ESTRUCTURAS ALGEBRAICAS

Contents

1. Clase 5/03/2021

1.1. **Grupos, Anillos y Cuerpos: Introducción.** Empezamos considerando el conjunto los números reales, $\mathbb{R}$. ¿Qué tipo de operaciones podemos realizar dentro del conjunto de números reales? ¿Qué propiedades tienen estas operaciones? Si en lugar de los números reales consideramos el conjunto de $\mathbb{Q}$ de los números racionales, o $\mathbb{Z}$, el conjunto de los enteros, ¿qué propiedades tienen común? ¿Qué operaciones podemos realizar con ellos?

En $\mathbb{Z}$ podemos sumar y restar, y el resultado será siempre un número entero. Además, estas operaciones son *commutativas*. Podemos multiplicar, pero no dividir. No así en $\mathbb{Q}$ o en $\mathbb{R}$, donde sí que podemos realizar estas operaciones. Las nociones de *grupo, anillo* y *cuerpo* estructuran estos objetos matemáticos en función de las operaciones que podemos imponer en ellos y las propiedades de dichas operaciones. Podríamos empezar con algo así

- Un grupo es un objecto en el que podemos *sumar*.
- Un anillo es un objeto en el que podemos *sumar y multiplicar*.
- Un cuerpo es un objeto en el que podemos *sumar, multiplicar y dividir*.

Por supuesto las nociones de "suma" o "multiplicación" aún quedan por definir. No es lo mismo multiplicar números enteros que números complejos, y sumar números reales que sumar matrices. A estas operaciones las llamamos *operaciones binarias*. De esta manera, podríamos mejorar las definiciones anteriores abstrayendo el concepto de suma y multiplicación como sigue:

Definición 1.1 (Protodefinición)**.**

- Un *grupo* es un conjunto G con una operación binaria
$$+ \colon G \times G \to G\,.$$
- Un *anillo* es un conjunto R con dos operaciones binarias
$$+ \colon G \times G \to G\,, \quad \cdot \colon G \times G \to G\,.$$
- Un *cuerpo* es un conjunto K que es un anillo y además, para cada elemento $a \in K$, existe $a^{-1} \in K$ de manera que $a \cdot a^{-1} = 1$.

Si queremos una definición general, tenemos que especificar qué tipo de propiedades tienen las operaciones que hemos defnido en 1.1. Por ejemplo, la multiplicación de números reales es commutativa, sin embargo la multiplicación de matrices cuadradas con coeficientes reales no lo es. Aún así, la multiplicación en $\mathbb{R}$ y en el conjunto de matrices cuadradas reales comparten ciertas propiedades:

1) Dados $a, b, c \in \mathbb{R}$,
$$a \cdot (b + c) = a \cdot b + a \cdot c\,.$$
Viceversa, dadas tres matrices cuadradas con coeficientes en $\mathbb{R}$, A, B y C,
$$A \cdot (B + C) = A \cdot B + A \cdot C\,.$$
2) $1 \in \mathbb{R}$ satisface la propiedad de que $a \cdot 1 = 1 \cdot a = a$ para cualquier $a \in \mathbb{R}$. En el conjunto de matrices reales cuadradas, la matriz identidad I satisface la misma relación.
3) Dados $a, b, c \in \mathbb{R}$,
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c\,.$$
La misma relación se mantiene cuando uno considera matrices cuadradas reales A, B, C.

En el caso de la suma, ocurre algo similar con la existencia de un elemento distinguido en los reales, o en los enteros, el 0, que cumple la propiedad de que $0 + a = a + 0 = a$ para cualquier a en uno de esos conjuntos. Con esto llegaríamos a las siguientes definicipmes:

Definición 1.2 (Grupo)**.**

Un *grupo* G consiste en lo siguiente:

- Un conjunto G.
- Una operación binaria $+\colon G \times G \to G$. Esta operación está sujeta a las siguientes propiedades:
  i) **Existencia de neutro:** Existe un elemento $0_G \in G$ de manera que
  $$g + 0_G = 0_G + g = g$$
  para todo $g \in G$.
  ii) **Existencia de inverso:** Para cada $g \in G$, existe un elemento $-g \in G$ de manera que
  $$g + (-g) = (-g) + g = 0_G\,.$$
  iii) **Asociatividad:** Dados $g_1, g_2, g_3 \in G$, se cumple
  $$g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3\,.$$

