ por el teorema 10.15. Por la proposición 10.8, $[N,N] \subseteq \Phi(N) \subseteq \Phi(G)$. Por propiedad universal, existe un morfismo $G/[N,N] \to G/\Phi(G)$ sobreyectivo que hace conmutar el diagrama



Como por hipótesis $G/[N,N]$ es nilpotente, $G/\Phi(G)$ es nilpotente por el teorema 6.20. Luego G es nilpotente por el teorema 10.16. □

Definición 10.18. Un **conjunto minimal de generadores** de un grupo G es un conjunto X de generadores de G tal que ningún subconjunto propio de X genera a G.

Observación 10.19. Es importante observar que un conjunto minimal de generadores puede no tener cardinal mínimo. Sea $G = \langle g \rangle \simeq C_6$. Si $a = g^2$ y $b = g^3$ entonces $\{a,b\}$ es un conjunto minimal de generadores de G, aunque no tiene cardinal mínimo pues por ejemplo $G = \langle ab \rangle$.

lemma:Burnside:minimal

Lema 10.20. *Sea p un número primo y sea G un p-grupo finito. Entonces $G/\Phi(G)$ es un espacio vectorial sobre $\mathbb{F}_p$.*

Demostración. Sea K un subgrupo maximal de G. Como G es nilpotente por la proposición 6.22, K es normal en G (ejercicio 6.48). Luego $G/K \simeq C_p$ por ser un p-grupo simple.

Basta ver que $G/\Phi(G)$ es p-grupo elemental abeliano. En un p-grupo pues G es un p-grupo. Sean $K_1, \ldots, K_m$ son los subgrupos maximales de G. Si $x \in G$ entonces $x^p \in K_j$ para todo $j \in \{1, \ldots, m\}$ y luego $x^p \in \Phi(G) = \cap_{j=1}^m K_j$. Además $G/\Phi(G)$ es abeliano pues $[G,G] \subseteq \Phi(G)$ por ser G nilpotente (teorema 10.15). □

theorem:Burnside:basis

Teorema 10.21 (Burnside). *Sea p un número primo y sea G un p-grupo finito. Si X es un conjunto minimal de generadores entonces $|X| = \dim G/\Phi(G)$.*

Demostración. Vimos en el lema 10.20 que $G/\Phi(G)$ es un espacio vectorial sobre $\mathbb{F}_p$. Sea $\pi\colon G \to G/\Phi(G)$ el morfismo canónico y sea $\{x_1, \ldots, x_n\}$ un conjunto minimal de generadores de G. Veamos que $\{\pi(x_1), \ldots, \pi(x_n)\}$ es un conjunto linealmente independiente de $G/\Phi(G)$. Supongamos sin perder generalidad que $\pi(x_1) \in \langle \pi(x_2), \ldots, \pi(x_n) \rangle$. Existe entonces $y \in \langle x_2, \ldots, x_n \rangle$ tal que $x_1 y^{-1} \in \Phi(G)$. Como G está generado por $\{x_1 y^{-1}, x_2, \ldots, x_n\}$ y $x_1 y^{-1} \in \Phi(G)$, el lema 10.9 implica que G también está generado por $\{x_2, \ldots, x_n\}$, una contradicción a la minimalidad. Luego $n = \dim G/\Phi(G)$. □

10. El subgrupo de Fitting

Definición 10.1. Sea G un grupo finito y sea p un número primo. Se define el **p-radical** de G como el subgrupo

$$O_p(G) = \bigcap_{P \in \mathrm{Syl}_p(G)} P.$$

lemma:core:Op(G)

Lema 10.2. *Sea G un grupo finito y sea p un número primo.*

1. *$O_p(G)$ es normal en G.*
2. *Si N es un subgrupo normal de G contenido en algún $P \in \mathrm{Syl}_p(G)$, entonces $N \subseteq O_p(G)$.*

Demostración. Sea $P \in \mathrm{Syl}_p(G)$ y hagamos actuar a G en G/P por multiplicación a izquierda. Tenemos entonces un morfismo $\rho : G \to \mathbb{S}_{G/P}$ con núcleo

$$\begin{aligned}\ker\rho &= \{x \in G : \rho_x = \mathrm{id}\} = \{x \in G : xgP = gP\ \forall g \in G\} \\ &= \{x \in G : x \in gPg^{-1}\ \forall g \in G\} = \bigcap_{g\in G} gPg^{-1} = O_p(G).\end{aligned}$$

Luego $O_p(G)$ es normal en G.

Sea ahora N un subgrupo normal de G tal que $N \subseteq P$. Como para todo $g \in G$ se tiene $N = gNg^{-1} \subseteq gPg^{-1}$, se concluye que $N \subseteq O_p(G)$. □

Definición 10.3. Sea G un grupo finito y sean $p_1, \ldots, p_k$ los factores primos de $|G|$. Se define el **subgrupo de Fitting** como el subgrupo

$$F(G) = O_{p_1}(G) \cdots O_{p_k}(G)$$

Ejercicio 10.4. Demuestre que $F(G)$ es característico en G.

Sea $f \in \mathrm{Aut}(G)$ y sea p un primo. Como f permuta los p-subgrupos de Sylow de G, $f(O_p(G)) = O_p(G)$. Luego $f(F(G)) = F(G)$.

Ejemplo 10.5. Sea $G = \mathbb{S}_3$. Es fácil ver que $O_2(G) = 1$ y que $O_3(G) = \langle(123)\rangle$. Entonces $F(G) = \langle(123)\rangle$.

theorem:Fitting

Teorema 10.6 (Fitting). *Sea G un grupo finito. El subgrupo de Fitting $F(G)$ es normal en G y nilpotente. Además $F(G)$ contiene a todo subgrupo normal nilpotente de G.*

Demostración. Por definición $|F(G)|$ es el producto de los órdendes de los $O_p(G)$. Como entonces $O_p(G) \in \mathrm{Syl}_p(F(G))$, se concluye que $F(G)$ es nilpotente por tener un p-subgrupo de Sylow normal para cada primo p. Luego $F(G)$ es nilpotente por el teorema 6.46.

Sea N un subgrupo normal de G nilpotente y sea $P \in \mathrm{Syl}_p(N)$. Como N es nilpotente, P es normal en N y entonces P es el único p-subgrupo de Sylow de N. Luego P es característico en N y entonces P es normal en G. Como N es nilpotente, N es producto directo de sus subgrupos de Sylow. Luego $N \subseteq O_p(G)$ por el lema 10.2. □

corollary:Z(G)subsetF(G)

Corolario 10.7. *Sea G un grupo finito. Entonces $Z(G) \subseteq F(G)$.*

Demostración. Como $Z(G)$ es nilpotente (por ser abeliano) y $Z(G)$ es normal en G, $Z(G) \subseteq F(G)$ por el teorema 10.6. □

corollary:Fitting

Corolario 10.8 (Fitting). *Sean K y L subgrupos normales nilpotentes de un grupo finito G. Entonces KL es nilpotente.*

Demostración. Por el teorema 10.6 sabemos que $K \subseteq F(G)$ y $L \subseteq F(G)$. Esto implica que $KL \subseteq F(G)$ y luego KL es nilpotente pues $F(G)$ es nilpotente. □

corollary:McapF(G)

Corolario 10.9. *Sea G un grupo finito y sea N un subgrupo normal de G. Entonces $N \cap F(G) = F(N)$.*

Demostración. Como $F(N)$ es característico en N, $F(N)$ es normal en G. Luego $F(N) \subseteq N \cap F(G)$ pues $F(N)$ es nilpotente. Recíprocamente, como $F(G)$ es normal en G, $F(G) \cap N$ es normal en N. Como $F(G) \cap N$ es nilpotente, $F(G) \cap N \subseteq F(N)$. □

Teorema 10.10. *Sea G un grupo no trivial y resoluble. Todo subgrupo normal N no trivial contiene un subgrupo normal abeliano no trivial.*

Demostración. Sabemos que $N \cap G^{(0)} = N \neq 1$. Como G es resoluble, existe $m \in \mathbb{N}$ tal que $N \cap G^{(m)} = 1$. Sea $n \in \mathbb{N}$ maximal tal que $N \cap G^{(n)} \neq 1$. Como $[N,N] \subseteq N$ y $[G^{(n)}, G^{(n)}] = G^{(n+1)}$,

$$[N \cap G^{(n)}, N \cap G^{(n)}] \subseteq N \cap G^{(n+1)} = 1.$$

Luego $N \cap G^{(n)}$ es un subgrupo abeliano de G. Como además es normal y nilpotente, $N \cap G^{(n)} \subseteq N \cap F(G)$. □

theorem:F(G)centraliza

Teorema 10.11. *Si G es un grupo finito y N es un subgrupo minimal-normal entonces entonces $F(G) \subseteq C_G(N)$.*

Demostración. Por el teorema 10.6, $F(G)$ es un subgrupo normal y nilpotente. Sea N un subgrupo minimal-normal de G. El subgrupo $N \cap F(G)$ es normal en G. Además $[F(G),N] \subseteq N \cap F(G)$. Si $N \cap F(G) = 1$ entonces $[F(G),N] = 1$. Si no, $N = N \cap F(G) \subseteq F(G)$ por la minimalidad de N. Como $F(G)$ es nilpotente, $N \cap Z(F(G)) \neq 1$ por el teorema 6.32. Como $Z(F(G))$ es característico en $F(G)$ y $F(G)$ es normal en G, $Z(F(G))$ es normal en G. Como $1 \neq N \cap Z(F(G))$ es normal en G, la minimalidad de N implica que $N = N \cap Z(F(G)) \subseteq Z(F(G))$ y luego $[F(G),N] = 1$. □

Corolario 10.12. *Sea G un grupo finito y resoluble.*

1. *Si N es un subgrupo minimal-normal entonces $N \subseteq Z(F(G))$.*
2. *Si H es un subgrupo normal entonces $H \cap F(G) \neq 1$.*

Demostración. Demostremos la primera afirmación. Como N es un p-grupo por el lema 4.23, N es nilpotente y luego $N \subseteq F(G)$. Además $F(G) \subseteq C_G(N)$ por el teorema 10.11. Luego $N \subseteq Z(F(G))$.

Demostremos ahora la segunda afirmación. El subgrupo H contiene un subgrupo minimal-normal N y $N \subseteq F(G)$. Luego $H \cap F(G) \neq 1$. □

Teorema 10.13. *Sea G un grupo finito.*

1. $\Phi(G) \subseteq F(G)$ *y* $Z(G) \subseteq F(G)$.
2. $F(G)/\Phi(G) \simeq F(G/\Phi(G))$.

Demostración. Demostremos la primera afirmación. Como $\Phi(G)$ es normal en G y nilpotente por el teorema 10.11 y $F(G)$ contiene a todo subgrupo normal nilpotente de G (teorema 10.6), $\Phi(G) \subseteq F(G)$. Además $Z(G)$ es normal y nilpotente (por ser abeliano) y luego $Z(G) \subseteq F(G)$.

Demostremos la segunda afirmación. Sea $\pi\colon G \to G/\Phi(G)$ el morfismo canónico. Como $F(G)$ es nilpotente, $\pi(F(G))$ es nilpotente y luego

$$\pi(F(G)) \subseteq F(G/\Phi(G))$$

por el teorema 10.6. Por otro lado, sea $H = \pi^{-1}(F(G/\Phi(G)))$. Por la correspondencia, H es un subgrupo normal de G que contiene a $\Phi(G)$. Si $P \in \mathrm{Syl}_p(H)$ entonces $\pi(P) \in \mathrm{Syl}_p(\pi(H))$ pues $\pi(P) \simeq P/P \cap \Phi(G)$ es un p-grupo y además $(\pi(H) : \pi(P))$ es coprimo con p pues

$$(\pi(H) : \pi(P)) = \frac{|\pi(H)|}{|\pi(P)|} = \frac{|H/\Phi(G)|}{|P/P \cap \Phi(G)|} = \frac{(H : P)}{(\Phi(G) : P \cap \Phi(G))}$$

es un divisor de $(H : P)$, que es coprimo con p. Como $\pi(H)$ es nilpotente, $\pi(P)$ es característico en $\pi(H)$ y luego $\pi(P)$ es normal en $\pi(G) = G/\Phi(G)$. Entonces $P\Phi(G) = \pi^{-1}(\pi(P))$ es normal en G. Como $P \in \mathrm{Syl}_p(P\Phi(G))$, el argumento de Frattini del lema 5.1 implica que $G = \Phi(G)N_G(P)$. Luego P es normal en G por el lema 10.7. Como P es nilpotente y normal en G, entonces $P \subseteq F(G)$ por el teorema 10.6. Luego $H \subseteq F(G)$ y entonces $F(G/\Phi(G)) = \pi(H) \subseteq \pi(F(G))$. □

Capítulo 11
Subnormalidad

11. Subnormalidad

Definición 11.1. Sea G un grupo. Un subgrupo H de G es **subnormal** si existe una sucesión de subgrupos

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G$$

con H_i normal en H_{i+1} para todo $i \in \{0, \ldots, k-1\}$.

Ejemplo 11.2. Sea $G = \mathbb{S}_4$. El subgrupo $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ es normal en G. El subgrupo $L = \{\mathrm{id}, (12)(34)\}$ no es normal en G pero es subnormal.

Ejercicio 11.3. Demuestre que el teorema de la correspondencia también preserva la subnormalidad.

theorem:subnormal

Teorema 11.4. *Sea G un grupo finito. Entonces G es nilpotente si y sólo si todo subgrupo es subnormal.*

Demostración. Supongamos que todo subgrupo de G es subnormal. Sea H un subgrupo subnormal de G, donde

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G$$

con H_i normal en H_{i+1}. Sin pérdida de generaliadad podemos suponer que $H \subsetneq H_1$. Como entonces $H \subsetneq H_1 \subseteq N_G(H)$, G es nilpotente por el ejercicio 6.48.

Supongamos ahora que G es nilpotente. Sea H un subgrupo de G. Procederemos por inducción en $(G : H)$. Si $(G : H) = 1$ entonces $H = G$ y no hay nada para demostrar. Si $H \neq G$, como $H \subsetneq N_G(H)$ por el lema 6.23,

$$(G : N_G(H)) < (G : H).$$

Por hipótesis inductiva, $N_G(H)$ es subnormal en G y luego, como H es normal en $N_G(H)$, se concluye que H subnormal en G. □

Corolario 11.5. *Sea G un grupo y sea K un subgrupo de G tal que $K \subseteq Z(G)$. Entonces G es nilpotente si y sólo si G/K es nilpotente.*

Demostración. Si G es nilpotente, entonces G/K es nilpotente por el teorema 6.20. Demostremos la afirmación recíproca. Sea $\pi\colon G \to G/K$ el morfismo canónico. Sea U un subgrupo de G. Como G/K es nilpotente, el teorema 11.4 implica que $\pi(U)$ es un subgrupo subnormal de G/K. La correspondencia implica que UK es un subgrupo subnormal de G, y luego, como K es central, U es normal en UZ. Luego U es subnormal en G y entonces G es nilpotente por el teorema 11.4. □

heorem:F(G)subnormalidad

Teorema 11.6. *Sea G un grupo finito y sea H un subgrupo de G. Entonces H es nilpotente y subnormal en G si y sólo si $H \subseteq F(G)$.*

Demostración. Supongamos que $H \subseteq F(G)$. Como $F(G)$ es nilpotente por el teorema 10.6, H es nilpotente por el teorema 6.20. Además, como H es subnormal en $F(G)$ por la teorema 11.4 y $F(G)$ es normal en G, H es subnormal en G.

Supongamos ahora que H es nilpotente y subnormal en G. Procederemos por inducción en $|G|$. Si $H = G$ el resultado es trivialmente cierto. Supongamos entonces que $H \neq G$. Como H es subnormal en G,

$$H = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G.$$

Sea $M = H_{k-1}$. Como $M \neq G$ y M es normal en G, $H \subseteq F(M)$ por hipótesis inductiva. Luego $H \subseteq F(M) = M \cap F(G) \subseteq F(G)$ por el corolario 10.9. □

lemma:McapN=1

Lema 11.7. *Sean M y N subgrupos normales de un grupo G tales que $M \cap N = 1$. Entonces $M \subseteq C_G(N)$.*

Demostración. Sean $m \in M$ y $n \in N$. Entonces $[n,m] = (nmn^{-1})m \in M$ pues M es normal en G y también $[n,m] = n(mn^{-1}m^{-1}) \in N$ pues N es normal en G. Luego $[n,m] \in M \cap N = 1$. □

theorem:MsubsetNG(S)

Teorema 11.8 (Wielandt). *Sea G un grupo finito. Si S es un subgrupo subnormal de G y M es un subgrupo minimal-normal de G entonces $M \subseteq N_G(S)$.*

Demostración. Procederemos por inducción en $|G|$. Si $S = G$ no hay nada para demostrar. Supongamos que $S \neq G$. Como S es subnormal en G, existe una sucesión

$$S = S_0 \triangleleft S_1 \triangleleft \cdots \triangleleft S_{k-1} \triangleleft S_k = G.$$

Sea $N = S_{k-1}$.

Si $M \cap N \neq 1$ entonces $M \subseteq N$ (pues como M y N son normales en G, $M \cap N = M$ por la minimalidad de M). Vamos a demostrar que $M \subseteq \mathrm{Soc}(N)$. Como $M \neq 1$ y M es normal en N, $M \cap \mathrm{Soc}(N) \neq 1$. Además $\mathrm{Soc}(N)$ es característico en N y N es normal en G, entonces $\mathrm{Soc}(N)$ es normal en G. Luego $M \cap \mathrm{Soc}(N)$ es un subgrupo normal de G. Como además $1 \neq M \cap \mathrm{Soc}(N) \subseteq M$, se concluye que $M \cap \mathrm{Soc}(N) = M$ por la minimalidad de M. Por hipótesis inductiva, todo subgrupo minimal-normal de N normaliza a S; entonces $\mathrm{Soc}(N) \subseteq N_N(S) \subseteq N_G(S)$ y luego

$$M \subseteq \mathrm{Soc}(N) \subseteq N_G(S).$$

Si $M \cap N = 1$, el lema 11.7 implica que

$$M \subseteq C_G(N) \subseteq C_G(S) \subseteq N_G(S).$$

□

Corolario 11.9. *Sea G finito y sea S un subgrupo subgrupo subnormal de G. Entonces* $\mathrm{Soc}(G) \subseteq N_G(S)$.

Demostración. Como todo subgrupo minimal-normal de G está contenido en $N_G(S)$ por el teorema 11.8, $\mathrm{Soc}(G) = \langle M : M \text{ subgrupo minimal-normal de } G \rangle \subseteq N_G(S)$. □

En el siguiente teorema demostraremos que los subgrupos normales forman un reticulado.

theorem:STsubnormal

Teorema 11.10 (Wielandt). *Sea G un grupo finito y sean S, T subgrupos subnormales. Entonces $S \cap T$ y $\langle S, T \rangle$ son subnormales en G.*

Demostración. Demostremos primero que $S \cap T$ es subnormal en G. Como la subnormalidad es transitivita, basta ver que $S \cap T$ es subnormal en T. Como S es subnormal en G, existe una sucesión

$$S = S_0 \triangleleft S_1 \triangleleft \cdots \triangleleft S_k = G.$$

Cada $S_{j-1} \cap T$ es normal en $S_j \cap T$ y luego $S \cap T$ es subnormal en T.

Para demostrar que $\langle S, T \rangle$ es subnormal en G procederemos por inducción en $|G|$. Supongamos que $G \neq 1$ y sea M un subgrupo minimal-normal de G. Sea $\pi \colon G \to G/M$ el morfismo canónico. Como $\pi(S)$ y $\pi(T)$ son subnormales en G/M y $|G/M| < |G|$, la hipótesis inductiva implica que

$$\pi(\langle S, T \rangle M) = \pi(\langle S, T \rangle) = \langle \pi(S), \pi(T) \rangle$$

es subnormal en G/M. Por la correspondencia, $\langle S, T \rangle M$ es subnormal en G. Por otro lado, el teorema 11.8 implica que $M \subseteq N_G(S)$ y $M \subseteq N_G(T)$. Luego $M \subseteq N_G(\langle S, T \rangle)$. Como entonces $\langle S, T \rangle$ es normal en $\langle S, T \rangle M$ y $\langle S, T \rangle M$ es subnormal en G, se concluye que $\langle S, T \rangle$ es subnormal en G. □

11. El teorema de la cremallera

El siguiente resultado de Wielandt es muy útil y se conoce como el **teorema de la cremallera**.

theorem:zipper

Teorema 11.1 (Wielandt). *Sea G un grupo finito y sea S un subgrupo de G tal que S es subnormal en todo subgrupo propio de G que contiene a S. Si S no es subnormal en G entonces existe un único maximal de G que contiene a S.*

Demostración. Procederemos por inducción en $(G:S)$. Si S no es subnormal en G entonces $S \neq G$ y entonces el caso $(G:S) = 1$ es trivialmente cierto.

Como S no es subnormal en G, $N_G(S) \neq G$. Entonces $S \subseteq N_G(S) \subseteq M$ para algún subgrupo maximal M de G. Supongamos que $S \subseteq K$ para algún subgrupo maximal K de G. Vamos a demostrar que $K = M$. Como $S \subseteq K \neq G$, S es subnormal en K. Si S es normal en K entonces $K \subseteq N_G(S) \subseteq M$ y luego $K = M$ por maximalidad de K. Si S no es normal en K, existen $m \geq 2$ subgrupos $S_0, \ldots, S_m$ de K tales que

$$S = S_0 \triangleleft S_1 \triangleleft \cdots \triangleleft S_m = K,$$

donde S no es normal en S_2. Sea $x \in S_2$ tal que $xSx^{-1} \neq S$ y sea $T = \langle S, xSx^{-1} \rangle \subseteq K$.

Como $xSx^{-1} \subseteq xS_1x^{-1} = S_1 \subseteq N_G(S)$, se tiene que $T \subseteq N_G(S) \subseteq M$. Además S es normal en T y luego $T \neq G$.

Veamos que el grupo T satisface las hipótesis del teorema. Si T fuera subnormal en G entonces, como S es normal en T, S sería subnormal en G. Si H es un subgrupo propio de G que contiene a T entonces, como $S \subseteq H$, S es subnormal en H. Además xSx^{-1} es también subnormal en H. Luego T es subnormal en H por el teorema 11.10.

Como $S \subsetneq T$, $(G:T) < (G:S)$. Por hipótesis inductiva, T está contenido en un único maximal de G. Luego $K = M$ pues $T \subseteq M$ y $T \subseteq K$. □

Aplicaciones del teorema de la cremallera

La primera aplicación es el siguiente criterio para detectar subnormalidad. Antes de enunciar y demostrar el teorema, necesitamos un lema.

lemma:H=G

Lema 11.2. *Sea G un grupo y H un subgrupo de G. Si $(xHx^{-1})H = G$ para algún $x \in G$ entonces $H = G$.*

Demostración. Escribimos $x = uv$ con $u \in xHx^{-1}$, $v \in H$. Como $u \in xHx^{-1}$ y $u^{-1}x = v \in H$, se tiene que $H = vHv^{-1} = u^{-1}(xHx^{-1})u = xHx^{-1}$. Luego $G = H$. □

Dos subgrupos S y T de un grupo G se dicen **permutables** si $ST = TS$.

Teorema 11.3. *Sea G un grupo finito y sea S un subgrupo de G permutable con todos sus conjugados. Entonces S es subnormal en G.*

Demostración. Procederemos por inducción en $|G|$. Supongamos que S es subnormal en todo subgrupo H tal que $S \subseteq H \subsetneq G$. Si S no es subnormal en G entonces, por el teorema 11.1, existe un único subgrupo maximal M de G tal que $S \subseteq M$. Sea $x \in G$ y sea $T = xSx^{-1}$. Por el lema 11.2 $ST \neq G$ (pues $S \neq G$) y entonces ST está contenido en algún subgrupo maximal de G. Como $S \subseteq ST$ y S está contenido en un

único maximal, se concluye que $T \subseteq ST \subseteq M$. Como $S^G = \langle xSx^{-1} : x \in G\rangle \subseteq M \neq G$, por hipótesis inductiva S es subnormal en S^G. Luego S es subnormal en G pues S^G es normal en G, una contradicción. □

theorem:Baer

Teorema 11.4 (Baer). *Sean G un grupo finito y H un subgrupo de G. Entonces $H \subseteq F(G)$ si y sólo si $\langle H, xHx^{-1}\rangle$ es nilpotente para todo $x \in G$.*

Demostración. Si $H \subseteq F(G)$ entonces $xHx^{-1} \subseteq F(G)$ para todo $x \in G$ pues $F(G)$ es normal en G. Luego $\langle H, xHx^{-1}\rangle$ es nilpotente por ser un subgrupo de $F(G)$.

Demostraremos la recíproca. Supongamos que $\langle H, xHx^{-1}\rangle$ es nilpotente para todo $x \in G$. Como $H \subseteq \langle H, xHx^{-1}\rangle$, H es nilpotente. Por el teorema 11.6 basta ver que H es subnormal en G. Procederemos por inducción en $|G|$. Supongamos que H no es subnormal en G. Si H está contenido propiamente en algún subgrupo K entonces, como $\langle H, kHk^{-1}\rangle$ es nilpotente para todo $k \in K$, H es subnormal en K por hipótesis inductiva. Por el teorema 11.1, existe un único maximal M de G que contiene a H. Vamos a considerar dos casos posibles: a) $G = \langle H, xHx^{-1}\rangle$ para algún $x \in G$. Como G entonces es nilpotente, H es subnormal en G por el teorema 11.4, una contradicción. b) $\langle H, xHx^{-1}\rangle \neq G$ para todo $x \in G$. En este caso, para cada $x \in G$ existe un subgrupo maximal que contiene a $\langle H, xHx^{-1}\rangle$. Como $H \subseteq \langle H, xHx^{-1}\rangle$ y H está contenido en un único maximal, se concluye que $\langle H, xHx^{-1}\rangle \subseteq M$ para todo $x \in G$. En particular, la clausura normal H^G de H está propiamente contenida en G. Como por hipótesis inductiva H es subnormal en H^G y H^G es normal en G, se concluye que H es subnormal en G, una contradicción. □

theorem:Zenkov

Teorema 11.5 (Zenkov). *Sean G un grupo finito y A, B subgrupos abelianos de G. Sea $M \in \{A \cap gBg^{-1} : g \in G\}$ tal que ningún $A \cap gBg^{-1}$ está propiamente contenido en M. Entonces $M \subseteq F(G)$.*

Demostración. Sin pérdida de generalidad podemos suponer que $M = A \cap B$. Demostraremos por inducción en $|G|$ que $M \subseteq F(G)$.

Supongamos que $G = \langle A, gBg^{-1}\rangle$ para algún $g \in G$. Como A y B son abelianos, $A \cap gBg^{-1} \subseteq Z(G)$. Luego

$$A \cap gBg^{-1} = g^{-1}(A \cap gBg^{-1})g \subseteq A \cap B = M.$$

Por la minimalidad de M, $M = A \cap gBg^{-1} \subseteq Z(G) \subseteq F(G)$ por el corolario 10.7.

