TIPOS DE GRUPOS

1. Generadores

Hemos visto que una buena idea para expresar un grupo es mediante generadores. Por ejemplo: $C_8 = \langle g_{2\pi/8} \rangle$, $D_6 = \langle g_{2\pi/6}, r_0 \rangle$, $S_3 = \langle (12), (123) \rangle$, $\mathrm{O}(2, \mathbb{R}) = \langle g_\alpha, r_0 : \alpha \in \mathbb{R} \rangle$ y

$$\mathrm{SL}(\mathbb{Z}_5) = \langle \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \rangle.$$

En el caso finito, no es una casualidad que el grupo se pueda expresar con tan pocos generadores, ya que por el teorema de Lagrange, si tomamos una cadena de subgrupos distintos dentro de G

$$\{e\} < \langle a_1 \rangle < \langle a_1, a_2 \rangle < \langle a_1, a_2, a_3 \rangle \ldots \leq G$$

cada uno de ellos debe tener orden divisor de $|G| = n$, y por eso se puede poner $G = \langle a_1, \ldots, a_k \rangle$, con k menor o igual que el número de primos de n (con multiplicidad). Por ejemplo, como $|\mathrm{SL}(2, \mathbb{Z}_5)| = 4 * 5 * 6 = 120 = 2 * 2 * 2 * 3 * 5$, sin saber nada más del grupo podemos afirmar que se podrá generar con como mucho 5 generadores.

Expresar el grupo mediante generadores permite sustituir su tabla por conocer sólo cómo se multiplican los generadores, es decir, permite describir el grupo en forma compacta. Por ejemplo, para describir la multiplicación en D_6 sólo necesitamos saber que $g_{2\pi/6} r_0 = r_0 g_{2\pi/6}^{-1}$, que $g_{2\pi/6}$ tiene orden 6 y r_0 orden 2.

Pero esto tiene el problema de que expresar todos los elementos del grupo mediante generadores, y también multiplicarlos, puede ser un proceso en el que no veamos mucha regularidad. Por ejemplo, el subgrupo de S_4

$$J = \{I, (12), (13)(24), (1324), (1423), (14)(23), (34), (12)(34)\}$$

puede escribirse como $J = \langle a, b \rangle$, con $a = (12)$ y $b = (13)(24)$. Si reescribimos el grupo usando dichos generadores tenemos que

$$J = \{e, a, b, ab, ba, aba, bab, abab\},$$

con a, b de orden 2 y $baba = abab$. Es sencillo ver que esto es lo único que necesitamos para multiplicar elementos del grupo.

Pero esta parametrización del grupo tiene el problema de que no entendemos muy bien por qué en este caso sólo aparecen palabras de longitud cuatro, y exactamente por qué aparecen esas precisamente.

Además, parece que esto no nos da una fórmula para saber cuál es la multiplicación de dos elementos cualesquiera del grupo. Vamos a buscar grupos para los cuales podamos describir sus elementos y su multiplicación de forma sencilla y compacta.

2. Grupos Cíclicos y Abelianos

El caso más sencillo es el de los grupos *cíclicos*, que son los que están generados por un sólo elemento, es decir $G = \langle g \rangle$. En el caso en que G tenga orden finito igual a n, sabemos que es siempre isomorfo a $C_n = \langle g_{2\pi/n} \rangle$, y cuando G tiene orden infinito es sencillo ver que es isomorfo a $\langle g_{2\pi\alpha_0} \rangle$ para α_0 cualquier número irracional. En el caso de orden finito, podemos parametrizar un grupo cíclico como

$$G = \{g^i : i < n\},$$

donde dicha expresión es única, con g de orden n, y podemos mutiplicar cualesquiera elementos según la fórmula $g^i g^j = g^{i+j}$ y reducir $i + j$ módulo n. Además, los cíclicos finitos tienen la propiedad de que satisfacen el inverso del Teorema de Lagrange y de que sus subgrupos son muy sencillos de describir.

