Lección nº 2 Junio, 2021

Capítulo 2

Acciones de Grupos

2.1. Acción de un Grupo sobre un Conjunto

Consideraremos S un conjunto, G un grupo y $\mathrm{Sym}(S)$ el grupo de permutaciones de S.

Definición. Decimos que G es un *grupo de permutaciones sobre S* si existe un homomorfismo

$$\phi\colon G \longrightarrow \mathrm{Sym}(S).$$

Es decir, para cada $x \in G$, $\phi(x) \in \mathrm{Sym}(S)$. Así

$$\begin{aligned}
&\phi(x)\colon S \xrightarrow{\sim} S \quad (\phi \text{ es una biyeción}),\\
&\phi(x)(s) \in S \quad \forall\, s \in S,\\
&\phi(xy)(s) = \phi(x)(\phi(y)s) \quad \forall\, x, y \in G,\ \forall\, s \in S.
\end{aligned}$$

Esto se puede interpretar de una forma equivalente a través de la siguiente noción.

Decimos que G *opera sobre S* si se tiene una aplicación, llamada una *acción de G sobre S*,

$$\begin{array}{rcl} G \times S & \dot{\longrightarrow} & S \\ (x, s) & \longmapsto & x \cdot s \end{array}$$

tal que

(1) $1 \cdot s = s \quad \forall\, s \in S.$

(2) $\forall\, x, y \in G,\ \forall\, s \in S, \quad (xy) \cdot s = x \cdot (y \cdot s).$

Observación. Ambas definiciones son equivalentes. En efecto, sea $\phi\colon G \to \mathrm{Sym}(S)$ un homomorfimo. Definamos la *acción de G sobre S*

$$\begin{array}{rcl} G \times S & \longrightarrow & S \\ (x, s) & \longmapsto & x \cdot s = \phi(x)(s). \end{array}$$

Entonces

(1) $1 \cdot s = \phi(1)s = \mathrm{id}_S(s) = s \quad \forall\, s \in S$.

(2) Sean $x, y \in G$ y $s \in S$, así

$$(xy) \cdot s = \phi(xy)s = \phi(x)(\phi(y)s) = x \cdot (y \cdot s).$$

Inversamente, sea $G \times S \to S$ una *acción* de G sobre S. Luego, para cada $x \in G$, las dos propiedades de acción nos permiten deducir que

$$\begin{array}{rcl} \phi(x)\colon S & \longrightarrow & S \\ s & \longmapsto & \phi(x)s = x \cdot s, \end{array}$$

es una biyección, y así

$$\begin{array}{rcl} \phi\colon G & \longrightarrow & \mathrm{Sym}(S) \\ x & \longmapsto & \phi(x), \end{array}$$

está bien definida, Además, estas mismas propiedades implican que ϕ es un homomorfismo de grupos.

Ejemplo 2.1. Sea G un grupo y $S = G$. Se define una acción de G sobre G

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gx. \end{array}$$

Esta acción define un homomorfismo

$$\begin{array}{rcl} \phi\colon G & \longrightarrow & \mathrm{Sym}(G) \\ g & \longmapsto & g \cdot \end{array}$$

el cual se denomina *acción regular por la izquierda de G sobre G*. Notemos que

$$\ker(\phi) = \{g \in G \mid gx = x,\ \forall\, x \in G\} = \{1\}.$$

Por tanto, G es isomorfo a un subgrupo de $\mathrm{Sym}(G)$. En particular, si $|G| = n$, tenemos que $G \hookrightarrow S_n$.

Observaciones.

(1) Todo grupo se puede representar como un subgrupo de un grupo de permutaciones.

(2) Si $|G| = n$, entonces $G \hookrightarrow S_n$.

