CLASIFICACIÓN DE GRUPOS PEQUEÑOS

1. Técnicas de clasificación

Vamos a usar conceptos que hemos visto para clasificar todos los grupos G de orden n. Los que sean abelianos ya los sabemos clasificar. Para el resto, vamos a seguir el siguiente esquema:

1. Buscamos un subgrupo $H \leq G$ de tamaño lo mayor posible, por ejemplo usando el teoream de Sylow.
2. Si H tiene índice k en G, la acción en el cociente G/H da un homomorfismo $G \to S_k$, por lo que si $|G| = n \nmid k! = |S_k|$ tenemos un núcleo no trivial $N \leq H$ normal en G (el corazón de H).
3. Usamos N para cocientar G/N, y a partir de eso acotar las posibilidades para G.
4. Si conocemos ejemplos de grupos que se comportan como los que quedan en el punto anterior, ya tenemos todos los de ese orden.

Vamos a hacer un ejemplo que muestre cómo usar dicho esquema. Clasifiquemos los grupos de orden 6. Si $|G| = 6$, sabemos que tiene un subgrupo H de orden 3. La acción de G en el cociente G/H nos da un homomorfismo $G \to S_2$, y como $|G| = 6 \nmid 2 = |S_2|$ no puede ser inyectivo, luego tiene un núcleo $1 \neq N \leq H$, el corazón de H. Como $|H| = 3$, debemos tener $N = H$, luego tenemos un subgrupo normal de orden 3.

Tenemos que como $|N| = 3$ y $|G/N| = 2$, se cumple que $N \cong C_3$ y $G/N \cong C_2$. En particular, G es resoluble y tenemos la parametrización única

$$G = \{a^i b^j : i < 2, j < 3\}$$

con $|b| = 3$ y $2||a|$. Por tanto $|a| = 6$ o $|a| = 2$. Si $|a| = 6$ tenemos que G es cíclico y por tanto $G \cong C_6$. Si $|a| = 2$, sólo nos queda ver cuánto es $a^{-1}ba$. Como $N = \langle b \rangle$ es normal en G, tenemos que en principio las posibilidades

$$a^{-1}ba = e \qquad a^{-1}ba = b \qquad a^{-1}ba = b^{-1}.$$

La primera no es posible, y la segunda daría que G es abeliano, luego quedaría de nuevo C_6. Así, la única posible es $a^{-1}ba = b^{-1}$. Luego queda un sólo grupo posible no abeliano, y como ya tenemos D_3, debe de ser ese grupo.

2. Restricciones en la multiplicación

De los cuatro puntos de la sección anterior, el que apenas hemos tratado por ahora es el 3. La idea es que sabemos que para todo $g \in G$, $c_g(x) = g^{-1}xg$ es un automorfismo de G. Pero además, si N es normal en G tenemos que su restricción a N es un automorfismo de N. Pero además, si $|g| = d$, entonces

$$c_g^d(n) = c_g \circ c_g \circ \ldots \circ c_g(n) = g^{-d}ng^d = n \qquad \forall n \in N$$

luego el orden de c_g en $\mathrm{Aut}(N)$ debe dividir a d. Podemos resumir esto como

Lema 2.1. *Sea $N \lhd G$. Para todo $g \in G$ de orden d, tenemos que $c_g \in Aut(N)$ y el orden de c_g divide a d, por lo que $|c_g|$ divide a d y a $|Aut(N)|$.*

Para poder usar este resultado, veamos que

Lema 2.2. *Tenemos que $Aut(C_n) \cong \mathbb{Z}_n^\times$.*

Demostración. Tenemos que cualquier isomorfismo de C_n en C_n debe enviar el generado $g_{2\pi/n}$ a otro generador $g_{2pi/n}^j$, es decir, que j debe ser coprimo con n. Si llamamos f_j al automorfimo que hace eso, vemos que $f_j \mapsto \overline{j}$ nos da el ismorfismo del enunciado, ya que

$$f_k \circ f_j(g_{2\pi/n}) = g_{2pi/n}^{jk} = f_{kj}(g_{2\pi/n}).$$

□

También vamos a usar que $\mathbb{Z}_p^\times$ *es cíclico* si p es primo, es decir $\mathbb{Z}_p^\times \cong C_{p-1}$. Por un ejercicio del tema A2, esto equivale a ver que $x^m = \overline{1}$ tiene como mucho m soluciones $x \in \mathbb{Z}_p^\times$ para todo $m| \mid |\mathbb{Z}_p^\times|$. La cuestión es que en los polinomios $\mathbb{Z}_p[x]$ tenemos un algoritmo de la división exactamente igual que en $\mathbb{C}[x]$, y por dicho algoritmo es inmediato ver que cualquier polinomio de grado m tiene a lo sumo m soluciones.