Lema 2.1 (Subgrupos de un cíclico)**.** *Sea $G = \langle g \rangle$ con g de orden n. Entonces, para cada divisor d de n hay exactamente un subgrupo de G, que es el cíclico $\langle g^{n/d} \rangle$.*

Demostración. Sólo hay que demostrar que los únicos subgrupos de G son los de la forma $\langle g^l \rangle$, con l divisor de n. Sea $H \leq G$ con $|H| = d < n$. En G todo subgrupo es claramente normal, así que podemos escribir

$$G/H = \{H, g^2H, \ldots, g^{n/d-1}H\}$$

ya que $g \notin H$. Además, tenemos que $g^{n/d}H = H$, luego $g^{n/d} \in H$, lo que implica $\langle g^{n/d} \rangle \leq H$, pero ambos subgrupos tienen tamaño d, luego son iguales. □

Además, podemos ver que los grupos cíclicos son los únicos grupos de orden primo

Lema 2.2 (Grupos de orden primo)**.** *Si $|G| = p$, entonces G es cíclico. Por tanto sólo hay un grupo de orden p salvo isomorfía, C_p.*

Demostración. Tomamos un elemento $g \in G$ distinto del neutro. Entonces $\langle g \rangle \leq G$, luego por Lagrange su orden debe dividir a p, y como no es 1 tenemos que $|\langle g \rangle| = p$, luego $G = \langle g \rangle$. □

Después de los cíclicos, los grupos más sencillos son los *abelianos*, que son los grupos G que satisfacen que todos sus elementos conmutan, es

decir que para todo $x, y \in G$ se tiene que $yx = xy$. Como hemos visto antes, cualquier grupo cíclico es abeliano.

En el caso finito, podemos escribir G como generado por a lo sumo r generadores, con $|G| = p_1 \dots p_r$ su factorización en primos. Así, tendremos que

$$G = \langle g_1, \dots, g_k \rangle = \{g_1^{i_1} \dots g_r^{i_k} : i_s < |g_s|\} \qquad (*)$$

con g_j ciertos elementos de G. Así, en este caso no ocurre lo que pasaba en subgrupo de S_4 que hemos visto antes, que teníamos elementos distintos como a, b, aba, bab, etc, sino que podemos escribir los elementos de G en forma compacta. Además, la multiplicación es muy sencilla:

$$(g_1^{i_1} \dots g_r^{i_r})(g_1^{j_1} \dots g_r^{j_r}) = g_1^{i_1+j_1} \dots g_r^{i_r+j_r}.$$

Lo que no sabemos es si dicha expresión de los elementos de G es única. Vamos a ver que puede hacerse única escogiendo los g_j de manera adecuada. Para demostrarlo la herramienta principal será cocientar por un subgrupo normal. Para ello, vamos a usar que *cualquier subgrupo de un grupo abeliano es normal*, que es trivial de comprobar ya que como todos los elementos conmutan tenemos $Hg = gH$.

3. Grupos Resolubles

Un problema que tienen los grupos abelianos es que se puede ver que la mayoría de los grupos finitos no son abelianos, y por tanto no estamos cubriendo mucho si conseguimos entender sólo los abelianos.

Así, vamos a ver que es posible demostrar que existe una parametrización del tipo $(*)$ para grupos mucho más generales que los abelianos. Para definirlos vamos a usar el cociente.

En general, si tenemos un grupo G y consideramos un subgrupo normal N de G, podemos «partir» el grupo G en los grupos $G_0 = G/N$ y $G_1 = N$. Podemos iterar este proceso, tomando un subgrupo N_0 normal de G_0 y otro N_1 normal de G_1, y entonces obtendríamos los grupos $G_{00} = G_0/N_0$, $G_{01} = N_0$, $G_{10} = G_1/N_1$, $G_{11} = N_1$. Podemos seguir así, duplicando en cada paso el número de subgrupos, obteniendo un árbol.

Definition 3.1. Vamos a llamar *troceado* del grupo G al proceso de repetir dicha operación un número finito k de veces, y vamos a llamar *piezas* a cada uno de los 2^k grupos resultantes de dicho proceso.

Esto nos permite definir un nuevo tipo de grupos que contiene a los grupos abelianos.

Definition 3.2 (Grupos resolubles)**.** Decimos que un grupo G es *resoluble* o soluble si existe un troceado de G en piezas abelianas.