Ejemplo 2.2. Nuevamente, sea G un grupo y $N \trianglelefteq G$, definimos la *acción de G sobre N por conjugación* como

$$\begin{array}{rcl} G & \xrightarrow{I} & \mathrm{Sym}(N) \\ g & \longmapsto & I_g, \end{array} \quad \text{donde} \quad \begin{array}{rcl} I_g\colon N & \longrightarrow & N \\ x & \longmapsto & gxg^{-1}. \end{array}$$

Notemos que la acción definida a través de I es

$$\begin{array}{rcl} G \times N & \longrightarrow & N \\ (g, x) & \longmapsto & g \cdot x = I_g(x) = gxg^{-1}. \end{array}$$

Además, tenemos que

$$\begin{aligned} \ker(I) &= \{g \in G \mid I_g = \mathrm{id}_N\} \\ &= \{g \in G \mid gxg^{-1} = x,\ \forall\, x \in N\} \\ &= \{g \in G \mid gx = xg,\ \forall\, x \in N\} \\ &= Z(G). \end{aligned}$$

Definición. Una acción $G \times S \to S$ es *fiel* si y solo si para cada $g \in G$ se verifica que

$$g \cdot x = x \quad \forall\, x \in S \Longrightarrow g = 1.$$

Ejemplos 2.3. En todos los ejemplos consideraremos G un grupo y S un conjunto no vacío.

(1) La *acción trivial* no es fiel, es decir, la acción definida como

$$g \cdot s = s \quad \forall\, s \in S, \forall\, x \in G.$$

(2) La acción regular de G sobre G por izquierda, o representación regular por izquierda,

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & xy \end{array}$$

es fiel.

Definición. Sea $G \times S \to S$ una acción. Esta acción es *transitiva* si para todo par $s, t \in S$, existe un $x \in G$ tal que

$$x \cdot s = t.$$

O equivalentemente, si para todo $s \in S$ se verifica que

$$S = \{x \cdot s \,|\, x \in G\} =: G \cdot s.$$

Ejercicio 2.4. Sea $n \geq 2$. Consideremos el grupo ortogonal $O(n)$ y $S = \{x \in \mathbb{R}^n \,|\, \|x\| = a\}$, con a fijo y $a \neq 0$. Demostrar que la aplicación

$$\begin{array}{rcl} O(n) \times S & \longrightarrow & S \\ (A, x) & \longmapsto & Ax \end{array}$$

es una acción transitiva de $O(n)$ sobre S.

Teorema 2.5. *Sean $x, y \in \mathbb{R}^n \setminus \{0\}$. Si $\|x\| = \|y\|$, entonces existe $A \in O(n)$ tal que $Ax = y$.*

Definición. Sean G un grupo, S un conjunto, y $G \times S \to S$ una acción. Dado $s \in S$, definimos la *órbita de s bajo G* por

$$\mathrm{Orb}_G(s) = G \cdot s = \{x \cdot s \,|\, x \in G\}.$$

Esta acción define una relación de equivalencia: Dados $t, s \in S$

$$s \sim t \Longleftrightarrow \exists\, x \in G \text{ tal que } x \cdot s = t.$$

Ejercicio 2.6. Comprobar que $\sim$ es una relación de equivalencia.

Las órbitas de los elementos de S son exactamente las clases de equivalencia de la relación $\sim$. Y, dados $s, t \in S$, las órbitas $G \cdot s$ y $G \cdot t$ satisfacen solo una de las dos siguientes afirmaciones:

- $\mathrm{Orb}_G(s) = \mathrm{Orb}_G(t)$.
- $\mathrm{Orb}_G(s) \cap \mathrm{Orb}_G(t) = \emptyset$.

Así

$$S = \bigsqcup_{i \in I} \mathrm{Orb}_G(s_i),$$

donde I recorre todas las órbitas distintas de los elementos de S bajo G. Es decir que $\{s_i \,|\, i \in I\}$ es un sistema de representantes.

Observación. Para todo $x \in G$, la familia $\{x \cdot s_i \,|\, i \in I\}$ también es un sistema de representantes.

Definición. Sean G un grupo, S un conjunto, y $s \in S$, el *estabilizador de s bajo G* por

$$\mathrm{Stab}_G(s) \colon = \{x \in G \,|\, x \cdot s = s\}$$

Ejercicio 2.7. Probar que $\mathrm{Stab}_G(s) \leq G$.

El conjunto cociente de S módulo G es el conjunto de todas las clases de equivalencia de la acción de G sobre S.

$$S/G = \{G \cdot s \,|\, s \in S\} = \{G \cdot s_i \,|\, i \in I\}.$$

Además, la función

$$\begin{aligned} \mathrm{Orb}_G \colon S &\to S/G \\ s &\mapsto \mathrm{Orb}_G(s) = G \cdot s \end{aligned}$$

es sobreyectiva. Se puede ver también que G opera transitivamente sobre S si y sólo si $S/G = \{G \cdot s\}$, $\forall s \in S$.