Definición 1.3 (Anillo)**.** Un *anillo* R consiste en lo siguiente:

- Un conjunto R.
- Una operación binaria $+\colon G \times G \to G$ de manera que $(G, +)$ es un grupo commutativo[a].
- Una operación binaria $\cdot\colon G \times G \to G$. Esta operación está sujeta a las siguientes propiedades:
  i) **Existencia de neutro:** Existe un elemento distinguido $1_R \in R$ de manera que
  $$r \cdot 1_R = 1_R \cdot r = r$$
  para cualquier $r \in R$.
  ii) **Asociatividad:** Dados $r_1, r_2, r_3 \in R$,
  $$r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3\,.$$
  iii) **Distribución con respecto a $+$:** Dados $r_1, r_2, r_3 \in R$,
  $$r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3\,.$$

[a] Un grupo es *abeliano* o *commutativo* si además satisface que para cualesquiera $a, b \in G$, $a + b = b + a$.

Definición 1.4 (Cuerpo)**.** Un *cuerpo* K consiste en lo siguiente:

-
- Un conjunto K.
- Dos operaciones binarias $+\colon G \times G \to G$ y $\cdot\colon G \times G \to G$ de manera que $(K, +, \cdot)$ es un anillo commutativo[a]. Además, la operación $\cdot$ satisface la siguiente propiedad:
  i) **Existencia de inverso:** Para todo $a \in K$ existe $a^{-1} \in K$ de manera que
  $$a \cdot a^{-1} = a^{-1} \cdot a = 1_K\,.$$

[a] Un anillo se dice que es *commutativo* si la operación $\cdot$ es commutativa, es decir, $r_1 \cdot r_2 = r_2 \cdot r_1$ para cualesquiera $r_1, r_2 \in R$.

Entre los ejemplos de grupos se encuentran el grupo de números enteros con respecto de la suma, $(\mathbb{Z}, +)$, o el de los racionales con la multiplicación, $(\mathbb{Q}, \cdot)$. Ambos son ejemplos de grupos abelianos. En el caso de los enteros, $(\mathbb{Z}, +, \cdot)$ es a su vez un anillo, y en el de los racionales, $(\mathbb{Q}, +, \cdot)$ forma un cuerpo.

Ejemplo 1.5 (Grupo no commutativo)**.** Todos los ejemplos de grupos que hemos visto hasta ahora son grupos abelianos. El ejemplo más sencillo de grupo no abeliano es el *grupo dihédrico* D_3. Este es el grupo de simetrías de un triángulo. Tenemos 3 simetrías rotacionales (una rotación de 120 grados), que denotamos como σ, y 3 *reflexiones* que denotamos por τ, una por cada vértice del triángulo. La operación es la composición de simetrías. Este es un ejemplo de grupo no abeliano (ejercicio). De hecho, es el grupo no-abeliano *más pequeño posible*.

Ejemplo 1.6 (Anillos y Cuerpos de Matrices)**.** Denotemos por $\mathcal{M}_{n\times n}(\mathbb{R})$ al conjunto de matrices cuadradas $n \times n$ con coeficientes reales. $\mathcal{M}_{n\times n}(\mathbb{R})$ es un ejemplo de anillo no-commutativo con las operaciones de suma de matrices.

Denotemos por $\mathrm{GL}_n(\mathbb{R})$ al *grupo lineal general*. Este grupo consiste de las matrices cuadradas $n \times n$ con coeficientes reales que son invertibles. Aunque en $\mathrm{GL}_n(\mathbb{R})$ todo elemento tiene inverso, este anillo sigue sin ser un cuerpo, pues la multiplicación de matrices no es commutativa.

Otros ejemplos de anillos de matrices incluyen:

- $\mathrm{SL}_n(\mathbb{R})$: *grupo linear especial*; anillo de matrices cuadradas con determinante igual a 1.
- $\mathrm{O}_n(\mathbb{R})$: *group ortogonal*; anillo de matrices ortogonales.
- $\mathrm{SO}_n(\mathbb{R})$: *grupo ortogonal especial*; anillo de matrices ortogonales con determinante igual a 1.

