EL GRUPO DIEDRAL

RESUMEN. Damos dos construcciones explícitas del grupo diedral $\mathbb{D}_n$ para $n \geq 3$, una como subgrupo de $GL_2(\mathbb{R})$ y otra como subgrupo de S_n.

Simetrías de polígonos. Sean $n \geq 3$ y

$$v_k = (\cos(2\pi k/n), \operatorname{sen}(2\pi k/n))$$

para cada $k \in \{0, \ldots, n-1\}$ los vértices del n-gono regular centrado en cero y con un vértice en 1. Notamos $V = \{v_0, \ldots, v_{n-1}\}$. El polígono convexo que tiene por vértices a V es

$$P_n = \operatorname{conv}(V) = \left\{ \sum_{i=0}^{n-1} t_i v_i : t_0 + t_2 + \cdots + t_{n-1} = 1, t_i \geq 0 \right\}.$$

El grupo diedral pretende capturar las *simetrías* de P_n que preservan ángulos. Dada una matriz inversible $A \in GL_2(\mathbb{R})$ y $X \subset \mathbb{R}^2$, notamos $A \cdot X = \{Ax : x \in X\}$. Se define

$$\mathbb{D}_n = \{A \in GL_2(\mathbb{R}) : A \text{ es ortogonal y } A \cdot P_n \subset P_n\};$$

una verificación muestra que resulta un subgrupo de $GL_2(\mathbb{R})$.

Observemos que por $\mathbb{R}$-linealidad $A \cdot P_n = \operatorname{conv}(A \cdot V)$. Por lo tanto, si $A \cdot V = V$, entonces $A \in \mathbb{D}_n$. La recíproca también es cierta:

Lema 1. *Si una matriz ortogonal $A \in GL_2(\mathbb{R})$ pertenece a $\mathbb{D}_n$ entonces $A \cdot V = V$.*

Demostración. Como A es inversible, multiplicar por A resulta inyectivo y entonces $A \cdot V$ tiene n elementos. Por lo tanto, basta ver que $A \cdot V \subset V$.

Como A preserva normas por ser ortogonal y los elementos de V tienen norma 1, es decir $V \subset S^1$, se tiene que $A \cdot V \subset S^1$. Además $A \cdot V \subset P_n$ ya que $A \in \mathbb{D}_n$. Estos dos hechos nos dicen que $A \cdot V \subset S^1 \cap P_n$. Resta ver que $S^1 \cap P_n = V$, lo cual puede consultarse en el Apéndice A. $\square$

El lema anterior nos permite ver que hay dos tipos de transformaciones ortogonales que seguro pertenecen a $\mathbb{D}_n$. La primera es la rotación de ángulo $2\pi/n$

$$R = \begin{pmatrix} \cos(2\pi/n) & -\operatorname{sen}(2\pi/n) \\ \operatorname{sen}(2\pi/n) & \cos(2\pi/n) \end{pmatrix},$$

que envía V a V pues $Rv_i = v_{i+1}$ para cada $i \in \{0, \ldots, n-2\}$ y $Rv_n = v_0$.

La segunda es la reflexión con respecto al eje $y = 0$,

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Es un elemento de $\mathbb{D}_n$ pues, usando que seno es impar y coseno par,

$$\begin{aligned} Sv_k &= (\cos(2\pi k/n), -\operatorname{sen}(2\pi k/n)) = (\cos(-2\pi k/n), \operatorname{sen}(-2\pi k/n)) \\ &= (\cos(2\pi(n-k)/n), \operatorname{sen}(2\pi(n-k)/n)) = v_{n-k} \in V. \end{aligned}$$

Una verificación directa muestra que se cumplen las siguientes identidades:

$$\operatorname{ord}(R) = n, \quad \operatorname{ord}(S) = 2, \quad RSRS = I_2.$$

Notar además que, como $\mathbb{D}_n$ es un subgrupo de $GL_2(\mathbb{R})$, se tiene que

$$R^i S^j \in \mathbb{D}_n \qquad (\forall i \in \{0, \dots, n-1\}, j \in \{0,1\}).$$

Para terminar probamos que estos elementos son todos distintos, y que son todos los elementos posibles de $\mathbb{D}_n$.