3. Orden $2p$

Veamos cómo usar el esquema descrito en el apartado anterior para clasificar los grupos de orden $2p$, con p primo $p > 2$. Ya conocemos dos grupos distintos de dicho orden, C_{2p} y D_p. Veamos que son los únicos.

Vamos a hacerlo en el caso $|G| = 2 * 5 = 10$ para verlo más claro y luego vemos que el mismo esquema funciona en general. Por Sylow tenemos un subgrupo H de orden 5, y por la acción en el cociente un homomorfismo $G \to S_2$, y como $10 \nmid 2$ vemos que debe tener un núcleo no trivial, luego $N = H$ es un subgrupo normal.

Ahora, $G/N \cong C_2$ y $N \cong C_5$. Por tanto, G es resoluble y se puede parametrizar de forma única como

$$G = \{a^i b^j : i < 2, j < 5\}.$$

con $|b| = 5$, $N = \langle b \rangle$ y $2 \mid |a|$. De nuevo el caso $|a| = 10$ da lugar a $G \cong C_{10}$, luego asumimos que $|a| = 2$.

Ahora, queremos ver que posibles ds hay para $a^{-1}ba = b^d$. Usamos que $n \mapsto a^{-1}na$ debe ser un automorfismo de N de orden que divide a 2. Si su orden es 1, tendríamos $a^{-1}ba = b$, luego G sería abeliano, $G \cong C_{10}$. Si es de orden 2, como $Aut(N) \cong \mathbb{Z}_5^\times$, y la única solución de $x^2 = \overline{1}$ en $\mathbb{Z}_5^\times$ es $x = \pm 1$, tenemos que $a^{-1}ba = b^{-1}$. Esto nos da un sólo grupo no abeliano, que debe ser por tanto D_5.

Si repasamos los pasos, vemos que funcionan exactamente igual en el caso de orden $2p$. Luego los grupos de orden $2p$ son C_{2p} y D_p.

4. Orden qp

Vamos a seguir las mismas ideas que en el apartado anterior para grupos de orden qp con $2 < q < p$. Comencemos por el caso más sencillo, el de grupos de orden $3 * 5 = 15$. Si $|G| = 15$, por Sylow tiene un subgrupo H de orden 5. Por la acción en el cociente tenemos un homomorfismo $G \to S_3$ y como $15 \nmid 6$ vemos que da un núcleo $N \leq H$ no trivial, luego $H = N$ es normal. Por tanto $N \cong C_5$ y $G/N \cong C_3$, luego

$$G = \{a^i b^j : i < 3, j < 5\}$$

con $|b| = 5$, $N = \langle b \rangle$, y $3 \mid |a|$. De nuevo si $|a| = 15$ tenemos que $G \cong C_{15}$ luego asumimos que $|a| = 3$. Sólo queda ver los posibles ds en $a^{-1}ba = b^d$.

Como $n \mapsto a^{-1}na$ está en $\mathrm{Aut}(N) \cong \mathbb{Z}_5^\times$ que es de orden 4, tenemos que su orden debe dividir a 4 y a $3 = |a|$, luego sólo puede ser 1. Pero entonces $a^{-1}ba = b$ que da que G es abeliano luego $G \cong C_{15}$.

Así, el único grupo de orden 15 es C_{15}. Como $|\mathbb{Z}_p^\times| = p - 1$, vemos que el mismo argumento funciona siempre que $q \nmid p - 1$. En estos casos el único grupo de orden qp es C_{qp}.