1.2. **Homomorfismos.** Una vez tenemos fijada la noción de grupo, anillo y cuerpo, nos interesa estudiar de qué manera podemos relacionar dos grupos, anillo, etcétera. Esto da lugar a la noción de *homomorfismo de grupos* (resp. *homomorfismo de anillos, cuerpos*). La idea es que cualquier aplicación entre estos objetos debería respetar su estructura: elementos neutros deberían ir a elementos neutros, y se debería preservar la operación en ambas estructuras. Formalizamos esta idea como sigue:

Definición 1.7 (Homomorfismo de Grupos)**.** Sean $(G_1, *), (G_2, \star)$ dos grupos. Un *homomorfismo de groups* $f\colon (G_1, *) \to (G_2, \star)$ consiste en el siguiente conjunto de datos:

1) Una aplicación $f\colon G_1 \to G_2$ entre los conjuntos subyacentes.
2) Para cualesquiera $a, b \in G_1$,
$$f(a * b) = f(a) \star f(b)\,.$$
3) Sean e_{G_1} y e_{G_2} los elementos neutros de G_1, G_2 respectivamente,
$$f(e_{G_1}) = e_{G_2}\,.$$

2. Clase 12/03/2021

2.1. **Repaso: Conjuntos Cocientes y Clases de Equivalencia.** Supongamos que tenemos dos conjuntos, X e Y, y uno está contenido dentro del otro, digamos $X \subset Y$. Esto no quiere decir más que todo elemento $x \in X$ satisface además la propiedad $x \in Y$. Una manera algo más adecuada de visualizar la idea de "estar contenido en" es a través de *inclusiones*. $X \subset Y$ es equivalente a decir que existe una aplicación inyectiva
$$i_X\colon X \hookrightarrow Y\,.$$
Me explico, si $x \in Y$ para todo $x \in X$, la aplicaión $i_X\colon X \to Y$ definida por
$$x\,(\in X) \mapsto x\,(x \in Y)$$
es inyectiva[1]. A la inversa, si empezamos con una aplicación inyectiva $f\colon X \to Y$, obtenemos una biyección entre los conjuntos X y $f(X)$ (esto debería ser bastante natural). En este sentido, podríamos decir que la noción de aplicación inyectiva conlleva la misma información que la noción de subconjunto: un par de conjuntos $X \subset Y$ dan lugar a una aplicación inyectiva y viceversa, una aplicación inyectiva da lugar a un par de conjuntos $f(X) \subset Y$.

La propiedad "existe un conjunto cociente" sustituirá la propiedad "existe un subconjunto" si cambiamos los papeles de *aplicación inyectiva*[2] por *aplicación inyectiva*. Empezamos recordando el paso previo a la definición de conjunto cociente, aquella de *relación de equivalencia*:

Definición 2.1 (Relación de Equivalencia)**.** Sea X un conjunto. Una *relación de equivalencia* en X es una relación binaria en X reflexiva, simétrica y transitiva. Denotaremos por $\sim$ a una relación de equivalencia,

[1] Recordad que una aplicación $f\colon X \to Y$ es inyectiva si de la relación $f(x_1) = f(x_2)$ se sigue $x_1 = x_2$ para todo $x_1, x_2 \in X$.
[2] Una aplicación $f\colon X \to Y$ si todo elemento $y \in Y$ es de la forma $f(x)$ para un cierto $x \in X$.

y diremos que dos elementos $x_1, x_2 \in X$ son *equivalentes* si $x_1 \sim x_2$, es decir, si están relacionados entre sí. Las propiedades de reflexividad, simetría y transitividad se definen como sigue:

1) **Reflexividad:** Todo elemento $x \in X$ está relacionado consigo mismo, es decir, $x \in x$ para todo x.
2) **Simetría:** Decir que un elemento x_1 está relacionado con otro elemento x_2 es equivalente a decir que x_2 está relacionado con x_2. En otras palabras,
$$x_1 \sim x_2 \text{ si y sólo si } x_2 \sim x_1 \,.$$
3) **Transitividad:** Si un elemento está relacionado con otro, y ese elemento a su vez está relacionado con un tercero, el primero y el tercero están relacionados. Dicho de otro modo, $x_1 \sim x_2$ y $x_2 \sim x_3$ implica que $x_1 \sim x_3$ para cualesquiera $x_1, x_2, x_3 \in X$.

Veamos un par de ejemplos y contraejemplos de relaciones de equivalencias.