En el caso finito, podemos trocearlos en piezas aún más sencillas

Lema 3.3 (Caracterización de resolubles finitos)**.** *Un grupo finito G es resoluble si existe un troceado de G en piezas cíclicas de orden primo o uno.*

Demostración. Es suficiente considerar G abeliano. Si $|G|$ es un primo o uno, el resultado es trivial. En otro caso, vamos a proceder por inducción en $|G|$. G siempre tiene algún subgrupo H no trivial, y va a ser normal, por lo que podemos partir G en G/H y H. Como $|G/H|$ y $|H|$ son menores que $|G|$ hemos terminado por inducción. □

De hecho, podemos demostrar mucho más: podemos encontrar una parametrización sencilla para un grupo resoluble de orden finito en términos de sus piezas cíclicas primas:

Lema 3.4 (Parametrización de resolubles finitos)**.** *Sea G grupo resoluble finito, con $|G| = n$. Podemos escribir los elementos de G de forma única como*

$$G = \{a_1^{i_1} a_2^{i_2} \dots a_r^{i_r} : i_k < p_k\}$$

para ciertos $a_k \in G$ y p_k primos (no necesariamente distintos), con $p_1 \dots p_r = n$. Además, el orden de a_i es un múltiplo de p_i y de hecho $a_i^{p_i} = a_{i+1}^{d_{i+1}(i)} \dots a_r^{d_r(i)}$ con $d_j < p_j$, y podemos describir la multiplicación mediante las fórmulas

$$a_j a_i = a_i a_{i+1}^{d_{i+1}(i,j)} \dots a_r^{d_r(i,j)} \qquad j > i$$

para ciertos $d_k(i,j) < p_k$.

Demostración. Vamos a demostrarlo por inducción en el número de pasos k del troceado de un grupo resolube en piezas cíclicas de orden primo o uno. Si $k = 0$ es cierto porque el grupo sería cíclico. Si un grupo G resoluble tiene un troceado en cíclicos de orden primo o uno de k pasos, en el primer paso lo habremos partido en N y G/N, con N normal en G. Entonces, G/N y N pueden trocearse en cíclicos primos o uno en $k-1$ pasos, luego por inducción podemos asumir que la parametrización del resultado es cierta para ambos. Así, podremos escribir los elementos de N de forma única como

$$N = \{b_1^{s_1} \dots b_l^{s_l} : s_k < q_k\}$$

para ciertos b_j de N, y $|N| = q_1 \dots q_l$, q_k primos. Además, se cumplirán ecuaciones de multiplicación como las del enunciado.

En el caso de G/N tendremos

$$G/N = \{\overline{a_1}^{i_1} \dots \overline{a_r}^{i_r} : i_k < p_k\}$$

con $\overline{a_k} = a_k N$, $a_k \in G$, $|G/N| = p_1 \dots p_r$, y también fórmulas de multiplicación como las del enunciado.

Ahora, cada elemento $g \in G$ está exactamente en una clase de G/N, luego

$$g \in a_1^{i_1} \dots a_r^{i_r} N$$

para ciertos $i_k < p_k$. Pero además, como también tenemos N parametrizado, podemos escribir esa pertenencia como

$$g = a_1^{i_1} \dots a_r^{i_r} b_1^{s_1} \dots b_l^{s_l}$$

para ciertos $s_k < q_k$. Además, dicha expresión es única, luego hemos encontrado una parametrización de G como la del enunciado:

$$G = \{a_1^{i_1} \dots a_r^{i_r} b_1^{s_1} \dots b_l^{s_l} : i_k < p_k, s_k < q_k\}.$$