Teorema 1. *El grupo diedral tiene orden* $2n$ *y*

$$\mathbb{D}_n = \{I_2, R, \dots, R^{n-1}, S, RS, \dots, R^{n-1}S\}.$$

Demostración. Sea $A \in \mathbb{D}_n$. Pensando en A como transformación $\mathbb{R}$-lineal, está determinada por lo que vale en una base. Como v_1 no tiene un cero en su segunda coordenada, no es múltiplo de v_0 y luego $B = \{v_0, v_1\}$ es una base de $\mathbb{R}^2$.

Para alivianar la notación,[1] dado $k \in \mathbb{Z}$ notamos $v_k = v_{r_n(k)}$; así $v_{n+k} = v_k$ y

$$R^i v_k = v_{k+i}, \qquad R^i S v_k = R^i v_{-k} = v_{i-k}.$$

De la observación precedente y estas igualdades se sigue inmediatamente que los $2n$ elementos $R^i S^j$ son distintos, pues ningún par de elementos coincide en la base B.

Para terminar, veamos que una matriz $A \in \mathbb{D}_n$ debe coincidir con alguno de estos $2n$ elementos. Como ya notamos A queda determinada por $(i,j) \in \{0, \dots, n-1\} \times \{0, \dots, n-1\}$ tal que $Av_0 = v_i$ y $Av_1 = v_j$.

Sin embargo, hay una dependencia entre i y j, que proviene de que A preserve productos internos y por lo tanto ángulos. El ángulo $\alpha = \operatorname{ang}(v_i, v_j) \in [0, 2\pi)$ entre v_i y v_j cumple

$$\begin{aligned} \cos(\operatorname{ang}(v_i, v_j)) = \frac{\langle v_i, v_j \rangle}{\|v_i\| \|v_j\|} &= \cos(2\pi i/n)\cos(2\pi j/n) + \operatorname{sen}(2\pi i/n)\operatorname{sen}(2\pi j/n) \\ &= \cos(2\pi i/n - 2\pi j/n) = \cos(2\pi(i-j)/n), \end{aligned}$$

así que $2\pi|i-j|/n = \operatorname{ang}(v_i, v_j)$. Se sigue que

$$2\pi/n = \operatorname{ang}(v_0, v_1) = \operatorname{ang}(Av_0, Av_1) = 2\pi|i-j|/n,$$

de lo cual se deduce que $|i-j| = 1$. En otras palabras $j = i \pm 1$. Si $j = i+1$, entonces $Av_0 = v_i$ y $Av_1 = v_{i+1}$, de manera que $A = R^i$ pues coinciden en B. Del mismo modo se prueba que si en cambio $Av_0 = v_i$ y $Av_1 = v_{i-1}$, entonces $A = R^i S$. □

Permutaciones de n puntos. La idea del teorema anterior fue notar que un elemento de $\mathbb{D}_n$ estaba determinado por cómo permutaba los n vértices de P_n. Bajo la biyección $k \mapsto v_k$, la rotación se corresponde con la permutación que envía $k \mapsto k+1$ si $k < n$ y $n \mapsto 1$. Es decir, el n-ciclo

$$\rho = (1\ 2\ \cdots\ n).$$

[1] Toda esta cuenta se podría hacer en $\mathbb{C}$, que es isomorfo a $\mathbb{R}^2$ como $\mathbb{R}$-espacio vectorial. Allí V se corresponde con G_n, la rotación R se corresponde con multiplicar por $e^{i2\pi/n} \in G_n$, y S se corresponde con la conjugación.