Supongamos ahora que $G \neq \langle A, gBg^{-1}\rangle$ para todo $g \in G$. Fijemos $g \in G$. Sean $H = \langle A, gBg^{-1}\rangle \neq G$ y $C = B \cap H$. Al usar que $A \subseteq H$ se obtiene fácilmente que $M = A \cap B = A \cap C$ y que $A \cap hCh^{-1} = A \cap hBh^{-1}$ para todo $h \in H$. Esto implica que ningún $A \cap hCh^{-1}$ está propiamente contenido en $A \cap C$. Al aplicar la hipótesis inductiva al subgrupo H obtenemos entonces

$$M = A \cap B = A \cap C \subseteq F(H).$$

Vamos a demostrar ahora que todo p-subgrupo de Sylow P de M está contenido en $F(G)$. Como M está generado por sus subgrupos de Sylow, esto implica que $M \subseteq F(G)$. Si $P \in \mathrm{Syl}_p(M)$ entonces $P \subseteq M \subseteq F(H)$. Como $O_p(H)$ es el único p-subgrupo de Sylow de $F(H)$, $P \subseteq O_p(H)$. Como $P \subseteq M \subseteq B$,

$$gPg^{-1} \subseteq gBg^{-1} \subseteq H$$

para todo $g \in G$. Entonces $O_p(H)(gPg^{-1})$ es un p-subgrupo de H que contiene a $\langle P, gPg^{-1}\rangle$. Luego $\langle P, gPg^{-1}\rangle$ es nilpotente para todo $g \in G$ por ser un p-grupo. Por el teorema de Baer 11.4, $P \subseteq F(G)$ para todo p-subgrupo de Sylow P de M. □

corollary:Zenkov **Corolario 11.6.** *Sea G un grupo finito no trivial y sea A un subgrupo abeliano tal que $|A| \geq (G:A)$. Entonces $A \cap F(G) \neq 1$.*

Demostración. Sea $g \in G$. Podemos suponer que $G \neq A$ y luego $(gAg^{-1})A \neq G$ por el lema 11.2. Como $|gAg^{-1}||A| = |A|^2 \geq |A|(G:A) = |G|$,

$$|G| > |gAg^{-1}A| = \frac{|A||gAg^{-1}|}{|A \cap gAg^{-1}|} \geq \frac{|G|}{|A \cap gAg^{-1}|}.$$

Luego $A \cap gAg^{-1} \neq 1$ para todo $g \in G$. En particular, ningún $A \cap gAg^{-1}$ está propiamente contenido en A y luego, por el teorema de Zenkov 11.5, $A \subseteq F(G)$. □

Corolario 11.7. *Sea $G = NA$ un grupo finito, donde N es normal en G, A es un subgrupo abeliano y $C_A(N) = 1$. Si $F(N) = 1$, entonces $|A| < |N|$.*

Demostración. Como N es normal en G, $N \cap F(G) = F(N) = 1$ por el corolario 10.9. Luego $[N, F(G)] = 1$ porque N y $F(G)$ son ambos normales en G. Como

$$|A| \geq |N| \geq \frac{|N|}{|N \cap A|} = (NA:A) = (G:A),$$

$A \cap F(G) \neq 1$ por el corolario 11.6. Si $1 \neq a \in A \cap F(G)$, entonces $a \in C_A(N) = 1$, una contradicción. □

theorem:Brodkey **Teorema 11.8 (Brodkey).** *Sea G un grupo finito tal que existe $P \in \mathrm{Syl}_p(G)$ abeliano. Entonces existen $S, T \in \mathrm{Syl}_p(G)$ tales que $S \cap T = O_p(G)$.*

Demostración. Al aplicar el teorema de Zenkov 11.5 con $A = B = P$ se tiene que $P \cap gPg^{-1} \subseteq F(G)$ para algún $g \in G$. Como $O_p(G)$ es el único p-subgrupo de Sylow de $F(G)$, $P \cap gPg^{-1} \subseteq O_p(G)$. Luego $P \cap gPg^{-1} = P_p(G)$ pues $O_p(G)$ está contenido en todo p-subgrupo de Sylow de G. □

corollary:GP2 **Corolario 11.9.** *Sea G un grupo finito. Si existe $P \in \mathrm{Syl}_p(G)$ abeliano,*

$$(G : O_p(G)) \leq (G:P)^2.$$

Demostración. Por el teorema de Brodkey 11.8, existen $S, T \in \mathrm{Syl}_p(G)$ tales que $S \cap T = O_p(G)$. Entonces

$$|G| \geq |ST| = \frac{|S||T|}{|S \cap T|} = \frac{|P|^2}{|O_p(G)|},$$

que implica el corolario. □

Corolario 11.10. *Sea G un grupo finito. Si existe un subgrupo $P \in \mathrm{Syl}_p(G)$ abeliano tal que $|P| < \sqrt{|G|}$ entonces $O_p(G) \neq 1$.*

Demostración. Como $(G:P)^2 < |G|$, el corolario 11.9 implica que $O_p(G) \neq 1$. □

exercise:G/Z(G)

Ejercicio 11.11. Sea G un grupo y sea Sea $K \subseteq Z(G)$. Demuestre que si G/K es cíclico entonces G es abeliano.

Sean $g,h \in G$ y sea $\pi\colon G \to G/K$ el morfismo canónico. Como G/K es cíclico, existe $x \in G$ tal que $G/K = \langle xK \rangle$. Sean k,l tales que $\pi(g) = x^k$, $\pi(h) = x^l$. Entonces existen $z_1, z_2 \in K$ tales que $g = x^k z_1$, $h = x^l z_2$. Luego $[g,h] = [x^k, x^l] = 1$.

Ejercicio 11.12. Sea G un grupo y sea A un subgrupo de G. Demuestre que $\mathrm{Core}_G(A) = \bigcap_{x \in G} xAx^{-1}$ es el mayor subgrupo normal de G contenido en A.

Hagamos actuar a G por multiplicación en las coclases de A: $g \cdot xA = gxA$. Esta acción induce un morfismo $\rho\colon G \to \mathbb{S}_{G/A}$ con núcleo

$$\ker \rho = \bigcap_{x \in G} xAx^{-1} = \mathrm{Core}_G(A).$$

Es claro entonces que $\mathrm{Core}_G(A)$ es un subgrupo normal de G contenido en A. Si K es un subgrupo normal de G tal que $K \subseteq A$, entonces $K = xKx^{-1} \subseteq xAx^{-1}$ para todo $x \in G$. Luego $K \subseteq \mathrm{Core}_G(A)$.

theorem:Lucchini

Teorema 11.13 (Lucchini). *Sea G un grupo finito y sea A un subgrupo cíclico propio. Si $K = \mathrm{Core}_G(A)$ entonces $(A:K) < (G:A)$.*

Demostración. Procederemos por inducción en $|G|$. Sea $\pi\colon G \to G/K$ el morfismo canónico. Observemos que $\mathrm{Core}_{G/K}\, \pi(A)$ es trivial.

Supongamos primero que $K \neq 1$. Como $\pi(A)$ es un subgrupo cíclico propio de G/K y $K \subseteq A$, la hipótesis inductiva implica que

$$(A:K) = |\pi(A)| = (\pi(A):\pi(K)) < (\pi(G):\pi(A)) = \frac{(G:K)}{(A:K)} = (G:A).$$

Supongamos ahora que $K = 1$. Queremos demostrar que $|A| < (G:A)$. Supongamos entonces que $|A| \geq (G:A)$. Como $A \neq G$, $A \cap F(G) \neq 1$ por el corolario 11.6. En particular, $F(G) \neq 1$. Sea E un subgrupo minimal-normal de G tal que $E \subseteq F(G)$. Por el teorema 6.32, $E \cap Z(F(G)) \neq 1$. Luego, como $E \cap Z(F(G))$ es normal en G y E es minimal, $E \cap Z(F(G)) = E$, es decir $E \subseteq Z(F(G))$. En particular, E es abeliano y luego, por la minimalidad de E, existe un primo p tal que $x^p = 1$ para todo $x \in E$.

Afirmación. $A \cap F(G)$ es un subgrupo normal de EA.

Como E es normal en G, EA es un subgrupo de G. Como $A\cap F(G)\subseteq A$, $A\cap F(G)$ es un subgrupo de EA. Como $F(G)$ es normal en G, $a(A\cap F(G))a^{-1}=A\cap F(G)$ para todo $a\in A$. Por otro lado $E\subseteq Z(F(G))$ y $A\cap F(G)\subseteq F(G)$ implican que $x(A\cap F(G))x^{-1}=A\cap F(G)$ para todo $x\in E$.

Afirmación. $EA\neq G$.

Si $G=EA$ entonces, como $A\cap F(G)$ es un subgrupo normal de G contenido en A, se concluye que $1\neq A\cap F(G)\subseteq K=1$, una contradicción. para todo $g\in G$. Luego $1\neq A\cap F(G)\subseteq K$, una contradicción pues $K=1$.

Sea $p\colon G\to G/E$ el morfismo canónico. Por la correspondencia, existe un subgrupo normal M de G con $E\subseteq M$ tal que $p(M)=\mathrm{Core}_{G/E}(p(A))$. Como $EA\neq G$, $p(A)$ es un subgrupo cíclico propio de $p(G)$. Como $p(A)\simeq A/A\cap E\simeq EA/E$ y $p(M)\simeq M/E$, la hipótesis inductiva implica que $(EA:M)<(G:EA)$ pues

$$\frac{|EA/E|}{|M/E|}=(p(A):p(M))<(p(G):p(A))=\frac{|G/E|}{|EA/E|}.$$

Afirmación. $MA=EA$.

Como $E\subseteq M$ entonces $EA\subseteq MA$. Recíprocamente, si $m\in M$ entonces, como $p(m)\in\mathrm{Core}_{G/E}(p(A))$, en particular $p(m)\in p(A)$. Luego $m\in EA$.

Sea $B=A\cap M$. Al usar que $(AE:M)<(G:EA)$, que

$$(A:B)=|A/A\cap M|=|AM/M|=(EA:M)$$

y la hipótesis inductiva obtenemos

$$\begin{aligned}(M:B)&=(M:A\cap M)=(MA:A)\\&=(EA:A)=\frac{(G:A)}{(G:EA)}<\frac{(G:A)}{(AE:M)}=\frac{(G:A)}{(A:B)}\leq|B|\end{aligned}\tag{11.1}$$

eq:(M:B)leq|B|

pues $|A|\geq(G:A)$.

Afirmación. $M=EB$.

Como $E\cup B\subseteq M$ entonces $EB\subseteq M$. Recíprocamente, si $m\in M$ entonces $m=ea$ para algún $e\in E$, $a\in A$. Como $e^{-1}m=a\in A\cap M=B$ pues $E\subseteq M$ entonces $m\in EB$.

Afirmación. M es no abeliano.

Supongamos que M es abeliano. La función $f\colon M\to M$, $m\mapsto m^p$, es un morfismo de grupos tal que $E\subseteq\ker f$. Como $M=EB$, $f(M)\subseteq f(B)\subseteq B\subseteq A$. Como M es normal en G, $f(M)$ es normal en G. Luego $f(M)=1$ pues $K=\mathrm{Core}_G(A)=1$ es el mayor subgrupo normal de G contenido en A; en particular, como B es normal en $M=EB$, M/B es un p-grupo. Como $B\subseteq M$, $f(B)=1$; además como $B\subseteq A$ es cíclico, $|B|\leq p$. Luego, por la fórmula (11.1), $(M:B)<|B|\leq p$. Esto implica que $M=B\subseteq A$ y que $M=E=1$ (porque M es normal en G y $\mathrm{Core}_G(A)=K=1$ es el mayor subgrupo normal de G que contiene a A), una contradicción.

Afirmación. $Z(M)$ es cíclico.

Como M es no abeliano y $M/E = EB/E \simeq B/E \cap B$ es ciclico, $E \not\subseteq Z(M)$ (ejercicio 11.11), es decir $E \cap Z(M) \subsetneq E$. Luego

$$E \cap Z(M) = 1 \tag{11.2}$$

equation:EcapZ(M)

por la minimalidad de E. Entonces

$$Z(M) = Z(M)/Z(M) \cap E \simeq p(Z(M)) \subseteq p(M) = \mathrm{Core}_{G/E}\, p(A) \subseteq p(A)$$

y luego $Z(M)$ es cíclico pues $p(A)$ es cíclico.

Como $B \subseteq A$ es abeliano y $(M : B) < |B|$, $B \cap F(M) \neq 1$ por el corolario 11.6. Entonces $[E, F(M)] = 1$ (pues $E \subseteq Z(F(G))$ y $F(M) \subseteq F(G)$ por el corolario 10.9). Luego $B \cap F(M) \subseteq Z(M)$ pues $M = BE$, $[B \cap F(M), E] \subseteq [F(M), E] = 1$ y también $[B \cap F(M), B] = 1$ porque B es abeliano. Como $Z(M)$ es cíclico, $B \cap F(M)$ es característico en $Z(M)$. Luego, como $Z(M)$ es normal en G, $1 \neq B \cap F(M)$ es un subgrupo normal de G contenido en A, una contradicción. □

Para terminar la sección veamos una aplicación del teorema de Lucchini.

Corolario 11.14 (Horosevskii). *Sea $G \neq 1$ un grupo finito y sea $\sigma \in \mathrm{Aut}(G)$. Entonces $|\sigma| < |G|$.*

Demostración. Sea $A = \langle \sigma \rangle$. Como A actúa por automorfismos en G, podemos considerar el grupo $\Gamma = G \rtimes A$ con la operación

$$(g, \sigma^k)(h, \sigma^l) = (g\sigma^k(h), \sigma^{k+l}).$$

Identificamos A con $1 \times A$ y G con $G \times 1$. Como $K \cap G \subseteq A \cap G = 1$ y $A \cap C_\Gamma(G) = 1$,

$$K \subseteq A \cap C_\Gamma(G) = 1$$

pues si $k \in K$ y $g \in G$ entonces $gkg^{-1}k^{-1} \in G \cap K = 1$ (porque K y G son normales en Γ). Por el teorema de Lucchini 11.13, $(A : K) < (\Gamma : A)$, es decir

$$|\sigma| = |A| = (A : K) < (\Gamma : A) = |G|.$$

□

11. El subgrupo de Chermak–Delgado

Veamos una aplicación del teorema de la cremallera al reticulado de Chermak–Delgado.

lemma:L(G)L(S)

Lema 11.1. *Sea G un grupo finito. Sea $H \in \mathscr{L}(G)$ y sea S un subgrupo de G tal que $HC_G(H) \subseteq S$. Entonces $H \in \mathscr{L}(S)$.*

Demostración. Como $C_G(H) \subseteq S$, $C_G(H) = C_S(H)$. Vimos en el ejercicio 10.6 que $M_S \leq M_G$. Luego $M_G = M_S$ pues

$$M_G = m_G(H) = |H||C_G(H)| = |H||C_S(H)| = m_S(H) \leq M_S.$$

□

theorem:L(G)subnormal

Teorema 11.2. *Sea G un grupo finito. Todo $H \in \mathscr{L}(G)$ es subnormal en G.*

Demostración. Procederemos por inducción en $|G|$. El caso $|G| = 1$ es trivial. Sea $H \in \mathscr{L}(G)$ y sea $K = HC_G(H)$. Como H es normal en K, basta con demostrar que K es subnormal en G. Si $K = G$ no hay nada para hacer. Supongamos entonces que $K \neq G$.

Supongamos que K no es subnormal en G. Por hipótesis inductiva y por el teorema de la cremallera 11.1, existe un único subgrupo maximal M que contiene a K. Por el teorema 10.8, $C_G(H) \in \mathscr{L}(G)$ y $K = HC_G(H) \in \mathscr{L}(G)$. Por el lema 11.1, $H \in \mathscr{L}(M)$ y luego $K \in \mathscr{L}(M)$. Por hipótesis inductiva, K es subnormal en M. Veamos que M es normal en G. Sea $x \in G$. Como $m_G(xKx^{-1}) = m_G(K)$, el subgrupo $xKx^{-1} \in \mathscr{L}(G)$ y luego $K(xKx^{-1}) \in \mathscr{L}(G)$.

Si $K(xKx^{-1}) = G$ entonces, como existen $k_1, k_2 \in K$ tales que $k_1(xk_2x^{-1}) = x^{-1}$, se tiene que $x \in K$ pues $x^{-1} = k_2k_1 \in K$; esto implica que $xKx^{-1} \subseteq K$ y entonces $K = G$, una contradicción.

Como $K(xKx^{-1}) \neq G$, existe un subgrupo maximal N tal que $K(xKx^{-1}) \subseteq N$. Como $K \subseteq N$, $N = M$ pues M es el único maximal que contiene a K. Como además $xKx^{-1} \subseteq M$, $K \subseteq x^{-1}Mx$. Luego $x^{-1}Mx = M$ pues $x^{-1}Mx$ es un maximal que contiene a K y M es el único maximal que contiene a K. □

Corolario 11.3. *Si G un grupo simple finito no abeliano entonces $\mathscr{L}(G) = \{1, G\}$.*

Demostración. Sea $K \in \mathscr{L}(G)$. Entonces K es subnormal en G por el teorema 11.2 y luego $K \in \{1, G\}$. Como $m_G(1) = m_G(G)$, el corolario queda demostrado. □

Corolario 11.4. *Sea $n \geq 5$. Entonces $\mathscr{L}(\mathbb{S}_n) = \{1, \mathbb{S}_n\}$.*

Demostración. Sea $G = \mathbb{S}_n$ y sea $K \in \mathscr{L}(G)$. Por el teorema 11.2, K es subnormal en G. Si $K \neq G$ entonces se tiene una sucesión estrictamente creciente de subgrupos

$$K = K_1 \lhd K_2 \lhd \cdots \lhd K_{n-1} \lhd K_n = G.$$

Como K_{n-1} es normal en G, $K_{n-1} \in \{1, \mathbb{A}_n\}$ y luego $K = 1$. El corolario queda demostrado al observar que $m_G(1) = m_G(G)$. □

11. El morfismo de transferencia

Sea G un grupo y sea H un subgrupo de índice finito. Vamos a definir un morfismo de grupos $G \to H/[H,H]$, el **morfismo de transferencia** de G en H. Fijemos un **transversal a izquierda**[1] T de H en G.

lemma:sigma

Lema 11.1. *Sean G un grupo y H un subgrupo de índice n. Sean $S = \{s_1, \dots, s_n\}$ y $T = \{t_1, \dots, t_n\}$ transversales de H en G. Dado $g \in G$, existen únicos $h_1, \dots, h_n \in H$ y una permutación $\sigma \in \mathbb{S}_n$ tales que*

$$gt_i = s_{\sigma(i)} h_i, \quad i \in \{1, \dots, n\}.$$

Demostración. Si $i \in \{1, \dots, n\}$ existe un único $j \in \{1, \dots, n\}$ tal que $gt_i \in s_j H$. Luego existe un único $h_i \in H$ tal que $gt_i = s_j h_i$. Al tomar $\sigma(i) = j$ queda entonces definida una función $\sigma\colon \{1, \dots, n\} \to \{1, \dots, n\}$. Para ver que $\sigma \in \mathbb{S}_n$ basta ver que σ es inyectiva. Si $\sigma(i) = \sigma(k) = j$, como $gt_i = s_j h_i$ y $gt_k = s_j h_k$, tenemos que $t_i^{-1} t_k = h_i^{-1} h_k \in H$ y luego $i = k$ pues $t_i H = t_k H$. □

definition:nu_T

Definición 11.2. Sea G un grupo y sea H un subgrupo de G de índice finito n. Si $T = \{t_1, \dots, t_n\}$ es un transversal de H en G, se define la función

$$\nu_T\colon G \to H/[H,H], \quad \nu_T(g) = \prod_{i=1}^{n} h_i$$

donde $gt_i = t_j h_i$.

lemma:nu_T

Lema 11.3. *Sea G un grupo y sea H un subgrupo de G de índice finito. Si T y S son transversales de H en G, entonces $\nu_T = \nu_S$.*

Demostración. Supongamos que $gs_i = s_{\sigma(i)} h_i$ para todo i y escribamos $s_i = t_i k_i$, $k_i \in H$. Entonces, si $l_i = k_{\sigma(i)} h_i k_i^{-1}$,

$$gt_i = g s_i k_i^{-1} = s_{\sigma(i)} h_i k_i^{-1} = t_{\sigma(i)} k_{\sigma(i)} h_i k_i^{-1} = t_{\sigma(i)} l_i$$

para todo $i \in \{1, \dots, n\}$. Además

$$s_{\sigma(i)}^{-1} g s_i = k_{\sigma(i)}^{-1} t_{\sigma(i)}^{-1} g t_i k_i.$$

Como $H/[H,H]$ es un grupo abeliano, tenemos

$$\begin{aligned} \nu_S(g) &= \prod_{i=1}^{n} s_{\sigma(i)}^{-1} g s_i = \prod_{i=1}^{n} k_{\sigma(i)}^{-1} t_{\sigma(i)}^{-1} g t_i k_i \\ &= \prod_{i=1}^{n} k_{\sigma(i)}^{-1} \prod_{i=1}^{n} k_i \prod_{i=1}^{n} t_{\sigma(i)}^{-1} g t_i = \prod_{i=1}^{n} t_{\sigma(i)}^{-1} g t_i = \nu_T(g). \end{aligned}$$

[1] Un transversal a izquierda de H en G es simplemente un conjunto de representantes de coclases a izquierda de H en G.

□

El lema 11.3 demuestra que si H es un subgrupo de G de índice finito, queda bien definida la función

$$\nu\colon G \to H/[H,H], \quad \nu(g) = \nu_T(g),$$

donde T es algún transversal de H en G.

theorem:transfer

Teorema 11.4. *Sea G un grupo y sea H un subgrupo de G de índice finito. Entonces $\nu(xy) = \nu(v)\nu(y)$ para todo $x, y \in G$.*

Demostración. Sea $T = \{t_1, \ldots, t_n\}$ un transversal de H en G. Sean $x, y \in G$. Por el lema 11.1 existen únicos $h_1, \ldots, h_n, k_1, \ldots, k_n \in H$ y existen $\sigma, \tau \in \mathbb{S}_n$ tales que $xt_i = t_{\sigma(i)}h_i$, $yt_i = t_{\tau(i)}k_i$. Como

$$xyt_i = xt_{\tau(i)}k_i = t_{\sigma\tau(i)}h_{\tau(i)}k_i,$$

y el grupo $H/[H,H]$ es abeliano,

$$\nu(xy) = \prod_{i=1}^{n} h_{\tau(i)}k_i = \prod_{i=1}^{n} h_{\tau(i)} \prod_{i=1}^{n} k_i = \nu(x)\nu(y).$$

□

El teorema 11.4 afirma que ν es un morfismo de grupos. Queda entonces justificada la siguiente definición:

Definición 11.5. Sea G un grupo y sea H un subgrupo de índice finito. El **morfismo de transferencia** es el morfismo $\nu\colon G \to H/[H,H]$, $\nu(g) = \nu_T(g)$, donde T es algún transversal de H en G.

Ejemplo 11.6. Sea p un número primo. Sean $G = \mathbb{F}_p^\times$ y $H = \{-1, 1\}$. Entonces $(G : H) = \frac{p-1}{2}$. Calculemos el morfismo de transferencia:

$$\nu\colon G \to H, \quad \nu(x) = x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ es un cuadrado,} \\ -1 & \text{en otro caso.} \end{cases}.$$

Elegimos un transversal $T = \{1, 2, \ldots, \frac{p-1}{2}\}$. Para $x \in G$, $t \in T$ definimos

$$\varepsilon(x,t) = \begin{cases} 1 & \text{si } xt \in T, \\ -1 & \text{si } xt \notin T. \end{cases}$$

Al calcular el morfismo de transferencia obtenemos el **lema de Gauss**:

$$\left(\frac{x}{p}\right) = \prod_{t \in T} \varepsilon(x,t).$$

theorem:P_noabeliano

Teorema 11.7. *Sea G un grupo finito. Sea p un primo que divide al orden de $[G,G]\cap Z(G)$. Si $P\in \mathrm{Syl}_p(G)$ entonces P es no abeliano.*

Demostración. Supongamos que P es abeliano y sea $T=\{t_1,\dots,t_n\}$ un transversal de P en G. Como $[G,G]\cap Z(G)$ es un subgrupo normal de G, podemos suponer que $P\cap[G,G]\cap Z(G)\neq 1$. Sea $z\in P\cap[G,G]\cap Z(G)$ tal que $z\neq 1$.

Sea $\nu\colon G\to P$ el morfismo de transferencia. Vamos a calcular $\nu(z)$ con el lema 11.1. Para cada $i\in\{1,\dots,n\}$ sean $x_1,\dots,x_n\in P$ y sea $\sigma\in\mathbb{S}_n$ tales que $zt_i=t_{\sigma(i)}x_i$. Como $z\in Z(G)$, se tiene $t_i=t_{\sigma(i)}x_iz^{-1}$ y luego la unicidad del lema 11.1 implica que $\sigma=\mathrm{id}$ y $x_i=z$ para todo i. Luego

$$\nu(z)=z^{|T|}=z^{(G:P)}.$$

Como P es abeliano, $[G,G]\subseteq\ker\nu$. Luego $\nu(z)=1$. Esto es una contradicción pues $1\neq z\in P$ y $z^{(G:P)}=1$ implica que z tiene orden no divisible por p. □

lemma:evaluation

Lema 11.8. *Sea G un grupo y sea H un subgrupo de índice n. Sea $T=\{t_1,\dots,t_n\}$ un transversal de H en G. Para cada $g\in G$ existen $s_1,\dots,s_m\in T$ y enteros positivos $n_1,\dots,n_m$ (que dependen de g) tales que $s_i^{-1}g^{n_i}s_i\in H$, $n_1+\cdots+n_m=n$ y*

$$\nu(g)=\prod_{i=1}^{m}s_i^{-1}g^{n_i}s_i.$$

Demostración. Para cada i existen $h_1,\dots,h_n\in H$ y $\sigma\in\mathbb{S}_n$ tales que $gt_i=t_{\sigma(i)}h_i$. Escribimos σ como producto de ciclos disjuntos

$$\sigma=\alpha_1\cdots\alpha_m.$$

Para cada $i\in\{1,\dots,n\}$, escribamos $\alpha_i=(j_1\cdots j_{n_i})$. Como

$$gt_{j_k}=t_{\sigma(j_k)}h_{j_k}=\begin{cases}t_{j_1}h_{n_i} & \text{si } i=n_i,\\ t_{j_{k+1}}h_k & \text{en otro caso,}\end{cases}$$

entonces

$$t_{j_1}^{-1}g^{n_i}t_{j_1}=t_{j_1}^{-1}gg^{n_i-1}t_{j_1}=t_{j_1}^{-1}gt_{j_r}h_{j_{r-1}}\cdots h_{j_1}=h_{j_r}\cdots h_{j_1}\in H,$$

y definimos $s_i=t_{j_1}$. Como $\nu(g)=h_1\cdots h_n$, de aquí se deduce inmediatamente el lema. □

proposition:v(g)=g^n

Proposición 11.9. *Sea G un grupo y sea H un subgrupo abeliano de índice n tal que $H\subseteq Z(G)$. Entonces $\nu(g)=g^n$ para todo $g\in G$.*

Demostración. Sea $g\in G$. Por el lema 11.8 existen $s_1,\dots,s_m\in H$ tales que $s_i^{-1}g^{n_i}s_i\in H$ y $\nu(g)=\prod_{i=1}^m s_i^{-1}g^{n_i}s_i$. Como H es normal en G por ser central,

$$g^{n_i}=s_i(s_i^{-1}g^{n_i}s_i)s_i^{-1}\in H\subseteq Z(G).$$

Luego

$$\nu(g) = \prod_{i=1}^{m} s_i^{-1} g^{n_i} s_i = \prod_{i=1}^{m} g^{n_i} = g^{\sum_{i=1}^{m} n_i} = g^n.$$

□

Corolario 11.10. *Si un grupo G tiene un subgrupo H de índice n tal que $H \subseteq Z(G)$ entonces $g \mapsto g^n$ es un morfismo de grupos.*

Demostración. La función $g \mapsto g^n$ es el morfismo de transferencia, ver la proposición 11.9 y el teorema 11.4. □

corollary:[x,y]^n=1

Corolario 11.11. *Sea G un grupo tal que $(G : Z(G)) = n$. Si $x, y \in G$ entonces $[x,y]^n = 1$.*

Demostración. Como $Z(G)$ es abeliano, el núcleo del morfismo de transferencia $\nu\colon G \to Z(G)$, $\nu(g) = g^n$, contiene al conmutador $[G,G]$. □

corollary:semidirecto

Corolario 11.12. *Sea G un grupo finito y sea H un subgrupo abeliano de índice n, donde n es coprimo con $|H|$. Sea $N = \ker(\nu\colon G \to H)$. Entonces $G \simeq N \rtimes H$.*

Demostración. Como H es abeliano, $H = H/[H,H]$ y el morfismo de transferencia es $\nu\colon G \to H$. Por el lema 11.8, podemos escribir

$$\nu(h) = \prod_{i=1}^{m} s_i^{-1} h^{n_i} s_i = \prod_{i=1}^{m} h^{n_i} = h^{\sum_{i=1}^{m} n_i} = h^n.$$

La composición $H \hookrightarrow G \xrightarrow{\nu} H$ es morfismo de grupos.

Vamos a demostrar que es un isomorfismo. Es inyectiva pues si $h^n = 1$ entonces $|h|$ divide a $|H|$ y divide a n; y como n y $|H|$ son coprimos, $h = 1$. Veamos que es sobreyectiva. Como n y $|H|$ son coprimos, existe $m \in \mathbb{Z}$ tal que $nm \equiv 1$ mód $|H|$. Si $h \in H$ entonces $h^m \in H$ y $\nu(h^m) = h^{nm} = h$.