Sólo queda ver que las reglas de multiplicación de G/N y N nos dan reglas de multiplicación en G como las del enunciado. La regla para $b_j b_i$ viene directamente de N. En el caso de $b_k a_i$, tenemos que como N es normal en G se cumple que

$$a_i^{-1} b_k a_i \in N$$

luego

$$b_k a_i = a_i n_{k,i}$$

par cierto $n_{k,i}$ de N, y por la parametrización de N tenemos una fórmula como la que buscábamos. Por último, para el caso $a_j a_i$, por la multiplicación en G/N tendríamos que

$$\overline{a_j}\,\overline{a_i} = \overline{a_i}\,\overline{a_{i+1}}^{d_{i+1}(i,j)} \dots \overline{a_r}^{d_r(i,j)}$$

para ciertos $d_l(i,j)$. Pero quitando las clases esa ecuación se puede escribir como

$$a_j a_i = a_i a_{i+1}^{d_{i+1}(i,j)} \dots a_r^{d_r(i,j)} \tilde{n}_{(i,j)}$$

para cierto $\tilde{n}_{(i,j)} \in N$, y lo mismo podemos hacer con la ecuación para $a_i^{p_i}$ y $b_i^{q_i}$. □

Además, de forma inversa, si tenemos un conjunto G descrito por la parametrización del resultado anterior, y definimos la multiplicación también mediante las reglas definidas ahí, en caso de que con esa definición se satisfagan los axiomas de grupo (no siempre será así), entonces es fácil ver que dicho grupo sería resoluble.

Este resultado nos sirve para dos cosas: por una parte nos puede ayudar a resolver problemas en un grupo conocido, y por otro nos puede servir para comparar grupos. Por ejemplo, si tenemos un grupo G que se puede parametrizar con $a_1, a_2, \dots, a_r$ y otro H que se puede parametrizar con $A_1, A_2, \dots, A_r$ de forma que los A_j satisfagan las mismas reglas de multiplicación que los a_j (es decir, que los ds que aparecen

en los exponentes son los mismos), en ese caso G y H serán isomorfos, porque

$$a_1^{i_1} \dots a_r^{i_r} \mapsto A_1^{i_1} \dots A_r^{i_r}$$

será un isomorfismo de G en H (una manera de verlo es que las tablas serán las mismas, ya que las sacamos de las mismas reglas de multiplicación para los generadores).

Históricamente, el nombre resoluble viene de que Galois asoció a cada polinomio un grupo G, y vio que las raíces del polinomio se podían expresar en términos de raíces iteradas de los coeficientes (resoluble por radicales) si y sólo si el grupo G era resoluble. En cierto sentido, las potencias $a_i^{p_i}$ en la parametrización corresponderían a tomar una raíz p_i-ésima de un número.

Como ejemplo un poco tonto de grupo resoluble, consideremos $G = \mathbb{Z}_{16}^{\times}$, con $|G| = 8 = 2{*}2{*}2$. Para encontrar la parametrización buscamos un elemento de orden 2, por ejemplo $\overline{9}$. Después buscamos un elemento que no esté en $\langle\overline{9}\rangle = \{\overline{1}, \overline{9}\}$ pero su cuadrado sí, por ejemplo $\overline{3}$. Por último, buscamos un elemento que no esté en $\langle\overline{3}, \overline{9}\rangle = \{\overline{1}, \overline{3}, \overline{9}, \overline{11}\}$ pero su cuadrado sí, por ejemplo $\overline{5}$. Así, tenemos que

$$\mathbb{Z}_{16}^{\times} = \{\overline{5}^{i_1}\overline{3}^{i_2}\overline{9}^{i_3} : i_k = 0, 1\}$$

con $\overline{3}^2 = \overline{9}$ y $\overline{5}^2 = \overline{9}$.

Un ejemplo más interesante es el subgrupo J de S_4 que hemos visto en la primera sección. J no es abeliano, pero $H = \langle abab\rangle$ es un subgrupo normal de J de orden 2, y

$$J/H = \{\overline{I}, \overline{a}, \overline{b}, \overline{a}\overline{b}\}.$$

Podemos ver que $\overline{b}\overline{a} = ba\{I, abab\} = \{ba, ab\}$ y $\overline{a}\overline{b} = ab\{I, abab\} = \{ab, ba\}$, luego J/H es abeliano. Así, podemos escribir la parametrización

$$J = \{a_1^{i_1}a_2^{i_2}a_3^{i_3} : i_k = 0, 1\}$$

donde $a_1 = a$, $a_2 = b$, $a_3 = abab$, por lo que a_j son todos de orden 2 y tenemos las multiplicaciones

$$a_2a_1 = a_1a_2a_3 \qquad a_3a_2 = a_2a_3 \qquad a_3a_1 = a_1a_3$$

que iterándolas dan lugar a la fórmula

$$(a_1^{i_1}a_2^{i_2}a_3^{i_3})(a_1^{j_1}a_2^{j_2}a_3^{j_3}) = a_1^{i_1+j_1}a_2^{i_2+j_2}a_3^{i_3+j_3+i_3j_3}$$

donde los exponentes de la parte derecha se pueden reducir módulo 2. Vemos que esto nos da una manera más compacta de describir los elementos de J y multiplicarlos.

