Capítulo 9
Acciones de grupos

Por sus obras los conoceréis.

Normalmente los grupos surgen junto con su acción sobre algún conjunto. En general, el concepto de acción es fundamental en las matemáticas.

9.1 Definiciones y primeros ejemplos

9.1.1. Definición. Sea G un grupo y X un conjunto. Se dice que G **actúa sobre** X **(por la izquierda)** si está definida una aplicación

$$\begin{aligned} \alpha\colon G \times X &\to X, \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

que satisface las siguientes propiedades.

A1) La identidad del grupo actúa como la identidad: para cualesquiera $x \in X$ se cumple

$$1 \cdot x = x.$$

A2) La acción es compatible con la multiplicación en G: para cualesquiera $h, g \in G$ y $x \in X$ se cumple

$$(hg) \cdot x = h \cdot (g \cdot x).$$

También se dice que X es un G**-conjunto (izquierdo)**.

9.1.2. Comentario. También hay una noción de acción por la derecha: es una aplicación

$$\begin{aligned} X \times G &\to X, \\ (x, g) &\mapsto x \cdot g \end{aligned}$$

que satisface

A1) $x \cdot 1 = x$ para todo $x \in X$,

A2) $x \cdot (gh) = (x \cdot g) \cdot h$ para cualesquiera $x \in X$, $g, h \in G$.

A toda acción por la derecha se puede asociar *de manera canónica* una acción por la izquierda definida por

$$g \cdot x := x \cdot g^{-1}.$$

Necesitamos tomar el inverso de g para que se cumpla el axioma A2): si la acción por la derecha cumple $x \cdot (gh) = (x \cdot g) \cdot h$, entonces

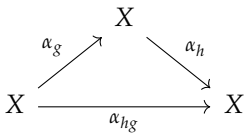
$$(gh) \cdot x := x \cdot (gh)^{-1} = x \cdot (h^{-1} g^{-1}) = (x \cdot h^{-1}) \cdot g^{-1} =: g \cdot (h \cdot x).$$

Vamos a trabajar exclusivamente con las acciones por la izquierda.

Dado una acción $\alpha\colon G \times X \to X$, fijando $g \in G$ se obtiene la aplicación de la acción por g

$$\begin{aligned} \alpha_g\colon X &\to X, \\ x &\mapsto g \cdot x. \end{aligned}$$

La condición A1) de arriba significa que $\alpha_1 = \mathrm{id}_X$ y la condición A2) nos dice que $\alpha_{hg} = \alpha_h \circ \alpha_g$:



Notamos que de A1) y A2) se sigue que $\alpha_g\colon X \to X$ es una biyección y su aplicación inversa es $\alpha_{g^{-1}}\colon X \to X$:

$$\alpha_{g^{-1}} \circ \alpha_g = \alpha_{g^{-1}g} = \mathrm{id}_X, \quad \alpha_g \circ \alpha_{g^{-1}} = \alpha_{gg^{-1}} = \mathrm{id}_X.$$

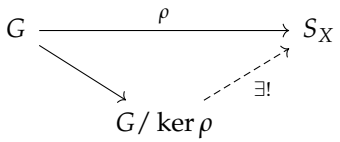
La identidad $\alpha_{hg} = \alpha_h \circ \alpha_g$ significa que tenemos un homomorfismo de grupos

$$\begin{aligned} \rho\colon G &\to S_X, \\ g &\mapsto \alpha_g, \end{aligned} \tag{9.1}$$

donde S_X es el grupo simétrico que consiste en las biyecciones $f\colon X \to X$ respecto a la composición $\circ$. Viceversa, cualquier homomorfismo de grupos (9.1) define una acción de G sobre X mediante $g \cdot x := (\rho(g))(x)$.

9.1.3. Definición. Se dice que la acción de G sobre X es **fiel** si diferentes elementos de G actúan de manera diferente; es decir, si el homomorfismo correspondiente $G \to S_X$ es mono. En general, $\ker(G \to S_X)$ se llama el **núcleo** de la acción.

9.1.4. Observación. *Toda acción $\rho\colon G \to S_X$ da lugar a una acción fiel $G/\ker\rho \to S_X$:*



Demostración. Esto es el teorema de isomorfía. ∎

9.1.5. Ejemplo. El ejemplo primordial: el grupo simétrico S_X actúa sobre X de manera evidente ($f \cdot x = f(x)$). Esta acción es fiel. En particular, el grupo S_n actúa sobre el conjunto $\{1, 2, \ldots, n\}$.

De la misma manera,

- el grupo de isometrías del plano $\mathbb{R}^2$ actúa sobre $\mathbb{R}^2$,

- el grupo diédrico actúa sobre un n-ágono regular,
- etcétera.

▲

9.1.6. Ejemplo. El grupo $\mathrm{GL}(V)$ actúa sobre un espacio vectorial V. Si G es cualquier grupo, entonces un homomorfismo

$$\rho\colon G \to \mathrm{GL}(V)$$

da lugar a una acción de G sobre V **por aplicaciones lineales**. En este caso se dice que ρ es una **representación lineal** de G sobre V. El estudio de representaciones lineales ayuda descubrir muchas propiedades de G. Es una herramienta muy poderosa de la teoría de grupos.

De la misma manera, se dice que un homomorfismo

$$\rho\colon G \to S_X$$

(que corresponde a un G-conjunto X) es una **representación por permutaciones** de G sobre X. ▲

9.1.7. Ejemplo. He aquí una variante sobre el tema de la acción de $\mathrm{GL}(V)$ sobre V. Sea R un anillo conmutativo y $\mathrm{GL}_n(R)$ el grupo de las matrices invertibles de $n \times n$. Consideremos los elementos de

$$R^n := \underbrace{R \times \cdots \times R}_{n}$$

como vectores columna; es decir, matrices de $n \times 1$

$$v = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Para $A \in \mathrm{GL}_n(R)$ el producto de matrices $A \cdot v$ es también un vector columna. Esto define una acción de $\mathrm{GL}_n(R)$ sobre el espacio de vectores columna R^n por la izquierda.