Ejemplo 2.8. Sea G un grupo. Notemos por χ al conjunto conformado por los subgrupos de G, y consideramos el operador

$$\begin{aligned} G \times \chi &\to \chi \\ (x, H) &\mapsto x \cdot H = xHx^{-1}. \end{aligned}$$

Veamos que este operador define una acción de G sobre χ: Sean $x, y \in G$ y $H \leq G$, se tiene

$$x \cdot (y \cdot H) = x \cdot (yHy^{-1}) = xyHy^{-1}x^{-1} = (xy)H(xy)^{-1}.$$

El estabilizador de H bajo G está dado por

$$\mathrm{Stab}_G(H) = \{x \in G \,|\, xHx^{-1} = H\}.$$

A este grupo se lo conoce como el *normalizador de H* y se denota por $N_G(H)$.

Ejemplo 2.9 (Acción de G sobre G por conjugación)**.**

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto xyx^{-1}. \end{aligned}$$

Las órbitas son las clases de conjugación de G:

$$\mathrm{Orb}_G(y) = \{xyx^{-1} \,|\, x \in G\}.$$

Y para los estabilizadores se tiene que

$$\mathrm{Stab}_G(y) = \{x \in G \,|\, xyx^{-1} = y\}.$$

Definición. Sea G un grupo, y $y \in G$.

(1) $\mathrm{cl}(y) = \{xyx^{-1} \,|\, x \in G\}$ se llama *clase de conjugación de* y.

(2) $C_G(y) = \{x \in G \,|\, xy = yx\}$ es llamado el *centralizador de* y *en* G.

Observaciones. (1) Para la acción de G sobre G por conjugación, gracias al ejemplo anterior sabemos que $\mathrm{Orb}_G(y) = \mathrm{cl}(y)$ y $\mathrm{Stab}_G(y) = C_G(y)$.

(2) Si $y \in Z(G)$, entonces $C_G(y) = G$.

(3) $\mathrm{cl}(y) = \{y\}$ si y sólo si $y \in Z(G)$.

Teorema 2.10 (Teorema de la órbita-estabilizador)**.** *Sea G un grupo, $G \times S \to S$ una acción. Para todo $s \in S$, se tiene que*

i. $\mathrm{Stab}_G(s) \leq G$*;*

ii. Se tiene una biyección entre $\mathrm{Orb}_G(s)$ *y* $G/\mathrm{Stab}_G(s)$*;*

iii. Si $|G| < +\infty$*,* $|\mathrm{Orb}_G(s)| = |G/\mathrm{Stab}_G(s)| = [G\colon \mathrm{Stab}_G(s)] = |G| \,/\, |\mathrm{Stab}_G(s)|$*. Por tanto* $|G| = |\mathrm{Orb}_G(s)|\,|\mathrm{Stab}_G(s)|$.

Demostración. i. Se sigue ejercicio 2.7.

ii. Sean $x, y \in G$ tales que $x \cdot s = y \cdot s$, entonces $(y^{-1}x) \cdot s = s$. Esto último imlica que $x\mathrm{Stab}_G(s) = x\mathrm{Stab}_G(s)$. En efecto, sea $z \in \mathrm{Stab}_G(s)$, notemos que $xz = y(y^{-1}xz)$, donde $y^{-1}xz \in \mathrm{Stab}_G(s)$ pues

$$(y^{-1}xz) \cdot s = (y^{-1}x) \cdot s = s.$$

Es decir, $x\mathrm{Stab}_G(s) \subseteq y\mathrm{Stab}_G(s)$. La otra contenencia se obtiene siguiendo el mismo procedimiento, notando que también tenemos $(x^{-1}y) \cdot s = s$.

De esta manera, la aplicación

$$\begin{aligned} \psi\colon \mathrm{Orb}_G(s) &\to G/\mathrm{Stab}_G(s) \\ x \cdot s &\mapsto \psi(x \cdot s) = x\mathrm{Stab}_G(s) \end{aligned}$$

está bien definida y es inyectiva. Además es fácil de ver que ψ también es sobreyectiva, siendo así una biyección entre $\mathrm{Orb}_G(s)$ y $G/\mathrm{Stab}_G(s)$.

iii. Se sigue de (ii).