Vamos a tratar el caso $q \mid p - 1$. La primera vez que ocurre es para órden $3 * 7 = 21$. Veamos que en estos casos conocemos algún grupo no abeliano de dicho orden. $|\mathrm{GL}(2, \mathbb{Z}_p)| = (p-1)^2 p(p+1)$, y $qp \mid (p-1)p$, luego podría ser que lo encontremos entre sus subgrupos. De hecho, si miramos al subgrupo contenido en las triangulares superiores

$$\mathrm{Aff}(\mathbb{Z}_p) = \{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Z}_p^\times, y \in \mathbb{Z}_p \}$$

vemos que tiene orden $(p-1)p$. Tenemos que

$$\begin{pmatrix} x_1 & y_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x_2 & y_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x_1x_2 & y_1 + x_1y_2 \\ 0 & 1 \end{pmatrix}$$

luego vemos que es un grupo no abeliano, y además que si restringimos $x \in \mathbb{Z}_p^\times$ a un subgrupo cualquiera de $J \leq \mathbb{Z}_p^\times$, obtenemos un subgrupo de $\mathrm{Aff}(\mathbb{Z}_p)$ de orden $|J|p \mid (p-1)p$. En nuestro caso, si tomamos

$$\mathrm{Aff}_q(\mathbb{Z}_p) = \{\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x, y \in \mathbb{Z}_p, x^q = \overline{1}\} \leq \mathrm{Aff}(\mathbb{Z}_p).$$

vemos que es un grupo de orden qp. Le llamamos $\mathrm{Aff}(\mathbb{Z}_p)$ porque es claramente isomorfo al grupo de transformaciones afines biyectivas $\mathbb{Z}_p \to \mathbb{Z}_p$, es decir

$$\mathrm{Aff}(\mathbb{Z}_p) = \{f_{a,b} : a \in \mathbb{Z}_p^\times, b \in \mathbb{Z}_p\}$$

con $f_{a,b}(z) = az + b$. En nuestro caso de grupos de orden $3 * 7 = 21$, vemos que

$$\mathrm{Aff}_3(\mathbb{Z}_7) = \{\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x = \overline{1}, \overline{2}, \overline{4};\ y \in \mathbb{Z}_7\}.$$

Vamos a ver que los únicos grupos de orden 21 son C_{21} y $\mathrm{Aff}_3(\mathbb{Z}_7)$. Si $|G| = 21$ entonces por Sylow tenemos un subgrupo H de orden 7, que la acción en el cociente G/H da un homomorfismo $G \to S_3$, y como $21 \nmid 6$ tenemos que $N = H$ es el núcleo, luego es normal. Por tanto, $N \cong C_7$ y $G/N \cong C_3$, lo que da

$$G = \{a^i b^j : i < 3, j < 7\}$$

con $|b| = 7$, $N = \langle b \rangle$ y $3 \mid |a|$. Como antes, sólo el caso $|a| = 3$ da lugar a grupos no abelianos. Así, queremos ver qué posibilidades hay para $a^{-1}ba = b^d$. Como debe corresponder a un elemento de $Aut(N) \cong \mathbb{Z}_7^\times$ que sea de orden 3 (ya que uno de orden uno corresponde de nuevo a G abeliano), entonces las únicas posibilidades son $a^{-1}ba = b^2$ y $a^{-1}ba = b^4$, ya que $\overline{2}$ y $\overline{4}$ son los elemento de orden 3 de $\mathbb{Z}_7^\times$. Así, vemos que aparentemente hay dos grupos no abelianos.

Pero si nos fijamos en $\mathrm{Aff}_3(\mathbb{Z}_7)$, vemos que podemos elegir como generadores

$$a = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad b = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad \text{con} \qquad a^{-1}ba = b^4$$

o

$$a = \begin{pmatrix} \overline{4} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad b = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad \text{con} \qquad a^{-1}ba = b^2$$

y como en cualquier caso $|a| = 3$ y $|b| = 7$, tenemos que ambas posibilidades corresponden en realidad al mismo grupo, $\mathrm{Aff}_3(\mathbb{Z}_7)$.

Repitiendo este procecidimiento en el caso general de un grupo de orden qp con $q \mid p-1$, se puede ver $a^{-1}ba = b^d$ con $\overline{d}$ un elemento de cualquiera de orden q en $\mathbb{Z}_p^\times$. Aunque haya $q-1$ posibilidades, todas vienen de elegir diferentes generadores

$$a = \begin{pmatrix} \overline{d^{-1}} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad b = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \qquad \text{que cumple} \qquad a^{-1}ba = b^d,$$

de $\mathrm{Aff}_q(\mathbb{Z}_p)$, luego todas corresponden al mismo grupo. Así, en el caso $q \mid p-1$ sólo hay dos grupos de orden qp, C_{qp} y $\mathrm{Aff}_q(\mathbb{Z}_p)$.