Ahora si trabajamos con vectores fila

$$v = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix},$$

el producto $v \cdot A$ es también un vector fila. El grupo $\mathrm{GL}_n(R)$ actúa sobre el espacio de vectores fila R^n por la derecha. ▲

9.1.8. Ejemplo. Consideremos el **semiplano superior** que es el subconjunto de $\mathbb{C}$ dado por

$$\mathcal{H} := \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}.$$

El grupo

$$\mathrm{SL}_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R},\ ad - bc = 1 \right\}$$

actúa sobre $\mathcal{H}$ mediante las **transformaciones de Möbius**:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}.$$

Esta fórmula tiene sentido, ya que $z \in \mathcal{H}$ es un número complejo con la parte imaginaria estrictamente positiva, así que $cz + d \neq 0$ si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$. Además, verificamos que $\frac{az+b}{cz+d} \in \mathcal{H}$:

$$\operatorname{Im} \frac{az+b}{cz+d} = \operatorname{Im} \frac{(az+b)\,(c\overline{z}+d)}{|cz+d|^2} = \operatorname{Im} \frac{ac\,|z|^2 + ad\,z + bc\,\overline{z} + bd}{|cz+d|^2} > 0,$$

puesto que $ad > bc$.

Comprobemos que se cumplen los axiomas A1) y A2). La matriz identidad nos da

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot z := \frac{1 \cdot z + 0}{0 \cdot z + 1} = z.$$

Para el producto de matrices se tiene

$$\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \cdot z = \begin{pmatrix} a'a + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{pmatrix} \cdot z = \frac{(a'a + b'c)\,z + a'b + b'd}{(c'a + d'c)\,z + c'b + d'd}$$

y

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z \right) = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \frac{az+b}{cz+d} = \frac{a' \dfrac{az+b}{cz+d} + b'}{c' \dfrac{az+b}{cz+d} + d'} = \frac{a'\,(az+b) + b'\,(cz+d)}{c'\,(az+b) + d'\,(cz+d)},$$

y las últimas dos expresiones coinciden.

La acción de $\mathrm{SL}_2(\mathbb{R})$ no es fiel: las matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

actúan de la misma manera. Dejo al lector como un pequeño ejercicio calcular que el núcleo de la acción es precisamente

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \;\middle|\; \frac{az+b}{cz+d} = z \text{ para todo } z \in \mathcal{H} \right\} = Z(\mathrm{SL}_2(\mathbb{R})) = \{\pm I\}$$

y por ende hay una acción fiel del grupo cociente

$$\mathrm{PSL}_2(\mathbb{R}) := \mathrm{SL}_2(\mathbb{R}) / Z(\mathrm{SL}_2(\mathbb{R})) = \mathrm{SL}_2(\mathbb{R}) / \{\pm I\}$$

sobre el semiplano superior.

La acción de $\mathrm{SL}_2(\mathbb{R})$ sobre $\mathcal{H}$ se restringe a una acción de

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Hemos visto que el grupo $\mathrm{SL}_2(\mathbb{Z})$ puede ser generado por dos matrices

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

Entonces, todas las acciones de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathcal{H}$ pueden ser escritas como composiciones de las aplicaciones

$$z \mapsto -1/z, \quad z \mapsto z + 1$$

y sus inversas.

Para obtener una acción fiel normalmente se considera la acción correspondiente del grupo

$$\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\} = \mathrm{SL}_2(\mathbb{Z})/\mathrm{Z}(\mathrm{SL}_2(\mathbb{Z})).$$

▲

9.1.9. Definición. Para dos G-conjuntos X e Y se dice que una aplicación $f\colon X \to Y$ es G**-equivariante** si esta conmuta con las acciones de G:

$$f(g \cdot x) = g \cdot f(x)$$

para cualesquiera $g \in G$, $x \in X$.

En otras palabras, si las acciones de G vienen dadas por aplicaciones $\alpha\colon G \times X \to X$ y $\beta\colon G \times Y \to Y$, entonces $f\colon X \to Y$ es equivariante precisamente cuando el diagrama de abajo conmuta:

$$\begin{array}{ccc} G \times X & \xrightarrow{\mathrm{id}\times f} & G \times Y \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ X & \xrightarrow[f]{} & Y \end{array}$$

9.1.10. Definición. Si X es un G-conjunto y $X_0 \subseteq X$ es un subconjunto tal que para cualesquiera $g \in G$ y $x \in X_0$ se cumple $g \cdot x \in X_0$, se dice que X_0 es un subconjunto G**-invariante**.

En este caso la acción de G sobre X se restringe a X_0 y el último también puede ser visto como un G-conjunto. En la siguiente sección vamos a estudiar cómo un G-conjunto puede ser descompuesto en subconjuntos G-invariantes.

9.1.11. Ejemplo. Sea k un cuerpo. El **espacio afín** n-dimensional sobre k es nada más el conjunto

$$\mathbb{A}^n(k) := k^n = \{(x_1, \ldots, x_n) \mid x_i \in k\}.$$

El grupo $k^\times$ actúa sobre $\mathbb{A}^n(k)$ mediante la multiplicación: para $\lambda \in k^\times$

$$\lambda \cdot (x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n).$$

El subconjunto $\mathbb{A}^n(k) \setminus \{(0, \ldots, 0)\}$ es $k^\times$-equivariante: multiplicando un punto no nulo por un escalar no nulo, se obtiene un punto no nulo. ▲

9.2 Órbitas y estabilizadores

9.2.1. Definición. Sea X un G-conjunto. Para un punto $x \in X$ su **órbita** $O_x \subseteq X$ es el conjunto de sus imágenes respecto a las acciones de G:

$$O_x := \{g \cdot x \mid g \in G\}$$

(este es visiblemente un subconjunto G-equivariante).