□

Corolario 2.11. *Si* $|G| < +\infty$*, entonces* $|\mathrm{Orb}_G(s)| \mid |G|$.

Ejemplo 2.12. Dados G un grupo finito y $y \in G$, tenemos que

$$|\mathrm{cl}(y)| = |\mathrm{Orb}_G(y)| = [G\colon \mathrm{Stab}_G(y)] = [G\colon C_G(y)] = |G| \,/\, |C_G(y)|\,.$$

Además

$$G = \bigsqcup_{i \in I} \mathrm{cl}(y_i),$$

donde I recorre las clases de conjugación distintas.

Denotaremos por $x_1, \ldots, x_k \in G$ los elementos que representan a todas las clases de conjugaciones con más de un elemento, es decir, tales que $|\mathrm{cl}(x_i)| > 0 \ \forall i \in \{1, \ldots, k\}$. Así

$$G = \bigsqcup_{y \in Z(G)} \{y\} \sqcup \bigsqcup_{1=i}^{k} \mathrm{cl}(x_i),$$

y

$$|G| = |Z(G)| + \sum_{i}^{k} |\mathrm{cl}(x_i)| = |Z(G)| + \sum_{i=1}^{k} [G \colon C_G(x_i)] \,.$$

Teorema 2.13 (Ecuación de clase)**.** *Dado G un grupo. Con las notaciones anteriores, se tiene que*

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G \colon C_G(x_i)] \,.$$

Dado $p \leq 2$, diremos que un grupo G es un p-grupo si existe $n \leq 1$ entero tal que $|G| = p^n$.

Ejemplo 2.14. Sea G un p-grupo, por definición, se tiene que $p \mid |G|$. Por otro lado, por el ejemplo 2.12 sabemos que $[G \colon C_G(x_i)] \mid |G|$, con $[G \colon C_G(x_i)] = |\mathrm{cl}(y)|$ estrictamente menor que $|G|$, pues si no, existiría $y \in G$ tal que $yx_iy^{-1} = 1$, entonces $x_i = 1$ y $|\mathrm{cl}(x_i)|$ sería únicamente la identidad, lo cual no es posible. De esta manera $[G \colon C_G(x_i)]$ es una potencia de p y por el teorema anterior, tenemos

$$|Z(G)| = p^n - \sum_{i=1}^{k} [G : C_G(x_i)] \,,$$

por ende $p \mid |Z(G)|$ y por lo tanto $Z(G)$ es no trivial.

Corolario 2.15. *Sea G un p-grupo. Entonces*

$$|Z(G)| > 1$$

y es potencia de p.

Corolario 2.16. *Sea G un p-grupo. Se tiene que*

$$Z(G) \trianglelefteq G$$

y es un p-grupo no trivial. Así, $|G/Z(G)| < |G|$ y $G/Z(G)$ es un p-grupo.

Esta propiedad sirve para demostrar por inducción ciertas propiedades sobre p-grupos.

Observación. En la ecuación de clase, todos los sumandos son divisores de $|G|$.

Ejemplo 2.17. Sean G un grupo y $H \leq G$, $G/H = \{xH \mid x \in G\}$ (como conjunto). G opera sobre G/H mediante la siguiente acción:

$$\begin{aligned} G \times G/H &\to G/H \\ (x, yH) &\mapsto xyH. \end{aligned}$$

Ejercicio 2.18. Probar que la aplicación del ejemplo anterior define una acción.

De forma equivalente, consideramos el homomorfismo

$$\begin{aligned} \phi\colon G &\to \mathrm{Sym}(G/H) \\ x &\mapsto \phi(x), \end{aligned}$$

con $\phi(x)(yH) = xyH$, $\forall yH \in G/H$. Buscamos el núcleo de ϕ:

$$\begin{aligned} x \in \ker(\phi) &\iff xyH = yH, && \forall y \in G \\ &\iff y^{-1}xyH = H, && \forall y \in G \\ &\iff y^{-1}xy \in H, && \forall y \in G \\ &\iff x \in yHy^{-1}, && \forall y \in G \\ &\iff x \in \textstyle\bigcap_{y\in G} yHy^{-1}. \end{aligned}$$

Así,

$$\ker(\phi) = \bigcap_{y\in G} yHy^{-1} =: H_G \trianglelefteq G.$$

$H_G \trianglelefteq H$ se denomina el *interior normal de* H. Además, por el primer teorema de isomorfía

$$G/H_G \hookrightarrow \mathrm{Sym}(G/H).$$

Sea G un grupo finito, entonces

$$\mathrm{Sym}(G/H) = S_{|G/H|},$$

y

$$[G\colon H_G] \mid \left|S_{|G/H|}\right|.$$

Observación. H_G es el subgrupo normal más grande de G contenido en H.