Tenemos entonces que $G \simeq N \rtimes H$ pues N es normal en G, $N \cap H = 1$ y $G = NH$ (pues $|NH| = |N||H|$ y $G/N \simeq H$). □

Corolario 11.13 (Frobenius). *Sea H un subgrupo central de un grupo finito G. Si $|H|$ y $|G/H|$ son coprimos entonces $G \simeq H \times G/H$.*

Demostración. Es consecuencia inmediata del corolario 11.12 pues H es normal por ser un subgrupo central. □

11. Un teorema de Schur

lemma:[s,t]

Lema 11.1. *Sea G un grupo y sea T un transversal de $Z(G)$ en G. Entonces todo conmutador de G es de la forma $[s,t]$, $s,t \in T$. En particular, G tiene finitos conmutadores si $Z(G)$ es de índice finito.*

Demostración. Todo elemento de G puede escribirse como sx, $s \in T$, $x \in Z(G)$. Para demostrar la primera afirmación basta observar que

$$[sx, ty] = [s,t]$$

pues $x, y \in Z(G)$. La segunda afirmación es evidente ya que $|T| = (G : Z(G))$. □

theorem:Dietzmann

Teorema 11.2 (Dietzmann). *Sea G un grupo y sea $X \subseteq G$ un subconjunto finito de G cerrado por conjugación. Si existe $n \in \mathbb{N}$ tal que $x^n = 1$ para todo $x \in X$, entonces $\langle X \rangle$ es un subgrupo finito de G.*

Demostración. Sea $S = \langle X \rangle$. Como $x^{-1} = x^{n-1}$, todo elemento de S puede escribirse como producto (finito) de elementos de X.

Fijemos $x \in X$. Vamos a demostrar que si $x \in X$ aparece $k \geq 1$ veces en la representación de s, podemos escribir a s como producto de m elementos de X donde los primeros k son iguales a x. Supongamos que

$$s = x_1 x_2 \cdots x_{t-1} x x_{t+1} \cdots x_m,$$

donde cada $x_j \neq x$ para todo $j \in \{1, \ldots, t-1\}$. Entonces

$$s = x(x^{-1}x_1x)(x^{-1}x_2x)\cdots(x^{-1}x_{t-1}x)x_{t+1}\cdots x_m$$

es producto de m elementos de X pues X es cerrado por conjugación, y el primer elemento es nuestro x. Este mismo argumento implica que s puede escribirse como

$$s = x^k y_{k+1} \cdots y_m,$$

donde los y_j son elementos de $X \setminus \{x\}$.

Sea $s \in S$ y escribamos a s como producto de m elementos de X, donde m es el mínimo posible. Para ver que S es finito basta ver que $m \leq (n-1)|X|$.

Si suponemos que $m > (n-1)|X|$, al menos un $x \in X$ aparecería n veces en la representación de s. Sin pérdida de generalidad, podríamos escribir

$$s = x^n x_{n+1} \cdots x_m = x_{n+1} \cdots x_m,$$

una contradicción a la minimalidad de m. □

theorem:Schur_commutador

Teorema 11.3 (Schur). *Si $Z(G)$ tiene índice finito en G entonces $[G,G]$ es finito.*

Demostración. Sea $X = \{[x,y] : x, y \in G\}$. Por el lema 11.1), X es finito. Además X es cerrado por conjugación pues

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

para todo $g, x, y \in G$. Si $n = (G : Z(G))$ entonces $x^n = 1$ para todo $x \in X$ por el corolario 11.11. Luego el teorema queda demostrado al aplicar el teorema 11.2. □

Corolario 11.4 (Sury). *Si el conjunto de conmutadores de un grupo G es finito, entonces $[G,G]$ es también finito.*

Demostración. Sea C el conjunto de conmutadores de G y sea H el subgrupo de G generado por C. Sabemos que H es finitamente generado, digamos por los elementos $h_1,\dots,h_n$. Como $h \in Z(H)$ si y sólo si $h \in C_H(H_i)$ para todo $i \in \{1,\dots,n\}$, se tiene que $Z(H) = \cap_{i=1}^n C_H(h_i)$. Además, si $h \in H$, entonces $hh_ih^{-1} = ch_i$ para algún $c \in C$. Luego la clase de conjugación de cada h_i tiene a lo sumo tantos elementos como C. Esto implica que

$$|H/Z(H)| = |H/\cap_{i=1}^n C_H(H_i)| \leq \prod_{i=1}^n (H : C_H(h_i)) \leq |C|^n.$$

Como entonces $H/Z(H)$ es finito, $[H,H]$ es finito. Luego $[G,G] = \langle C\rangle \subseteq [H,H]$ es también un grupo finito. □

El corolario anterior puede utilizarse también para dar una demostración alternativa del teorema que demostraremos elementalente a condituación.

Teorema 11.5 (Hilton–Niroomand). *Sea G un grupo finitamente generado. Si $[G,G]$ es finito y $G/Z(G)$ está generado por n elementos, entonces*

$$|G/Z(G)| \leq |[G,G]|^n.$$

Demostración. Supongamos que $G/Z(G) = \langle x_1Z(G),\dots,x_nZ(G)\rangle$. Sea

$$f\colon G/Z(G) \to [G,G]\times\cdots\times[G,G], \quad y \mapsto ([x_1,y],\dots,[x_n,y]).$$

Primero observamos que f está bien definida: si $y \in G$ y $z \in Z(G)$ entonces

$$f(yz) = [x_i,yz] = [x_i,y] = f(y).$$

Ahora veamos que f es inyectiva: Supongamos que $f(xZ(G)) = f(yZ(G))$. Entonces $[x_i,x] = [x_i,y]$ para todo $i \in \{1,\dots,n\}$. Para cada i calculamos

$$\begin{aligned}[x^{-1}y,x_i] &= x^{-1}[y,x_i]x[x^{-1},x_i] \\ &= x^{-1}[y,x_i][x_i,x]x = x^{-1}[x_i,y]^{-1}[x_i,x]x = x^{-1}[x_i,y]^{-1}[x_i,y]x = 1.\end{aligned}$$

Luego $x^{-1}y \in Z(G)$ pues, como todo $g \in G$ puede escribirse como $g = x_kz$ para algún $k \in \{1,\dots,n\}$ y algún $z \in Z(G)$, se tiene que $[x^{-1}y,g] = [x^{-1}y,x_kz] = [x^{-1}y,x_k] = 1$. Esto implica que f es inyectiva y luego $|G/Z(G)| \leq |[G,G]|^n$. □

Veamos una aplicación del morfismo de transferencia a grupos infinitos.

Teorema 11.6. *Sea G un grupo sin torsión que contiene un subgrupo de índice finito isomorfo a $\mathbb{Z}$. Entonces $G \simeq \mathbb{Z}$.*

Demostración. Podemos suponer que G contiene un subgrupo normal de índice finito isomorfo a $\mathbb{Z}$ pues si H un subgrupo de G de índice finito isomorfo a $\mathbb{Z}$, $K = \cap_{x\in G} xHx^{-1}$ es normal en G, K es no trivial (pues $K = \mathrm{Core}_G(H)$ y G no tiene torsión) y luego $K \simeq \mathbb{Z}$ (pues $K \subseteq H$) y $(G:K) = (G:H)(H:K)$ es finito.

La acción de G en K por conjugación induce un morfismo $\varepsilon\colon G \to \mathrm{Aut}(K)$. Como $\mathrm{Aut}(K) = \{-1,1\}$ pues $K \simeq \mathbb{Z}$, hay que considerar dos casos.

Supongamos primero que $\varepsilon = \mathrm{id}$. Como entonces $K \subseteq Z(G)$, sea $\nu\colon G \to K$ el morfismo de transferencia. Por la proposición 11.9, $\nu(g) = g^n$, donde n es el índice de K en G. Como G no tiene torsión, ν es inyectiva. Luego $G \simeq \mathbb{Z}$ por ser isomorfo a un subgrupo de K.

Supongamos ahora que $\varepsilon \neq \mathrm{id}$. Sea $N = \ker\varepsilon \neq G$. Como $K \simeq \mathbb{Z}$ es abeliano, $K \subseteq N$. Al aplicar el resultado del párrafo anterior al caso $\varepsilon|_N = 1$, se concluye que $N \simeq \mathbb{Z}$ pues N posee un subgrupo de índice finito isomorfo a $\mathbb{Z}$. Sea $g \in G \setminus N$. Como N es normal en G, g actúa por conjugación en N y entonces se tiene un morfismo de grupos $c_g \in \mathrm{Aut}(N) \simeq \{-1,1\}$. Como $K \subseteq N$ y g actúa de forma no trivial en K, $c_g(n) = gng^{-1} = n^{-1}$ para todo $n \in N$. Como $g^2 \in N$, entonces

$$g^2 = gg^2g^{-1} = g^{-2}.$$

Luego $g^4 = 1$, una contradicción porque $g \neq 1$ y G no tiene torsión. □

11. El teorema del complemento normal

lemma:normal_complement

Lema 11.1. *Sea G un grupo finito y sea p un primo que divide al orden de G. Sea $P \in \mathrm{Syl}_p(G)$. Si $g,h \in C_G(P)$ son conjugados en G entonces son conjugados en $N_G(P)$.*

Demostración. Sea $x \in G$ tal que $g = xhx^{-1}$. Entonces $g \in C_G(xPx^{-1})$. Luego P y xPx^{-1} son subgrupos de Sylow de $C_G(g)$. Por el teorema de Sylow, existe $c \in C_G(g)$ tal que $P = cxP(cx)^{-1}$. Tenemos $cx \in N_G(P)$ y

$$(cx)h(cx)^{-1} = c(xhx^{-1})c^{-1} = cgc^{-1} = g.$$

□

Definición 11.2. Sea G un grupo finito y sea p un primo que divide al orden de G. Un **p-complemento normal** es un subgrupo normal N de orden coprimo con p y tal que $(G:N)$ es una potencia de p.

Definición 11.3. Un grupo finito se dice **p-nilpotente** si tiene un p-complemento normal.

Proposición 11.4. *Si G tiene un p-complemento normal N, entonces N es un subgrupo característico de G.*

Demostración. Supongamos que $|G| = p^\alpha n$, donde n es coprimo con p, y sea $\pi\colon G \to G/N$ el morfismo canónico. Por hipótesis, N tiene orden n. Vamos a demostrar que N es el único subgrupo de G de orden n. Si K es un subgrupo de G de orden n, entonces $\pi(K) \simeq K/K\cap N$ y luego el orden de $\pi(K)$ divide a m. Pero además el orden de $\pi(K)$ divide al primo p pues $\pi(K) \leq G/N$. Luego $\pi(K)$ es trivial y

entonces $K = N$ y luego G tiene un único subgrupo de orden n. En particular, N es un subgrupo característico de G. □

rnside:normal_complement

Teorema 11.5 (Burnside). *Sea G un grupo finito y sea p un primo que divide a $|G|$. Sea $P \in \mathrm{Syl}_p(G)$ tal que $P \subseteq Z(N_G(P))$. Entonces G es p-nilpotente.*

Demostración. Como P es abeliano, sea $\nu\colon G \to P$ el morfismo de transferencia. Sea $g \in P$. Por el lema 11.8 existen $s_1, \ldots, s_m \in G$ y existen $n_1, \ldots, n_m$ tales que $n_1 + \cdots + n_m = n$, $s_i^{-1} g^{n_i} s_i \in P$ y

$$\nu(g) = \prod_{i=1}^{m} s_i^{-1} g^{n_i} s_i.$$

Como P es abeliano, $P \subseteq C_G(P)$. Por el lema 11.1, existe $c_i \in N_G(P)$ tal que

$$s_i^{-1} g^{n_i} s_i = c_i^{-1} g^{n_i} c_i,$$

y luego $s_i^{-1} g^{n_i} s_i = g_i^{n_i}$ pues $P \subseteq Z(N_G(P))$. Tenemos entonces que $\nu(g) = g^n$, donde $n = (G : P)$. Como n y $|P|$ son coprimos, existen $r, s \in \mathbb{Z}$ tales que $rn + s|P| = 1$. Esto implica que $\nu|_P$ es sobreyectiva pues

$$g = (g^r)^n = \nu(g^r).$$

Por el teorema de isomorfismos, $P/\ker\nu \cap P \simeq \nu(P) = P$. Luego $\ker\nu \cap P = 1$. Además $\nu(G) = \nu(P)$ pues $P \supseteq \nu(G) \supseteq \nu(P) = P$.

Veamos que $\ker\nu$ es un p-complemento normal en G. Es claro que $\ker\nu$ es normal en G. Como $(G : \ker\nu) = |\nu(G)| = |P|$ y P es un p-subgrupo de Sylow, se concluye que $\ker\nu$ tiene orden coprimo con p. □

lemma:NC

Lema 11.6. *Sea G un grupo y H un subgrupo de G. Entonces $C_G(H)$ es un subgrupo normal de $N_G(H)$ y $N_G(H)/C_G(H)$ es isomorfo a un subgrupo de* $\mathrm{Aut}(H)$.

Demostración. Sea $\phi\colon N_G(H) \to \mathrm{Aut}(H)$, $\phi(g) = c_g|H$, donde $c_g(h) = ghg^{-1}$. La función ϕ está bien definida (pues su dominio es $N_G(H)$) y es morfismo de grupos. Como $\ker\phi = C_G(H)$, se tiene que $C_G(H)$ es normal en $N_G(H)$. Por el primer teorema de isomorfismo, $N_G(H)/C_G(H) \simeq \phi(N_G(H)) \leq \mathrm{Aut}(H)$. □

corollary:Sylow_ciclico

Corolario 11.7. *Sea G un grupo finito y sea p el menor primo que divide a $|G|$. Si algún $P \in \mathrm{Syl}_p(G)$ es cíclico, G es p-nilpotente.*

Demostración. Supongamos que $|P| = p^m$. Por el lema 11.6, $N_G(P)/C_G(P)$ es isomorfo a un subgrupo de $\mathrm{Aut}(P)$. Como P es cíclico, $|N_G(P)/C_G(P)|$ divide a

$$|\mathrm{Aut}(P)| = \phi(|P|) = p^{m-1}(p-1).$$

Como $P \subseteq C_G(P)$ por ser P abeliano, p es coprimo con $|N_G(P)/C_G(P)|$. Luego $|N_G(P)/C_G(P)|$ divide a $p-1$. Pero $p-1$ y $|G|$ son coprimos, pues p es el menor primo que divide a $|G|$. Como además $|N_G(P)/C_G(P)|$ divide al orden de G, se concluye que $|N_G(P)/C_G(P)| = 1$, es decir: $N_G(P) = C_G(P)$.

Como P es abeliano, $P \subseteq Z(C_G(P)) = Z(N_G(P))$. El teorema de Burnside 11.5 implica entonces que G es p-nilpotente. □

Ejercicio 11.8. Sea G un grupo finito tal que todos sus subgrupos de Sylow son cíclicos. Entonces G es resoluble.

Vamos a demostrar algo más fuerte:

Sylow_ciclicos:resoluble

Corolario 11.9. *Sea G un grupo finito tal que todos sus subgrupos de Sylow son cíclicos. Entonces G es superresoluble.*

Demostración. Supongamos que G es no trivial y hagamos inducción en $|G|$. Si p es el menor primo que divide a $|G|$, por el corolario 11.7 el grupo G tiene un p-complemento normal N. Por hipótesis inductiva, N es resoluble. Como G/N es un p-grupo, es resoluble. Luego G es resoluble. □

Corolario 11.10. *Sea G un grupo finito cuyo orden es libre de cuadrados. Entonces G es resoluble.*

Demostración. Es consecuencia del corolario 11.9 pues en este caso todo subgrupo de Sylow es cíclico. □

Corolario 11.11. *Sea G un grupo finito simple no abeliano y sea p el menor primo que divide a $|G|$. Entonces p^3 divide a $|G|$ o bien 12 divide a $|G|$.*

Demostración. Sea $P \in \mathrm{Syl}_p(G)$. Por el corolario 11.7, P no es cíclico, y entonces $|P| \geq p^2$. Si p^3 no divide a $|G|$, $P \simeq C_p \times C_p$ es un $\mathbb{F}_p$-espacio vectorial de dimensión dos. Como $|N_G(P)/C_G(P)|$ divide al orden de G, los divisores primos de $|N_G(P)/C_G(P)|$ son $\geq p$. Además, como $N_G(P)/C_G(P)$ es isomorfo a un subgrupo de $\mathrm{Aut}(P)$ por el lema 11.6 y $\mathrm{Aut}(P) \simeq \mathbf{GL}_2(p)$ tiene orden $(p^2-1)(p^2-p) = p(p+1)(p-1)^2$, $|N_G(P)/C_G(P)|$ divide a $p(p+1)(p-1)^2$. Como P es abeliano, $P \subseteq C_G(P)$. Entonces $|N_G(P)/C_G(P)|$ es coprimo con p y luego $|N_G(P)/C_G(P)|$ divide a $(p+1)(p-1)^2$. Como p es el menor primo que divide a $|G|$, los números $p-1$ y $|N_G(P)/C_G(P)|$ son coprimos, y entonces $|N_G(P)/C_G(P)|$ divide a $p+1$. Además, por el teorema de Burnside 11.5, $|N_G(P)/C_G(P)| \neq 1$. Esto implica que $p = 2$ pues si p es impar el menor primo que divide a $|N_G(P)/C_G(P)|$ es $\geq p+2$. Como entonces $p = 2$, se concluye que $|N_G(P)/C_G(P)| = 3$ y luego $|G|$ es divisible por $12 = 2^2 3$. □

theorem:[GG]PZNG(P)=1

Teorema 11.12. *Sea G un grupo finito y sea P un subgrupo de Sylow abeliano. Entonces $[G,G] \cap P \cap Z(N_G(P)) = 1$.*

Demostración. Sea $x \in [G,G] \cap P \cap Z(N_G(P))$ y sea $v\colon G \to P$ el morfismo de transferencia. Por el lema 11.8 existen $s_1, \ldots, s_m \in G$ y existen $n_1, \ldots, n_m$ tales que $n_1 + \cdots + n_m = (G:P)$, $s_i^{-1} g^{n_i} s_i \in P$ y

$$v(x) = \prod_{i=1}^{m} s_i^{-1} x^{n_i} s_i.$$

Como P es abeliano, $P \subseteq C_G(P)$. Entonces x^{n_i} y $s_i^{-1}x^{n_i}s_i$ son conjugados en $N_G(P)$ por el lema 11.1. Como x^{n_i} es central en $N_G(P)$ y $[G,G] \subseteq \ker \nu$, se concluye que $x = 1$ pues $1 = \nu(x) = x^{(G:P)}$ y $x \in P$. □

Corolario 11.13. *Sea G un grupo finito no abeliano y sea $P \in \mathrm{Syl}_2(G)$ tal que $P \simeq C_{a_1} \times \cdots \times C_{a_k}$ con $a_1 > a_2 \geq a_3 \geq \cdots \geq a_k \geq 2$. Entonces G no es simple.*

Demostración. Sea $S = \{x^{n/2} : x \in P\}$. Es fácil ver que S es un subgrupo de P y que S es característico en P, es decir: $f(S) \subseteq S$ para todo $f \in \mathrm{Aut}(P)$. Como $S \simeq C_2$, podemos escribir $S = \{1, s\}$. Entonces $s \in Z(N_G(P))$ pues $gsg^{-1} \in S$ para todo $g \in N_G(P)$. Por el teorema 11.12, $s \notin [G,G]$ y luego $[G,G] \neq G$. Si G fuera simple, G sería abeliano pues $[G,G] = 1$. □

Vimos en el corolario 11.9 que todo grupo tal que todos sus subgrupos de Sylow son cíclicos es resoluble.

Definición 11.14. Un Z-grupo es un grupo finito G tal que odos sus subgrupos de Sylow son cíclicos.

Un grupo G se dice *meta-cíclico* si G tiene un subgrupo normal N cíclico tal que G/N es cíclico.

Lema 11.15. *Si G es un grupo resoluble, entonces $C_G(F(G)) = F(G)$.*

Demostración. □

theorem:Z=>metacyclic

Teorema 11.16. *Todo Z-grupo es meta-cíclico.*

Demostración. Sea G un Z-grupo. Por el corolario 11.9, G es resoluble y entonces, por el lema, el subgrupo de Fitting $F(G)$ satisface $C_G(F(G)) \subseteq F(G)$.

Demostremos que $F(G)$ es cíclico. En efecto, como $F(G)$ es nilpotente, $F(G)$ es producto directo de sus subgrupos de Sylow. Como todo subgrupo de Sylow de $F(G)$ es un p-subgrupo de G, todo Sylow de $F(G)$ es cíclico (por estar contenido en algún subgrupo de Sylow de G).

Como $F(G)$ es cíclico, $F(G)$ es en particular abeliano y luego $F(G) \subseteq C_G(F(G))$. Si G actúa en $F(G)$ por conjugación, se tiene un morfismo $\gamma\colon G \to \mathrm{Aut}(F(G))$ tal que $\ker \gamma = C_G(F(G)) = F(G)$ (pues $\gamma_g(x) = gxg^{-1}$). En particular, $G/F(G)$ es abeliano por ser isomorfo a un subgrupo del grup abeliano $\mathrm{Aut}(F(G))$. Como además los subgrupos de Sylow de $G/F(G)$ son cíclicos (pues son cocientes de los subgrupos de Sylow de G), $G/F(G)$ es cíclico. □

Capítulo 12
Extensiones

extensiones

12. Extensiones

Definición 12.1. Sean K y Q grupos. Una **extension** de K por Q es un grupo G que tiene un subgrupo normal N isomorfo a K tal que $G/N \simeq Q$. Equivalentemente: una **extensión** de K por Q es una sucesión exacta corta[1]

$$1 \to K \xrightarrow{\iota} G \xrightarrow{p} Q \to 1.$$

Ejemplo 12.2. C_6 y $\mathbb{S}_3$ son extensiones de C_3 por C_2.

Ejemplo 12.3. C_6 es extensión de C_2 por C_3.

Ejemplo 12.4. Sean K y Q grupos. El producto directo $K \times Q$ es extensión de K por Q. También es extensión de Q por K.

remark:extension

Observación 12.5. Sea G una extensión de K por Q. Si L es un subgrupo de G que contiene a K entonces L es una extensión de K por L/K.

Definición 12.6. Un **morfismo** entre las extensiones

$$1 \to K \xrightarrow{\iota} G \xrightarrow{p} Q \to 1, \quad 1 \to K_1 \xrightarrow{\iota_1} G_1 \xrightarrow{p_1} Q_1 \to 1,$$

es una terna (α, β, γ) de morfismos tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{\iota} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & K_1 & \xrightarrow{\iota_1} & G_1 & \xrightarrow{p_1} & Q_1 & \longrightarrow & 1 \end{array}$$

Definición 12.7. Diremos que las extensiones

[1] ι es inyectiva, p es sobreyectiva y $\ker p = \iota(N)$.

$$E\colon 1 \to K \xrightarrow{\iota} G \xrightarrow{p} Q \to 1, \quad E_1\colon 1 \to K_1 \xrightarrow{\iota_1} G_1 \xrightarrow{p_1} Q \to 1,$$

son **isomorfas** si existe un morfismo $(\alpha,\beta,\mathrm{id})$ entre E y E_1 con α isomorfismo. Las extensiones E y E_1 se diran **equivalentes** si $K = K_1$ y $(\mathrm{id},\beta,\mathrm{id})$ es un isomorfismo entre E y E_1.

Ejercicio 12.8. Demuestre que si $(\alpha,\beta,\mathrm{id})$ es un isomorfismo de extensiones entonces β es un isomorfismo de grupos.

Veamos que $\ker\beta = 1$. Sea $g \in G$ tal que $\beta(g) = 1$. Como $g \in \ker p = \iota(K)$ pues $p(g) = p_1\beta(g) = p_1(1) = 1$, existe $k \in K$ tal que $g = \iota(k)$. Entonces $1 = \beta(g) = \beta\iota(k) = \iota_1\alpha(k)$. Como ι_1 y α son morfismos inyectivos, $k = 1$ y luego $g = 1$.

Veamos ahora que $\beta(G) = G_1$. Sea $g_1 \in G_1$. Como p es sobreyectiva, $p_1(g_1) = p(g)$ para algún $g \in G$. Como $\beta(g)g_1^{-1} \in \ker p_1 = \iota_1(K_1)$ y α es epimorfismo, existe $k \in K$ tal que $\beta(g)g_1^{-1} = \iota_1(\alpha(k)) = \beta(\iota(k))$. Luego $\beta(g\iota(k)^{-1}) = g_1$.

Definición 12.9. Sea $E\colon 1 \to K \xrightarrow{\iota} G \xrightarrow{p} Q \to 1$ una extensión. Un **levantamiento** para E es una función $\ell\colon Q \to G$ tal que $p(\ell(x)) = x$ para todo $x \in Q$.

exercise:lifting

Ejercicio 12.10. Sea $E\colon 1 \to K \xrightarrow{\iota} G \xrightarrow{p} Q \to 1$ una extensión. Demuestre las siguientes afirmaciones:

1. Si $\ell\colon Q \to G$ es un levantamiento, $\ell(Q)$ es un transversal para $\ker p$ en G.
2. Todo transversal a $\ker p$ en G induce un levantamiento $\ell\colon Q \to G$.
3. Si $\ell\colon Q \to G$ es un levantamiento entonces $\ell(xy)\ker p = \ell(x)\ell(y)\ker p$.

Sea $N = \iota(K) = \ker p$.

1. Veamos que las $\ell(x)N$ son disjuntas. Si $\ell(x)N = \ell(y)N$, existe $n \in N$ tal que $\ell(x) = \ell(y)n$. Luego

   $$x = p(\ell(x)) = p(\ell(y)n) = p(\ell(y))p(n) = y.$$

   Sea $g \in G$ y sea $x = p(g) \in Q$. Como $x = p(\ell(x))$ y p es morfismo de grupos, $x^{-1} = p(\ell(x)^{-1})$. Luego $g = \ell(x)\left(\ell(x)^{-1}g\right)$ y $\ell(x)^{-1}g \in N$ pues

   $$p(\ell(x)^{-1}g) = p(\ell(x)^{-1})p(g) = x^{-1}x = 1.$$

2. Sea L un transversal a N en G. Si $x \in Q$ entonces existe $g \in G$ tal que $x = p(g)$. Sea $\ell(x) \in L \subseteq G$ tal que $gN = \ell(x)N$. Como $g^{-1}\ell(x) \in N = \ker p$, se concluye que $p(\ell(x)) = x$ pues

   $$x^{-1}p(\ell(x)) = p(g)^{-1}p(\ell(x)) = p(g^{-1}\ell(x)) = 1.$$

3. Sean $x,y \in Q$ y sean $g,h \in G$ tales que $x = p(g)$, $y = p(h)$. Como por definición $gN = \ell(x)N$, $hN = \ell(y)N$ y p es morfismo de grupos,

$$\ell(xy)N = (gh)N = (gN)(hN) = \ell(x)\ell(y)N.$$

Definición 12.11. Se dice que una extensión se **parte** si existe un levantamiento que es morfismo de grupos.

12. Derivaciones y complementos

Definición 12.1. Sean Q y K grupos. Supongamos que Q actúa por automorfismos en K. Una función $\varphi\colon Q \to K$ se dice un 1-**cociclo** (o una **derivación**) si

$$\varphi(xy) = \varphi(x)(x \cdot \varphi(y))$$

para todo $x,y \in Q$. El conjunto de **derivaciones** de Q en K se define como

$$\mathrm{Der}(Q,K) = Z^1(Q,K) = \{\delta\colon Q \to K : \delta \text{ es 1-cociclo}\}.$$

Ejercicio 12.2. Sea Q un grupo que actúa por automorfismos en K. Para cada $k \in K$, la función $Q \to K$, $x \mapsto [k,x] = kxk^{-1}x^{-1}$, es una derivación.

Para $k \in K$ y $x \in Q$ escribimos $\delta_k(x) = [k,x]$. Entonces

$$\delta_k(x)(x\delta_k(y)x^{-1}) = kxk^{-1}x^{-1}xkyk^{-1}y^{-1}x^{-1} = k(xy)k^{-1}(xy)^{-1} = \delta_k(xy).$$

exercise:1cocycle

Ejercicio 12.3. Sea $\varphi\colon Q \to K$ un 1-cociclo. Demuestre las siguientes afirmaciones:

1. $\varphi(1) = 1$.
2. $\varphi(y^{-1}) = (y^{-1} \cdot \phi(y))^{-1} = y^{-1} \cdot \phi(y)^{-1}$.
3. El conjunto $\ker\varphi = \{x \in Q : \varphi(x) = 1\}$ es un subgrupo de Q.