5. Órdenes pequeños: Orden 8

Vamos a ver cómo clasificar otros casos de órdenes pequeños con las mismas ideas. Si $|G| = p^2$ ya sabemos que como su centro es no trivial, debe ser abeliano, luego isomorfo a C_{p^2} o $C_p \times C_p$. Con esto y los casos p y qp que hemos visto ya, cubrimos la mayoría de grupos de orden pequeño.

El primero que no cubrimos es el de orden 8. Aparte de los abelianos $C_8, C_4 \times C_2, C_2^3$, conocemos dos grupos no abelianos de orden 8: D_4 y $\mathrm{O}(2, \mathbb{Z}_3)$. Este último no es isomorfo a D_4 porque el número de elementos de orden 2 en ambos grupos varía; es isomorfo al grupo de cuaterniones.

Si $|G| = 8$ no abeliano, veamos que siempre tiene un elemento de orden 4. Si no fuera así, todos serían de orden 2, es decir $x^{-1} = x$ para todo $x \in G$. Si $a^{-1} = a$, $b^{-1} = b$ y $(ab)^{-1} = ab$, como $(ab)^{-1} = b^{-1}a^{-1} = ba$, tendríamos que $ab = ba$, luego G sería abeliano.

Así, existe un elemento b de orden 4 en G. Mirando al subgrupo N que genera, debe ser normal porque es de índice 2. Así, tenemos que

$$G = \{a^i b^j : i < 2, j < 4\},$$

con $|b| = 4$. Además, $a^{-1}ba$ debe ser un elemento de $\langle b \rangle$ de orden igual que b, y para que sea no G no abeliano la única posibilidad es $a^{-1}ba = b^{-1}$.

Además, a debe tener orden 2 o 4 (si fuera 8 el grupo sería abeliano). Esto da lugar a dos posibles grupos. Como tenemos dos grupos no isomorfos y no abelianos, D_4 y $\mathrm{O}(2, \mathbb{Z}_3)$, deben ser ellos.

6. Orden 12

Tenemos dos grupos abelianos de orden 12, C_{12} y $C_6 \times C_2$. En el caso no abeliano, conocemos los grupos D_6 y A_4, que son no isomorfos porque A_4 no tiene elementos de orden 6. Si observamos los grupos de matrices, vemos que podemos encontrar otro subgrupo, parecido al que vimos para orden qp. Tenemos que $\mathrm{Aff}(\mathbb{Z}_{15})$ tiene orden $|\mathbb{Z}_{15}^\times|15 = 8*15 = 2*4*3*5$, múltiplo de 12, y podemos observar que el subgrupo

$$\mathrm{Aff}_{4,3}(\mathbb{Z}_{15}) = \{\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x, y \in \mathbb{Z}_{15}, x^4 = \overline{1}, \overline{3}y = \overline{0}\}$$

tiene orden 12, y no es isomorfo a D_6 o A_4 porque tiene elementos de orden 4.

Vamos a ver que esos son todos los grupos de orden 12. Si $|G| = 12$, entonces por Sylow tenemos un subgrupo H de orden 3. Por la acción en el cociente tenemos un homomorfismo de $G \to S_4$. Pero ahora $|G| = 12 \mid 24 = |S_4|$, así que podría ser un encaje. Pero si es un encaje, G sería isomorfo a un subgrupo de orden 12 de S_4, y el único subgrupo de orden 12 de S_4 es A_4, así que en ese caso $G \cong A_4$.

Eso nos deja con el caso en que el homomorfismo $G \to S_4$ anterior no es un encaje. En ese caso $N = H$ debe ser el núcleo, por lo que N es normal de orden 3, luego $N \cong C_3$ y $|G/N| = 4$, luego $G/N \cong C_4$ o $G/N \cong C_2 \times C_2$. En el primer caso

$$G = \{a^i b^j : i < 4, b < 3\}$$

con $|b| = 3$, $N = \langle b \rangle$ y $4 \mid |a|$. Si $|a| = 12$ estaríamos en el caso cíclico, así que podemos asumir $|a| = 4$. Sólo nos quedan ver los posibles ds en $a^{-1}ba = b^d$. Como conjugación por a debe ser un automorfimo de N de orden 2 o 4 (para que no dé el abeliano), y $\mathrm{Aut}(N) \cong \mathbb{Z}_3^\times$ tiene orden 2, entonces debe tener orden 2 y el único posible es el correspondiente a $\overline{-1} \in \mathbb{Z}_3^\times$, que da $a^{-1}ba = b^{-1}$. Por tanto, sólo hay un posible grupo de este tipo, que debe ser $\mathrm{Aff}_{4,3}(\mathbb{Z}_{15})$.