Se dice que x es un **punto fijo** si $g \cdot x = x$ para todo $g \in G$; es decir, si

$$O_x = \{x\}.$$

El conjunto de los puntos fijos se denota por X^G.

El **estabilizador** de x viene dado por todos los elementos de G que dejan x fijo:

$$G_x := \{g \in G \mid g \cdot x = x\} \subseteq G.$$

9.2.2. Observación. *G_x es un subgrupo de G.*

Demostración. Primero, $1 \cdot x = x$. Luego, si $g \cdot x = x$, entonces actuando por g^{-1} se obtiene $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$, donde en la parte izquierda está $g^{-1} \cdot (g \cdot x) = 1 \cdot x = x$. Por fin, si $g \cdot x = x$ y $h \cdot x = x$, entonces $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$. ■

A veces se dice que G_x es el **grupo de isotropía** de x.

9.2.3. Definición. Se dice que una acción de G sobre X es **transitiva** si todos los puntos de X están en la misma órbita; es decir, si para cualesquiera $x, y \in X$ existe $g \in G$ tal que $x = g \cdot y$.

En este caso también se dice que X es un G-conjunto **homogéneo**.

9.2.4. Ejemplo. La acción del grupo simétrico S_X sobre X es transitiva. En particular, la acción de S_n sobre $\{1, 2, \ldots, n\}$ es transitiva. El estabilizador de $1 \leq i \leq n$ es el subgrupo

$$\{\sigma \in S_n \mid \sigma(i) = i\} \cong S_{n-1}.$$

▲

9.2.5. Ejemplo. La acción de $\mathrm{SL}_2(\mathbb{R})$ sobre $\mathcal{H}$ es transitiva. Para verlo, sería suficiente probar que para todo $z \in \mathcal{H}$ existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ tal que

$$z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \sqrt{-1}.$$

Luego, la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ aplica z en $\sqrt{-1}$. Dados dos puntos $z_1, z_2 \in \mathcal{H}$, para enviar z_1 en z_2, sería suficiente aplicar z_1 a $\sqrt{-1}$ y luego $\sqrt{-1}$ en z_2.

Ahora para cualesquiera $z = x + y\sqrt{-1}$ con $y > 0$ tenemos

$$\begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}), \quad \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \cdot \sqrt{-1} = \frac{\sqrt{y}\sqrt{-1} + x/\sqrt{y}}{1/\sqrt{y}} = x + y\sqrt{-1}.$$

▲

9.2.6. Ejemplo. Para la acción de $k^\times$ sobre $\mathbb{A}^n(k)$ el punto $(0, \ldots, 0)$ es fijo. Para un punto $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ su órbita consiste en todos los puntos no nulos que están en la recta que pasa por $(0, \ldots, 0)$ y $(x_1, \ldots, x_n)$:

$$\{(\lambda x_1, \ldots, \lambda x_n) \mid \lambda \in k^\times\}.$$

▲

El siguiente resultado nos dice que todo G-conjunto se descompone en una unión disjunta de G-conjuntos homogéneos.

9.2.7. Observación. *Sea X un G-conjunto. La relación*

$$x \sim_G y \iff x = g \cdot y \text{ para algún } g \in G$$

es una relación de equivalencia sobre X. Las clases de equivalencia son las órbitas. En particular, X se descompone en la union disjunta de las órbitas:

$$X = \bigsqcup_{[x] \in X/G} O_x,$$

donde X/G denota el conjunto de las órbitas.

Demostración. $x \sim_G x$, puesto que $1 \cdot x$. Ahora, si $x \sim_G y$, entonces $x = g \cdot y$ y luego $g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = y$. Por fin, si $x \sim_G y$ e $y \sim_G z$, tenemos $x = g \cdot y$ e $y = h \cdot z$, así que $x = g \cdot (h \cdot z) = (gh) \cdot z$. ■

9.2.8. Ejemplo. El grupo multiplicativo $k^\times$ actúa sobre $\mathbb{A}^{n+1} \setminus \{\underline{0}\}$. El conjunto de las órbitas correspondiente

$$\mathbb{P}^n(k) := (\mathbb{A}^{n+1} \setminus \{\underline{0}\})/k^\times = \{[x_0 : x_1 : \cdots : x_n] \mid x_i \in k,\ (x_0, x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)\}$$

se llama el **espacio proyectivo** de dimensión n sobre k. Sus elementos son las rectas en el espacio $\mathbb{A}^{n+1}$ que pasan por el origen. Para más información sobre el espacio proyectivo, el lector puede consultar Wikipedia y libros de texto de geometría.