Ejemplo 2.2. Sea $X = \mathbb{Z}$ el conjunto de números enteros. La relación de igualdad ($a \sim b$ si y sólo si $a = b$) es una relación de equivalencia.

Otra relación de equivalencia, esta vez en el conjunto $\mathbb{C}$ de números enteros viene dada por "tener el mismo módulo", es decir $z_1 \sim z_2$ si y sólo si $|z_1| = |z_2|$.

Denotemos por $C([0,1])$ el conjunto de functiones continuas en el intervalo $[0,1]$, y definamos $f \sim g$ si y sólo si
$$\int_0^1 f(x)\ \mathrm{d}\,x = \int_0^1 g(x)\ \mathrm{d}\,x \,.$$
La relación $\sim$ es una relación de equivalencia.

Ejemplo 2.3. Denotemos por X el conjunto de miembros de una familia y sea $\sim$ la relación "ser hermano de". La relación es claramente transitiva y simétrica. Sin embargo, no es reflexiva (nadie dice que es hermano de sí mismo).

Consideremos el conjunto $\mathbb{R}$ con la relación $\leq$, es decir, $x \sim y$ si y sólo si $x \leq y$. Este es un ejemplo de relación binaria transitiva y reflexiva que no es simétrica. Por ejemplo, $3 \leq 10$ pero $10 \not\leq 3$.

La definición anterior puede resultar algo obstrusa y el sentido se pierde un poco. Vamos a intentar entenderla mejor bajo el siguiente refrán:

"Una relación de equivalencia ordena los elementos de un conjunto en *particiones* disjuntas."

En efecto, dado un conjunto X con una relación de equivalencia $\sim$ en X, denotemos por $[x]$ el conjunto de elementos de X relacionados con α. Esto es,

$$[x] := \{x \in X \mid x \sim \alpha\} \,. \tag{1}$$

Dado $y \in X$, consideremos $[y]$ definido de la misma manera que $[x]$. Veamos que $[x]$ e $[y]$ son disjuntos si $x \neq y$. Supongamos que existe un elemento $z \in [x]$ tal que $z \in [y]$ y veamos que en ese caso $[x] = [y]$. Dado $a \in [x]$, tenemos que $a \sim x$. Como $z \sim x$, por simetría y transitividad de la relación, $a \sim z$. Pero $z \in [y]$, con lo que $a \sim y$ también, es decir, $a \in [y]$. Conversamente, dado $b \in [y]$, tenemos que $b \sim y$. Ya que $z \sim y$ por hipótesis, tenemos que $b \sim z$, y a su vez, ya que $z \in [x]$, $b \sim z$ de nuevo por simetría y transitividad. En otras palabras, $b \sim x$, luego $b \in [x]$.

Los conjuntos $[x]$ que hemos denotado en el argumento anterior tienen una nomenclatura establecida y se conocen como *clases de equivalencia*.

Definición 2.4 (Clase de Equivalencia)**.** Sea X un conjunto y $\sim$ una relación de equialencia en X. Denotemos por $[x]$ la definición de (1). El conjunto $[x]$ recibe el nombre de *clase de equivalencia*.

Las clases de equivalencia sobre un conjunto definen una *partición* de este. Con esto nos referimos a que una relación de equivalencia divide al conjunto en pequeños "subconjuntos" disjuntos dos a dos, que a su vez cubren en su totalidad al conjunto X.

Definición 2.5 (Partición)**.** Una *partición* de un conjunto X consiste en una clase de subconjuntos $\{X_\alpha\}_\alpha$ de manera que:

1) Para todo $x \in X$, existe X_α con $x \in X_\alpha$.
2) Dados X_α y X_β con $\alpha \neq \beta$, $X_\alpha \cap X_\beta = \emptyset$.

En nuestro caso, dado un conjunto X con una relación de equivalencia $\sim$ sobre el mismo, el conjunto de clases de equivalencia define una partición de X. Claramente, $x \in [x]$ por simetría de $\sim$, y hemos visto que $[x] \cap [y] = \emptyset$ si $x \neq y$ en el argumento previo. Es decir, una elemento de una partición de X y una clase de equivalencia vienen decir lo mismo.