Ejercicio 2.19. Supongamos que G es un grupo finito y sea $H \leq G$, notemos $n = [G\colon H]$ y supongamos que $|G| \nmid n!$. Entonces existe un subgrupo normal $K \trianglelefteq G$ tal que $K \neq \{1\}$ y $K \leq H$. En particular, G no es simple.

Teorema 2.20 (Cauchy)**.** *Sea G un grupo finito y $p \geq 2$ un número primo tal que $p \mid |G|$. Entonces existe $x \in G$ tal que*

$$|x| = p.$$

En particular G contiene un subgrupo cíclico de orden p.

Demostración. Consideremos el grupo $\underbrace{G \times \cdots \times G}_{p \text{ veces}} = \{(x_1, \ldots, x_p) \,|\, x_1, \ldots, x_p \in G\}$. Consideremos además el conjunto

$$S = \langle \{(x_1, \ldots, x_p) \in G \times \cdots \times G\rangle \,|\, x_1 \ldots x_p = 1\} \setminus \{1, \ldots, 1\}$$

Observemos que $x_1 \ldots x_p = 1$ si y sólo si $x_p = x_{p-1}^{-1} \ldots x_1^{-1}$, es decir que x_p está determinado por $x_1 \ldots x_{p-1}$. Luego, $|S| = |G|^{p-1} - 1$. Sean C un grupo cíclico de orden p y $z \in C$ tal que $C = \langle z \rangle$. Definamos la acción de C sobre S

$$\begin{aligned} C \times S &\to S \\ (z, (x_1, \ldots, x_p)) &\mapsto z \cdot (x_1, \ldots, x_p) = (x_2, \ldots, x_p, x_1) \\ (z^n, (x_1, \ldots, x_p)) &\mapsto z \cdot (z^{n-1} \cdot (x_1, \ldots, x_p)). \end{aligned}$$

Veamos que esta acción está bien definida. Sea $(x_1, \ldots, x_n) \in S$, basta probar que $z \cdot (x_1, \ldots, x_n)$ pertenece a S, es decir, probar que

$$x_2 \ldots x_p x_1 = 1.$$

Lo cual se tiene pues, como $x_1 \ldots x_p = 1$, entonces

$$x_2 \ldots x_p x_1 = x_1^{-1} x_1 = 1.$$

Vimos que el número de elementos de cada órbita de esta acción divide a $|C| = p$ (teorema 2.10). Si todas las órbitas de esta acción tuvieran orden p, entonces $|S|$ sería un múltipo de p, es decir, $p \mid |S|$. Pero $|S| = |G|^{p-1} - 1$, de donde, como $p \mid |G|$, tendríamos $p|1$, lo cual no es posible. Así, existe una órbita con un sólo elemento, es decir que existe $(x_1, \ldots, x_p) \in S$ tal que $z^n \cdot (y_1, \ldots, y_p) = (x_1, \ldots, x_p)$ para todo $n \in \{1, \ldots, p\}$. Esto implica que todos los x_i sean iguales, para todo $i \in \{1, \ldots, p\}$, y por tanto este único elemento tiene la forma $(x, \ldots, x)$, que además satisface

$$x \ldots x = 1,$$

es decir $|x| = p$. □

¿Cómo encontrar el número de órbitas de una acción sobre un conjunto X?
Sean G un grupo, X un conjunto y $G \times X \to X$ una acción de grupo. G también opera sobre cada órbita, mediante la acción

$$\begin{aligned} G \times \mathrm{Orb}_G(x) &\to \mathrm{Orb}_G(x) \\ (g, h \cdot x) &\mapsto gh \cdot x. \end{aligned}$$

Ejercicio 2.21. Probar que esta acción es transitiva.

Sabemos que

$$X = \bigsqcup_{i \in I} \mathrm{Orb}_G(s_i),$$

donde I recorre todas las órbitas distintas de los elementos de X bajo G. Si X y G son finitos podemos numerar estos elementos de 1 a h, con $h \in \mathbb{N}$. El subsiguiente teorema es una consecuencia inmediata de esta discusión.