Consideremos el caso $n = 1$. La definición nos dice que hay que considerar los elementos $(x, y) \in \mathbb{A}^2 \setminus \{(0, 0)\}$ módulo la relación de equivalencia

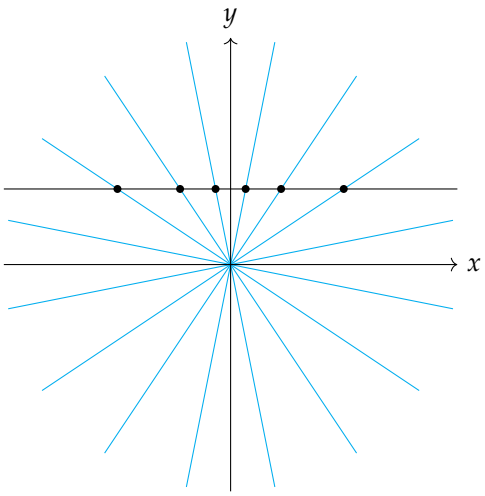
$$(x, y) \sim (\lambda x, \lambda y) \quad \text{para } \lambda \in k^\times.$$

Ahora si $y \neq 0$, tenemos $(x, y) \sim (x/y, 1)$. Si $y = 0$, entonces $x \neq 0$ y $(x, 0) \sim (1, 0)$. Esto nos dice que

$$\mathbb{P}^1(k) = \{[x : 1] \mid x \in k\} \sqcup \{[1 : 0]\}.$$

El conjunto $\{[x : 1] \mid x \in k\}$ está en una biyección natural con la recta afín $\mathbb{A}^1(k)$, y además hay un punto extra $[1 : 0]$ que se llama el **punto al infinito** y normalmente se denota por ∞.

Geométricamente, lo que está pasando es lo siguiente. La recta proyectiva es el conjunto de las rectas en el plano que pasan por el origen. Para parametrizar estas rectas, podemos tomar la proyección sobre una recta paralela a x, por ejemplo $y = 1$:



La recta que corresponde a $[x : y]$ con $y \neq 0$ interseca a la recta $y = 1$ en el punto $(x/y, 1)$. Nos queda la recta $y = 0$ que no tiene intersecciones con $y = 1$. Esta recta corresponde al punto al infinito. ▲

9.2.9. Proposición. *Hay una biyección natural entre la órbita O_x y el conjunto de las clases laterales G/G_x.*

Demostración. Definamos

$$O_x \to G/G_x,$$
$$g \cdot x \mapsto g\, G_x.$$

Esta aplicación está bien definida y es biyectiva:

$$g \cdot x = h \cdot x \iff h^{-1}g \cdot x = x \iff h^{-1}g \in G_x \iff g\,G_x = h\,G_x.$$

■

Los estabilizadores de los elementos de la misma órbita están relacionados de la siguiente manera.

9.2.10. Observación. *Sea X un G-conjunto. Para los estabilizadores se cumple*

$$G_{g\cdot x} = g\,G_x\,g^{-1}.$$

Demostración. Tenemos

$$G_{g\cdot x} = \{h \in G \mid h \cdot g \cdot x = g \cdot x\} = \{h \in G \mid g^{-1} \cdot h \cdot g \cdot x = x\} = g\,G_x\,g^{-1}.$$

■

En general, G_x no es un subgrupo normal de G. Por ejemplo, para el grupo simétrico S_3 que actúa sobre $\{1,2,3\}$ el estabilizador de 3 es el subgrupo $\{\mathrm{id}, (1\ 2)\} \cong S_2$ que no es normal en S_3. Sin embargo, se puede hablar de las clases laterales G/G_x.

9.2.11. Teorema (Ecuación de clase). *Sea X un G-conjunto finito. Sea X^G el subconjunto de puntos fijos y $O_{x_1}, \ldots, O_{x_n}$ las órbitas de la acción que contienen más de un elemento. Entonces,*

$$|X| = |X^G| + \sum_{1\le i\le n} |G : G_{x_i}|.$$

Demostración. Sigue del resultado anterior y la descomposición en la unión disjunta de clases de equivalencia

$$X = \bigsqcup_{x\in X^G} \{x\} \sqcup \bigsqcup_{1\le i\le n} O_{x_i}.$$

■

9.3 Acción de G sobre sí mismo por multiplicación

Algunos conceptos y resultados de la teoría de grupos pueden ser investigados en términos de acciones específicas de G sobre $X = G$.

Para $g, x \in G$ la fórmula

$$g \cdot x := gx$$

define una acción de G: los axiomas A1) y A2) son evidentes. Se dice que G actúa sobre sí mismo por multiplicación (por la izquierda).

9.3.1. Proposición. *La acción de G sobre sí mismo por multiplicación es fiel.*

Demostración. Esta acción corresponde a un homomorfismo

$$\begin{aligned} L\colon G &\to S_G, \\ g &\mapsto (L_g\colon x \to gx). \end{aligned}$$

Tenemos $L_g(1) = g \cdot 1 = g$, así que $L_g = \mathrm{id}_G$ si y solamente si $g = 1$. ■

9.3.2. Corolario (Teorema de Cayley). *Para todo grupo G existe un monomorfismo $G \rightarrowtail S_G$.*

Entonces, todo grupo G es isomorfo a un subgrupo de S_G. En particular, todo grupo finito es isomorfo a un subgrupo de S_n para algún n.

9.3.3. Comentario. La teoría de grupos surgió del estudio de permutaciones de raíces de polinomios en los trabajos de Lagrange (1770) y Galois (1831). De hecho, la palabra "grupo" viene de la expresión "grupo de permutaciones". La primera definición axiomática de grupo dio Cayley[*]. El último resultado nos dice que todos los grupos pueden ser realizados como subgrupos de grupos de permutaciones.

9.3.4. Ejemplo. La construcción de arriba no es muy efectiva: el grupo simétrico S_G es mucho más grande que G. El ejemplo mínimo no trivial sería de

$$G = \mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}.$$

La aplicación $x \mapsto [0] + x$ es la permutación identidad de los elementos de G. Luego, $x \mapsto [1] + x$ es la permutación

$$\begin{pmatrix} [0] & [1] & [2] \\ [1] & [2] & [0] \end{pmatrix}$$

e $x \mapsto [2] + x$ es la permutación

$$\begin{pmatrix} [0] & [1] & [2] \\ [2] & [0] & [1] \end{pmatrix}$$

La biyección $\{[0], [1], [2]\} \leftrightarrow \{1, 2, 3\}$ nos da un isomorfismo entre $S_{\mathbb{Z}/3\mathbb{Z}}$ y S_3 respecto al cual la imagen de G en S_3 puede ser identificada con

$$\left\{ \mathrm{id},\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3),\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) \right\}.$$

De hecho, es A_3, el único subgrupo de orden 3 en S_3. ▲

9.3.5. Comentario. En general, si $H \subseteq G$ es un subgrupo, entonces G actúa sobre el conjunto de las clases laterales izquierdas G/H mediante multiplicación:

$$g_1 \cdot g_2 H := g_1 g_2 H.$$

Esta acción es transitiva.