La primera afirmación es fácil pues, como

$$\varphi(1) = \varphi(11) = \varphi(1)(1 \cdot \varphi(1)) = \varphi(1)^2,$$

se concluye que $\varphi(1) = 1$.

Veamos que $\ker\varphi$ es un subgrupo. Como $\varphi(1) = 1$, K es no vacío. Sean $x,y \in \ker\varphi$. Como $1 = \varphi(y^{-1}y) = \varphi(y^{-1})(y^{-1} \cdot \varphi(y))$, se tiene que

$$\varphi(y^{-1}) = (y^{-1} \cdot \phi(y))^{-1}.$$

Similarmente se demuestra que

$$\varphi(y^{-1}) = y^{-1} \cdot \phi(y)^{-1}.$$

De estas fórmulas se deduce que si $x \in \ker\varphi$ entonces $x^{-1} \in \ker\varphi$. Luego $\ker\varphi$ es un subgrupo pues si $x, y \in \ker\varphi$, $\varphi(xy) = \varphi(x)(x \cdot \varphi(y)) = 1(x \cdot 1) = 1$.

theorem:complementos

Teorema 12.4. *Sea Q un grupo que actúa por automorfismos en el grupo K. Existe una biyección entre el conjunto de complementos de K en $K \rtimes Q$ y el conjunto* $\mathrm{Der}(Q,K)$.

Demostración. El grupo Q actúa en K por conjugación, entonces $\delta \in \mathrm{Der}(Q,K)$ si y sólo si $\delta(xy) = \delta(x)x\delta(y)x^{-1}$, $x, y \in Q$. En este caso, las fórmulas del ejercicio 12.3 quedan así: $\delta(1) = 1$, $\delta(x^{-1}) = x^{-1}\delta(x)^{-1}x$.

Sea $\mathscr{C}$ el conjunto de complementos de K en $K \rtimes Q$. Sea $C \in \mathscr{C}$. Si $x \in Q$, por el lemma **??** existen únicos $k \in K$ y $c \in C$ tales que $x = k^{-1}c$. Queda bien definida entonces la función $\delta_C \colon Q \to K$, $x \mapsto k$. Vale que $\delta(x)x = c \in C$.

Veamos que $\delta_C \in \mathrm{Der}(Q,K)$. Si $x, x_1 \in Q$, escribimos $x = k^{-1}c$ y $x_1 = k_1^{-1}c_1$, donde $k, k_1 \in K$ y $c, c_1 \in C$. Como K es normal en $K \rtimes Q$, podemos escribir a xx_1 como $xx_1 = k_2c_2$, donde $k_2 = k^{-1}(ck_1^{-1}c^{-1}) \in K$, $c_2 = cc_1 \in C$. Luego

$$\delta(xx_1)xx_1 = cc_1 = \delta(x)x\delta(x_1)x_1$$

implica que $\delta(xx_1) = \delta(x)x\delta(x_1)x^{-1}$. Tenemos así una función $F \colon \mathscr{C} \to \mathrm{Der}(Q,K)$, $F(C) = \delta_C$.

Vamos a construir ahora $G \colon \mathrm{Der}(Q,K) \to \mathscr{C}$. Para cada $\delta \in \mathrm{Der}(Q,K)$ vamos a definir un complemento Δ de K en $K \rtimes Q$:

$$\Delta = \{\delta(x)x : x \in Q\}.$$

Veamos que Δ es un subgrupo de $K \rtimes Q$. Como $\delta(1) = 1$, $1 \in X$. Si $x, y \in \Delta$ entonces $\delta(x)x\delta(y)y = \delta(x)x\delta(y)x^{-1}xy = \delta(xy)xy \in \Delta$. Por último si $x \in \Delta$ entonces $(\delta(x)x)^{-1} = x^{-1}\delta(x)^{-1}xx^{-1} = \delta(x^{-1})x^{-1}$. Veamos que $\Delta \cap K = 1$. Si $x \in Q$ es tal que $\delta(x)x \in K$ entonces, como $\delta(x) \in K$, $x \in K \cap Q = 1$. Si $g \in G$ entonces existen únicos $k \in K$, $x \in Q$ tales que $g = kx$. Escribimos $g = k\delta(x)^{-1}\delta(x)x$. Como $k\delta(x)^{-1} \in K$ y $\delta(x)x \in \Delta$, se concluye que $G = K\Delta$. Queda bien definida entonces la función $G \colon \mathrm{Der}(Q,K) \to \mathscr{C}$, $G(\delta) = \Delta$.

Veamos ahora que $G \circ F = \mathrm{id}_{\mathscr{C}}$. Sea $C \in \mathscr{C}$. Entonces

$$G(F(C)) = G(\delta_C) = \{\delta_C(x)x : x \in Q\} = C,$$

por construcción. (Vimos que $\delta_C(x)x \in C$. Recíprocamente, si $c \in C$, escribimos $c = kx$ para únicos $k \in K$, $x \in Q$ y luego $x = k^{-1}c$ que implica $c = \delta_c(x)x$.)

Por último veamos que $F \circ G = \mathrm{id}_{\mathrm{Der}(Q,K)}$. Sea $\delta \in \mathrm{Der}(Q,K)$. Entonces

$$F(G(\delta)) = F(\Delta) = \delta_\Delta.$$

Queremos demostrar que $\delta_\Delta = \delta$. Sea $x \in Q$. Existe $\delta(y)y \in \Delta$ para algún $y \in Q$ tal que $x = k^{-1}\delta(y)y$. Luego $\delta_\Delta(x)x = \delta(y)y$ y luego $\delta(x) = \delta(y)$ por la unicidad de la escritura. □

Definición 12.5. Sean Q y K grupos. Supongamos que Q actúa por automorfismos en K. Un $\delta \in \mathrm{Der}(Q,K)$ se dice **interior** si existe $k \in K$ tal que $\delta(x) = [k,x]$ para todo $x \in Q$. El conjunto de **derivaciones interiores** será denotado por

$$\mathrm{Inn}(Q,K) = B^1(Q,K) = \{\delta \in \mathrm{Der}(Q,K) : \delta \text{ es interior}\}.$$

Una derivación interior también se llama 1**-coborde**.

theorem:Sysak

Teorema 12.6. *Sean Q y K grupos tales que Q actúa por automorfismos en K. Sea $\delta \in \mathrm{Der}(Q,K)$.*

1. *$\Delta = \{\delta(x)x : x \in Q\}$ es un complemento para K en $K \rtimes Q$.*
2. *$\delta \in \mathrm{Inn}(Q,K)$ si y sólo si Q y Δ son conjugados en K.*
3. *$\ker\delta = Q \cap \Delta$.*
4. *δ es sobreyectiva si y sólo si $K \rtimes Q = \Delta Q$.*

Demostración. Vimos en la demostración del teorema 12.4 que el conjunto Δ es un complemento para K en $K \rtimes Q$.

Demostremos la segunda afirmación. Si suponemos que δ es interior, existe $k \in K$ tal que $\delta(x) = [k,x] = kxk^{-1}x^{-1}$ para todo $x \in Q$. Como $\delta(x)x = kxk^{-1}$ para todo $x \in Q$, $\Delta = kQk^{-1}$. Recíprocamente, si existe $k \in K$ tal que $\Delta = kQk^{-1}$, para cada $x \in Q$ existe $y \in Q$ tal que $\delta(x)x = kyk^{-1}$. Como $[k,y] = kyk^{-1}y^{-1} \in K$, $\delta(x) \in K$ y $\delta(x)x = [k,y]y \in KQ$, se concluye que $x = y$ y luego $\delta(x) = [k,x]$.

Demostremos la tercera afirmación. Si $x \in Q$ es tal que $\delta(x)x = y \in Q$ entonces $\delta(x) = yx^{-1} \in K \cap Q = 1$. Recíprocamente, si $x \in Q$ es tal que $\delta(x) = 1$ entonces $x = \delta(x)x \in Q \cap \Delta$.

Demostremos la cuarta afirmación. Si δ es sobreyectiva, para cada $k \in K$ existe $y \in Q$ tal que $\delta(y) = k$. Luego $K \rtimes Q \subseteq \Delta Q$ pues $kx = \delta(y)x = (\delta(y)y)y^{-1}x \in \Delta Q$. Además $\Delta Q \subseteq K \rtimes Q$ pues si $\delta(x) \in K$ para todo $x \in Q$. Recíprocamente, si $k \in K$ y $x \in Q$ existen $y,z \in Q$ tales que $kx = \delta(y)yz$; en particular, por la unicidad de la escritura de $K \rtimes Q$, $k = \delta(y)$. □

Definición 12.7. Un grupo G admite una **factorización triple** si tiene subgrupos A, B y M tales que $G = MA = MB = AB$ y $A \cap M = B \cap M = 1$.

Corolario 12.8. *Supongamos que el grupo Q actúa por automorfismos en K. Sea $\delta \in \mathrm{Der}(Q,K)$ sobreyectivo. Entonces $G = K \rtimes Q$ admite una factorización triple.*

Demostración. Es consecuencia inmediata del teorema 12.6. □

exercise:ker1cocycle

Ejercicio 12.9. Sea $\delta \in \mathrm{Der}(Q,K)$. Entonces δ es inyectiva si y sólo si $\ker\delta = 1$.

Demostración. Sean $x,y \in Q$ tales que $\delta(x) = \delta(y)$. Como $\delta(x^{-1}y) = 1$ pues

$$\delta(x^{-1}y) = \delta(x^{-1})(x^{-1}\delta(y)x) = \delta(x^{-1})x^{-1}\delta(x)x = \delta(x^{-1}x) = \delta(1) = 1$$

y δ es inyectiva, $x^{-1}y = 1$. La afirmación recíproca es trivial. □

Corolario 12.10. *Si $\delta \in \mathrm{Der}(Q,K)$ es biyectivo entonces K admite un complemento Δ en $K \rtimes Q$ tal que $K \rtimes Q = K \rtimes \Delta = \Delta Q$ y $Q \cap \Delta = 1$.*

Demostración. Vimos en el teorema 12.6 que δ es sobreyectiva si y sólo si $K \rtimes Q = \Delta Q$ y que $\ker \delta = Q \cap \Delta$. □

12. Cohomología

Definición 12.1. Sea G un grupo. Un G-módulo es un grupo abeliano A con una acción por automorfismos de G.

En esta sección G es un grupo y A es un G-módulo. El grupo A será escrito aditivamente.

Definición 12.2. Sea $n \geq 0$. Una **cocadena** de grado n (o n-cocadena) de G con valores en A es una función $f\colon G \times \cdots \times G \to A$, $(s_1,\ldots,s_n) \mapsto f(s_1,\ldots,s_n)$.

Observación 12.3. El conjunto $C^n(G,A)$ de n-cocadenas de G con valores en A es un grupo abeliano.

Definición 12.4. Sea $f \in C^n(G,A)$. Se define el **coborde** de f como el elemento $df \in C^{n+1}(G,A)$ dado por

$$\begin{aligned} df(s_1,\ldots,s_{n+1}) &= s_1 \cdot f(s_2,\ldots,s_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(s_1,\ldots,s_{i-1},s_is_{i+1},s_{i+2},\ldots,s_{n+1}) + (-1)^{n+1} f(s_1,\ldots,s_n). \end{aligned}$$

Ejemplo 12.5. Veamos la función $d\colon C^0(G,A) \to C^1(G,A)$. Si $a \in C^0(G,A) = A$ entonces

$$da(s) = s \cdot a - a.$$

Luego $da = 0$ si y sólo si $s \cdot a = 0$ para todo $s \in G$.

Ejemplo 12.6. Veamos ahora la función $d\colon C^1(G,A) \to C^2(G,A)$. Si $f \in C^1(G,A)$ entonces

$$df(s,t) = s \cdot f(t) - f(st) + f(s).$$

Ejemplo 12.7. Veamos ahora la función $d\colon C^2(G,A) \to C^3(G,A)$. Si $f \in C^2(G,A)$ entonces

$$df(u,v,w) = u \cdot f(v,w) - f(uv,w) + f(u,vw) - f(u,v).$$

lemma:dd=0 **Lema 12.8.** *La composición* $C^n(G,A) \xrightarrow{d} C^{n+1}(G,A) \xrightarrow{d} C^{n+2}(G,A)$ *es cero.*

Definición 12.9. Sea f una cocadena f de grado n. Se dice que f es un **cociclo** de grado n si $df = 0$. Denotaremos por $Z^n(G,A)$ al conjunto de n-cociclos de G en A. Se dice que f es un **coborde** de grado n si existe una cocadena g de grado $(n-1)$ tal que $f = dg$. Denotaremos por $B^n(G,A)$ al conjunto de n-cobordes de G en A.

Obviamente $Z^n(G,A)$ es un grupo abeliano y $B^n(G,A) \subseteq Z^n(G,A)$.

Definición 12.10. El n-ésimo **grupo de cohomología** de G con valores en A es el grupo abeliano

$$H^n(G,A) = Z^n(G,A)/B^n(G,A).$$

Ejercicio 12.11. Demuestre que $H^0(G,A) = A^G$, donde

$$A^G = \{a \in A : s \cdot a = a \text{ para todo } s \in G\}.$$

Pues para todo $a \in A = C^0(G,A)$ se tiene que $da = 0$ si y sólo si $a \in A^G$.

Ejemplo 12.12. $f \in Z^1(G,A)$ si y sólo si $f(st) = s \cdot f(t) + f(s)$ para todo $s,t \in G$. En particular, si G actúa trivialmente en A, $Z^1(G,A) = \hom(G,A)$. Como en este caso $B^1(G,A) = 0$, se concluye que $H^1(G,A) \simeq \hom(G,A)$.

Ejemplo 12.13. $f \in Z^2(G,A)$ si y sólo si f es un **factor**, es decir:

$$u \cdot f(v,w) - f(uv,w) + f(u,vw) - f(u,v) = 0 \tag{12.1}$$ eq:2cociclo

para todo $u,v,w \in G$.

Ejercicio 12.14. Sea $f \in Z^2(G,A)$ tal que $f(1,1) = 0$. Demuestre que

$$f(1,x) = f(x,1) = 0$$

para todo $x \in G$.

Al usar la fórmula (12.1) con $(u,v,w) = (1,1,x)$ se obtiene $f(1,x) = f(1,1)$.
Con $(u,v,w) = (x,1,1)$ se obtiene $x \cdot f(1,1) = f(x,1)$.

Definición 12.15. Sean $f,g \in Z^2(G,A)$. Se dice que f y g son **cohomólogos** si existe algún coborde h tal que $f - g = dh$.

Un factor $f \in Z^2(G,A)$ se dice **normalizado** si $f(1,1) = 0$.

lemma:normalizado **Lema 12.16.** *Todo* $f \in Z^2(G,A)$ *es cohomólogo a un factor normalizado.*

Demostración. Sea γ: $G \to A$ tal que $\gamma(1) = -f(1,1)$. Sea $g = f + d\gamma$. Entonces $g \in Z^2(G,A)$, $g(1,1) = 0$ y $dg = d(f + d\gamma) = df$ pues $d^2 = 0$. □

theorem:|G|H^2=0

Teorema 12.17. *Sea G un grupo finito y sea A un G-módulo. Entonces*

$$|G|H^n(G,A) = 0.$$

Demostración. Sea $m = |G|$. Sea $f \in Z^n(G,A)$. Vamos a demostrar que mf es un coborde. Sea

$$F(s_1,\ldots,s_{n-1}) = \sum_{s\in G} f(s_1,\ldots,s_{n-1},s).$$

Como $f \in Z^n(G,A)$,

$$0 = s_1 \cdot f(s_2,\ldots,s_{n+1}) - f(s_1s_2,s_3,\ldots,s_{n+1}) + \cdots + (-1)^n f(s_1,\ldots,s_ns_{n+1}) + (-1)^{n+1} f(s_1,\ldots,s_n).$$

Al sumar estas igualdades sobre todo $s_{n+1} \in G$ obtenemos

$$0 = s_1 \cdot F(s_2,\ldots,s_n) - F(s_1s_2,\ldots,s_n) + \cdots + (-1)^n F(s_1,\ldots,s_{n-1}) + (-1)^{n+1} mf(s_1,\ldots,s_n).$$

Luego $0 = dF(s_1,\ldots,s_n) - (-1)^n mf(s_1,\ldots,s_n)$, es decir $mf = d((-1)^n F)$. □

corollary:a->|G|a

Corolario 12.18. *Sea G un grupo finito y A un G-módulo. Si $a \mapsto |G|a$ es un automorfismo de A entonces $H^n(G,A) = 0$ para todo $n \geq 1$.*

Demostración. Como la función $x \mapsto |G|x$ es un automorfismo de $C^n(G,A)$ que conmuta con d, induce un automorfismo $H^n(G,A) \to H^n(G,A)$, $x \mapsto |G|x$. Como $|G|H^n(G,A) = 0$ por el teorema 12.17, se concluye que $H^n(G,A) = 0$. □

corollary:H^n=0

Corolario 12.19. *Sea G un grupo finito y A un G-módulo. Si A es finito y de orden coprimo con $|G|$ entonces $H^n(G,A) = 0$ para todo $n \geq 1$.*

Demostración. Como $|G|H^n(G,A) = 0$ por el teorema 12.17 y $a \mapsto |G|a$ es un automorfismo de A, $H^n(G,A)$ por el corolario 12.18. □

Corolario 12.20. *Sea G un grupo finito y A un G-módulo finitamente generado. Entonces $H^n(G,A)$ es finito para todo $n \geq 1$.*

Demostración. Como $C^n(G,A)$ es finitamente generado, $H^n(G,A)$ es finitamente generado. Luego $H^n(G,A)$ es finito por ser un grupo abeliano finitamente generado y de torsión. □

12. Extensiones abelianas

Definición 12.1. Un **dato** es un par (Q,K), donde Q es un grupo y K es Q-módulo. Se dice que un grupo G **realiza** el dato (Q,K) si G es una extensión de K por Q y

para todo levantamiento $\ell\colon Q \to G$ se tiene

$$x \cdot a = \ell(x) a \ell(x)^{-1}, \quad a \in K, x \in Q.$$

Definición 12.2. Sea Q un grupo y sea K un Q-módulo. Sea $1 \to K \to G \to Q \to 1$ una extensión de K por Q que realiza el dato (K,Q) y sea $\ell\colon Q \to G$ un levantamiento tal que $\ell(1) = 1$. Un **factor** para ℓ es una función $f\colon Q \times Q \to K$ tal que

$$\ell(x)\ell(y) = f(x,y)\ell(xy) \tag{12.2}$$

eq:ell

para todo $x, y \in Q$.

Lema 12.3. *Sea Q un grupo y sea K un Q-módulo. Sea $1 \to K \to G \to Q \to 1$ una extensión de K por Q que realiza el dato (K,Q). Si f es un factor para ℓ entonces*

$$f(1,x) = f(x,1) = 1, \tag{12.3}$$

eq:f(1x)

$$f(x,y)f(xy,z) = (x \cdot f(y,z))f(x,yz) \tag{12.4}$$

eq:fcocycle

para todo $x, y, z \in Q$.

Demostración. Si hacemos $x = 1$ en (12.3) obtenemos $1 = f(1,y)$. De la misma forma se obtiene la otra igualdad. Para demostrar la igualdad (12.4) calculamos

$$(\ell(x)\ell(y))\ell(z) = (f(x,y)\ell(xy))\ell(z) = f(x,y)(\ell(xy)\ell(z)) = f(x,y)f(xy,z)\ell(xyz).$$

Por otro lado, como la extensión realiza el dato (K,Q),

$$\begin{aligned} \ell(x)(\ell(y)\ell(z)) &= \ell(x)(f(y,z)\ell(yz)) \\ &= (x \cdot f(y,z))\ell(x)\ell(yz) = (x \cdot f(y,z))f(x,yz)\ell(xyz). \end{aligned}$$

La igualdad (12.4) se obtiene al observar que el producto de G es asociativo. □

lemma:G(K,Q,f)

Lema 12.4. *Sea Q un grupo y sea K un Q-módulo. Sea $f\colon Q \times Q \to K$ una función que satisface* (12.3) *y* (12.4)*. Entonces existe una extensión $1 \to K \to G \to Q \to 1$ de K por Q que realiza el dato (K,Q) y existe un levantamiento $\ell\colon Q \to G$ cuyo factor es f.*

Demostración. Sea $G = K \times Q$ con el producto

$$(a,x)(b,y) = (a(x \cdot b)f(x,y), xy).$$

Veamos que el producto es asociativo:

$$\begin{aligned} ((a,x)(b,y))(c,z) &= (a(x \cdot b)f(x,y), xy)(c,z) \\ &= (a(x \cdot b)f(x,y)((xy) \cdot c))f(xy,z), xyz) \end{aligned}$$

Por otro lado

$$\begin{aligned}(a,x)((b,y)(c,z)) &= (a,x)(b(y\cdot c)f(y,z),yz)\\ &= (a(x\cdot(b(y\cdot c)f(y,z))f(x,yz),xyz)\\ &= (a(x\cdot b)(xy)\cdot c)(x\cdot f(y,z))f(x,yz),xyz).\end{aligned}$$

Es fácil verificar que el neutro es $(1,1)$ y el inverso de (a,x) es

$$(a,x)^{-1} = (x^{-1}\cdot(f(x,x^{-1})a)^{-1},x^{-1}).$$

Sea $\ell\colon Q\to G$ un levantamiento. Si $x\in Q$ existe $b\in K$ tal que $\ell(x)=(b,x)$. Veamos que la extensión realiza el dato (K,Q). Como $f(x,1)=1$ y K es abeliano,

$$\begin{aligned}\ell(x)(a,1)\ell(x)^{-1} &= (b,x)(a,1)(b,x)^{-1}\\ &= (b(x\cdot a)f(x,1),x)(x^{-1}\cdot(f(x,x^{-1})b)^{-1},x^{-1})\\ &= (b(x\cdot a)b^{-1}f(x,x^{-1})^{-1}f(x,x^{-1}),1)\\ &= (x\cdot a,1).\end{aligned}$$

Por último, para ver que existe un levantamiento con factor f basta considerar $\ell\colon Q\to G$, $\ell(x)=(1,x)$ pues

$$\ell(x)\ell(y)(\ell(xy)^{-1} = (1,x)(1,y)(1,xy)^{-1} = (f(x,y),1).$$

□

Si Q es un grupo, K es un Q-módulo y $f\colon Q\times Q\to K$ es una función que satisface (12.3) y (12.4). El grupo G del lema 12.4 será denotado por $G(K,Q,f)$.

lemma:existe_f

Lema 12.5. *Sea Q un grupo y sea K un Q-módulo. Sea $1\to K\to G\to Q\to 1$ una extensión de K por Q que realiza el dato (K,Q). Entonces existe un factor $f\colon Q\times Q\to K$ tal que $G\simeq G(K,Q,f)$.*

Demostración. Sea $\ell\colon Q\to G$ un levantamiento y sea f su factor. Como G es unión disjunta de coclases

$$G = \bigcup_{x\in Q} K\ell(x),$$

para cada $g\in G$ existen únicos $a\in K$ y $x\in Q$ tales que $g=a\ell(x)$. Queda entonces bien definida una función biyectiva $\phi\colon G\to G(K,Q,f)$, $a\ell(x)\mapsto(a,x)$. Veamos que ϕ es un morfismo de grupos:

$$\begin{aligned}\phi(a\ell(x)b\ell(y)) &= \phi(a\ell(x)b\ell(x)^{-1}\ell(x)\ell(y))\\ &= \phi(a\ell(x)b\ell(x)^{-1}f(x,y)\ell(xy))\\ &= \phi(a(x\cdot b)f(x,y)\ell(xy))\\ &= (a(x\cdot b)f(x,y),xy)\\ &= \phi(a\ell(x))\phi(b\ell(y)).\end{aligned}$$

□

lemma:coborde

Lema 12.6. *Sean Q un grupo, K un Q-módulo y $1 \to K \to G \to Q \to 1$ una extensión de K por Q que realiza el dato (K,Q). Para $j \in \{1,2\}$ sea $\ell_j \colon Q \to G$ un levantamiento con factor f_j tal que $\ell_j(1) = 1$. Entonces existe $\gamma \colon Q \to K$ tal que $\gamma(1) = 1$ y*

$$f_2(x,y) = \gamma(x)(x \cdot \gamma(y)) f_1(x,y) \gamma(xy)^{-1}$$

para todo $x, y \in Q$.

Demostración. Como $\ell_1(x)$ y $\ell_2(x)$ están en la misma coclase de K, existe $\gamma(x) \in K$ tal que $\ell_2(x) = \gamma(x)\ell_1(x)$. Como $\ell_1(1) = \ell_2(1) = 1$, $\gamma(1) = 1$. Además

$$\begin{aligned} f_2(x,y)\ell_2(xy) &= \ell_2(x)\ell_2(y) = \gamma(x)\ell_1(x)\gamma(y)\ell_1(y) \\ &= \gamma(x)\ell_1(x)\gamma(y)\ell_1(x)^{-1}\ell_1(x)\ell_1(y) \\ &= \gamma(x)(x \cdot \gamma(y)) f_1(x,y)\ell_1(xy) = \gamma(x)(x \cdot \gamma(y)) f_1(x,y)\gamma(xy)^{-1}\ell_2(xy), \end{aligned}$$

que implica lo que se quería demostrar. □

Definición 12.7. Sean Q un grupo y K un Q-módulo. Una función $g \colon Q \times Q \to K$ se dice un **coborde** si existe una función $\gamma \colon Q \to K$ con $\gamma(1) = 1$ tal que

$$g(x,y) = (x \cdot \gamma(y))\gamma(xy)^{-1}\gamma(x)$$

para todo $x, y \in Q$.

lemma:equivalencia

Lema 12.8. *Sean Q un grupo y K un Q-módulo. Dos extensiones G_1 y G_2 de K por Q que realizan el dato (K,Q) son equivalentes si y sólo existe un factor f_1 de G_1 y un factor f_2 de G_2 tales que $f_1 f_2^{-1}$ es un coborde.*

Demostración. Para cada $j \in \{1,2\}$ sea $\ell_j \colon Q \to G$ un levantamiento con factor f_j y tal que $\ell_j(1) = 1$. Como G es unión disjunta de coclases

$$G = \bigcup_{x \in Q} K\ell_1(x)$$

todo $g_1 \in G_1$ se escribe unívocamente como $g_1 = a\ell_1(x)$ para $a \in K$ y $x \in Q$. Sea $\phi \colon G_1 \to G_2$, $a\ell_1(x) \mapsto a\gamma(x)\ell_2(x)$. Es evidente que ϕ hace conmutar al diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & G_1 & \xrightarrow{p_1} & Q & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \phi} & & \| & & \\ 0 & \longrightarrow & K & \longrightarrow & G_2 & \xrightarrow{p_2} & Q & \longrightarrow & 0 \end{array} \tag{12.5}$$

eq:diagrama

Veamos que ϕ es morfismo. Por un lado tenemos

$$\phi(a\ell_1(x)b\ell_1(y)) = \phi(a(x \cdot b) f_1(x,y)\ell_1(xy)) = a(x \cdot b) f_1(x,y)\gamma(xy)\ell_2(xy).$$

Por otro lado, se tiene

$$\begin{aligned}\phi(a\ell_1(x))\phi(b\ell_1(y)) &= a\gamma(x)\ell_2(x)b\gamma(y)\ell_2(y)\\ &= a\gamma(x)(x\cdot b)\ell_2(x)\gamma(y)\ell_2(y)\\ &= a\gamma(x)(x\cdot b)(x\cdot\gamma(y))\ell_2(x)\ell_2(y)\\ &= a\gamma(x)(x\cdot b)(x\cdot\gamma(y))f_2(x,y)\ell_2(xy)\\ &= a(x\cdot b)\gamma(x)(x\cdot\gamma(y))f_2(x,y)\ell_2(xy)\end{aligned}$$

pues K es abeliano. Por el lema 12.6, existe una función $\gamma\colon Q\to K$ con $\gamma(1)=1$ y tal que $f_1(x,y)=\gamma(x)(x\cdot\gamma(y))f_2(x,y)\gamma(xy)^{-1}$ para todo $x,y\in Q$. Luego ϕ es morfismo de grupos.