Teorema 2.22 (Ecuación de clases II)**.** *Sean G un grupo y X un conjunto, ambos finitos. Se satisface la siguiente igualdad*

$$|X| = \sum_{i=1}^{h} |\mathrm{Orb}_G(x_i)| = |G| \sum_{i=1}^{h} \frac{1}{|\mathrm{Stab}_G(x_i)|}.$$

Corolario 2.23. *Sea G un grupo finito, entonces*

$$1 = \sum_{i=1}^{h} \frac{1}{|C_G(x_i)|}.$$

Definición. Dados X un conjunto, G un grupo que opera sobre X y $g \in G$. Notaremos:

$$\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}, \quad F_g = |\mathrm{Fix}(g)|.$$

Teorema 2.24 (Lema de Burnside)**.** *Sean X un conjunto y G un grupo finito que opera sobre X. Entonces se verifica la igualdad*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = \frac{1}{|G|}\sum_{g\in G}F_g.$$

Demostración. Usaremos el hecho de que G opera sobre cada órbita de esta acción transitivamente y dividiremos la demostración en dos partes.

(1) Supongamos que G opera transitivamente sobre X (entonces hay una sola órbita $G\cdot x$, $x\in X$). Entonces

$$X/G = \{G\cdot x\} = \{X\}.$$

Así $|X/G| = 1$. Probaremos que $|G| = \sum_{g\in G}F_g$. Definimos

$$Y = \{(g,x)\in G\times X \mid g\cdot x = x\}\subseteq G\times X.$$

Contaremos $|Y|$ de dos maneras distintas. Para la primera, fijamos $x\in X$. Dado $g\in G$, $(g,x)\in Y$ si y sólo si $g\cdot x = x$, es decir, si $g\in \mathrm{Stab}_G(x)$. Luego

$$|\{(g,x)\mid g\cdot x = x\}| = |\mathrm{Stab}_G(x)|,$$

y $|Y| = \sum_{y\in X}|\mathrm{Stab}_G(y)|$.

Ejercicio 2.25. Sean X un conjunto y G un grupo que opera sobre X. Sean $x, y\in X$ y $g\in G$ tales que $g\cdot x = y$ ($x\in \mathrm{Orb}_G(y)$). Entonces $\mathrm{Stab}_G(x) = g\mathrm{Stab}_G(y)g^{-1}$. En particular $|\mathrm{Stab}_G(x)| = |\mathrm{Stab}_G(y)|$.

Del ejercicio anterior, puesto que $G\cdot x$ es la única órbita, obtenemos

$$|Y| = \sum_{y\in X}|\mathrm{Stab}_G(y)| = |G\cdot x|\,|\mathrm{Stab}_G(x)| = |G|.$$

Calculamos $|Y|$ de otra manera: Sea $g\in G$, tenemos que

$$\{x\in X\mid (g,x)\in Y\} = \mathrm{Fix}(g).$$

Así $|Y| = \sum_{g\in G}F_g$, con lo cual $|G| = \sum_{g\in G}F_g$.

(2) Para el caso general, notemos por I al índice que recorre todas las órbitas distintas, de modo que

$$X = \bigsqcup_{i\in I}\mathrm{Orb}_G(x_i).$$

Dados g e $i\in I$, notemos $\mathrm{Fix}^i(g) = \{x\in \mathrm{Orb}_G(x_i)\mid g\cdot x = x\}$. Dado que G opera transitivamente sobre cada $\mathrm{Orb}_G(x_i)$, $i\in I$, por lo ya visto, sabemos que

$$\sum_{y\in Y}\left|\mathrm{Fix}^i(g)\right| = |G|, \quad \forall i\in I.$$

Por otro lado, dado $g\in G$, se cumple también que

$$\mathrm{Fix}(g) = \bigsqcup_{i\in I}\mathrm{Fix}^i(g).$$

Finalmente

$$\sum_{g\in G}F_g = \sum_{i\in I}\sum_{g\in G}\left|\mathrm{Fix}^i(g)\right| = \sum_{i\in I}|G| = |X/G|\,|G|.$$

□

Ejemplo 2.26. Supongamos que G opera sobre X transitivamente. Entonces

$$1 = \frac{1}{|G|} \sum_{g \in G} F_g. \tag{2.1}$$

Como $F_1 = |X|$, si suponemos que $|X > 1|$ se sigue que $F_1 > 1$. Por (2.1), existe $g \in G$ tal que $F_g < 1$, y así g no tiene puntos fijos (que $F_g = 0$).