En el segundo caso, $G/N \cong C_2 \times C_2$. En este caso, vamos a ver que siempre podemos encontrar un subgrupo cíclico M de orden 6, luego normal en G. Usando dicho subgrupo $M \cong C_6$, $G/M \cong C_2$, es posible ver, como $\mathbb{Z}_6^\times = \{\overline{1}, \overline{-1}\}$, que sólo hay una posibilidad no abeliana para G, que debe ser por tanto D_6. Como $G/N \cong C_2 \times C_2$, tenemos la parametrización

$$G = \{a^i b^j c^k : i, j < 2, k < 3\}$$

con $|c| = 3$, $N = \langle c \rangle$. Tenemos que $a^{-1}ca$ es igual a c o c^{-1}. Si $a^{-1}ca = c$, tenemos que a conmuta con c y por tanto $\langle a, c \rangle \cong C_6$ luego hemos acabado. Si $b^{-1}cb = c$ ocurre lo mismo. Por tanto, podemos asumir $a^{-1}ca = c^{-1}$ y $b^{-1}cb = c^{-1}$. Pero entonces $b^{-1}a^{-1}cab = c$, luego $\langle ab, c \rangle \cong C_6$.

7. Otros casos de orden pequeño

De la misma forma, es posible ver que sólo hay a lo sumo 3 grupos no abelianos de orden 20. Tenemos dos ejemplos distintos, que son D_5 y $\mathrm{Aff}(\mathbb{Z}_5)$. De hecho podemos encontrar un tercer ejemplo buscando en $\mathrm{SL}(2,\mathbb{Z}_5)$, que es de orden $4*5*6$, múltiplo de 20. Dicho ejemplo es

$$ST(2,\mathbb{Z}_5)=\{\begin{pmatrix} x & y \\ 0 & x^{-1}\end{pmatrix} : x\in\mathbb{Z}_5^{\times}, y\in\mathbb{Z}_5\}$$

el subgrupo de matrices triangulares de $\mathrm{SL}(2,\mathbb{Z}_5)$. Así que estos son todos los grupos no abelianos de orden 20.

Igualmente, se puede ver que sólo hay a lo sumo 3 grupos no abelianos de orden 18. Tenemos D_9 y $D_3\times C_3$ y podemos encontrar otro de matrices,

$$T(3,\mathbb{Z}_3)=\{\begin{pmatrix} \overline{\pm 1} & 0 & x \\ 0 & \overline{\pm 1} & y \\ 0 & 0 & \overline{1}\end{pmatrix} : x,y\in\mathbb{Z}_5\}\leq \mathrm{Aff}(\mathbb{Z}_3^2)$$

luego estos serán los únicos.

8. Lista de grupos de orden pequeño

n	Grupos de orden n	n	Grupos de orden n
1	Id	14	C_{14}, D_7
2	C_2	15	C_{15}
3	C_3	16	$C_{16}, C_8\times C_2, C_4^2, C_4\times C_2^2, C_2^3, D_8, \dots$
4	$C_4, C_2\times C_2$	17	C_{17}
5	C_5	18	$C_{18}, C_6\times C_3, D_9, D_3\times C_3, T(3,\mathbb{Z}_3)$
6	C_6, D_3	19	C_{19}
7	C_7	20	$C_{20}, C_{10}\times C_2, D_{10}, ST(\mathbb{Z}_5), \mathrm{Aff}(\mathbb{Z}_5)$
8	$C_8, C_4\times C_2, C_2^3, D_4, \mathrm{O}(2,\mathbb{Z}_3)$	21	$C_{21}, \mathrm{Aff}_3(\mathbb{Z}_7)$
9	$C_9, C_3\times C_3$	22	C_{22}, D_{11}
10	C_{10}, D_5	23	C_{23}
11	C_{11}	24	$C_{24}, C_{12}\times C_2, D_{12}, S_4, \mathrm{SL}(2,\mathbb{Z}_3)\dots$
12	$C_{12}, C_6\times C_2, D_6, A_4, \mathrm{Aff}_{4,3}(\mathbb{Z}_{15})$	25	$C_{25}, C_5\times C_5$
13	C_{13}	26	C_{26}, D_{13}