Recíprocamente, supongamos que existe γ tal que el diagrama (12.5) conmuta. En particular, $\gamma(a)=a$ para todo $a\in K$ y la función $\phi\ell_1\colon Q\to G_2$ es un levantamiento pues $x=p_1\ell_1(x)=p_2\phi\ell_1(x)$ para todo $x\in Q$. Como

$$\phi\ell_1(x)\phi\ell_1(y)=\phi f_1(x,y)\phi\ell_1(xy)=f_1(x,y)\phi\ell_1(xy)$$

para todo $x,y\in Q$, f_1 es también un factor para la extensión G_2. Si f_2 es un factor para G_2, entonces $f_1f_2^{-1}$ es un coborde por el lemma 12.6. □

Ejemplo 12.9. Sea p un número primo impar. Sean $K=\langle a\rangle\simeq C_p$, $G=\langle g\rangle\simeq C_{p^2}$ y $Q=\langle gK\rangle=G/K\simeq C_p$. Veamos que las extensiones

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{\iota_1} & G_1 & \xrightarrow{p_1} & Q & \longrightarrow & 0\\ & & \| & & \downarrow\phi & & \| & & \\ 0 & \longrightarrow & K & \xrightarrow{\iota_2} & G_2 & \xrightarrow{p_2} & Q & \longrightarrow & 0 \end{array}$$

donde $\iota_1(a)=g^p$, $\iota_2(a)=g^{2p}$ y $p_1(g)=p_2(g)=gK$, no son equivalentes. Si existe ϕ entonces $\phi(g^p)=\phi\iota_1(a)=\iota_2(a)=g^{2p}$. Esto implica que $\phi(g)=g^2$ y luego $g\in K$ pues $gK=p_1(g)=p_2\phi(g)=g^2K$, una contradicción.

Sea Q un grupo y sea K un Q-módulo. Sea $E(Q,K)$ el conjunto de clases de equivalencia de extensiones $1\to K\to G\to Q\to 1$ que realizan el dato (Q,K).

er:extensiones_abelianas

Teorema 12.10 (Schreier). *Sean Q un grupo y K un Q-módulo. Existe una correspondencia biyectiva entre $H^2(Q,K)$ y el conjunto $E(Q,K)$ de clases de equivalencia de extensiones que realizan el dato (Q,K). Bajo esta correspondencia, el factor nulo se corresponde con la clase de equivalencia de extensiones que se parten.*

Demostración. Sea $[G]$ la clase de equivalencia de $1\to K\to G\to Q\to 1$. Sea $\phi\colon H^2(Q,K)\to E(Q,K)$ dado por $f+B^2(Q,K)\mapsto[G(K,Q,f)]$, donde $[G(K,Q,f)]$ es la clase de una extensión que realiza el dato (Q,K) (existe gracias al lemma 12.4). El lemma 12.8 implica que ϕ está bien definida y es una función inyectiva. La función ϕ es sobreyectiva pues el lemma 12.5 implica que si $[G]\in E(Q,K)$ entonces $[G]=[G(K,Q,f)]=\phi(f+B^2(Q,K))$ para algún f. □

Observación 12.11. Como aplicación del teorema de Schreier podemos dar una demostración breve de la existencia del complemento en el teorema de Schur–Zassenhaus 13.3. Para $Q = G/N$ consideramos la extensión $1 \to N \to G \to Q \to 1$. Como $|N|$ y $|Q|$ son coprimos, $H^2(Q,N) = 0$ por el corolario 12.19. Por el teorema de Schreier 12.10, $E(Q,N)$ contiene un único elemento y luego la extensión $1 \to N \to G \to Q \to 1$ se parte.

Capítulo 13
El teorema de Schur–Zassenhaus

13. El teorema de Schur–Zassenhaus

lemma:1cocycle

Lema 13.1. *Si $\varphi\colon G \to N$ es un 1-cociclo con núcleo K entonces $\varphi(x) = \varphi(y)$ si y sólo si $xK = yK$. En particular, $(G:K) = |\varphi(G)|$.*

Demostración. Si $\varphi(x) = \varphi(y)$ entonces, como

$$\varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1}\cdot\varphi(y)) = \varphi(x^{-1})(x^{-1}\cdot\varphi(x)) = \varphi(x^{-1}x) = \varphi(1) = 1,$$

tenemos $xK = yK$. Recíprocamente, si $x^{-1}y \in K$, entonces, como

$$1 = \varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1}\cdot\varphi(y)),$$

tenemos que $\varphi(y) = x\cdot\varphi(x^{-1})^{-1}$. De acá obtenemos $\varphi(x) = \varphi(y)$.

La segunda afirmación resulta ahora evidente pues φ es constante en cada coclase de K y toma $(G:K)$ valores distintos. □

lemma:d

Lema 13.2. *Sea G un grupo finito, N un subgrupo normal abeliano de G y S,T,U transversales de N en G. Sea*

$$d(S,T) = \prod st^{-1} \in N,$$

donde el producto se hace sobre todos los $s \in S$ y $t \in T$ tales que $sN = tN$. Valen las siguientes afirmaciones:

1. $d(S,T)d(T,U) = d(S,U)$.
2. $d(gS,gT) = gd(S,T)g^{-1}$ *para todo* $g \in G$.
3. $d(nS,S) = n^{(G:N)}$ *para todo* $n \in N$.

Demostración. Si $s \in S$, $t \in T$, $u \in U$ con $sN = tN = uN$ entonces, como N es abeliano y $(st^{-1})(tu^{-1}) = su^{-1}$,

$$d(S,T)d(T,U) = \prod(st^{-1})(tu^{-1}) = \prod su^{-1} = d(S,U).$$

Como $sN = tN$ si y sólo si $gsN = gtN$ para todo $g \in G$,

$$g\left(\prod st^{-1}\right)g^{-1} = \prod gst^{-1}g^{-1} = \prod (gs)(gt)^{-1} = d(gS, gT).$$

Por último, como N es normal, $nsN = sN$ para todo $n \in N$. Luego

$$d(nS, S) = \prod (ns)s^{-1} = n^{(G:N)}.$$

□

SchurZassenhaus:abeliano

Teorema 13.3 (Schur–Zassenhaus). *Sea G un grupo finito y sea N un subgrupo normal abeliano de G. Si $|N|$ y $(G:N)$ son coprimos, N se complementa en G. Si N se complementa en G, todos los complementos son conjugados.*

Demostración. Sea T un transversal de N en G. Sea $\theta\colon G \to N$, $\theta(g) = d(gT, T)$. Como N es abeliano, el lema 13.2 implica que θ es un 1-cociclo, donde G actúa en N por conjugación:

$$\begin{aligned}\theta(xy) &= d(xyT, T) = d(xyT, xT)d(xT, T)\\ &= (xd(yT, T)x^{-1})d(xT, T) = (x \cdot \theta(y))\theta(x).\end{aligned}$$

Afirmación. $\theta|_N\colon N \to N$ es sobreyectiva.

Si $n \in N$, el lema 13.2 implica que $\theta(n) = d(nT, T) = n^{(G:N)}$. Pero como los números $|N|$ y $(G:N)$ son coprimos, existen $r, s \in \mathbb{Z}$ tales que $r|N| + s(G:N) = 1$. Luego

$$n = n^{r|N|+s(G:N)} = (n^s)^{(G:N)} = \theta(n^s).$$

Sea $H = \ker\theta$. Vamos a demostrar que H es un complemento para N. Por el ejercicio 12.3, H es un subgrupo de G. Como

$$|N| = |\theta(G)| = (G:H)$$

por el lema 13.1, se concluye que $|H|$ divide a $(G:N)$. Como $N \cap H$ es un subgrupo de N y de H, entonces $N \cap H = 1$ pues $|N|$ y $(G:N) = |H|$ son coprimos. Como $|NH| = |N||H| = |G|$, se concluye que $G = NH$ y entonces H es un complemento para N.

Veamos ahora que dos complementos para N son conjugados. Sea K un complemento de N en G. Como $NK = G$ y $N \cap K = 1$, K es un transversal para N. Sea $m = d(T, K) \in N$. Como $\theta|_N$ es sobreyectiva, existe $n \in N$ tal que $\theta(n) = m$. Por el lema 13.2, para todo $k \in K$ se tiene

$$kmk^{-1} = kd(T, K)k^{-1} = d(kT, kK) = d(kT, K) = d(kT, T)d(T, K) = \theta(k)m,$$

y luego $\theta(k) \in N$. Entonces, como N es abeliano, $\theta(n^{-1}) = m^{-1}$ y luego

$$\begin{aligned}\theta(nkn^{-1}) &= \theta(n)n\theta(kn^{-1})n^{-1} = m\theta(kn^{-1})\\ &= m\theta(k)k\theta(n^{-1})k^{-1} = m\theta(k)km^{-1}k^{-1} = 1.\end{aligned}$$

Queda demostrado entonces que $nKn^{-1} \subseteq H = \ker\theta$. Como $|K| = (G:N) = |H|$, se concluye que $nKn^{-1} = H$. □

En el siguiente teorema vemos que no es necesario suponer que el subgrupo normal N es abeliano.

theorem:SchurZassenhaus

Teorema 13.4 (Schur–Zassenhaus). *Sea G un grupo finito y sea N un subgrupo normal de G. Si $|N|$ y $(G:N)$ son coprimos entonces N se complementa en G.*

Demostración. Procederemos por inducción en $|G|$. Si existe un subgrupo propio K de G tal que $NK = G$ entonces, como $(K : K\cap N) = (G:N)$ es coprimo con $|N|$, es también coprimo con $|K\cap N|$. Como además $K\cap N$ es normal en K, por hipótesis inductiva, $K\cap N$ se complementa en K, y luego existe un subgrupo H de K tal que $|H| = (K : K\cap N) = (G:N)$.

Supongamos entonces que no existe un subgrupo propio K de G tal que $NK = G$. Podemos suponer que $N \neq 1$ (de lo contrario, basta tomar G como complemento de N en G). Como N está contenido en todo subgrupo maximal de G (pues si existe un maximal $M \subsetneq G$ tal que $N \not\subseteq M$ entonces $NM = G$), se tiene que $N \subseteq \Phi(G)$. Por el teorema de Frattini 10.11, $\Phi(G)$ es nilpotente y luego N es nilpotente; en particular, $Z(N) \neq 1$. Sea $\pi\colon G \to G/Z(N)$ el morfismo canónico. Como N es normal en G y $Z(N)$ es característico en N, $Z(N)$ es normal en G. Además

$$(\pi(G) : \pi(N)) = \frac{|\pi(G)|}{|\pi(N)|} = \frac{|G/Z(N)|}{|N/N\cap Z(N)|} = (G:N)$$

es coprimo con $|N|$, y entonces es también coprimo con $|\pi(N)|$. Por hipótesis inductiva, $\pi(N)$ admite un complemento en $G/Z(N)$, digamos $\pi(K)$ para algún subgrupo K de G. Luego $G = NK$ pues $\pi(G) = \pi(N)\pi(K) = \pi(NK)$. Como entonces $K = G$ (pues sabíamos que no existe K tal que $G = NK$), $\pi(N)$ es abeliano pues

$$\pi(Z(N)) = \pi(N)\cap\pi(K) = \pi(N)\cap\pi(G) = \pi(N).$$

Luego $N \subseteq Z(N)$ es abeliano y entonces, por el teorema 13.3, el subgrupo N admite un complemento. □

urZassenhaus:conjugacion

Teorema 13.5. *Sea G un grupo finito y sea N un subgrupo normal de G tal que $|N|$ y $(G:N)$ son coprimos. Si N es resoluble o G/N es resoluble, todos los complementos de N en G son conjugados.*

Demostración. Sea G un contraejemplo minimal, es decir: existen complementos K_1 y K_2 a N en G tales que K_1 y K_2 no son conjugados, y $|G|$ toma el menor valor posible.

Afirmación. Todo subgrupo U de G satisface las hipótesis del teorema con respecto al subgrupo normal $U\cap N$.

Como N es normal en G, $U\cap N$ es normal en U. Además $|U\cap N|$ y $(U : U\cap N)$ son coprimos pues $|U\cap N|$ divide a $|N|$ y $(U : U\cap N) = (UN : N)$ divide a $(G:N)$. Si G/N es resoluble, entonces $U/U\cap N$ es resoluble pues $U/U\cap N$ es isomorfo a un subgrupo de G/N. Si N es resoluble, $U\cap N$ es resoluble.

Afirmación. Si existe un subgrupo normal L de G tal que $\pi(N)$ es normal en $\pi(G)$, donde $\pi\colon G \to G/L$ es el morfismo canónico, entonces $\pi(G)$ satisface las hipótesis del teorema con respecto a $\pi(N)$. En este caso, si H es un complemento para N en G, $\pi(H)$ es un complemento para $\pi(N)$ en $\pi(G)$.

Si N es resoluble, $\pi(N)$ es resoluble. Si G/N es resoluble, $\pi(G)/\pi(N) \simeq G/NL$ es resoluble. Además $(\pi(G) : \pi(N)) = \frac{|G/L|}{|N/N\cap L|}$ divide a $(G : N)$.

Si H es un complemento para N en G, $|\pi(H)|$ y $|\pi(N)|$ son coprimos. Luego $\pi(H)$ es un complemento para $\pi(N)$ pues $\pi(G) = \pi(N)\pi(H) = \pi(NH)$ y la intersección $\pi(N) \cap \pi(H)$ es trivial.

Afirmación. N es minimal-normal en G.

Sea $M \neq 1$ normal tal que $M \subseteq N$. Sea $\pi\colon G \to G/M$ el morfismo canónico. Vimos que $\pi(G)$ satisface las hipótesis del teorema con respecto al subgrupo normal $\pi(N)$. Por la minimalidad de G, existe $x \in G$ tal que $\pi(xK_1x^{-1}) = \pi(K_2)$. Sabemos que el subgrupo $U = MK_2$ también satisface las hipótesis del teorema con respecto al subgrupo normal $U \cap N$. Como además $xK_1x^{-1} \cup K_2 \subseteq U$, podemos concluir que xK_1x^{-1} y K_2 complementan a $U \cap N$ en U. Luego $MK_2 = G$ pues xK_1x^{-1} y K_2 no son conjugados y G es minimal. Esto implica que $M = N$ pues

$$\frac{|K_2|}{|M \cap K_2|} = |MK_2| = |G| = |NK_2| = |N||K_2|.$$

Afirmación. N no es resoluble y G/N es resoluble.

En caso contrario, por el lema 4.23 tendríamos que N es abeliano ya que N es minimal-normal, y luego tendríamos una contradicción al utilizar el teorema 13.3 que implicaría que K_1 y K_2 son conjugados.

Sea $p\colon G \to G/N$ el morfismo canónico y sea S tal que $p(S)$ minimal-normal en $p(G) = G/N$. Por el lema 4.23, $p(S)$ un p-grupo para algún primo p. Como $G = NK_1 = NK_2$ y $N \subseteq S$, el lema de Dedekind 10.6 implica que

$$S = N(S \cap K_1) = N(S \cap K_2).$$

Luego $S \cap K_1$ y $S \cap K_2$ complementan a N en S. En particular $S \cap K_1$ y $S \cap K_2$ son p-subgrupos de Sylow de S pues

$$|S \cap K_1| = |S : N| = |S \cap K_2|,$$

y p no divide a $|N|$. Por el teorema de Sylow, existe $s \in S$ tal que

$$S \cap sK_1s^{-1} = S \cap K_2.$$

En particular $S \neq G$ gracias a la minimalidad de G. Sea

$$L = S \cap K_2 = S \cap sK_1s^{-1} \neq 1.$$

Como S es normal en G, $sK_1s^{-1} \cup K_2 \subseteq N_G(L)$ (pues L es normal en sK_1s^{-1} y en K_2). Los subgrupos $sK_1s^{-1} \subseteq N_G(L)$ y $K_2 \subseteq N_G(L)$ complementan a $N \cap N_G(L)$ en $N_G(L)$, y luego $N_G(L) = G$ por la minimalidad de G (si $N_G(L) \neq G$ entonces sK_1s^{-1} y K_2 serían conjugados en G por serlo en $N_G(L)$). Luego L es normal en G.

Sea $\pi_L \colon G \to G/L$ el morfismo canónico. Como $\pi_L(K_1)$ y $\pi_L(K_2)$ complementan a $\pi_L(N)$ en $\pi_L(G)$, la minimalidad de $|G|$ implica que existe $g \in G$ tal que $\pi_L(gK_1g^{-1}) = \pi_L(K_2)$, es decir: existe $g \in G$ tal que $(gK_1g^{-1})L = K_2L$. Luego $gK_1g^{-1} \cup K_2 \subseteq \langle K_2, L\rangle = K_2$ pues $L \subseteq K_2$. Tenemos entonces que $gK_1g^{-1} = K_2$, una contradicción por la minimalidad de G.

□

Observación 13.6. Por el teorema de Feit–Thompson, no es necesario suponer que N o G/N es resoluble en el teorema 13.5: como todo grupo de order impar es resoluble y $|N|$ es coprimo con $(G : N)$, alguno de estos grupos tiene orden impar.

Veamos una aplicación a grupos resolubles finitos.

theorem:solvable_maximal

Teorema 13.7. *Sea G un grupo finito resoluble y sea p un primo que divide al orden de G. Entonces existe un maximal M de indice una potencia de p.*

Demostración. Procederemos por inducción en $|G|$. Si G es un p-grupo, el resultado es verdadero. Veamos el caso general. Sea p un primo que divide al orden de G, sea N un subgrupo minimal-normal y sea $\pi \colon G \to G/N$ el morfismo canónico. Como G es resoluble, Por el lema 4.23, N es un q-grupo para algún primo q. Como G/N es resoluble, si p divide a $(G : N)$ entonces, por hipótesis inductiva, G/N tiene un subgrupo maximal M_1 de índice una potencia de p. Por el teorema de la correspondencia, $M = \pi^{-1}(M_1)$ es un subgrupo maximal de G de índice una potencia de p. Si p no divide a $(G : N)$, p divide a $|N|$ y luego $N \in \mathrm{Syl}_p(G)$. Como N es normal en G y $|N|$ es coprimo con $|G/N|$, el teorema de Schur–Zassenhaus 13.4 implica que existe un complemento K a N en G, es decir $G = NK$ y $N \cap K = 1$. Sea M un subgrupo maximal que contiene a K. Entonces $(G : M)$ es una potencia de p. □

Veamos ahora una aplicación a grupos superresolubles finitos.

Definición 13.8. Un grupo finito G se dice **lagrangiano** si para cada d que divide a $|G|$ existe un subgrupo de G de orden d.

Ejemplo 13.9. El grupo $\mathbb{A}_4$ no es lagrangiano pues no tiene subgrupos de orden seis.

Teorema 13.10. *Todo grupo finito superresoluble es lagrangiano.*

Demostración. Sea p un primo que divide al orden de G. Como los subgrupos de un grupo superresoluble son superresolubles, basta ver que existe un subgrupo índice p. Como G es resoluble, existe un subgrupo maximal M de índice p^α por el teorema 13.7. Como los maximales de superresolubles tienen índice primo (teorema 9.12), se concluye que $\alpha = 1$. □

13. Aplicación: teoría de Hall

Hall

Sea G un grupo finito y sea π un conjunto de números primos. Diremos que G es un π-grupo si todo primo que divide a $|G|$ pertenece a π. Obviamente un π-subgrupo de G es un subgrupo de G que además es un π-grupo. Un π-número es un entero tal que sus divisores primos están en π. El complemento de π en el conjunto de los números primos será denotado por π'. Luego un π'-número será un entero no divisible por los primos de π.

Definición 13.1. Sea π un conjunto de números primos. Un subgrupo H de G se dice un **π-subgrupo de Hall** si H es π-subgrupo de G y el índice $(G:H)$ es un π'-número.

theorem:HallE

Teorema 13.2 (Hall). *Sea π un conjunto de primos y sea G un grupo finito resoluble. Entonces G tiene un π-subgrupo de Hall.*

Demostración. Supongamos que G tiene orden $nm > 1$ con $(n:m) = 1$. Demostraremos por inducción en $|G|$ que existe un subgrupo de orden m. Sea K un subgrupo de G minimal-normal. Sea $\pi\colon G \to G/K$ el morfismo canónico. Como G es resoluble, K es un p-grupo por el lema 4.23.

Hay dos casos a considerar. Supongamos primero que p divide a m. Como $|G/K| < |G|$, por hipótesis inductiva y por la correspondencia, existe un subgrupo J de G que contiene a K tal que $\pi(J)$ es un subgrupo de $\pi(G) = G/K$ de orden $m/|K|$. Entonces J tiene orden m pues

$$m/|K| = |\pi(J)| = \frac{|J|}{|K \cap J|} = (J:K).$$

Supongamos ahora que p no divide a m. Por hipótesis inductiva y por la correspondencia, existe un subgrupo H de G que contiene a K tal que $\pi(H)$ es un subgrupo de G/K de orden m. Como $|H| = m|K|$, K es normal en H y $|K|$ es coprimo con $|H:K|$, el teorema de Schur–Zassenhaus 13.4 implica que existe un complemento J de K en H. Luego J es un subgrupo de G de orden $|J| = m$. □

Ejemplo 13.3. El grupo $\mathbb{A}_5$ contiene un un $\{2,3\}$-subgrupo de Hall isomorfo a $\mathbb{A}_4$.

Ejemplo 13.4. El grupo simple $\mathbf{PSL}_3(2)$ de orden 168 no contiene $\{2,7\}$-subgrupos de Hall.

Observación 13.5. El teorema 13.2 dice que para todo conjunto de primos π todo grupo finito contiene π-subgrupos de Hall.

theorem:HallC

Teorema 13.6 (Hall). *Sea G un grupo finito resoluble y sea π un conjunto de primos. Todos los π-subgrupos de Hall de G son conjugados.*

Demostración. Podemos suponer que $G \neq 1$. Procederemos por inducción en $|G|$. Sean H y K dos π-subgrupos de Hall de G. Sea M un subgrupo de G minimal-normal

y sea $\pi\colon G \to G/M$ el morfismo canónico. Como G es resoluble, el lema 4.23 implica que M es un p-grupo para algún primo p. Como $\pi(H)$ y $\pi(K)$ son π-subgrupos de Hall de G/M, los subgrupos $\pi(H)$ y $\pi(K)$ con conjugados en G/M. Luego existe $g \in G$ tal que $gHMg^{-1} = KM$.

Hay dos casos a considerar. Supongamos primero que $p \in \pi$. Como $|HM|$ y $|KM|$ son π-números y $|H| = |K|$ es el mayor π-número que divide al orden de G, se concluye que $H = HM$ y $K = KM$. En particular, $gHg^{-1} = K$.

Supongamos ahora que $p \notin \pi$. Es evidente que K complementa a M en KM pues $K \cap M = 1$. Veamos que gHg^{-1} complementa a M en KM: como M es normal en G,

$$(gHg^{-1})M = gHMg^{-1} = KM,$$

y $gHg^{-1} \cap M = 1$ ya que $p \notin \pi$. Estos complementos tienen que ser conjugados por el teorema de Schur–Zassenhaus 13.5. □

Corolario 13.7. *Sea G un grupo finito y sea N un subgrupo normal de G de orden n. Supongamos que N o G/N es resoluble. Si $|G : N| = m$ es coprimo con n y m_1 divide a m, todo subgrupo de G de orden m_1 está contenido en algún subgrupo de orden m.*

Demostración. Sea H un complemento para N en G. Entonces $|H| = m$. Sea H_1 subgrupo de G tal que $|H_1| = m_1$. Como n y m son coprimos, $m_1 = |H_1| = |H \cap NH_1|$ pues

$$\frac{|H||N||H_1|}{|H \cap NH_1|} = \frac{|H||NH_1|}{|H \cap NH_1|} = |H(NH_1)| = |G| = |NH| = |N||H|.$$

Como H_1 y $H \cap NH_1$ son complementos para N en NH_1, ambos de orden coprimo con n, existe $g \in G$ tal que $H_1 = g(H \cap NH_1)g^{-1}$. Luego $H_1 \subseteq gHg^{-1}$ y $|gHg^{-1}| = m$. □

13. Sistemas de Sylow

Dado un grupo finito G escribimos $\pi(G) = \{p_1, \ldots, p_k\}$ para denotar el conjunto de divisores primos de $|G|$.

Definición 13.1. Sea G un grupo finito y sea $\pi(G) = \{p_1, \ldots, p_k\}$. Para cada $j \in \{1, \ldots, k\}$ sea Q_j un p_j'-subgrupo de Hall de G. El conjunto $\{Q_1, \ldots, Q_k\}$ se denomina un **sistema de Sylow** de G.

La teoría de Hall demuestra el siguiente teorema:

Teorema 13.2. *Sea G un grupo finito. Entonces G es resoluble si y sólo si G admite un sistema de Sylow.*

Demostración. Sea $\pi(G) = \{p_1, \ldots, p_k\}$. Si G es resoluble, entonces por el teorema de Hall 13.2 aplicado al conjunto $\pi(G) \setminus \{p_j\}$, para cada $j \in \{1, \ldots, k\}$ existe un p_j'-subgrupo de Hall H_j. Luego $\{H_1, \ldots, H_k\}$ es un sistema de Sylow de G. La recíproca es consecuencia directa del teorema de Hall 5.2. □

Recordemos que dos subgrupos A y B se dicen **permutables** si $AB = BA$.

Ejemplo 13.3. Si $A \subseteq N_G(B)$ entonces A y B son permutables.

Ejemplo 13.4. Sean $G = \mathbb{S}_4$, $A = \mathbb{S}_3$ y $B = \langle(1234)\rangle$. Entonces $AB = BA = G$ pero $A \not\subseteq N_G(B)$ y $B \not\subseteq N_G(A)$.

Ejercicio 13.5. Sean $A_1, \ldots, A_n$ subgrupos permutables dos a dos. Demuestre que $A_1 \cdots A_n$ es un subgrupo de G.

El caso $n = 2$ es el ejercicio 1.21. Si por hipótesis inductiva $A_1 \cdots A_{n-1}$ es subgrupo, es entonces permutable con A_n pues

$$(A_1 \cdots A_{n-1})A_n = (A_1 \cdots A_{n-2})A_nA_{n-1} = \cdots = A_n(A_1 \cdots A_{n-1}).$$

lemma:indices_coprimos

Lema 13.6. *Sean H y K dos subgrupos de G de índices finitos y coprimos. Entonces $(G : H \cap K) = (G : H)(G : K)$.*

Demostración. La función $G/H \cap K \to G/H \times G/K$, $x(H \cap K) \mapsto (xH, xK)$, está bien definida y es inyectiva; en particular $(G : H \cap K) \leq (G : H)(G : K)$. Como $(G : H \cap K) = (G : H)(H : H \cap K) = (G : K)(K : H \cap K)$ y los índices $(G : H)$ y $(G : K)$ son coprimos, $(G : H)(G : K)$ divide a $(G : H \cap K)$. Luego

$$(G : H \cap K) = (G : H)(G : K).$$

□

lemma:system=>basis

Lema 13.7. *Sea $\{Q_1, \ldots, Q_k\}$ un sistema de Sylow de un grupo finito resoluble G. Entonces $P_i = \cap_{j \neq i} Q_j$ es un p_i-subgrupo de Sylow y los P_j son permutables dos a dos.*

Demostración. Sea π un conjunto de primos. Supongamos que $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Para cada j, $(G : Q_j) = p_j^{\alpha_j}$. Sea $Q = \cap_{p_i \notin \pi} Q_i$. Entonces Q es un π-subgrupo de Hall pues, por el lema 13.6, $(G : Q) = \prod_{p_i \notin \pi} p_i^{\alpha_i}$. En particular, si $\pi = \{p_i, p_j\}$ con $i \neq j$, el subgrupo $K = \cap_{k \notin \{i,j\}} Q_k$ es un π-subgrupo de Hall de orden $p_i^{\alpha_i} p_j^{\alpha_j}$. Como K contiene a $P_i \cup P_j$ y $|P_iP_j| = p_i^{\alpha_i} p_j^{\alpha_j}$, se concluye que $P_iP_j = P_jP_i = K$. □

Definición 13.8. Sea G un grupo finito. Una **base de Sylow** para G es un conjunto $\{P_1, \ldots, P_k\}$ de subgrupos de Sylow de G, uno por cada primo p_j que divide a $|G|$, donde $P_iP_j = P_jP_i$ para todo $i \neq j$.

oposition:sistemas=bases

Proposición 13.9. *Sea G un grupo finito resoluble. Existe una biyección entre el conjunto de sistemas de Sylow para G y el conjunto de bases de Sylow para G.*

Demostración. Vimos en el lema 13.7 que todo sistema de Sylow $\{Q_1,\dots,Q_k\}$ nos da una base de Sylow $\{P_1,\dots,P_k\}$ para G, donde $P_i = \cap_{j\neq i} Q_j$. Recíprocamente, si $\{P_1,\dots,P_k\}$ es una base de Sylow, sea $Q_i = \prod_{j\neq i} P_j$. Como los P_j son permutables dos a dos, Q_i es un subgrupo de orden p_i'. Luego $\{Q_1,\dots,Q_k\}$ es un sistema de Sylow para G. Para completar la demostración queda como ejercicio verificar que

$$\bigcap_{i\neq k}\prod_{j\neq i} P_j = P_j, \quad \prod_{k\neq i}\bigcap_{j\neq k} Q_j = Q_i.$$

□

Dos sistemas de Sylow $\{Q_1,\dots,Q_k\}$ y $\{Q_1',\dots,Q_k'\}$ se dicen **conjugados** si existen $x\in G$ y $\sigma\in\mathbb{S}_k$ tales que $xQ_jx^{-1} = Q'_{\sigma(j)}$ para todo $j\in\{1,\dots,k\}$.

theorem:sistemas_conj

Teorema 13.10. *En un grupo finito y resoluble G todos los sistemas de Sylow son conjugados.*

Demostración. Sea $\mathscr{S}_i$ el conjunto de p_i'-subgrupos de Hall. Como para todo conjunto de primos π, los π-subgrupos de Hall son conjugados, el grupo G actúa transitivamente en $\mathscr{S}_i$. En particular, $|\mathscr{S}_i| = (G : N_G(Q_i))$ para todo $Q_i\in\mathscr{S}_i$. Como

$$(G : N_G(Q_i))(N_G(Q) : Q_i) = (G : Q_i)$$

es una potencia de p_i, se concluye que $|\mathscr{S}_i|$ es una potencia del primo p_i.