9.4 Acción de G sobre sí mismo por conjugación

9.4.1. Definición. Para $g, x \in G$ la **conjugación** de x por g viene dada por

$${}^g x := g\, x\, g^{-1}.$$

Notamos que para la identidad se tiene ${}^1 x = x$ y para cualesquiera $g, h, x \in G$

$$ {}^h({}^g x) = h\,(g\, x\, g^{-1})\, h^{-1} = (hg)\, x\, (hg)^{-1} = {}^{hg} x. \tag{9.2}$$

Entonces, lo que tenemos es una acción de G sobre sí mismo. La notación "${}^g x$" es una especie de "potencia", pero con el exponente escrito a la izquierda, puesto que la acción es por la izquierda.

[*] Arthur Cayley (1821–1895), uno de los fundadores de la escuela británica moderna de matemáticas puras.

9.4.2. Definición. Para la acción de G sobre sí mismo por conjugación la órbita

$$^G x := \{^g x = g\,x\,g^{-1} \mid g \in G\}$$

se llaman la **clase de conjugación** de x. El estabilizador

$$C_G(x) := \{g \in G \mid {}^g x := g\,x\,g^{-1} = x\} \subseteq G$$

se llama el **centralizador** de x.

9.4.3. Ejemplo. Como todo estabilizador, $C_G(x)$ no es necesariamente un subgrupo normal. Por ejemplo, en $G = S_3$ tenemos

$$C_{S_3}((1\ 2)) = \{\mathrm{id}, (1\ 2)\}.$$

De todos modos, podemos considerar las clases laterales $S_3/C_{S_3}((1\ 2))$. Estas están representadas por $(1\ 2), (1\ 3), (2\ 3)$ que son los elementos de la clase de conjugación de $(1\ 2)$. ▲

Notamos que $x \in G$ es un punto fijo si y solamente si x pertenece al centro de G:

$$^g x := g\,x\,g^{-1} = x \text{ para todo } g \in G \iff x \in Z(G).$$

9.4.4. Observación. *Un subgrupo $H \subseteq G$ es normal si y solamente si H es una unión de clases de conjugación en G.*

Demostración. $H \subseteq G$ es normal si y solamente si para todo elemento $h \in H$ se tiene $^G h \subseteq H$. ■

9.4.5. Ejemplo. Prometí que íbamos a demostrar directamente que el grupo alternante A_5 es simple. En efecto, las clases de conjugación son las siguientes.

clase:	$^G\mathrm{id}$	$^G(1\,2)\,(3\,4)$	$(1\,2\,3)$	$^G(1\,2\,3\,4\,5)$	$^G(1\,2\,3\,5\,4)$
tamaño:	1	15	20	12	12

Ya que todo subgrupo normal es una unión de clases de conjugación y contiene id, un cálculo tedioso nos dice que los posibles órdenes de subgrupos normales son

$$1,\ 13,\ 16,\ 21,\ 25,\ 28,\ 33,\ 36,\ 40,\ 45,\ 48,\ 60.$$

Ningún número de estos, salvo 1 y 60, divide a $|A_5| = 60$, y gracias al teorema de Lagrange podemos concluir que A_5 es un grupo simple. ▲

9.4.6. Teorema (Ecuación de clase). *Para un grupo finito G sean $x_1, \ldots, x_n$ los representantes de las clases de conjugación no triviales. Entonces*

$$|G| = |Z(G)| + \sum_{1 \le i \le n} |G : C_G(x_i)|.$$

Demostración. Es un caso particular de 9.2.11. ■

Notamos que para cualesquiera $g, x, y \in G$ se tiene

$$^g(xy) = g\,(xy)\,g^{-1} = (g\,x\,g^{-1})\,(g\,y\,g^{-1}) = {}^g x\,{}^g y,$$

así que las aplicaciones

$$I_g \colon x \mapsto {}^g x$$

no son simplemente biyecciones $G \to G$ sino automorfismos. Tenemos entonces un homomorfismo de grupos

$$\begin{aligned} I\colon G &\to \mathrm{Aut}(G) \subset S_G, \\ g &\mapsto (I_g\colon x \mapsto {}^g x). \end{aligned}$$

El núcleo de I coincide con el centro de G:

$$\ker I = \{g \in G \mid I_g = \mathrm{id}_G\} = \{g \in G \mid {}^g x := g\,x\,g^{-1} = x \text{ para todo } x \in G\} = Z(G).$$

Entonces, la acción de G sobre sí mismo por conjugación es fiel si y solamente si $Z(G) = \{1\}$.

De la misma manera, se ve que $x \in G$ es un punto fijo de la acción por conjugación si y solamente si $x \in Z(G)$.

9.4.7. Digresión. Los automorfismos de la forma

$$\begin{aligned} I_g\colon G &\to G, \\ x &\mapsto {}^g x \end{aligned}$$

se llaman los **automorfismos internos** de G. Estos forman un grupo (es la imagen del homomorfismo I) que se denota por $\mathrm{Inn}(G)$. El teorema de isomorfía nos dice que

$$G/Z(G) \cong \mathrm{Inn}(G).$$

Por ejemplo, $Z(S_n) = \{\mathrm{id}\}$ para $n \geq 3$, entonces todos los automorfismos de S_n son internos.