Por otro lado, la simetría se corresponde con $\sigma \in S_n$ que envía k a $n-k$, es decir

$$\sigma = \prod_{k=1}^{\lfloor n/2 \rfloor} (k\ (n-k)).$$

Por definición $\operatorname{ord}(\rho) = n$. Como σ está dado por un producto de transposiciones disjuntas, entonces $\operatorname{ord}(\sigma) = 2$. Además, un cálculo muestra que $\rho\sigma\rho\sigma = 1$. De aquí podremos probar que $\langle \rho, \sigma \rangle \leq S_n$ resulta isomorfo a $\mathbb{D}_n$, definiendo tal isomorfismo como $\rho^i\sigma^j \mapsto r^i s^j$.

Notar que el particular hemos construido un monomorfismo $\mathbb{D}_n \to S_n$. Esto puede pensarse como una versión explícita del teorema de Cayley, en la cual tenemos control sobre el tamaño del grupo de simetrías en cuestión.

Apéndice A.

Lema 2. *Si $x \in S^1$ e $y \in \mathbb{R}^2$ tiene norma menor o igual a* 1, *entonces* $S^1 \cap \operatorname{conv}(x, y) \subset \{x, y\}$.

Demostración. Veamos que los únicos posibles puntos en los que el segmento $\operatorname{conv}(x, y) = \{xt + (1-t)y \colon t \in [0, 1]\}$ tiene un punto de norma 1 es cuando $t = 0$ o $t = 1$. Consideremos

$$\begin{aligned} p(t) = \|tx + (1-t)y\|^2 &= t^2\|x\|^2 + (1-t)^2\|y\|^2 + 2t(1-t)\langle x, y\rangle \\ &= t^2(\|x\|^2 + \|y\|^2 - 2\langle x, y\rangle) + 2t(\langle x, y\rangle - \|y\|^2) + \|y\|^2 \\ &= \|x-y\|^2 t^2 + 2\langle x-y, y\rangle t + \|y\|^2. \end{aligned}$$

Esta es una función cuadrática con coeficiente principal positivo, por lo que no tiene máximos locales. De esta forma, en $[0, 1]$ alcanza su máximo únicamente en alguno de los extremos,

$$f(t) < \text{máx}\{f(0), f(1)\} \leq 1 \qquad \forall t \in (0, 1).$$

Tomando raíz obtenemos que $\|tx + (1-t)y\| < 1$ si $t \in (0, 1)$, lo cual concluye la prueba. $\square$

Lema 3. *Sea $n \geq 1$ y $V = \{v_0, \dots, v_n\} \subset S^1$ es un conjunto finito, entonces* $S^1 \cap \operatorname{conv}(V) = V$.

Demostración. Siempre vale que $V \subset S^1 \cap \operatorname{conv}(V)$, veamos la recíproca. Haremos inducción en n. El caso base es implicado por el lema anterior tomando $x = v_0$ e $y = v_1$. Sea

$$x = \sum_{i=0}^{n} t_i v_i \in \operatorname{conv}(V)$$

con $t_0, \dots, t_n \geq 0$ y $t_0 + \cdots + t_n = 1$. Supongamos que $t_0 > 0$, pues en caso contrario $x = v_0 \in V$ y no hay nada que decir. Definiendo $z = \sum_{i=1}^{n-1} \frac{t_i}{1-t_0} v_i \in \operatorname{conv}(V)$, el punto x está en el segmento entre v_0 y z,

$$x = t_0 v_0 + (1-t_0)z \in \operatorname{conv}(v_0, z).$$

Como $\|v_0\| = 1$ y $\|z\| \leq \sum_{i=1}^{n-1} \frac{t_i}{1-t_0} = 1$, aplicando el lema anterior a v_0 y z obtenemos que x pertenece a $\{v_0, z\}$. Si $x = v_0 \in V$ no hay nada que decir, en caso contrario podemos aplicar la hipótesis inductiva a $x = z \in \operatorname{conv}(x_1, \dots, x_n) \cap S^1$, obteniendo $x \in V \setminus \{v_0\} \subset V$. $\square$