Ejemplo 2.6. Denotemos por X el conjunto de todas las personas y sea $\sim$ la relación "tener el mismo cumpleaños". Esta es una relación de equivalencia (¡escríbelo!). Una clase de equivalencia bajo esta relación consiste en todas las personas que cumplen años el mismo día del año. Notad que en este caso el hecho de que las clases de equivalencia son disjuntas es bastante obvio (al fin y al cabo una persona tiene un único cumpleaños). Notad también que en este caso tenemos precisamente 366 clases de equivalencia (recordad esto cuando vemamos *órbitas*).

El conjunto de clases de equivalencia de un conjunto X con una relación de equivalencia $\sim$ recibe el nombre de *conjunto cociente*.

Definición 2.7 (Conjunto Cociente)**.** Sea X un conjunto y $\sim$ una relación de equivalencia sobre este. Denotamos por $X/\sim$ el conjunto de todas las clases de equivalencia de X. En otras palabras

$$X/\sim := \{[x] \mid x \in X\}.$$

2.2. **Subgrupos Normales y Teoremas de Isomorfía.** La noción de subgrupo normal nos ayuda a la hora de construir cocientes de grupos. Recordamos que cualquier noción de cociente se construye de manera análoga a lo visto anteriormente, con la condición extra de que además, éste tiene que ser un grupo.

Definición 2.8. Sea G un grupo. Decimos que un subgrupo $H \trianglelefteq G$ es *normal*, denotado por $H \trianglelefteq G$ si para cualesquiera elementos $g \in G, h \in H$, la siguiente relación es cierta:

$$ghg^{-1} \in H.$$

Observación. Otras nomenclaturas para denotar la propiedad de que un subgrupo es normal dentro de un grupo G incluyen $gHg^{-1} = H$, o $gH = Hg$.

Definimos una relación de equivalencia en G, $\sim_H$ como sigue:

- Dos elementos $g_1, g_2 \in G$ son equivalentes (decimos que son *congruentes* respecto de H) si $g_1 g_2^{-1} \in H$.

Afirmamos que esta es un relación de equivalencia. En efecto, dado $g \in G$, $gg^{-1} = e \in H$. Por otro lado, si $g_1 g_2^{-1} \in H$, $g_2 g_1^{-1} \in H$ (si $g_1 g_2^{-1} = h$ para un cierto $h \in H$, $g_2 g_1^{-1} = h^{-1} \in H$). Finalmente, si $g_1 g_2^{-1} \in H$ y $g_2 g_3^{-1} \in H$ para $g_1, g_2, g_3 \in G$, tenemos que $g_1 g_3^{-1} \in H$, ya que $g_1 g_2^{-1} = h_1 \in H$, $g_2 g_3^{-1} = h_2 \in H$, y

$$g_1 g_3^{-1} = g_1 g_2^{-1} g_2 g_3^{-1} = h_1 h_2 \in H.$$

Es interesante estudiar cómo son las clases de equivalencia definidas por la relación anterior. Dado $g \in G$, tenemos que

$$[g] = \{x \in G \mid x \sim_H g\} = \{x \in G \mid xg^{-1} \in H\} = \{hg \mid h \in H\}.$$

Utilizaremos la notación $[g] = Hg$ para denotar la clase de equivalencia de un elemento $g \in Hg$ bajo la relación $\sim_H$.

De manera similar, podemos definir una relación de equivalencia ${}_H\sim$ completamente dual a la anterior, donde decimos que dos elementos $g_1, g_2 \in G$ son congruentes (por la izquierda) si $g_1^{-1} g_2 \in H$. Podemos entonces considerar dos conjuntos cocientes, $G/{}_H\sim$ y $G/\sim_H$, y sería interesante estudiar si los conjuntos cocientes obtenidos son el mismo. Análogamente, tenemos que

$$[g] = \{gh \mid h \in H\}.$$

Denotaremos las clases de equivalencia por la relación ${}_H\sim$ mediante $[g] = gH$.

Observación. En general, estas dos clases de equivalencia no son iguales y por lo tanto no dan lugar al mismo conjunto cociente. Veremos ahora que a no ser que H sea un subgrupo normal de G, no podemos garantizar la equivalencia de estas dos clases, ya que en general, no se cumple $gH = Hg$. Como hemos visto, esta propiedad es equivalente a afirmar que $H \trianglelefteq G$, es decir que H es un subgrupo normal de G.