Corolario 2.27. *Si G opera transitivamente sobre X, con $|X| > 1$, entonces al menos un $g \in G$ no tiene puntos fijos.*

Observemos una aplicación de esto. Sea $H \leq G$ y $X = G/H = \{xH \mid x \in G\}$. Supongamos que H es distinto de G, es decir $|X| > 1$. G opera transitivamente sobre X (por multiplicación a la izquierda). Por el corolario anterior existe $g \in G$ con $F_g = 0$, es decir $\mathrm{Fix}(g) = \emptyset$. Por tanto, g no fija ninguna clase lateral de H.

El estabilizador de alguna clase lateral xH es $G_{xH} = xHx^{-1}$. Por lo anterior, g no deja fijo a xH para todo $x \in G$. De donde

$$g \notin \bigcap_{x \in G} xHx^{-1} = H_G.$$

Corolario 2.28. *Si $H \leq G$ finito tal que*

$$G = \bigcup_{g \in G} gHg^{-1},$$

entonces $H = G$.

Una aplicación de este corolario se muestra en la siguiente proposición.

Proposición 2.29. *Sea G un grupo finito tal que todo par de elementos distintos de 1 sean conjugados en G (es decir, hay a los mas dos clases de conjugación en G). Entonces*

$$|G| \leq 2.$$

Demostración. Sea $n = |G|$. Supongamos que $n > 1$. Entonces G contiene una clase de conjugación con $n-1$ elementos. Por tanto, como el número de elementos de una órbita divide el orden del grupo, y dado que la clase de conjugación es una órbita, se sigue que

$$n - 1 \mid n.$$

Así, $n \geq 2(n-1)$, lo que implica que $n \leq 2$. □

El resultado anterior puede generalizarse de la siguiente manera.

Teorema 2.30. *Para todo entero $k \geq 1$, existe un entero $B(k) > 0$ tal que para todo grupo finito que tiene exactamente k clases de conjugación distintas, se tiene que*

$$|G| \leq B(k).$$

Lema 2.31. *Sea $k > 0$ un entero y $A \in \mathbb{R}$. Entonces la ecuación (diofántica)*

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = A$$

tiene a lo más un número finito $N(k, A)$ de soluciones en $\mathbb{Z}^+$.

Demostración del Lema 2.31. Sin pérdida de generalidad suponemos que $A > 0$, pues sino el conjunto de soluciones es vacío.

Haremos la demostración por inducción sobre k. Para $k = 1$ el resultado es trivial. Ahora, supongamos que el lema es verdadero para $k-1$ y probemos que también lo es para k. Elijamos x_k el entero más pequeño que aparece en todas las posibles soluciones, es decir

$$x_k \leq x_i \quad \forall\, i,$$

de donde

$$\frac{1}{x_k} \geq \frac{1}{x_i} \quad \forall\, i.$$

Sumando estas desigualdades obtenemos

$$\frac{k}{x_k} \geq \frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = A,$$

lo que implica que

$$x_k \leq \frac{k}{A}.$$

Por ende, el número x_k está acotado por k/A. Pero

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_{k-1}} = A - \frac{1}{x_k},$$

y esta última ecuación tiene un número finito de soluciones $N(k-1, A-1/k)$, y el resultado se sigue por inducción. □

Demostración del Teorema 2.30. Sean $C_1, \ldots, C_k$ las distintas clases de conjugación de G. Entonces

$$G = \bigsqcup_{i=1}^{k} C_i.$$

Así

$$|G| = \sum_{i=1}^{k} |C_i|,$$

y en consecuencia

$$1 = \sum_{i=1}^{k} \frac{|C_i|}{|G|}.$$

Cada C_i es una órbita de la acción de G sobre G por conjugación, entonces $|C_i| \mid |G|$ para cada $i \in \{1, \ldots, k\}$, es decir $|G| = |C_i| x_i$ para algún $x_i > 0$. Así, reemplazando