Notamos que $\mathrm{Inn}(G)$ es un subgrupo normal en $\mathrm{Aut}(G)$. De hecho, tenemos para cualquier automorfismo $f\colon G \to G$

$$f \circ I_g \circ f^{-1}(x) = f(g\,f^{-1}(x)\,g^{-1}) = f(g)\,x\,f(g)^{-1} = I_{f(g)}(x).$$

Así que $f \circ I_g \circ f^{-1} = I_{f(g)} \in \mathrm{Inn}(G)$. El grupo cociente

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$$

se llama el **grupo de automorfismos externos**.

Para terminar esta sección, notamos que la conjugación es una acción sobre el conjunto de subgrupos.

9.4.8. Observación. *Sea G un grupo y H su subgrupo. Entonces para todo $g \in H$ el conjunto*

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}$$

es también un subgrupo de G.

Demostración. Por supuesto, tenemos $1 = g \cdot 1 \cdot g^{-1}$. Ahora para $g\,h_1\,g^{-1}, g\,h_2\,g^{-1} \in gHg^{-1}$ se tiene

$$(g\,h_1\,g^{-1})\,(g\,h_2\,g^{-1}) = g\,(h_1h_2)\,g^{-1} \in gHg^{-1}.$$

Por fin, para $ghg^{-1} \in gHg^{-1}$ se tiene

$$(ghg^{-1})^{-1} = g\,h^{-1}\,g^{-1} \in gHg^{-1}.$$

■

Esto quiere decir que la acción de G sobre sí mismo por conjugación induce una acción sobre el conjunto de los subgrupos de G. Los puntos fijos de esta acción son precisamente los subgrupos normales.

9.5 Isomorfismos excepcionales: $\mathrm{PGL}_2(\mathbb{F}_3)$ y $\mathrm{PGL}_2(\mathbb{F}_5)$

En el capítulo 7 durante la discusión de grupos simples mencioné los isomorfismos excepcionales $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$ y $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$. Ahora tenemos las herramientas adecuadas para deducirlos. Esta sección es opcional.

9.5.1. Ejemplo. El grupo $\mathrm{GL}_2(k)$ actúa sobre el plano afín $\mathbb{A}^2(k)$ mediante aplicaciones lineales. Toda aplicación lineal preserva cada recta que pasa por el origen, así que esta acción da lugar a una acción de $\mathrm{GL}_2(k)$ sobre la recta proyectiva $\mathbb{P}^1(k)$. Esta acción no es fiel: dos matrices actúan de la misma manera si y solamente si una es un múltiplo escalar de la otra. Esto quiere decir que el núcleo de la acción es el subgrupo de las matrices escalares $Z(\mathrm{GL}_2(k)) \cong k^\times$. Luego, el cociente de $\mathrm{GL}_2(k)$ por este subgrupo:

$$\mathrm{PGL}_2(k) := \mathrm{GL}_2(k)/Z(\mathrm{GL}_2(k))$$

actúa sobre $\mathbb{P}^1(k)$ de manera fiel. Esto significa que existe un monomorfismo

$$\mathrm{PGL}_2(k) \rightarrowtail S_{\mathbb{P}^1(k)}.$$

Nos interesa el caso cuando $k = \mathbb{F}_p$ es un cuerpo finito. El orden de $\mathrm{PGL}_2(\mathbb{F}_p)$ viene dado por

$$|\mathrm{PGL}_2(\mathbb{F}_p)| = |\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times| = |\mathrm{GL}_2(\mathbb{F}_p)|/|\mathbb{F}_p^\times| = \frac{(p^2-1)\,(p^2-p)}{p-1} = p^3 - p.$$

Luego,

$$|S_{\mathbb{P}^1(\mathbb{F}_p)}| = (|\mathbb{P}^1(\mathbb{F}_p)|)! = (p+1)!$$

—la descomposición de $\mathbb{P}^1(\mathbb{F}_p)$ en $\mathbb{A}^1(\mathbb{F}_p)$ y ∞ nos dice que

$$|\mathbb{P}^1(\mathbb{F}_p)| = p + 1.$$

Ya que hay un monomorfismo $\mathrm{PGL}_2(\mathbb{F}_p) \rightarrowtail S_{\mathbb{P}^1(\mathbb{F}_p)}$, podemos comparar los órdenes de estos grupos para diferentes p. El factorial crece mucho más rápido que $p^3 - p$, así que solamente para valores pequeños de p se puede esperar algo interesante. Y en efecto, tenemos lo siguiente:

p	$\lvert\mathrm{PGL}_2(\mathbb{F}_p)\rvert$	$\lvert S_{\mathbb{P}^1(\mathbb{F}_p)}\rvert$
2	6	$3! = 6$
3	24	$4! = 24$
5	120	$6! = 720$
7	336	$8! = 40\,320$

Las primeras dos filas nos dicen que hay isomorfismos

$$\mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) \cong S_3, \quad \mathrm{PGL}_2(\mathbb{F}_3) \cong S_4.$$

Notamos que para $p \neq 2$ se tiene

$$\begin{aligned}|\mathrm{PSL}_2(\mathbb{F}_p)| = |\mathrm{SL}_2(\mathbb{F}_p)/Z(\mathrm{SL}_2(\mathbb{F}_p))| = |\mathrm{SL}_2(\mathbb{F}_p)/\{\pm I\}| &= \frac{1}{2}\,|\mathrm{SL}_2(\mathbb{F}_p)| \\ &= \frac{1}{2}\cdot\frac{1}{p-1}\,|\mathrm{GL}_2(\mathbb{F}_p)| = \frac{1}{2}\,|\mathrm{PGL}_2(\mathbb{F}_p)|,\end{aligned}$$

así que $\mathrm{PSL}_2(\mathbb{F}_p)$ es un subgrupo de índice 2 en $\mathrm{PGL}_2(\mathbb{F}_p)$. Siendo un subgrupo de índice 2, es normal. En $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$ hay un subgrupo único de índice 2: es isomorfo al grupo alternante. Podemos concluir que

$$\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4.$$

▲

Ya que $|\mathrm{PGL}_2(\mathbb{F}_5)| = 120 = 5!$, esto nos da esperanzas de encontrar un isomorfismo $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$. Sin embargo, las consideraciones de arriba nos dicen nada más que $\mathrm{PGL}_2(\mathbb{F}_5)$ puede ser realizado como un subgrupo de índice 6 en S_6, y hay que usar otro argumento.