Hemos probado lo siguiente:

Proposición 2.9. *Sea $H \trianglelefteq G$. Las relaciones $\sim_H$ y ${}_H\sim$ coinciden. Se sigue por lo tanto que los conjuntos cocientes $G/\sim_H$ y $G/{}_H\sim$ son iguales.*

Cuando $H \trianglelefteq G$, sabemos que ambas relaciones coinciden. Utilizaremos la notación

$$G/H$$

para referirnos independientemente a los conjuntos cocientes $G/\sim_H$ y $G/{}_H\sim$. Veamos ahora cómo podemos dar una estructura de grupo a este conjunto cociente. Sabemos que el conjunto cociente depende exclusivamente de las clases de equivalencia, es decir,

$$G/H = \{gH \mid g \in G\}.$$

Dados dos elementos $g_1, g_2 \in G$, definimos

$$(g_1H)(g_2H) := (g_1g_2)H\,.$$

Veamos que esta operación está bien definida. Para ello tenemos que ver que el $(g_1g_2)H$ no depende de g_1 ni de g_2. En efecto, supongamos que $g_1H = xH$ y $g_2H = yH$ para $g_1, g_2, x, y \in G$. Tenemos que comprobar que

$$(g_1g_2)H = (x_1x_2)H\,.$$

Esto a su vez es equivalente a demostrar que $(g_1g_2)^{-1}(xy) = g_2^{-1}g_1xy \in H$. Ahora bien, sabemos que $g_1^{-1}x = h_1 \in H$, y a su vez $g_2^{-1}y = h_2 \in H$. Además, como $ghg^{-1} \in H$ para cualesquiera $g \in G, h \in H$, tenemos que

$$(g_1g_2)^{-1}(xy)g_1^{-1}(g_2^{-1}x_1)x_2 = g_1^{-1}h_1x_2 \in H$$

ya que H es un subgrupo normal.

Visto esto, es sencillo demostrar que G/H es un grupo con esta relación definida. El elemento neutro de G/H es e_GH, y el inverso de la clase gH es la clase $g^{-1}H$. El resto de detalles quedan como un ejercicio.

2.2.1. *Toeremas de Isomorfía.* Probablemente uno de los teoremas más importante de Teoría de grupos es el siguiente:

Teorema 2.10 (Primer Teorema de Isomorfía)**.** *Sean G_1 y G_2 dos grupos. Dado un homomorfismo de grupos $f\colon G_1 \to G_2$, la aplicación*

$$\varphi\colon G_1/\ker f \to \operatorname{im} f$$

definida por

$$g_1 \ker f \mapsto \varphi(g_1)$$

es un isomorfismo de grupos.

Para demostrar este enunciado, veamos en primer lugar que la aplicación φ está bien definida. En efecto, supongamos que $x\ker f = y\ker f$ para dos $x, y \in G_1$. Por definición, $x^{-1}y \in \ker f$, o en otras palabras

$$e_{G_1} = f(x^{-1}y) = f(x)^{-1}f(y)\,.$$

Esta última igualdad es equivalente a afirmat que $f(x) = f(y)$, que es precisamente la imagen de $\varphi(x)$ y $\varphi(y)$, luego φ está bien definida.

Veamos ahora que se trata de una aplicación inyectiva. Para ello, supongamos que $x\ker f \in \ker\varphi$. Esto quiere decir que $e_{G_2} = \varphi(x\ker f) = f(x)$, es decir, $x \in \ker f$. Por lo tanto,

$$x\ker f = e_{G_1}\ker f = e_{G_1/\ker f}$$

y por lo tanto, φ es inyectiva. Finalmente, para demostrar que se trata de una aplicación sobreyectiva, notemos que todo elemento en $\operatorname{im} f$ es de la orma $f(x)$ para un cierto $x \in G_1$. Pero precisamente $f(x) = \varphi(x\ker f)$, luego es claramente sobreyectiva.

Una vez demostrado el primer teorema de isomorfía, podemos concluir resultados similares utilizando este resultado como paso intermedio.

Corolario 2.11 (Segundo Teorema de Isomorfía)**.** *Sean H, K subgrupos normales de un grupo G tales que $H \subset K$. Los grupos*

$$\frac{G/H}{K/H} \quad y \quad G/K$$

son isomorfos.