El grupo G actúa por conjugación en $\mathscr{S} = \mathscr{S}_1\times\cdots\times\mathscr{S}_k$. Como el estabilizador de $(Q_1,\dots,Q_k)$ es $N = \bigcap_{i=1}^k N_G(Q_i)$, y además $(G:N) = \prod_{i=1}^k |\mathscr{S}_i| = |\mathscr{S}|$, la acción de G en $\mathscr{S}$ es transitiva y luego todos los sistema de Sylow son conjugados. □

Dos bases de Sylow $\{P_1,\dots,P_k\}$ y $\{P_1',\dots,P_k'\}$ se dicen **conjugadas** si existen $x\in G$ y $\sigma\in\mathbb{S}_k$ tales que $xP_jx^{-1} = P'_{\sigma(j)}$ para todo $j\in\{1,\dots,k\}$.

Corolario 13.11. *En un grupo finito y resoluble G todos las bases de Sylow son conjugadas.*

Demostración. Es consecuencia del teorema 13.10 y de la biyección de la proposición 13.9. □

Si $\{P_1,\dots,P_k\}$ es una base de Sylow de G, el grupo

$$N = \bigcap_{i=1}^k N_G(P_i)$$

se conoce como **el normalizador de la base de Sylow**.

Teorema 13.12. *Sea G finito y resoluble. Si $\{P_1,\dots,P_k\}$ es una base de Sylow de G, su normalizador es un grupo nilpotente.*

Demostración. Por definición $N = \bigcap_{i=1}^{k} N_G(P_i) \subseteq N_G(P_i)$. Entonces P_i es un subgrupo normal del subgrupo NP_i. Como $(N : N \cap P_i) = (NP_i : P_i)$ divide a $(G : P_i)$, se concluye que $P_i \cap N \in \mathrm{Syl}_p(N)$. Luego N es nilpotente pues cada subgrupo de Sylow $P_i \cap N$ de N es normal en N. □

Ejemplo 13.13. Para calcular bases de Sylow se utiliza la función `SylowSystem`. Una base de Sylow para el grupo $\mathbf{SL}_2(3)$ es el conjunto $\{A, B\}$, donde

$$A = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq C_3, \quad B = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \simeq Q_8.$$

El normalizador N del sistema es el subgrupo N generado por la matriz $\begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$. Veamos el código:

```
gap> SL23 := SL(2,3);;
gap> basis := SylowSystem(SL23);
[ Group([ [ [ Z(3)^0, Z(3)^0 ], [ Z(3)^0, Z(3) ] ],
      [ [ Z(3), Z(3)^0 ], [ Z(3)^0, Z(3)^0 ] ],
      [ [ Z(3), 0*Z(3) ], [ 0*Z(3), Z(3) ] ] ]),
  Group([ [ [ Z(3)^0, Z(3)^0 ], [ 0*Z(3), Z(3)^0 ] ] ]) ]
gap> N := Intersection(Normalizer(SL23, basis[1]), \
> Normalizer(SL23, basis[2]));;
gap> GeneratorsOfGroup(N);
[ [ [ Z(3)^0, Z(3)^0 ], [ 0*Z(3), Z(3)^0 ] ],
  [ [ Z(3), 0*Z(3) ], [ 0*Z(3), Z(3) ] ] ]
gap> Order(N);
6
```

Capítulo 14
Factorización en grupos

14. Preliminares

Diremos que un grupo G admite una factorización con respecto a los subgrupos A y B si $G = AB = \{ab : a \in A, b \in B\}$. Observemos que no se pide que los subgrupos A y B sean normales ni se pide que la intersección entre A y B sea trivial.

Proposición 14.1. *Si G se factoriza y N es un subgrupo normal de G, entonces G/N también se factoriza.*

Demostración. Si $\pi\colon G \to G/N$ es el morfismo canónico y $G = AB$, entonces $\pi(G) = \pi(AB) = \pi(A)\pi(B)$. □

Si $G = AB$ es un grupo factorizado y S es un subgrupo de G, diremos que S es un subgrupo factorizado si $S = (A \cap S)(B \cap S)$. No siempre un subgrupo de un grupo factorizado será un subgrupo factorizado.

orized_subgroup:Wielandt

Lema 14.2 (Wielandt). *Sea $G = AB$ un grupo factorizado y sea S un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

1. *Si $ab \in S$ con $a \in A$ y $b \in B$, entonces $a \in S$.*
2. *$S = (A \cap S)(B \cap S)$.*

Demostración. Veamos que $(1) \implies (2)$. Sea $x = ab \in S$ con $a \in A$ y $b \in B$. Como $a \in A \cap S$ y $b \in a^{-1}S \subseteq S$, se tiene que $S = (A \cap S)(B \cap S)$. Si $x \in A \cap B$, entonces $xx^{-1} = 1 \in S$ y luego $x \in S$.

Veamos ahora que $(2) \implies (1)$. Sea $x = ab \in S$ con $a \in A$ y $b \in B$. Si escribimos $x = a_1 b_1$ con $a_1 \in A \cap S$ y $b_1 \in B \cap S$, entonces $a_1^{-1}a = b_1 b^{-1} \in A \cap B \subseteq S$. Luego $a \in S$. □

Proposición 14.3. *Sea $G = AB$ un grupo factorizado. Si S es un subgrupo factorizado, entonces $S = AS \cap BS$.*

Demostración. Si $x \in AS \cap BS$, entonces $x = au = bv$ con $a \in A$, $b \in B$ y $u, v \in S$. Luego $a^{-1}b = uv^{-1} \in S$ y entonces, como S es un subgrupo factorizado, el lema anterior nos dice que $a^{-1} \in S$. Esto implica que $a \in S$ y en consecuencia $x \in S$. □

Lema 14.4. *Sea $G = AB$ un grupo factorizado. Valen las siguientes afirmaciones:*

1. *Toda intersección de subgrupos factorizados es un subgrupo factorizado.*
2. *Todo subgrupo generado por subgrupos normales factorizados es un subgrupo factorizado.*
3. *Si N es un subgrupo normal de G y $\pi\colon G \to G/N$ es el morfismo canónico, un subgrupo $\pi(S)$ de G/N es factorizado si y sólo si S es factorizado.*

Demostración. La primera afirmación es trivial: si $\{S_i : i \in I\}$ es una familia de subgrupos factorizados y $S = \cap_{i\in I} S_i$, entonces $S = (A \cap S)(B \cap S)$.

Demostremos la segunda afirmación. Sea $\{S_i : i \in I\}$ es una familia de subgrupos normales factorizados y sea $S = \langle S_i : i \in I\rangle$. Basta ver que $S \subseteq (A \cap S)(B \cap S)$. Si $x \in S$, entonces existen $i_1, \ldots, i_k \in I$ tales que $x \in S_{i_1} \cdots S_{i_k}$. Al usar la normalidad de los S_{i_j} vemos que

$$\begin{aligned} x \in S_{i_1} \cdots S_{i_k} &= (A \cap S_{i_1})(B \cap S_{i_1}) S_{i_2} \cdots S_{i_k} \\ &= (A \cap S_{i_1}) S_{i_2} (B \cap S_{i_1}) S_{i_3} \cdots S_{i_k} \\ &= (A \cap S_{i_1})(A \cap S_{i_2})(B \cap S_{i_2})(B \cap S_{i_1}) S_{i_3} \cdots S_{i_k} \\ &\;\;\vdots \\ &= (A \cap S_{i_1})(A \cap S_{i_2}) \cdots (A \cap S_{i_k})(B \cap S_{i_k}) \cdots (B \cap S_{i_1}) \\ &\subseteq (A \cap S)(B \cap S). \end{aligned}$$

Para demostrar la tercera afirmación

□

14. El teorema de Kegel–Wielandt

Teorema 14.1 (Gruenberg). *Sea G un grupo finito. Si $G = HK$ con K nilpotente y H un p-grupo, entonces G es resoluble.*

Demostración. Supongamos que el resultado no es cierto y sea G un contraejemplo minimal. En particular, $K \neq 1$. Como K es nilpotente, $Z(K) \neq 1$. Sea $x \in Z(K)$ tal que $x \neq 1$.

Afirmamos que G no es simple. En efecto, si $x \in Z(G)$, entonces claramente $Z(G) \neq 1$ y luego G no es simple. Si $x \notin Z(G)$, veremos que tampoco G puede ser simple pues la clase de conjugación de x en G tiene p^m elementos para algún m. Para demostrar esta última afirmación observamos que si $g \in G$ entonces $g = hk$ para algún $h \in H$ y $k \in K$ y luego, como $x \in Z(K)$,

$$gxg^{-1} = (hk)x(hk) = hxh^{-1}.$$

Esto implica que la cantidad de conjugados de x en G es un divisor del orden de H y H es, por hipótesis, un p-grupo.

Sabemos que G no es simple. Sea N un subgrupo propio no trivial de G y sea $\pi\colon G \to G/N$ el morfismo canónico. Sabemos que $\pi(G) = \pi(H)\pi(K)$, donde $\pi(H)$ es un p-grupo y $\pi(K)$ es nilpotente. Por la minimalidad de G, entonces $\pi(G)$ es resoluble. Por otro lado, $K \cap N \subseteq K$ es nilpotente y

$$(N : K \cap N) = \frac{|N|}{|K \cap N} = \frac{|KN|}{|K|}$$

es una potencia del primo p pues KN es un subgrupo de $KH = G$. Por la minimalidad de G, N es resoluble. Luego G es resoluble. □

Veamos qué pasa cuando un grupo finito no admite una factorización, que significa que no es posible escribir a G como $G = AB$ para dos subgrupos propios A y B.

Ejercicio 14.2. Un grupo finito cíclico no admite factorización si y sólo si $n = p^k$ para algún número primo p.

Proposición 14.3. *Sea G un grupo finito que no admite factorización. Si $\Phi(G) = 1$, entonces G es simple.*

Demostración. Si G no es simple, sea N un subgrupo normal no trivial de G. Si todo maximal de G contiene a N, entonces $1 = \Phi(G) \supseteq N$, una contradicción. Luego sabemos que tiene que existir un subgrupo maximal M de G tal que no contiene a N. Pero entonces $G = NM$, una contradicción. □

Proposición 14.4. *Si G tiene un único subgrupo maximal, entonces G es cíclico de orden una potencia de un primo.*

Demostración. Para cada primo p que divide al orden de G sea $P \in \mathrm{Syl}_p(G)$. Sea M el único subgrupo maximal de G. Sea $g \in G \setminus M$ y sea $H = \langle g \rangle$. Si $H \neq G$, entonces existe un subgrupo maximal que contiene a H, y ese maximal tiene que ser M. Luego $g \in M$, una contradicción. Luego $H = G$ y entonces $G = \langle g \rangle$ es cíclico. completar □

Proposición 14.5. *Si G no admite factorización , entonces $G/\Phi(G)$ es simple.*

Demostración. Supongamos que G admite una factorización $G = AB$. Sin perder generalidad podemos suponer que A y B son subgrupos maximales de G. En efecto, si A no es maximal, entonces existe un maximal M tal que $A \subseteq M$. Como $B \not\subseteq M$, entonces $G = AB = MB$. Similarmente vemos que también puede suponerse que B es un subgrupo maximal.

El párrafo anterior nos dice que G no se factoriza si y sólo si $|AB| < |G|$ para todo par de subgrupos maximales A y B. Observemos que la condición $|AB| < |G|$ puede reescribirse como $(B : A \cap B) < (G : A)$.

Si G admite una factorización, digamos $G = AB$ con A y B subgrupos maximales, entonces $G/\Phi(G)$ también admite una factorización.

Como $\Phi(G/\Phi(G)) = 1$, $G/\Phi(G)$ no admite una factorización y luego $G/\Phi(G)$ es un grupo simple. VER □

Capítulo 15
El problema de Hughes

Sea G un grupo y sea p un número primo. Se define el **subgrupo de Hughes** $H_p(G)$ de G como el subgrupo generado por todos los elementos de G que no tienen orden p. En 1957 Hughes formuló la siguiente conjetura [1]: Si $H_p(G)$ es propio y no trivial, entonces $H_p(G)$ tiene índice p en G.

15. Primeras observaciones

Proposición 15.1 (Hughes). *Si G es un grupo, entonces $H_2(G) = 1$, $H_2(G) = G$ o bien $H_2(G)$ tiene índice dos.*

Demostración. Sea $H = H_2(G)$ y supongamos que H es propio y no trivial. Si $h \in H$ y $a \in G \setminus H$, entonces $ah \notin H$. Luego ah tiene orden dos y entonces, como $(ah)^2 = 1$, se concluye que $aha = h^{-1}$.

Sean ahora $a, b \in G \setminus H$ tales que $ab \notin H$. En particular, a, b y ab son elementos de orden dos y entonces $1 = (ab)^2 = abab$, lo que implica que $ab = ba$. Si $h \in H$,

$$h^{-1} = (ab)h(ab) = (ba)h(ab) = b(aha)b = bh^{-1}b = h$$

y luego $h^2 = 1$, una contradicción. Se concluye entonces que si $a, b \in G \setminus H$, se tiene que $ab \in H$. En consecuencia, $(G : H) = 2$. □

15. El teorema de Straus–Szejeres

Sea H un subgrupo normal de un grupo G. Sobre el conjunto R de funciones $H \to H$ definimos dos operaciones

$$(f+g)(x) = f(x)g(x), \quad (fg)(x) = f(g(x)), \quad f, g \in R, x \in H.$$

Entonces $(R,+)$ es un grupo: el neutro es la función $0(x) = 1$ para todo $x \in H$ y el inverso de una función f está dado por $(-f)(x) = f(x)^{-1}$. Vale además la siguiente propiedad distributiva: $(f+g)h = fh+gh$.

Para cada $x \in G$ definimos $\gamma_x \colon H \to H$, $\gamma_x(y) = xyx^{-1}$. Luego

$$\Gamma = \{\gamma_x : x \in G\} \subseteq R.$$

lem:SS1 **Lema 15.1.** *Si $h \in H_3(G)$ y $x \notin H_3(G)$, entonces $0 = \gamma_{x^2} + \gamma_x + \mathrm{id}$.*

Demostración. Como x tiene orden tres, x^2 tiene orden tres y luego $x^2 \notin H_3(G)$. Todos los elementos de la coclase $x^2H_3(G)$ tienen orden tres (pues si $y = x^2h \in H_3(G)$ para algún $h \in H_3(G)$, entonces $x \in H_3(G)$). En particular,

$$1 = (x^2h)^3 = (x^2h)(x^2h)(x^2h) = (x^2hx))(xhx^2)h.$$

□

Lema 15.2. *Si $H_3(G)x \neq H_3(G)y$, entonces $\gamma_x + \gamma_y = \gamma_y + \gamma_x$.*

Demostración. Sea $z = yx^{-1} \notin H_3$ y sea $h_1 = \gamma_{z^2x}(h) = (z^2x)h(z^2x)^{-1}$. Como h_1 y h son elementos del mismo orden, $h_1 \in H_3$. Como z y z^2 son elementos de orden tres, el lema anterior implica que

$$\gamma_{z^2}(h_1)\gamma_z(h_1)h_1 = 1 = \gamma_z(h_1)\gamma_{z^2}(h_1)h_1.$$

Como además $\gamma_{z^2}(h_1) = yhy^{-1}$ y $\gamma_z(h_1) = xhx^{-1}$, se concluye que

$$(yhy^{-1})(xhx^{-1}) = (xhx^{-1})(yhy^{-1}).$$

□

Teorema 15.3 (Straus–Szejeres). *Si G es un grupo tal que $(G : H_3(G)) > 3$, entonces H_3 es trivial.*

Demostración. Sea $H = H_3(G)$. Claramente H es un subgrupo normal. Supongamos que $(G : H) > 3$. Como todo elemento de G/H tiene orden tres, el teorema de Burnside implica que G/H es finito (de orden 27) y tal que posee un subgrupo de orden nueve isomorfo a $C_3 \times C_3$, digamos generado por dos coclases distintas Hx y Hy. Por el lema anterior, $\gamma_x + \gamma_y = \gamma_y + \gamma_x$. Observemos que

$$\begin{aligned} 3 = (1 + yx^2 + xy^2) + (1 + yx + x^2y^2) \\ - (1 + x + x^2)y^2 - y(1 + x + x^2) + (1 + y + y^2) = f(x,y). \end{aligned}$$

Si $h \in H$, entonces $h^3 = h^{f(x,y)} = 1$. Luego H es trivial. □

Capítulo 16
p-grupos

16. El subgrupo de Frattini

Lema 16.1 (Blackburn). *Sea G un p-grupo finito y sea N un subgrupo normal de G de orden p^2. Entonces $C_G(N)$ es un subgrupo normal de G de índice $\leq p$. En particular, $[G,G] \subseteq C_G(N)$.*

Demostración. Sea $\gamma\colon G \to \mathrm{Aut}(N)$ dado por $x \mapsto \gamma_x$, donde $\gamma_x(n) = xnx^{-1}$. Un cálculo directo muestra que γ es un morfismo de grupos tal que $\ker\gamma = C_G(N)$. Luego $C_G(N)$ es un subgrupo normal de G. Por el primer teorema de isomorfismos, $G/C_G(N) \simeq \gamma(G) \leq \mathrm{Aut}(N)$. Como $|N| = p^2$, entonces $N \simeq C_{p^2}$ o bien $N \simeq C_p \times C_p$. Luego $\mathrm{Aut}(N) \simeq \mathbb{C}_{p(p-1}$ o bien $\mathrm{Aut}(N) \simeq \mathbf{GL}(2,p)$. Además, como G es un p-grupo, $\gamma(G)$ es también un p-grupo. Luego $(G : C_G(N)) = |\gamma(G)|$ es una potencia del primo p que divide a $p(p-1)$ o a $p(p-1)(p^2-1)$. En cualquier caso, se tiene que $(G : C_G(N)) \leq p$. En particular, $G/C_G(N)$ es cíclico y luego abeliano, lo que implica que $[G,G] \subseteq C_G(N)$. □

Supongamos ahora que G es un grupo finito y que existe un subgrupo $\Psi(G)$ con las siguientes propiedades:

1. $\Psi(G)$ es característico en G,
2. $\Psi(G) \subseteq \Phi(G)$, y
3. $\Psi(G/N) = \Psi(G)/N$ si N es normal en G y $N \subseteq \Psi(G)$.

Tendremos dos ejemplos en mente: $\Psi(G) = \Phi(G)$ y $\Psi(G) = [G,G]$.

Lema 16.2. *Si H es un grupo no abeliano de orden p^3, entonces no existe un p-grupo G tal que $\Psi(G) = H$.*

Demostración. Supongamos que $H = \Psi(G)$ para algún p-grupo G. Como H es característico en G, H es normal en G. Además H contiene un subgrupo normal N de índice p. Como H es característico en G, N es normal en G y luego $|N| = p^2$. Por el lema anterior $(G : C_G(N)) \leq p$. Esto implica que $N \subseteq Z(H)$, lo

que es una contradicción pues en grupos no abelianos de orden p^3 el centro tiene orden p. Si $(G : C_G(N)) = 1$, entonces $G = C_G(N)$ y luego $N \subseteq H \subseteq C_G(N)$. En particular, Supongamos entonces que $(G : C_G(N)) = p$. En este caso también $H \subseteq C_G(N) \ldots$ Why?. □

Parte I
Grupos de permutaciones

Capítulo 17
El teorema de Iwasawa

Ejemplo 17.1. El grupo $\mathbb{A}_4$ actúa 2-transitivamente en $X = \{1,2,3,4\}$.

Ejemplo 17.2. El grupo

$$\mathrm{Aff}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R} \right\}$$

actúa 2-transitivamente en $\mathbb{R}$.

thm:Iwasawa

Teorema 17.3 (Iwasawa). *Sea G un grupo que actúa 2-transitivamente en un conjunto X. Si $[G,G] = G$ y algún estabilizador G_x contiene un subgrupo normal abeliano A tal que $G = \langle gAg^{-1} : g \in G \rangle$, entonces G/K es un grupo simple, donde K es el núcleo de la acción de G en X.*

Antes de demostrar el teorema necesitamos dos lemas.

lem:paraIwasawa1

Lema 17.4. *Si G actúa 2-transitivamente en un conjunto X y $x \in X$, entonces G_x es un subgrupo maximal de G.*

Demostración. Primero veamos que $G_x \neq G$. En efecto, sean $x, y \in X$ tales que $x \neq y$. Existe entonces un $g \in G$ tal que $g \cdot x = y$, es decir $g \notin G_x$ y luego $G_x \neq G$.

Veamos ahora que si $G_x \subseteq H \subsetneq G$, entonces $G_x = H$. Si $G_x \subsetneq H$, sea $h \in H \setminus G_x$ y sea $g \in G \setminus H$. Como se tiene [1] que $\#\{x, h \cdot x, g \cdot h\} = 3$. Si utilizamos la 2-transitividad con los puntos $(x, g \cdot x)$ y $(x, h \cdot x)$, sabemos que existe un $g_1 \in G$ tal que $g_1 \cdot x = x$ y $g_1 \cdot (h \cdot x) = g \cdot x$. Luego $g_1 \in G_x$ y además $g^{-1} g_1 h \in G_x \subseteq H$. Esto implica que $g^{-1} \in H$ y luego $g \in H$, una contradicción. □

Observación 17.5. En realidad, el lema anterior se obtiene fácilmente del lema... pues los grupos doblemenete transitivos son primitivos.

lem:paraIwasawa2

Lema 17.6. *Si G actúa 2-transitivamente en X y N es normal en G, entonces N actúa trivial o transitivamente en X.*

[1] Si $x = g \cdot x$, entonces $g \in G_x \subseteq H$, una contradicción; si $h \cdot x = g \cdot x$, entonces $h^{-1} g \in G_x \subseteq H$ y luego $g \in H$, una contradicción; y por último si $h \cdot x = x$, entonces $h \in G_x$, una contradicción

Demostración. Si N no actúa trivialmente, entonces existen $n \in N$ y $x \in X$ tales que $n \cdot x \neq x$. Sean $y, z \in X$ tales que $y \neq z$. Como en particular G es transitivo, existe $g \in G$ tal que $g \cdot y = z$. Luego N actúa transitivamente en X pues

$$z = (gn) \cdot x = (gng^{-1}) \cdot (g \cdot x) = (gng^{-1}) \cdot y.$$

y $gng \in^{-1} \in N$ por la normalidad de N. □

Ejemplo 17.7. El grupo $\mathbb{A}_4$ actúa 2-transitivamente en $X = \{1,2,3,4\}$ y el subgrupo $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ es normal en $\mathbb{A}_4$ y actúa transitivamente en X.

Ejemplo 17.8. El subgrupo

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} :\in \mathbb{R} \right\}$$

es normal en $\mathrm{Aff}(\mathbb{R})$ y actúa transitivamente en $\mathbb{R}$.

Ahora sí estamos en condiciones de demostrar el teorema 17.3 de Iwasawa.

del teorema 17.3. Sea N un subgrupo normal de G tal que $K \subseteq N \subseteq G$. Como N es normal en G, NG_x es un subgrupo de G que contiene a G_x. La maximalidad de G_x demostrada en el lema 17.4 implica entonces que $NG_x = G_x$ o bien $NG_x = G$.

Si $NG_x = G_x$, entonces $N \subseteq G_x$ y luego N no actúa transitivamente. Por el lema 17.6, N actúa trivialmente en X y luego $N \subseteq K$. En consecuencia, $N = K$.

Si $NG_x = G$, entonces NA es normal en $NG_x = G$ pues A es normal en G_x. Como entonces $gAg^{-1} \subseteq g(NA)g^{-1} = NA$, se concluye que $NA = G$ pues por hipótesis sabemos que $G = \langle gAg^{-1} : g \in G \rangle$. En consecuencia,

$$G/N = NA/A \simeq A/N \cap A$$

es un grupo abeliano (por ser cociente de un grupo abeliano) y luego $G = [G,G] \subseteq N$. Se concluye entonces que en este caso $G = N$. □

Ejemplo 17.9. Veamos otra demostración de la simplicidad del grupo $\mathbb{A}_5$. Sabemos que $\mathbb{A}_5$ actúa 2-transitivamente en $X = \{1,2,3,4,5\}$. El estabilizador $G_5 \simeq \mathbb{A}_4$ contiene un subgrupo normal abeliano $A = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Además $\mathbb{A}_5 = \langle gAg^{-1} : g \in \mathbb{A}_5 \rangle$ pues los productos de dos trasposiciones de $\mathbb{A}_5$ generan al grupo $\mathbb{A}_5$ y $[\mathbb{A}_5, \mathbb{A}_5] = \mathbb{A}_5$ pues

$$(ab)(cd) = (abc)(abd(abc)^{-1}(abd)^{-1}$$

si $a, b, c, d \in X$ son elementos distintos. Luego $\mathbb{A}_5$ es simple gracias al teorema de Iwasawa.

Capítulo 18
Grupos de permutaciones

18. El teorema de Deaconescu–Walls

Sea A un grupo que actúa por automorfismos en un grupo finito G. El grupo $C_G(A) = \{g \in G : a \cdot g = g \ \forall a \in A\}$ actúa en el conjunto de las A-órbitas pues $g \in G$ y $c \in C_G(A)$ entonces

$$c(A \cdot g) = \{c(a \cdot g) : a \in A\} = \{(a \cdot c)(a \cdot g) : a \in A\} = \{a \cdot (cg) : a \in A\} = A \cdot (cg).$$

El siguiente teorema fue descubierto por Deaconescu y Walls [3]. La prueba que presentamos se debe a Isaacs [6].

theorem:DeaconescuWalls

Teorema 18.1 (Deaconescu–Walls). *Sea A un grupo que actúa por automorfismos en un grupo finito G. Sea $C = C_G(A)$ y sea $N = C \cap [A,G]$, donde $[A,G]$ es el subgrupo de G generado por $[a,g] = (a \cdot g)g^{-1}$, $a \in A$, $g \in G$. Entonces $(C : N)$ divide a la cantidad de A-órbitas de G.*

Demostración. El grupo C actúa por multiplicación a izquierda en el conjunto Ω de A-órbitas de G. Sea $X = A \cdot g \in \Omega$ y sea C_X el estabilizador en C de X. Si $c \in C_X$ entonces $cX = X$; en particular, si $c \in C_X$ entonces $cg = a \cdot g$ para algún $a \in A$, es decir: $c = (a \cdot g)g^{-1} = [a,g] \in [A,G]$. Esto implica que $C_X \subseteq N$.