9.5.2. Ejemplo. Los puntos de $\mathbb{P}^1(\mathbb{F}_5)$ son

$$0 = [0:1], \quad 1 = [1:1], \quad 2 = [2:1], \quad 3 = [3:1], \quad 4 = [4:1], \quad \infty = [1:0].$$

En $S_{\mathbb{P}^1(\mathbb{F}_5)}$ hay 15 permutaciones de orden 2 sin puntos fijos (en otras palabras, permutaciones de tipo $(\bullet\,\bullet)\,(\bullet\,\bullet)\,(\bullet\,\bullet)$):

$$\begin{array}{lll}
(0\,1)\,(2\,3)\,(4\,\infty), & (0\,1)\,(2\,4)\,(3\,\infty), & (0\,1)\,(2\,\infty)\,(3\,4),\\
(0\,2)\,(1\,3)\,(4\,\infty), & (0\,2)\,(1\,4)\,(3\,\infty), & (0\,2)\,(1\,\infty)\,(3\,4),\\
(0\,3)\,(1\,2)\,(4\,\infty), & (0\,3)\,(1\,4)\,(2\,\infty), & (0\,3)\,(1\,\infty)\,(2\,4),\\
(0\,4)\,(1\,2)\,(3\,\infty), & (0\,4)\,(1\,3)\,(2\,\infty), & (0\,4)\,(1\,\infty)\,(2\,3),\\
(0\,\infty)\,(1\,2)\,(3\,4), & (0\,\infty)\,(1\,3)\,(2\,4), & (0\,\infty)\,(1\,4)\,(2\,3).
\end{array}$$

Solamente 10 de estas permutaciones vienen de la acción de $\mathrm{PGL}_2(\mathbb{F}_5)$:

$$\begin{array}{ll}
\begin{pmatrix}1&4\\4&4\end{pmatrix} \mapsto (0\,1)\,(2\,3)\,(4\,\infty), & \begin{pmatrix}1&4\\3&4\end{pmatrix} \mapsto (0\,1)\,(2\,\infty)\,(3\,4),\\
\begin{pmatrix}1&3\\4&4\end{pmatrix} \mapsto (0\,2)\,(1\,3)\,(4\,\infty), & \begin{pmatrix}1&3\\2&4\end{pmatrix} \mapsto (0\,2)\,(1\,4)\,(3\,\infty),\\
\begin{pmatrix}1&2\\3&4\end{pmatrix} \mapsto (0\,3)\,(1\,4)\,(2\,\infty), & \begin{pmatrix}1&2\\1&4\end{pmatrix} \mapsto (0\,3)\,(1\,\infty)\,(2\,4),\\
\begin{pmatrix}1&1\\2&4\end{pmatrix} \mapsto (0\,4)\,(1\,2)\,(3\,\infty), & \begin{pmatrix}1&1\\1&4\end{pmatrix} \mapsto (0\,4)\,(1\,\infty)\,(2\,3),\\
\begin{pmatrix}0&1\\3&0\end{pmatrix} \mapsto (0\,\infty)\,(1\,2)\,(3\,4), & \begin{pmatrix}0&1\\2&0\end{pmatrix} \mapsto (0\,\infty)\,(1\,3)\,(2\,4).
\end{array}$$

Y otras 5 permutaciones no vienen de la acción de $\mathrm{PGL}_2(\mathbb{F}_5)$:

$$(0\,1)\,(2\,4)\,(3\,\infty), \quad (0\,2)\,(1\,\infty)\,(3\,4), \quad (0\,3)\,(1\,2)\,(4\,\infty), \quad (0\,4)\,(1\,3)\,(2\,\infty), \quad (0\,\infty)\,(1\,4)\,(2\,3).$$

El grupo $S_{\mathbb{P}^1(\mathbb{F}_5)}$, y en particular su subgrupo $\mathrm{PGL}_2(\mathbb{F}_5)$, actúa por conjugación sobre las 15 permutaciones de tipo $(\bullet\,\bullet)\,(\bullet\,\bullet)\,(\bullet\,\bullet)$. La acción de $\mathrm{PGL}_2(\mathbb{F}_5)$ se restringe a una acción fiel sobre las 5 permutaciones de arriba. Esto nos da un monomorfismo $\mathrm{PGL}_2(\mathbb{F}_5) \rightarrowtail S_5$. Ya que $|\mathrm{PGL}_2(\mathbb{F}_5)| = |S_5|$, podemos concluir que

$$\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5.$$

Además, $\mathrm{PSL}_2(\mathbb{F}_5)$ es un subgrupo de índice 2 en $\mathrm{PGL}_2(\mathbb{F}_5)$, así que

$$\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5.$$

▲

9.6 Ejercicios

Ejercicio 9.1. *Consideremos la acción del grupo* $\mathrm{SL}_2(\mathbb{R})$ *sobre el semiplano superior* $\mathcal{H}$*. Demuestre que el estabilizador para el punto* $\sqrt{-1} \in \mathcal{H}$ *es el grupo*