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = 1.$$

Sabemos que hay un número finito $B(k)$ de soluciones de esta ecuación, y $|x_i| \leq B(k)$ para todo i. Además, la clase de 1 es C_i para algún i, pero

$$x_i \mid |\{1\}| = |G| \leq B(k).$$

□

Ejercicio 2.32. Sea G un grupo arbitrario finitamente generado, es decir, $G = \langle g_1, \ldots, g_r \rangle$. Sea $n \geq 1$ un entero. Probar que

$$|\{H < G \mid [G\colon H] \leq n\}|$$

es finito. *Sugerencia:* Considerar la acción de G sobre G/H

$$\begin{array}{rcl} G \times G/H & \longrightarrow & G/H \\ (g, xH) & \longrightarrow & gxH, \end{array}$$

con $[G\colon H] = |G/H| = n$. Esta acción induce un homomorfismo

$$\begin{array}{rcl} p^H : G & \longrightarrow & \mathrm{Sym}(G/H) = S_n \\ g & \longmapsto & p^H(g), \end{array}$$

donde

$$\begin{array}{rcl} p^H(g)\colon G/H & \longrightarrow & G/H \\ xH & \longmapsto & g \cdot xH. \end{array}$$

2.2. Producto semidirecto de grupos

Sean H y K dos grupos, $\phi\colon H \to \mathrm{Aut}(K)$ un homomorfismo y consideremos la acción de H sobre K

$$\begin{array}{rl} H \times K & \to K \\ (h, k) & \mapsto h \times k = \phi(h)(k). \end{array}$$

Tomando ahora $G = K \times H$, podemos definir la aplicación binaria

$$\begin{array}{rl} \cdot\colon G \times G & \to G \\ ((x, y), (u, v)) & \mapsto (x, y) \cdot (u, v) = (x\phi(y)(u), yv). \end{array}$$

Ejercicio 2.33. Probar que $(G, \cdot)$ es un grupo.

G es llamado el producto *semidirecto* de H y K respecto a ϕ, y se nota por $G = K \underset{\phi}{\rtimes} H$.

Observación. Si $\phi(h) = \mathrm{id}_K$ para todo $h \in H$, entonces $K \underset{\phi}{\rtimes} H = K \times H$.

Ejercicio 2.34. Dados H y K dos grupos y $\phi\colon H \to \mathrm{Aut}(K)$, definimos

$$\begin{array}{c} \mathcal{H} = \{(x, 1_k) \mid x \in H\} \\ \mathcal{K} = \{(1_h, y) \mid y \in K\}. \end{array}$$

(1) Pruebe que $\mathcal{K} \trianglelefteq K \underset{\phi}{\rtimes} H$ y que $\mathcal{H} \leq K \underset{\phi}{\rtimes} H$.

(2) Calcule el grupo $K \underset{\phi}{\rtimes} H/\mathcal{H}$.

(3) Note además que $\mathcal{KH} = K \underset{\phi}{\rtimes} H$ y $\mathcal{K} \cap \mathcal{H} = \{(e_h, e_k)\}$, y que la representación de $G = K \underset{\phi}{\rtimes} H = \mathcal{KH}$ es única.

Definición. Sean G un grupo, $K, H \leq G$, con $K \trianglelefteq G$. Si $G = KH$ y $K \cap H = \{1\}$, entonces la representación $g = kh$, con $k \in K$ y $h \in H$, es única y en este caso se dice que G es el *producto semidirecto interno* de K y H.

Ejercicio 2.35. Sean G un grupo, $H, K \leq G$, con $K \trianglelefteq G$. Consideremos el homomorfismo

$$\begin{aligned} \phi\colon H &\to \mathrm{Aut}(K) \\ h &\mapsto \mathrm{I_h}, \end{aligned}$$

donde $I_h(k) = hkh^{-1}$. Probar que G es isomorfo a $K \underset{\phi}{\rtimes} H$.

Ejercicio 2.36. Consideremos los grupos $H = \{1, (1\,2)\}$ y $K = V_4 \trianglelefteq A_4$ y el homomorfo $\phi\colon H \to \mathrm{Aut}(V_4)$ tal que $\phi(1) = \mathrm{id}_{V_4}$, $\phi(1\,2) \mapsto I_{(1\,2)}$. Calcule el grupo $V_4 \underset{\phi}{\rtimes} H$.