Para demostrar que $(C : N)$ divide al cardinal de Ω, basta ver que $(C : N)$ divide al tamaño de cada C-órbita. Si $X \in \Omega$ entonces $C \cdot X$ tiene cardinal

$$(C : C_X) = (C : N)(N : C_X)$$

y luego $(C : N)$ divide al cardinal de la órbita $C \cdot X$. □

orollary:Z(G)subset[G,G]

Corolario 18.2. *Sea G un grupo finito no trivial con $k(G)$ clases de conjugación. Si el orden de $Z(G)$ es coprimo con $k(G)$ entonces $Z(G) \subseteq [G,G]$.*

Demostración. El grupo $A = G$ actúa en G por conjugación. Como $C_G(A) = Z(G)$ y $[A,G] = [G,G]$, el teorema de Deaconescu–Walls 18.1 implica que el índice

$(Z(G) : Z(G) \cap [G,G])$ divide a $k(G)$. Pero como $k(G)$ y $|Z(G)|$ son coprimos, $Z(G) = Z(G) \cap [G,G] \subseteq [G,G]$. □

Definición 18.3. Sean G un grupo y $f \in \mathrm{Aut}(G)$. Se dice que f es **central** si $f(x)x^{-1} \in Z(G)$ para todo $x \in G$.

Observación 18.4. Un automorfismo f es central si y sólo si $f \in C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$.

Corolario 18.5. *Sea G un grupo finito con $k(G)$ clases de conjugación y $c(G)$ automorfismos centrales. Si el orden de G es coprimo con $k(G)c(G)$ entonces $[G,G] = Z(G)$.*

Demostración. El corolario 18.2 prueba que $Z(G) \subseteq [G,G]$. Para demostrar la otra contención sea $A = C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$. Como $|G|$ y $k(G)c(G)$ son coprimos, y $(C_G(A) : C_G(A) \cap [A,G])$ divide a $c(G)$ por el teorema de Deaconescu–Walls 18.1, entonces $C_G(A) = C_G(A) \cap [A,G]$. Como $[G,G] \subseteq C_G(A)$ pues

$$a \cdot [x,y] = [(a \cdot x)x^{-1}x, (a \cdot y)y^{-1}y] = [x,y]$$

para todo $a \in A$, $x,y \in G$.y además $[A,G] \subseteq Z(G)$, se concluye que

$$[G,G] \subseteq C_G(A) = C_G(A) \cap [A,G] \subseteq [A,G] \subseteq Z(G).$$

□

Corolario 18.6. *Sea p un número primo. Si G un grupo con p clases de conjugación, entonces $Z(G) \subseteq [G,G]$ o bien $|G| = p$.*

Demostración. Hacemos actuar a G en G por conjugación. Como cada elemento de $C = Z(G)$ es una clase de conjugación, $|C| \leq p$. Si $|C| = p$ entonces $G = C = Z(G)$ tiene orden p. Si no, $|C|$ es coprimo con p y luego $C \subseteq N = [G,G]$. □

18. Grupos transitivos

Definición 18.1. Sea G un grupo. Un conjunto X se dice un G-conjunto si existe una acción $G \times X \to X$, $(g,x) \mapsto g \cdot x$.

Si X es un G-conjunto entonces $\lambda : G \to \mathbb{S}_X$, $g \mapsto \lambda_g$, donde $\lambda_g(x) = g \cdot x$, es un morfismo de grupos. Recíprocamente, todo morfismo $\lambda : G \to \mathbb{S}_X$ define una acción de G en X así $g \cdot x = \lambda(g)(x)$.

Definición 18.2. Un G-conjunto X se dice **fiel** si el morfismo $G \to \mathbb{S}_X$ es inyectivo, es decir: si $g \cdot x = x$ para todo $x \in X$ implica que $g = 1$.

Ejemplo 18.3. Sea X un G-conjunto con acción λ. Sea

$$N = \ker \lambda = \{g \in G : g \cdot x = x \, \forall x \in X\}.$$

Entonces X es un (G/N)-conjunto fiel, donde $(gN) \cdot x = g \cdot x$, $g \in G$, $x \in X$.

Un grupo G se dice **grupo de permutaciones** si existe un G-conjunto fiel X. Dos grupos $G \subseteq \mathbb{S}_X$ y $H \subseteq \mathbb{S}_Y$ son **isomorfos como grupos de permutación** si existe una biyección $\alpha\colon X \to Y$ y existe un isomorfismo $f\colon G \to H$ tal que

$$\alpha(g \cdot x) = f(g) \cdot \alpha(x)$$

para todo $g \in G$, $x \in X$.

Ejemplo 18.4. Sea G un grupo. Sea $R\colon G \to \mathbb{S}_G$, $g \mapsto R_g$, donde $R_g(x) = xg^{-1}$ y sea $L\colon G \to \mathbb{S}_G$, $g \mapsto L_g$, donde $L_g(x) = gx$. Entonces (G,L) y (G,R) son isomorfos pues $\iota\colon G \to G$, $x \mapsto x^{-1}$, es inversible y vale

$$\iota(L_g(x)) = \iota(gx) = (gx)^{-1} = x^{-1}g^{-1} = \iota(x)g^{-1} = R_g(\iota(x))$$

para todo $g, x \in G$.

Observación 18.5. Dos grupos de permutaciones $G \subseteq \mathbb{S}_X$ y $H \subseteq \mathbb{S}_X$ son isomorfos como grupos de permutación si y sólo si G y H son conjugados en $\mathbb{S}_X$.

Definición 18.6. Un G-conjunto X se dice **transitivo** si dados $x, y \in X$ existe $g \in G$ tal que $g \cdot x = y$.

Un grupo G se dice **transitivo** si existe un G-conjunto X fiel y transitivo. El **grado** de G es el cardinal del conjunto X.

Ejemplo 18.7. El grupo $\{\mathrm{id}, (12)(34), (14)(23), (13)(24)\} \simeq C_2 \times C_2$ actúa naturalmente en $\{1,2,3,4\}$ y es un grupo transitivo de grado cuatro.

Ejemplo 18.8. Los grupos transitivos de grado cuatro (módulo conjugación en $\mathbb{S}_4$) son $\mathbb{S}_4$, $\mathbb{A}_4$, $\{\mathrm{id}, (12)(34), (14)(23), (13)(24)\} \simeq C_2 \times C_2$, $\langle (1234) \rangle \simeq C_4$ y $\langle (1234), (12) \rangle \simeq \mathbb{D}_8$.

Sea X un G-conjunto. Recordemos que la G-órbita de un elemento $x \in G$ es el conjunto $G \cdot x = \{g \cdot x : g \in G\}$. Claramente X es transitivo si y sólo si existe $x \in X$ tal que $G \cdot x = X$.

Ejercicio 18.9. Demuestre que todo G-conjunto X se descompone como unión disjunta de G-conjuntos transitivos.

Si $x, y \in X$ se define la relación $x \sim y$ si y sólo si existe $g \in G$ tal que $g \cdot x = y$. Como $\sim$ es una relación de equivalencia en X, el conjunto X se descompone como unión disjunta de clases de equivalencia. Por definición, cada clase de equivalencia es un G-conjunto transitivo.

Sea X un G-conjunto. El **estabilizador** de un elemento $x \in X$ se define como el subgrupo $G_x = \{g \in G : g \cdot x = x\}$.

Ejercicio 18.10. Si X es un G-conjunto transitivo de grado n entonces existe $x \in X$ tal que $|G| = n|G_x|$. Si además X es fiel entonces $|G_x|$ divide a $(n-1)!$.

Como X es transitivo, $n = |X| = (G : G_x) = |G|/|G_x|$. Si además X es fiel, G_x es un subgrupo de $\mathbb{S}_{X\setminus\{x\}} \simeq \mathbb{S}_{n-1}$. Luego $|G_x|$ divide a $(n-1)!$.

Ejercicio 18.11. Si G es un grupo finito con dos clases de conjugación, entonces $G \simeq C_2$.

Sea $X = G \setminus \{1\}$. Como X es un G-conjunto transitivo con la conjugación, $|X| = |G| - 1$ divide al orden de G. Luego $|G| = 2$.

lemma:rango

Lema 18.12. *Sea G un grupo transitivo en X y sean $x, y \in X$. Si $g \in G$ es tal que $g \cdot x = y$, entonces $G_y = gG_xg^{-1}$. En particular, la cantidad de G_x-órbitas es igual a la cantidad de G_y-órbitas.*

Demostración. Si $h \in G_x$ entonces $h \cdot x = x$ y luego

$$ghg^{-1} \cdot y = gh \cdot x = g \cdot (h \cdot x) = g \cdot x = y.$$

Recíprocamente, si $h \in G_y$ entonces

$$g^{-1}hg \cdot x = g^{-1}h \cdot y = g^{-1} \cdot y = x.$$

Sean $x_1, \ldots, x_m \in X$ tales que los conjuntos $G_x \cdot x_j$ son las G_x-órbitas de X. Para cada $j \in \{1, \ldots, m\}$ sea $y_j = g \cdot x_j$. Cada $G_y \cdot y_j$ es una G_x-órbita pues

$$G_y \cdot y_j = (gG_xg^{-1}) \cdot y_j = (gG_x) \cdot x_j = g \cdot (G_x \cdot x_j)$$

ya la acción de g permuta las G_x-órbitas de X. □

El lemma 18.12 justifica la siguiente definición:

Definición 18.13. Sea X un G-conjunto transitivo. Se define el **rango** de X como la cantidad de G_x-órbitas de X.

Teorema 18.14. *Sea X un G-conjunto y sea $x \in X$. El rango de X es igual a la cantidad de (G_x, G_x)-coclases dobles de G.*

Demostración. Sean $S = G_x$,

$$f\colon \{S\text{-órbitas}\} \to \{(S,S)\text{-coclases dobles}\}, \quad S \cdot y \mapsto SgS,$$

donde $g \cdot x = y$.

Probemos que f está bien definida: si $g,h \in G$ son tales que $g\cdot x = h\cdot x = y$, entonces $g^{-1}h \in S$; luego $h = 1g(g^{-1}h) \in SgS$ y $ShS = SgS$. Probemos ahora que f es inyectiva: Si $f(S\cdot y) = f(S\cdot z)$ y $g,h \in G$ son tales que $g\cdot x = y$ y $h\cdot x = z$, entonces existen $a,b \in S$ tales que $g = ahb$. Luego

$$y = g\cdot x = (ahb)\cdot x = a\cdot z \in S\cdot z,$$

y entonces $S\cdot y = S\cdot z$. Por último f es sobreyectiva pues $SgS = f(S\cdot(g\cdot x))$. □

Definición 18.15. Sea X un G-conjunto. Sea $k \in N$ tal que $k \leq |X|$. Se dice que X es k-transitivo si dados dos subconjuntos ordenados $\{x_1,\ldots,x_k\}$ y $\{y_1,\ldots,y_k\}$ de X de k elementos, existe $g \in G$ tal que $g\cdot x_j = y_j$ para todo $j \in \{1,\ldots,k\}$.

Claramente un G-conjunto es 1-transitivo si y sólo si es transitivo. Un grupo se dice k-transitivo si existe un G-conjunto fiel k-transitivo. Un G-conjunto se dice **doblemente transitivo** si $k \geq 2$, **triplemente transitivo** si $k \geq 3$, etc.

Lema 18.16. *Sea X un G-conjunto y sea $k \geq 2$. Entonces X es k-transitivo si y sólo si todo G_x actúa $(k-1)$-transitivamente en $X \setminus \{x\}$.*

Demostración. Sean $\{x_1,\ldots,x_k\}$ y $\{y_1,\ldots,y_k\}$ conjuntos ordenados de k elementos de X. Como G_{x_k} actúa $(k-1)$-transitivamente en $X\setminus\{x_k\}$ existe $g \in G_{x_k}$ tal que $g\cdot x_i = y_i$ para todo $i \in \{1,\ldots,k-1\}$. También existe $h \in G_{y_1}$ tal que $h\cdot y_j = y_j$ para todo $j \in \{1,\ldots,k-1\}$ y $h\cdot x_k = y_k$. Entonces $(hg)\cdot x_j = y_j$ para todo $j \in \{1,\ldots,k\}$.

Si $\{x_1,\ldots,x_{k-1}\}$ y $\{y_1,\ldots,y_{k-1}\}$ son conjuntos ordenados de $k-1$ elementos de $X\setminus\{x\}$, existe $g \in G$ tal que $g\cdot x = x$, $g\cdot x_j = y_j$ para todo j. □

Proposición 18.17. *Si X es un G-conjunto 2-transitivo, X tiene rango dos.*

Demostración. Como G_x es transitivo en $X\setminus\{x\}$, hay dos G_x-órbitas: $\{x\}$ y $X\setminus\{x\}$. □

Si X es un G-conjunto y $x_1,\ldots,x_k \in X$ se define el estabilizador

$$G_{x_1,\ldots,x_k} = \{g \in G : g\cdot x_j = x_j,\ 1 \leq j \leq k\} = \bigcap_{j=1}^{k} G_{x_j}.$$

Si $g\cdot x_j = y_j$ para todo $j \in \{1,\ldots,k\}$ entonces $G_{y_1,\ldots,y_k} = gG_{x_1,\ldots,x_k}g^{-1}$.

proposition:k_transitivo

Proposición 18.18. *Sean X un G-conjunto k-transitivo de grado n y $x_1,\ldots,x_k \in X$ elementos disntintos. Entonces*

$$|G| = n(n-1)\cdots(n-k+1)|G_{x_1,\ldots,x_k}|.$$

Si además X es fiel, $|G_{x_1,\ldots,x_k}|$ divide a $(n-k)!$.

Demostración. Si $x_1 \in X$ entonces $|G| = n|G_{x_1}|$. Como G_{x_1} es $(k-1)$-transitivo en $X\setminus\{x_1\}$, podemos escribir

$$|G_{x_1}| = (n-1)\cdots(n-k+1)|G_{x_1,\ldots,x_k}|.$$

Luego $|G| = n(n-1)\cdots(n-k+1)|G_{x_1,\ldots,x_k}|$. Para demostrar la segunda afirmación observemos que si además X es fiel, G es isomorfo a un subgrupo de $\mathbb{S}_{X\setminus\{x_1,\ldots,x_k\}}$. □

Definición 18.19. Un G-conjunto X de grado n se dice **fuertemente k-transitivo** si es k-transitivo y $G_{x_1,\ldots,x_k} = 1$ para todo $x_1,\ldots,x_k \in X$ elementos distintos.

Grupo!regular

Un G-conjunto X se dice **regular** si es fuertemente transitivo.

Ejemplo 18.20. El grupo $\mathbb{S}_n$ actúa fuerte y n-transitivamente en $\{1,\ldots,n\}$.

Ejemplo 18.21. El grupo $\mathbb{A}_n$ actúa fuerte y $(n-2)$-transitivamente en $\{1,\ldots,n\}$. Para demostrar esta afirmación procederemos por inducción en n. El caso $n = 3$ es evidente. Si $n > 3$ y $j \in \{1,\ldots,n\}$ entonces $(\mathbb{A}_n)_j \simeq \mathbb{A}_{n-1}$. Por hipótesis inductiva, $\mathbb{A}_{n-1}$ actúa fuerte y $(n-3)$-transitivamente en $\{1,\ldots,n\}\setminus\{j\}$.

Proposición 18.22. *Sea G transitivo en X y sea N regular normal en X. Entonces $G = N \rtimes G_x$ para algún $x \in X$.*

Demostración. Sean $x, y \in X$. Existe $g \in G$ tal que $g \cdot y = x$ y existe $n \in N$ tal que $n \cdot x = y$. Como

$$(gn)\cdot x = g\cdot(n\cdot x) = g\cdot y = x,$$

$gn \in G_x$ y luego $g = (gn)n^{-1} \in G_x N$. Como N es regular $N \cap G_x = 1$ y el resultado entonces se obtiene de la normalidad de N. □

lemma:Tits

Lema 18.23. *Sea G transitivo en X y sea $x \in X$. Si N es normal y regular en X, la función*

$$\varphi\colon N\setminus\{1\} \to X\setminus\{x\}, \quad n \mapsto n\cdot x$$

es biyectiva y $\varphi(gng^{-1}) = g\cdot\varphi(n)$ para todo $g \in G_x$.

Demostración. La función φ está bien definida pues N es regular. Es inyectiva pues si $n\cdot x = m\cdot x$, $n, m \in N\setminus\{1\}$, entonces $m^{-1}n \in N_x = 1$ y luego $m = n$. Es sobreyectiva pues si $y \in X\setminus\{x\}$ existe $n \in N\setminus\{1\}$ tal que $n\cdot x = y$. Por último, si $g \in G_x$ y $n \in N$, entonces

$$\varphi(gng^{-1}) = gng^{-1}\cdot x = g\cdot(n\cdot x) = g\cdot\varphi(n).$$

□

oposition:regular_normal

Proposición 18.24. *Sea G un grupo k-transitivo con $k \geq 2$ y de grado n, y sea N un subgrupo regular normal. Entonces $k \leq 4$ y valen las siguientes afirmaciones:*

1. *Si $k = 2$, N es un p-grupo elemental abeliano para algún primo p.*
2. *Si $k = 3$, $|N| = 3$ o bien N es un 2-grupo elemental abeliano.*
3. *Si $k = 4$, $|N| = 4$.*

Demostración. Supongamos primero que $k = 2$. Sean $x \in X$ y $n_1, n_2 \in N \setminus \{1\}$. Como G es 2-transitivo, existe $g \in G_x$ tal que

$$\varphi(gn_1g^{-1}) = g \cdot \varphi(n_1) = \varphi(n_2),$$

ver lema 18.23. Como φ es biyectiva, $gn_1g^{-1} = n_2$, y entonces $|n_1| = |n_2|$. Supongamos que $|n_1| = rs$. Como n_1^r tiene orden s, se concluye que N es un p-grupo para algún primo p. Veamos que $Z(N) = N$. Si $n \in N \setminus Z(N)$ y $m \in Z(N)$, entonces existe $g \in G_x$ tal que $gmg^{-1} = n$ pues $g \cdot \varphi(m) = \varphi(gmg^{-1}) = \varphi(n)$. Luego, como $Z(M)$ es característico en N y N es normal en G, $gmg^{-1} = n \in Z(M)$, una contradicción.

Supongamos ahora que $k = 3$. Supongamos además que $|N| > 3$ y que existe $n \in N$ tal que $n^2 \neq 1$. Sean $x \in X$ y $m \in N \setminus \{1, n, n^2\}$. La 3-transitividad implica que existe $g \in G_x$ tal que

$$g \cdot \varphi(n) = \varphi(gng^{-1}) = \varphi(n), \quad g \cdot \varphi(n^2) = \varphi(gn^2g^{-1}) = \varphi(m).$$

Luego $gng^{-1} = n$ y $gn^2g^{-1} = m$, una contradicción.

Supongamos ahora que $k = 4$. Sabemos que entonces $|N| \geq 4$; supongamos que $|N| > 4$. Como N es un 2-grupo, existen $n_1, n_2 \in N$ tales que $|\{n_1, n_2, n_1n_2\}| = 3$. Sean $x \in X$ y $n \in N \setminus \{n_1, n_2, n_1n_2\}$. Como G es 4-transitivo, existe $g \in G_x$ tal que

$$g \cdot \varphi(n_1) = \varphi(n_1), \quad g \cdot \varphi(n_2) = \varphi(n_2), \quad g \cdot \varphi(n_1n_2) = \varphi(n),$$

una contradicción pues $g \cdot \varphi(n_1n_2) = g(n_1n_2)g^{-1} = (gn_1g^{-1})(gn_2g^{-1}) = n_1n_2$. Luego $|N| = 4$.

Por último, si G es k-transitivo y $k > 4$, $|N| = 4$ y luego $k \leq |X| = |N| = 4$, una contradicción. □

18. Grupos primitivos

Definición 18.1. Sea X un G-conjunto. Diremos que un subconjunto $B \subseteq X$ es un **bloque** si para todo $g \in G$ se tiene que $g \cdot B = B$ o bien $g \cdot B \cap B = \emptyset$.

Ejemplo 18.2. Si X es un G-conjunto y $x \in X$, $\emptyset$, X y $\{x\}$ son los **bloques triviales** de X.

Definición 18.3. Un G-conjunto X se dice **primitivo** si X no contiene bloques no triviales.

Ejemplo 18.4. El grupo de permutaciones

$$G = \{\mathrm{id}, (123)(456), (132)(465), (15)(24)(36), (14)(26)(35), (16)(25)(34)\}$$

no es primitivo pues posee bloques no triviales tales como $\{1,2,3\}$ y $\{1,4\}$.

Un grupo G se dice **primitivo** si existe un G-conjunto X fiel y primitivo.

Ejemplo 18.5. El grupo $G = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ actúa transitivamente en $\{1,2,3,4\}$. Los subconjuntos $\{1,4\}$ y $\{2,3\}$ son bloques no triviales. Luego G no es primitivo.

proposition:primitive

Proposición 18.6. *Sea X un G-conjunto transitivo de grado n. Sea $B \subseteq X$ un bloque no trivial. Valen las siguientes afirmaciones:*

1. *Todo $g \cdot B$ es un bloque.*
2. *Existen $g_1, \ldots, g_m \in G$ tales que $\{g_1 \cdot B, \ldots, g_m \cdot B\}$ es una partición de X.*
3. *G actúa transitivamente en $\{g_1 \cdot B, \ldots, g_m \cdot B\}$ y $m = n/|B|$.*

Demostración. Demostremos la primera afirmación: Si existe $h \in G$ tal que

$$h \cdot (g \cdot B) \cap g \cdot B \neq \emptyset$$

entonces $(g^{-1}hg) \cdot B \cap B \neq \emptyset$. Como B es un bloque, esto implica que $(g^{-1}hg) \cdot B = B$ y luego $h \cdot (g \cdot B) = (hg) \cdot B = g \cdot B$.

Demostremos la segunda afirmación. Los $g \cdot B$ son disjuntos pues si $g \cdot B \neq h \cdot B$, $g, h \in G$, entonces $h^{-1}g \cdot B \neq B$. Luego $h^{-1}g \cdot B \cap B = \emptyset$ y entonces $g \cdot B \cap h \cdot B = \emptyset$ pues B es un bloque. Como G es transitivo en X,

$$\bigcup_{g \in G} g \cdot B = \bigcup_{j=1}^{m} g_j \cdot B = X.$$

La tercera afirmación es fácil: es obvio que el grupo G actúa transitivamente en $\{g_j \cdot B : 1 \leq j \leq m\} = \{g \cdot B : g \in B\}$ y $m|B| = n$ pues $|g \cdot B| = |B|$ para todo $g \in G$. □

Corolario 18.7. *Todo G-conjunto transitivo X de orden primo es primitivo.*

Demostración. Si $B \subseteq X$ es un bloque, $|B| \in \{1, |X|\}$ por la proposición 18.6. Luego B es trivial y entonces X es primitivo. □

Si X es un G-conjunto y $S \subseteq X$ es un subconjunto, se define el estabilizador conjuntista como

$$G_{(S)} = \{g \in G : g \cdot S = S\}.$$

Es fácil verificar que $G_{(S)}$ es un subgrupo de G.

lemma:primitivo_maximal

Lema 18.8. *Sea X un G-conjunto transitivo de grado n y sea $x \in X$. Si K es un subgrupo tal que $G_x \subseteq K$ entonces $K \cdot x$ es un bloque de tamaño $(K : G_x)$. Además la función*

$$\varphi \colon \{K : G_x \subseteq K \subseteq G\} \to \{\textit{bloques que contienen a } x\}, \quad K \mapsto K \cdot x,$$

es una biyección.

Demostración. Primero observamos que $K \cdot x$ es un bloque. Si $g \in G$ es tal que $g \cdot (K \cdot x) \cap K \cdot x \neq \emptyset$ entonces $g \in K$ pues existen $k_1, k_2 \in K$ tales que $(gk_1) \cdot x = k_2 \cdot x$ y entonces $k_2^{-1} g k_1 \in G_x \subseteq K$. Esto demuestra que $K \cdot x$ es un bloque y que

$$G_{(K\cdot x)} = K.$$

Como $K_x = K \cap G_x = G_x$, $|K\cdot x| = (K : K_x) = (K : G_x)$.

La función φ está bien definida. Es inyectiva pues si $\varphi(K_1) = \varphi(K_2)$ entonces

$$K_1 = G_{(\varphi(K_1))} = G_{(\varphi(K_2))} = K_2.$$

Veamos que φ es sobreyectiva. Sea $B \subseteq X$ un bloque tal que $x \in B$ y sea $K = G_{(B)}$. Sabemos que K es un subgrupo de G. Veamos que $G_X \subseteq K$. Si $g \in G_x$ entonces $g\cdot B \cap B \neq \emptyset$ pues $g\cdot x = x$; luego, como B es un bloque, $g\cdot B = B$. Afirmamos que $K\cdot x = \varphi(K) = B$. Si $k \in K$ entonces $k\cdot x \in B$ pues $x \in B$. Recíprocamente, si $b \in B$ entonces, como G es transitivo en X, existe $g \in G$ tal que $g\cdot x = b$. Como entonces $g \in K$ (pues $g\cdot B = B$ y $g\cdot B \cap B \neq \emptyset$), $b = g\cdot x \in K\cdot x$. □

Teorema 18.9. *Sea X un G-conjunto transitivo de grado n. Entonces G es primitivo si y sólo si cada G_x es un subgrupo maximal.*

Demostración. Sea $x \in X$ tal que G_x es maximal. Por el lema 18.8, los únicos bloques que contienen a x son $\{x\}$ y X. Si B es un bloque, existe $g \in G$ tal que $x \in g\cdot B$. Como $g\cdot B$ es un bloque que contiene a x, $g\cdot B = X$ o $g\cdot B = \{x\}$. Luego B es trivial.

Recíprocamente, supongamos que X es primitivo y sea $x \in X$. Como todo bloque que contiene a x es trivial, los únicos subgrupos que contienen a G_x son G_x y G. Luego G_x es maximal. □

lemma:2trans=>prim

Lema 18.10. *Si G es un grupo doblemente transitivo, G es primitivo.*

Demostración. Supongamos que G actúa en X y sea $B \subseteq X$ un bloque no trivial. Sean $x, y, z \in X$ tales que $x, y \in B$ y $z \notin B$. Como G es doblemente transitivo, existe $g \in G$ tal que $g\cdot x = y$ y $g\cdot y = z$. Luego $x \in B \cap g\cdot B$ y además $g\cdot B \neq B$, una contradicción. □

lemma:Gtrans+abel=reg

Lema 18.11. *Si G es abeliano y transitivo en X entonces G es regular.*

Demostración. Sea $x \in X$. Si $y \in X$ entonces existe $g \in G$ tal que $g\cdot x = y$. Como $G_y = G_{g\cdot x} = gG_xg^{-1} = G_x$, G_x fija a cualquier $y \in X$ y luego $G_x = 1$. □

lemma:GprimNtran

Lema 18.12. *Sea G un grupo primitivo. Si $N \neq 1$ es un subgrupo normal de G, entonces N es transitivo.*

Demostración. Sea B una N-órbita. Veamos que para cada $g \in G$, $g\cdot B$ es una N-órbita: si $x = g\cdot b_1 \in g\cdot B$, $y = g\cdot b_2 \in g\cdot B$ con $b_1, b_2 \in B$, entonces, como existe $n \in N$ tal que $n\cdot b_1 = b_2$, $gng^{-1} \in N$ (pues N es normal en G) y $gng^{-1}\cdot x = y$. Luego B es un bloque pues $g\cdot B \cap B = \emptyset$ o $g\cdot B = B$. Como G es primitivo, $|B| \in \{1, |X|\}$. Si $|B| = 1$, digamos $B = \{x\}$, entonces $N = 1$ pues

$$N = gNg^{-1} = gN_xg^{-1} = N_{g\cdot x} = N_y$$

para todo $y \in X$. Luego $B = X$ y N es transitivo. □

Teorema 18.13. *Sea G primitivo de grado n y sea $N \neq 1$ normal y abeliano. Entonces N es el único subgrupo minimal-normal de G y $n = |N| = p^m$ para algún primo p.*

Demostración. Por el lema 18.12, N es transitivo en X. Como N es abeliano, N es regular por el lema 18.11 y entonces $|N| = n$.

Veamos que $C_G(N) = N$. Sea $g \in C_G(N) \setminus N$ y sea $H = \langle g, N \rangle$. Como H es abeliano y transitivo en X (pues $N \subseteq H$), H es regular por el lema 18.11 y luego $|H| = n = |N|$, una contradicción.