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\phi & -\operatorname{sen}\phi \\ \operatorname{sen}\phi & \cos\phi \end{pmatrix} \;\middle|\; 0 \leq \phi < 2\pi \right\} = O_2(\mathbb{R}) \cap \mathrm{SL}_2(\mathbb{R}).$$

Ejercicio 9.2. *Consideremos la acción del grupo* $\mathrm{SL}_2(\mathbb{Z})$ *sobre el semiplano superior* $\mathcal{H}$*. Calcule el estabilizador para los puntos* $\sqrt{-1}$ *y* $\omega := -\frac{1}{2} + \frac{\sqrt{3}}{2}\sqrt{-1}$*.*

Ejercicio 9.3. *Demuestre que el núcleo de la acción de* $\mathrm{SL}_2(\mathbb{R})$ *sobre* $\mathcal{H}$ *es el subgrupo* $Z(\mathrm{SL}_2(\mathbb{R})) = \{\pm I\}$*.*

Ejercicio 9.4. *Sea* p *un número primo y sea* X *un* G*-conjunto finito. Supongamos que para todo subgrupo* $H \subsetneq G$ *su índice es divisible por* p*:*

$$p \mid |G : H|.$$

Deduzca que el número de los puntos fijos es congruente módulo p *al número de los elementos de* X*:*

$$|X| \equiv |X^G| \pmod{p}.$$

Indicación: considere la ecuación de clase.

Ejercicio 9.5. *Supongamos que* G *es un grupo finito de orden* p^k *donde* p *es primo. Demuestre que* $p \mid |Z(G)|$*, y en particular* $Z(G) \neq \{1\}$*.*

Ejercicio 9.6. *Demuestre que si* G *es un grupo finito de orden* p^2*, entonces* G *es abeliano.*

Ejercicio 9.7 (Teorema de Cayley). *Sea* G *un grupo finito y sea* p *un número primo tal que* $p \mid |G|$*. En este ejercicio vamos a probar que en* G *hay un elemento de orden* p*. Para esto consideremos el conjunto*

$$X := \{(g_0, g_1, \ldots, g_{p-1}) \mid g_i \in G,\ g_0 g_1 \cdots g_{p-1} = 1\}.$$

1) *Demuestre que* $|X| = |G|^{p-1}$*.*

2) *Para* $[n]_p \in \mathbb{Z}/p\mathbb{Z}$ *sea* $[n]_p \cdot (g_0, g_1, \ldots, g_{p-1}) := (g_{[0+n]}, g_{[1+n]}, \ldots, g_{[p-1+n]})$*. Demuestre que esto define una acción de* $\mathbb{Z}/p\mathbb{Z}$ *sobre* X *y sus puntos fijos son* $(g, g, \ldots, g)$ *donde* $g^p = 1$*.*

3) *Demuestre que el número de elementos* $g \in G$ *tales que* $g^p = 1$ *es divisible por* p*. Concluya que existe* $g \neq 1$ *tal que* $g^p = 1$*.*

Ejercicio 9.8. *Supongamos que un grupo finito* G *actúa sobre un conjunto finito* X*. Para un elemento* $g \in G$ *denotemos por* X^g *el conjunto de todos los puntos fijos por* g*:*

$$X^g := \{x \in X \mid g \cdot x = x\}.$$

Demuestre que

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |X^g|.$$

Deduzca la siguiente identidad combinatoria[*]*:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

(en palabras: el número de órbitas es igual al número promedio de puntos fijos).
Indicación: use las biyecciones $O_x \cong G/G_x$*.*

[*] Este identidad se conoce como el **lema de Burnside** y es muy común en combinatoria y matemáticas recreativas.

Ejercicio 9.9. *Verifique la descripción de las clases de conjugación en A_5.*

Ejercicio 9.10. *Hemos probado que en A_n para $n \geq 5$ todos los 3-ciclos forman una clase de conjugación. Demuestre que en A_4 no todos los 3-ciclos son conjugados entre sí.*

Ejercicio 9.11. *Encuentre las clases de conjugación en el grupo de cuaterniones Q_8.*

Ejercicio 9.12. *En este ejercicio encontraremos las clases de conjugación del grupo diédrico D_n.*

1) *Demuestre que cada rotación r^i está conjugada con r^{-i} y consigo misma.*
2) *Demuestre que la clase de conjugación de la reflexión fr^i viene dada por las reflexiones fr^{i-2j} para $j \in \mathbb{Z}$.*
3) *Termine la descripción de las clases de conjugación. (La respuesta depende de la paridad de n.)*

Ejercicio 9.13. *Hemos visto que $\mathbb{P}^1(k) = \mathbb{A}^1(k) \sqcup \{\infty\}$.*

1) *Demuestre que en general $\mathbb{P}^n(k) = \mathbb{A}^n(k) \sqcup \mathbb{P}^{n-1}(k)$.*
2) *Deduzca que $\mathbb{P}^n(k) = \mathbb{A}^n(k) \sqcup \mathbb{A}^{n-1}(k) \sqcup \cdots \sqcup \mathbb{A}^0(k)$.*
3) *Calcule el número de puntos en el espacio proyectivo $\mathbb{P}^n(\mathbb{F}_p)$ usando 2).*
4) *Calcule el mismo número a partir de la definición $\mathbb{P}^n(\mathbb{F}_p) := (\mathbb{A}^{n+1}(\mathbb{F}_p) \setminus \{\underline{0}\})/\mathbb{F}_p^\times$.*

Ejercicio 9.14. *Describa la permutación de $\{0, 1, 2, 3, 4, \infty\}$ que corresponde a la acción de $\begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_5)$ sobre $\mathbb{P}^1(\mathbb{F}_5)$.*