Lo bueno de tener más o menos controlados los grupos resolubles, es que se sabe que en cierto sentido la mayoría de los grupos finitos son

resolubles. Por ejemplo, se sabe que *todo grupo de orden impar es resoluble*, pero no vamos a demostrarlo ya que es difícil y la demostración original ocupó 255 páginas. Por otra parte, se conjetura que la proporción del número de grupos de orden menor que n que son resolubles tiende a 1 cuando $n \to \infty$, pero esto no se ha demostrado todavía.

4. Grupos Simples

En el caso de un grupo general G, podemos partirlo de forma no trivial siempre que encontremos un subgrupo normal N no trivial. Esto no es posible por ejemplo cuando $G = C_p$, y motiva la siguiente definición

Definition 4.1 (Grupos Simples)**.** Decimos que un grupo G es *simple* cuando no tiene subgrupos normales no triviales.

Hay grupos simples no abelianos, y por tanto no resolubles. Uno de los ejemplos más importantes es $\mathrm{PSL}(2, K) = \mathrm{SL}(2, K)/\{I, -I\}$, para K igual a $\mathbb{C}, \mathbb{R}$ o $\mathbb{Z}_p$, $p \geq 5$. Es decir, son las matrices de determinante uno si identificamos A con $-A$, lo que es equivalente a olvidarnos del signo. La demostración de que dichos grupos de matrices son simples está en uno de los ejercicios.

Lo importante es que muchas veces podemos trocear un grupo en grupos simples. Por ejemplo, siempre que el grupo sea finito. Por tanto, los grupos simples son el equivalente (dentro de los grupos finitos) a los números primos.

Lema 4.2 (Troceado de finitos en simples)**.** *Sea G un grupo finito. Existe un troceado de G en piezas simples y de tamaño uno.*

Demostración. La demostración es trivial, por inducción en $n = |G|$. Si G es simple o de tamaño uno ya hemos acabado. Si no lo es, podemos encontrar un subgrupo normal no trivial N, y por tanto podemos partir G en G/N y N. Por inducción G/N y N se pueden trocear en piezas simples, luego lo mismo es cierto para G. □

Así, podríamos construir una parametrización de los elementos de cualquier grupo finito en producto de elementos que corresponderían a las piezas simples, aunque sería un poco más oscura que la que tenemos para el caso particular de los resolubles.

De hecho, una idea para intentar comprender los grupos finitos es primero entender los grupos finitos simples. Hace unos años consiguieron clasificar todos los grupos finitos simples (podéis ver dicha clasificación en Wikipedia). No vamos a ver la clasificación ni su demostración, que ocupa más de 10000 páginas. Pero podemos resumirla diciendo que hay cuatro tipos de grupos simples finitos:

- C_p, cíclicos de orden p primo.
- 16 familias de grupos de matrices, siendo una de ellas $\mathrm{PSL}(2, \mathbb{Z}_p)$ que tiene orden $\frac{(p-1)p(p+1)}{2}$.
- A_n, $n \geq 5$, que es un subgrupo especial de S_n de índice dos que describiremos en el siguiente tema.
- Los llamados grupos esporádicos, que son 26 grupos no clasificados en familias.

Otra cosa importante es saber que los grupos simples distintos de los C_p son muy especiales. Por ejemplo, el número de dichos grupos de tamaño menor que n es asintóticamente el mismo que el de los números $\frac{(p-1)p(p+1)}{2}$ menores que n, con p primo. Por eso, podemos decir que casi todos los grupos simples son de la forma C_p, y por eso los grupos resolubles son tan importantes.