Sea $M \neq 1$ un subgrupo normal de G. Supongamos que $M \cap N \neq 1$. Como $M \cap N$ es normal en G, es transitivo en X por el lema 18.12. Como $M \cap N$ es abeliano, $M \cap N$ es regular por el lema 18.11. Luego $|M \cap N| = n = |N|$ y entonces $N \subseteq M$. Supongamos ahora que $M \cap N = 1$. Como M y N son normales en G,

$$[M, N] \subseteq M \cap N = 1$$

y luego $M \subseteq C_G(N) = N$. Luego N es el único subgrupo minimal-normal de G. □

18. Conjuntos de Jordan

lemma:Jordan

Lema 18.1. *Sea G un grupo transitivo en $X = \{1, \ldots, n\}$. Sea H un subgrupo de G y sea $S \subseteq X$ una H-órbita. Si H es primitivo en S y $|S| > n/2$, entonces G es primitivo en X.*

Demostración. Sea $\emptyset \neq B \subsetneq X$ un bloque para la acción G. Vamos a demostrar que $B \cap S \subseteq S$ es un bloque para la acción de H. Si $h \in H$ es tal que $h \cdot (B \cap S) \neq B \cap S$ entonces, como $h \cdot (B \cap S) = h \cdot B \cap S$, $h \cdot B \neq B$. Luego $(h \cdot (B \cap S)) \cap (B \cap S) = \emptyset$ pues $h \cdot B \cap B = \emptyset$.

Como H es primitivo en S, hay tres posibilidades: a) $B \cap S = \emptyset$, b) $B \cap S = S$, y c) $B \cap S = \{x\}$ para algún $x \in X$. Si $B \cap S = S \subseteq B$ entonces, como $n/2 < |S| \leq |B|$ y $|B|$ divide a n, se concluye que $B = X$, una contradicción. Luego $|B \cap S| \leq 1$.

Sabemos que existen $g_1, \ldots, g_m \in G$ tales que

$$X = \bigcup_{j=1}^{m} g_j \cdot B$$

es una partición de X. Como cada $g_j \cdot B \subsetneq X$ es un bloque, $|(g_j \cdot B) \cap S| \leq 1$ para todo j. Además $m = n/|B|$ y entonces $|B| < 2$ pues

$$n/2 < |S| \leq m = n/|B|.$$

Luego $|B| = 1$. □

Definición 18.2. Sea G un grupo transitivo en X. Un subconjunto $S \subseteq X$ se dice **de Jordan** si el subgrupo

$$G_S = \{g \in G : g \cdot s = s \text{ para todo } s \in S\}$$

de G actúa transitivamente en $X \setminus S$, y S se dice **fuertemente de Jordan** si G_S actúa primitivamente en $X \setminus S$.

Ejemplo 18.3. Si G es 2-transitivo en X y $x \in X$, entonces $\{x\}$ es un conjunto de Jordan.

lemma:ScapT_Jordan

Lema 18.4. *Sea G un grupo que actúa transitivamente en X y sean $S, T \subseteq X$ subconjuntos (fuertemente) de Jordan tales que $S \cup T \neq X$. Entonces $S \cap T$ es (fuertemente) de Jordan.*

Demostración. Observemos que $G_S \cup G_T \subseteq G_{S\cap T}$ y que el estabilizador $G_{S\cap T}$ actúa en $X \setminus (S \cap T) = (X \setminus S) \cup (X \setminus T)$. Sean $x, y \in X \setminus (S \cap T)$. Como G_S es transitivo en $X \setminus S$ y G_T es transitivo en $X \setminus T$, basta ver que dados $x \in X \setminus S$ e $y \in X \setminus T$, existe $g \in G_{S\cap T}$ tal que $g \cdot x = y$. Sea

$$z \in X \setminus (S \cup T) = (X \setminus S) \cap (X \setminus T).$$

Sabemos que existen $g_1 \in G_S$ y $g_2 \in G_T$ tales que $g_1 \cdot x = z$ y $g_2 \cdot y = z$. Entonces $g = g_2^{-1} g_1 \in G_{S\cap T}$ y $g \cdot x = y$.

Supongamos ahora que $|S| \leq |T|$. Como $S \cup T \neq X$,

$$|X \setminus S \cap T| = |(X \setminus S) \cup (X \setminus T)| = |X \setminus S| + |X \setminus T| - |(X \setminus S) \cap (X \setminus T)| > 2|X \setminus S|.$$

Por hipótesis, G_S es primitivo en $X \setminus S$. Probamos que el subgrupo $G_{S\cap T}$ es transitivo en $X \setminus S \cap T$ y que $|X \setminus S| > \frac{1}{2}|X \setminus S \cap T|$. Por el lema 18.1, $G_{S\cap T}$ es primitivo en $X \setminus S \cap T$. □

proposition:Jordan

Proposición 18.5. *Sea G un grupo primitivo en X. Supongamos que existe $S \subseteq X$ un conjunto de Jordan tal que $0 < |S| < |X| - 1$. Entonces G es 2-transitivo en X. Si además S es fuertemente de Jordan entonces cada G_x es primitivo en $X \setminus \{x\}$.*

Demostración. Sea S es minimal entre los subconjuntos no vacíos (fuertemente) de Jordan. Vamos a demostrar que $|S| = 1$, y como todo conjunto de un elemento es de Jordan, el resultado quedaría demostrado.

Supongamos que $|S| > 1$. Vamos a considerar dos casos. Supongamos primero que $|S| < |X|/2$. Como $1 < |S| < |X|$ y G es primitivo, S no puede ser un bloque. Existe entonces $g \in G$ tal que $g \cdot S \neq S$ y $g \cdot S \cap S \neq \emptyset$. Como $|S \cup g \cdot S| \leq 2|S| < |X|$, se tiene $S \cup g \cdot S \neq X$; entonces, por el lema 18.4, $S \cap g \cdot S$ es (fuertmente) de Jordan, una contradicción pues $S \cap g \cdot S \subsetneq S$ y S es minimal.

Supongamos ahora que $|S| \geq |X|/2$. Sea $T = X \setminus S$. Como $|S| < |X| - 1$, se tiene que $|T| \notin \{1, |X|\}$. Como G es primitivo, T no es un bloque: existe $g \in G$ tal que $g \cdot T \neq T$ y $g \cdot T \cap T \neq \emptyset$. El conjunto S es (fuertemente) de Jordan, y entonces $g \cdot S$ también lo es. Luego, como

$$S \cup g \cdot S = (X \setminus T) \cup (X \setminus g \cdot T) = X \setminus (T \cap g \cdot T) \subsetneq X,$$

el lema 18.4 nos dice que $S \cap g \cdot S$ es (fuertemente) de Jordan. Como

$$\begin{aligned} |S| &\geq \frac{1}{2}|X| > \frac{1}{2}|S \cup g \cdot S| \\ &= \frac{1}{2}(|S| + |g \cdot S| - |S \cap g \cdot S|) = |S| - \frac{1}{2}|S \cap g \cdot S|, \end{aligned}$$

se concluye que $S \cap g \cdot S \neq \emptyset$. Luego $S \cap g \cdot S \subsetneq S$ es un conjunto (fuertemente) de Jordan, una contradicción a la minimalidad de S. □

theorem:Jordan

Teorema 18.6 (Jordan). *Sea G un grupo primitivo en X y sea $S \subseteq X$ un conjunto fuertemente de Jordan tal que $|S| \leq |X| - 2$. Entonces G es $(|S|+1)$-transitivo en X.*

Demostración. Supongamos que $|X| > 2$ y que $|S| > 0$. Procederemos por inducción en $|X|$. Sean $s \in S$ y $T = S \setminus \{s\}$. Como S es fuertemente de Jordan y vale que $|S| \leq |X| - 2$, la proposición 18.5 implica que G_s es primitivo en $X \setminus \{s\}$. El conjunto T es fuertemente de Jordan pues

$$G_S = (G_s)_T$$

es primitivo en $X \setminus S = (X \setminus \{s\}) \setminus T$. Como además $|T| \leq |X| - 3$, al aplicar la hipótesis inductiva con respecto a la acción de G_s en $X \setminus \{s\}$, obtenemos que G_s es $(|X|-1)$-transitivo en X. □

Corolario 18.7 (Jordan). *Sea $G \subseteq \mathbb{S}_n$ un grupo primitivo. Si G contiene una trasposición entonces $G = \mathbb{S}_n$.*

Demostración. Sea $X = \{1, \ldots, n\}$. Supongamos que $(xy) \in G$ y sea $S = \{x, y\}$. Como $(xy) \in G_S$, G_S actúa transitivamente en $X \setminus S = \{x, y\}$. Pero $X \setminus S = \{x, y\}$ tiene dos elementos, y entonces G actúa primitivamente en $X \setminus S$. Por el teorema de Jordan 18.6, G actúa $(n-1)$-transitivamente en X. □

Corolario 18.8. *Sea $G \subseteq \mathbb{S}_n$ un grupo primitivo. Si G contiene un 3-ciclo, entonces $G \in \{\mathbb{A}_n, \mathbb{S}_n\}$.*

Demostración. Supongamos que $(xyz) \in G$. Sean $X = \{1, \ldots, n\}$ y $S = X \setminus \{x, y, z\}$. Como $(xyz) \in G_S$, G_S es transitivo en $X \setminus S$. Como $X \setminus S = \{x, y, z\}$ tiene tres elementos, G_S es primitivo en $X \setminus S$. Como $|S| + 1 = n - 2$, G es $(n-2)$-transitivo en X por el teorema de Jordan 18.6. Luego

$$|G| = n(n-1) \cdots 3 |G_{x_1, \ldots, x_{n-2}}|.$$

El resultado se obtiene al observar que $|G_{x_1, \ldots, x_{n-2}}|$ divide a 2. □

18. Teoremas de Jordan y de Wagner

theorem:Jordan:k-1

Teorema 18.1 (Jordan). *Para $k \geq 2$ sea $G \neq \mathbb{S}_k$ un grupo k-transitivo y sea N un subgrupo normal no trivial. Entonces N es $(k-1)$-transitivo, a menos que $k = 3$ y N sea un 2-grupo elemental abeliano,*

Demostración. Procederemos por inducción en k. Si $k = 2$, G es primitivo y luego N es transitivo por los lemas 18.10 y 18.12.

Supongamos entonces que $k \geq 3$. Sea $x \in X$. Primero observemos que $G_x \neq \mathbb{S}_{k-1}$ pues $1 < (\mathbb{S}_k : G) = (\mathbb{S}_{k-1} : G_x)$. Como G_x es $(k-1)$-transitivo y N_x es normal en G_x, la hipótesis inductiva implica que estamos dentro de alguno de los siguientes casos: a) $N_x = 1$, b) N_x es $(k-2)$ transitivo, y c) $k = 4$ y N_x es un 2-grupo elemental abeliano.

Si $k = 4$, tendríamos que... completar

Supongamos que $N_x = 1$. Como N es regular y $k \neq 4$, $k = 3$ y N es un 2-grupo elemental abeliano por la proposición 18.24.

Supongamos ahora que N_x es $(k-2)$-transitivo. Como N es transitivo, entonces N_y es $(k-2)$-transitivo para todo $y \in X$. Luego N es $(k-1)$-transitivo. □

Ejemplo 18.2. Sea G el subgrupo de $\mathbb{S}_8$ generado por $(1346)(2857)$ y $(12)(4857)$; G es el grupo número 11686 de tamaño 1344 de la base de datos de grupos pequeños de GAP.

```
gap> gr := SmallGroup(1344, 11686);;
gap> GeneratorsOfGroup(gr);
[ (1,3,4,6)(2,8,5,7), (1,2)(4,8,5,7) ]
gap> MovedPoints(gr);
[ 1, 2, 3, 4, 5, 6, 7, 8 ]
```

El grupo G actúa 3-transitivamente en $\{1,\ldots,8\}$ y tiene un único subgrupo normal propio y no trivial, digamos N. El subgrupo N está generado por $(12)(36)(45)(78)$, $(17)(28)(35)(46)$, $(13)(26)$ y $(48)(57)$, es un grupo abeliano de orden ocho y actúa transitivamente en $\{1,2,\ldots,8\}$:

```
gap> Transitivity(gr, [1..8]);
3
gap> NormalSubgroups(gr);
[ Group(()), Group([ (1,2)(3,6)(4,5)(7,8),
  (1,7)(2,8)(3,5)(4,6), (1,3)(2,6),
  (4,8)(5,7) ]), Group([ (1,3,4,6)(2,8,5,7),
  (1,2)(4,8,5,7) ]) ]
gap> N := last[2];;
gap> IsAbelian(N);
true
gap> Order(N);
8
gap> Transitivity(N, [1..8]);
1
```

Como aplicación del teorema de Jordan vamos a demostrar un teorema de A. Wagner [7] que permite demostrar muy fácilmente la simplicidad de ciertos grupos lineales.

theorem:Wagner

Teorema 18.3 (Wagner). *Sea G un grupo 3-transitivo de grado impar $d > 3$. Si N es un subgrupo normal no trivial, entonces N es también 3-transitivo.*

Demostración. Supongamos que G actúa en el conjunto X. Los lemas 18.10 y 18.12 implican que N es transitivo en X y entonces el orden de N divide a $|X| = d$, que es un número impar. Por el teorema de Jordan 18.1, N es entonces 2-transitivo en X. Sean $x, y \in X$ elementos distintos y sea $S = \{x, y\}$.

El grupo $N_{(S)}$ actúa en $X \setminus S$; veamos que todas las $N_{(S)}$-órbitas tienen el mismo tamaño. Sean $u, v \in X \setminus S$. Como G es 3-transitivo, existe $g \in G$ tal que $g \cdot x = x$, $g \cdot y = y$, $g \cdot u = v$. Entonces, como la conjugación por g es un automorfismo,

$$\begin{aligned} |N_{(S)} \cdot u| &= (N_{(S)} : (N_{(S)})_u) = (gN_{(S)}g^{-1} : g(N_{(S)})_u g^{-1}) \\ &= (N_{(S)} : (N_{(S)})_{g\cdot u}) = (N_{(S)} : (N_{(S)})_v) = |N_{(S)} \cdot v|. \end{aligned}$$

Hay k órbitas de tamaño l; como $kl = n-2$ es impar, l es impar.

Afirmación. $N_{(S)} = N_{x,y} \sqcup nN_{x,y}$ para algún $n \in$N. En particular, $N_{x,y}$ es normal en $N_{(S)}$.

Como N es 2-transitivo, existe $n \in N$ tal que $n \cdot x = y$, $n \cdot y = x$. Es fácil ver que $N_{x,y} \cap nN_{x,y} = \emptyset$ pues si existe $m \in N_{x,y}$ tal que $nm \in N_{x,y}$ entonces $nm \cdot x = y$, una contradicción. Si $m \in N_{(S)} \setminus N_{x,y}$ entonces $n^{-1}m \in N_{x,y}$.

Afirmación. Para todo $u \in X \setminus S$ se tiene $N_{(S)} \cdot u = N_{x,y} \cdot u$. En particular, todas las $N_{x,y}$-órbitas tienen el mismo tamaño.

Sabemos que $N_{x,y} \cdot u \subseteq N_{(S)} \cdot u$. Si la inclusión fuera estricta, tendríamos

$$l = |N_{(S)} \cdot u| = |N_{x,y} \cdot u| + |nN_{x,y} \cdot u| = 2|N_{x,y} \cdot u|$$

pues, como $nN_{x,y} \cdot u = nN_{x,y}n^{-1} \cdot (n \cdot u) = N_{x,y} \cdot (n \cdot u)$, entonces $|N_{x,y} \cdot u| = |nN_{x,y} \cdot u|$, una contradicción.

Afirmación. $k = 1$.

Supongamos que $k \geq 2$. Sea $P \in \mathrm{Syl}_2(N_{(S)})$ y sea $\sigma \in P$. Como cada órbita $N_{(S)} \cdot u$ tiene tamaño impar, σ tiene al menos un punto fijo en $N_{(S)} \cdot u$. Luego σ tiene al menos k puntos fijos (uno en cada $N_{(S)}$-órbita), digamos

$$\sigma = (a)(b)\sigma_1, \quad a, b \in X \setminus S.$$

Como N es 2-transitivo, existe $n \in N$ tal que $n \cdot a = x$, $n \cdot b = y$. Esto implica que $n\sigma n^{-1} \in N_{x,y}$. Demostramos entonces que $P \subseteq n^{-1}N_{x,y}n$ y luego $|P|$ divide a $|n^{-1}N_{x,y}n| = |N_{x,y}| = |N_{(S)}|/2$, una contradicción. □

Ejercicio 18.4. Utilice el teorema de Wagner para demostrar que $\mathbb{A}_5$ es simple.

Aplicación: transformaciones de Moebius

Sean p un número primo y $k = \mathsf{GF}(p^n)$ el cuerpo finito de p^n elementos. Sea $\widetilde{k} = k \cup \{\infty\}$, donde por convención definimos

$$1/\infty = 0, \quad 1/0 = \infty, \quad \infty/\infty = 1, \quad 1 - \infty = \infty - 1 = \infty.$$

Una **transformación de Möbius** es una función $f\colon \widetilde{k} \to \widetilde{k}$ de la forma

$$f(x) = \frac{ax+b}{cx+d},$$

donde $a, b, c, d \in \widetilde{k}$ son tales que $ad - bc \neq 0$. El conjunto $L(p^n)$ de transformaciones de Möbius forma un grupo con la composición de funciones.

Ejercicio 18.5. Demuestre que $L(p^n) \simeq \mathbf{PGL}(2, p^n)$.

Es fácil verificar que la función

$$\varphi\colon \mathbf{GL}_2(p^n) \to L(p^n), \quad \varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = x \mapsto \frac{ax+b}{cx+d}$$

es un morfismo sobreyectivo de grupos. Además

$$\ker\varphi = Z(\mathbf{GL}_2(p^n)) = \{\lambda I : \lambda \in k\}.$$

Como $\varphi(\lambda I) = \mathrm{id}$, existe un único isomorfismo $\mathbf{PGL}_2(p^n) \to L(p^m)$ tal que el diagrama

$$\begin{array}{ccc} \mathbf{GL}_2(p^n) & \xrightarrow{\varphi} & L(p^n) \\ \downarrow & \nearrow & \\ \mathbf{PGL}_2(p^n) & & \end{array}$$

conmuta.

Lema 18.6. *El grupo $L(p^n)$ actúa fuerte y 3-transitivamente en $\widetilde{k}$. En particular, $|L(p^n)| = p^n(p^n+1)(p^n-1)$.*

Demostración. Sea $L = L(p^n)$. El grupo L actúa transitivamente en $\widetilde{k}$ pues el subgrupo $\{x \mapsto x + b : b \in k\}$ actúa transitivamente en $k \setminus \{0\}$ y además si $g(x) = \frac{1}{x}$ entonces $g(0) = \infty$ y $g(\infty) = 0$. El estabilizador

$$L_\infty = \{x \mapsto ax + b : a, b \in k, a \neq 0\}$$

es fuertemente 2-transitivo en k pues si $\alpha_1 \neq \alpha_2$ y $\beta_1 \neq \beta_2$ son elementos de k, el sistema

$$\begin{cases} a\alpha_1 + b = \beta_1, \\ a\alpha_2 + b = \beta_2, \end{cases}$$

tiene solución única. Luego $L(p^n)$ es fuertemente 3-transitivo de grado $|\widetilde{k}| = p^n + 1$. En particular, $|L(p^n)| = (p^n+1)p^n(p^n-1)$ por la proposición 18.18. □

Corolario 18.7. *Para todo $n \geq 2$, $L(2^n)$ es un grupo simple.*

Demostración. Sea N un subgrupo normal no trivial de $L(2^n)$. Como $L(2^n)$ es 3-transitivo y de grado impar, N es también 3-transitivo por el teorema de Wagner 18.3. En particular, N es fuertemente 3-transitivo pues $N_{x,y,z} = G_{x,y,z} \cap N = 1$ para todo x, y, z. Luego $N = G$ pues $|N| = 2^n(2^n-1)(2^n-2) = |G|$. □

Capítulo 19
Algunos grupos simples

19. Criterios

theorem:primitivo_simple

Teorema 19.1. *Sea $G \subseteq \mathbb{S}_n$ un grupo primitivo tal que algún G_j es simple. Entonces G es simple o todo subgrupo normal no trivial N es regular.*

Demostración. Sea N un subgrupo normal de G no trivial. Como N es transitivo y $N \cap G_j$ es normal en G_j, $N \cap G_j \in \{1, G_j\}$. Si $N \cap G_j = 1$ entonces N es regular. En cambio, si $G_j = N \cap G_j \subseteq N$, entonces, como G_j es maximal $N = G$ (el caso $G_j = N$ queda excluido porque N es transitivo); luego G es simple. □

Como primera aplicación vamos a demostrar que el grupo alternado $\mathbb{A}_n$ es simple si $n \geq 5$.

lemma:A5_simple

Lema 19.2. *El grupo $\mathbb{A}_5$ es simple.*

Demostración. Sea $N \neq 1$ un subgrupo normal de $\mathbb{A}_5$. Como $\mathbb{A}_5$ es triplemente transitivo, es primitivo y entonces N es transitivo. En particular, $(N : N_j) = 5$ para todo $j \in \{1, \ldots, 5\}$. Sea $\sigma \in N$ tal que $|\sigma| = 5$. Sin pérdida de generalidad podemos suponer que $\sigma = (12345)$. Entonces $P = \langle \sigma \rangle \in \mathrm{Syl}_5(N)$ y como $|\mathbb{A}_5| = 2^2 \cdot 3 \cdot 5$, $P \in \mathrm{Syl}_5(\mathbb{A}_5)$. Como cantidad m de 5-subgrupos de Sylow de N divide a 60 y por el teorema de Sylow $n \equiv 1$ mód 5, entonces $m \in \{1, 6\}$. Si P fuera normal en N, sería característico en N y entonces sería normal en $\mathbb{A}_5$, una contradicción pues

$$(123)\sigma(123)^{-1} = (23145) \notin P.$$

Luego $m = 6$ y entonces 30 divide al orden de N, es decir $|N| \in \{30, 60\}$. Si $|N| = 30$ entonces existe $\sigma \in N$ de orden dos, digamos $\sigma = (ab)(cd)$. Como N es normal,

$$\{\mathrm{id}, (ab)(cd), (ac)(bd), (ad)(bc)\} \subseteq N,$$

una contradicción pues 4 no divide a 30. Probamos entonces que $N = \mathbb{A}_5$. □

theorem:An_simple

Teorema 19.3. *Si $n \geq 5$ entonces $\mathbb{A}_n$ es simple.*

Demostración. Procederemos por inducción en n. El caso $n = 5$ es el lema 19.2. Supongamos entonces que $n \geq 6$ y que $\mathbb{A}_{n-1}$ es simple. Como $\mathbb{A}_n$ es 4-transitivo de grado $n > 4$, $\mathbb{A}_n$ no tiene subgrupos normales regulares (proposición 18.24). El teorema 19.1 implica que $\mathbb{A}_n$ es simple pues $(\mathbb{A}_n)_j \simeq \mathbb{A}_{n-1}$ es simple. □

19. Grupos de Mathieu

Vamos a demostrar que los grupos de Mathieu M_{11} y M_{23} son simples. Seguiremos la demostración de [2].

lemma:p||G| **Lema 19.1.** *Sea $G \leq \mathbb{S}_p$. Entonces G es transitivo si y sólo si p divide a $|G|$.*

Demostración. Si p divide a $|G|$ entonces existe $g \in G$ de orden p. Como $g \in \mathbb{S}_p$, el elemento g es un p-ciclo y luego G es transitivo. Si G es transitivo y $j \in \{1,\ldots,p\}$ entonces $p = (G : G_j)$. Luego p divide a $|G|$. □

lemma:ne **Lema 19.2.** *Si $G \leq \mathbb{S}_p$ es transitivo y $|\mathrm{Syl}_p(G)| > 1$ entonces $P \subsetneq N_G(P)$.*

Demostración. Como G es transitivo, p divide a $|G|$ por el lema 19.1 y luego todo p-subgrupo de Sylow de G tiene orden p. Entonces, dos subgrupos de Sylow distintos van a tener intersección trivial. Por uno de los teoremas de Sylow podemos escribir

$$|G| = |P|(N_G(P) : P)(G : N_G(P)) = p(N_G(P) : P)|\mathrm{Syl}_p(G)|. \tag{19.1}$$ equation:GPN

Supongamos que $P = N_G(P)$. Sea $F = \{g \in G : g(j) = j \text{ para algún } j\}$. Como G tiene exactamente $|\mathrm{Syl}_p(G)|(p-1)$ elementos de orden p, entonces, al escribir

$$G = F \sqcup (G \setminus F)$$

y observar que los elementos de orden p pertenecen al conjunto $G \setminus F$, se concluye que G tiene a lo sumo $|\mathrm{Syl}_p(G)|$ elementos que fijan algún punto de $\{1,\ldots,p\}$. En efecto, como $|G| - |\mathrm{Syl}_p(G)|(p-1) \geq |F|$,

$$|F| \leq |G| - |\mathrm{Syl}_p(G)|(p-1) = |G| - \frac{|G|}{p}(p-1) = |G|/p = |\mathrm{Syl}_p(G)|.$$

Como $(G : G_j) = p$ para todo $j \in \{1,\ldots,p\}$, la igualdad (19.1) implica entonces que $|G_j| = |\mathrm{Syl}_p(G)|$ para todo $j \in \{1,\ldots,p\}$. Luego $F = \bigcup_{j=1}^{p} G_j$ tiene $|\mathrm{Syl}_p(G)|$ elementos y entonces $G_1 = G_2 = \cdots = G_p$. En particular, $1 = |G_1| = |\mathrm{Syl}_p(G)|$. □

lemma:1/2 **Lema 19.3.** *Sea G un grupo transitivo y sea N normal en G. Entonces G actúa transitivamente en el conjunto de N-órbitas y todas las N-órbitas tienen el mismo tamaño.*

Demostración. Sean $x, y \in X$ y sea $g \in G$ tal que $g \cdot x = y$. Como N es normal en G y la conjugación por g es un automorfismo,

$$|N \cdot x| = (N : N_x) = (gNg^{-1} : gN_xg^{-1}) = (N : N_{g\cdot x}) = (N : N_y) = |N \cdot y|.$$

□

Teorema 19.4. *Sea p un número primo. Sea $G \leq \mathbb{S}_p$ transitivo tal que $|G| = pmr$ con $m > 1$, $m \equiv 1$ mód p, $r < p$ y r primo. Entonces G es simple.*

Demostración. Sea N un subgrupo normal no trivial de G. Por el lema 19.3 el grupo G actúa transitivamente en las N-órbitas y todas las N-órbitas tienen el mismo tamaño $s \in \{1, p\}$. Si $s = 1$ entonces, como $N \leq \mathbb{S}_p$, se tiene que $N = 1$, una contradicción. Luego $s = p$ y N es transitivo en $\{1, \ldots, p\}$. Como p divide entonces a $|N|$, algún $P \in \mathrm{Syl}_p(G)$ de Sylow está contenido en N. Luego, como

$$gPg^{-1} \subseteq gNg^{-1} = N$$

para todo $g \in G$ y los p-subgrupos de Sylow de G son conjugados, todos los p-subgrupos de Sylow de G están contenidos en N. En particular, como la cantidad de p-subgrupos de N es igual a $m = (G : N_G(P)) = (N : N_N(P))$,

$$|N| = |P|(N_N(P) : P)(N : N_N(P)) = pmt,$$

donde $t = (N_N(P) : P)$ un divisor de r. Por el lema 19.2, $t \neq 1$. Luego $t = r$ pues r es primo y entonces $N = G$. □

Teorema 19.5. *El grupo M_{11} es simple.*

Demostración. Pues $M_{11} \leq \mathbb{S}_{11}$ es transitivo de orden $7920 = pmr$, donde $p = 11$, $m = 144 > 1$ y $r = 5$. □

Teorema 19.6. *El grupo M_{23} es simple.*

Demostración. Pues $M_{23} \leq \mathbb{S}_{23}$ es transitivo de orden $10200960 = pmr$, donde $p = 11$, $m = 40320 > 1$ y $r = 11$. □

Referencias

1. Research problems. *Bull. Amer. Math. Soc.*, 63(3):209, 1957.
2. R. J. Chapman. An elementary proof of the simplicity of the Mathieu groups M_{11} and M_{23}. *Amer. Math. Monthly*, 102(6):544–545, 1995.
3. M. Deakonesku and G. L. Uolls. On the orbits of automorphism groups. *Sibirsk. Mat. Zh.*, 46(3):533–537, 2005.
4. W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.
5. P. R. Halmos and H. E. Vaughan. The marriage problem. *Amer. J. Math.*, 72:214–215, 1950.
6. I. M. Isaacs. Group actions and orbits. *Arch. Math. (Basel)*, 98(5):399–401, 2012.
7. A. Wagner. Normal subgroups of triply-transitive permutation groups of odd degree. *Math. Z.*, 94:219–222, 1966.

Índice alfabético