Proof. Para demostrar estos resultados, buscamos aplicar siempre el primer teorema de isomorfía. Es decir, en este caso buscamos un homomorfismo $f\colon G_1 \to G_2$ de manera que $G_1/\ker f \cong \frac{G/H}{K/H}$ e $\operatorname{im} f \cong G/K$. Para ello, tomemos $G_1 = G/H$, $G_2 = G/K$, y definamos $f\colon G_1 \to G_2$ mediante

$$gH \mapsto gK\,.$$

Puesto que $H \subset K$, este homomorfismo es claramente sobreyectivo, y por lo tanto $\operatorname{im} f = G/K$. Por otro lado,

$$\begin{aligned}\ker f &= \{gH \mid gK = e_{G/K}\}\\ &= G/K\,.\end{aligned}$$

□

2.3. **Intuición detrás de la noción de cociente.** Hemos visto que el grupo cociente G/H donde H es un subgrupo normal de G viene a ser básicamente "el conjunto de clases de equivalencia de elementos de g". Esta definición, aunque correcta, no da mucha inspiración a lo que ocurre detrás de la construcción del cociente.

El grupo cociente G/H consiste en los elementos de G que no pertenecen a H.

La definición de arriba no es del todo correcta, pero es aún mantiene algo de verdad. Pongamos un ejemplo algo más concreto, donde $G = \mathbb{Z}$, el grupo de los enteros y $H = n\mathbb{Z}$, el subgrupo de $\mathbb{Z}$ que contiene a los múltiplos de n. Uno podría decir y discriminar a los enteros en función a su relación con $n\mathbb{Z}$:

- ¿Qué elementos de $\mathbb{Z}$ pertenecen a $n\mathbb{Z}$?

Esta pregunta es fácil de responder: los múltiplos de n. Vamos a separar a los enteros que pertenecen a $n\mathbb{Z}$ y los vamos a denotar como $0+n\mathbb{Z}$. Sin embargo, podríamos intentar medir de alguna manera otros elementos de $\mathbb{Z}$ que, pese no pertenecer a $n\mathbb{Z}$ como tal, mantienen cierta relación con este como para considerarles "útiles" de alguna manera. La relación que imponemos es similar a la relación de igualdad, pero un poco más relajada. A este tipo de relaciones las denominamos *relaciones de equivalencia*. En el caso de los enteros, nos interesa particularmente no la relación de igualdad. sino otra un poco menos estricta. Diremos que dos enteros son "iguales" con respecto a $n\mathbb{Z}$ si su resto al dividirlos entre n es el mismo. De esta manera, obtenemos no sólamente aquellos enteros múltiplos de n, sino una división de los enteros en función de la relación de equivalencia que hemos definido. Tendremos una división de los enteros en función de aquellos cuyo resto al dividir entre n es 0, y así sucesivamente hasta cubrir todos los posibles restos al dividir entre n:

$$\begin{gathered} 0 + n\mathbb{Z}\ (= n\mathbb{Z}) \\ 1 + n\mathbb{Z} \\ 2 + n\mathbb{Z} \\ \vdots \\ (n-1) + n\mathbb{Z}\,. \end{gathered}$$

De esta manera, estamos relacionando elementos de $\mathbb{Z}$ en función a su relación con el subgrupo $n\mathbb{Z}$ de múltiplos de n. Podemos verlo como aquellos enteros que, pese a no pertenecer a $n\mathbb{Z}$, guardan cierta relación con este subgrupo como para considerarlos "interesantes".

Vamos a dar un paso más e intentar abstraer la noción de "restos módulo n" a grupos algo más generales que el de los enteros. Empecemos con $\mathbb{Z}/3\mathbb{Z}$, por ejemplo, y consideremos los enteros 5 y 8. El resto de ambos al dividir entre 3 es el mismo, y hemos dicho que nos gustaría poder identificar ambos. Y vale, 5 y 8 no pertenecen a $3\mathbb{Z}$ ya que no son múltiplos de 3, pero $8 + (-5) = 3 \in n\mathbb{Z}$. Si cogemos en su lugar 20 y 122, tenemos que $122 + (-20) = 102 = 3 \cdot 34$, que es un múltiplo de 3. ¿Qué estamos haciendo realmente? Si empezamos con un grupo cualquiera, G, estamos diciendo que dos elementos $g_1, g_2 \in G$ son equivalentes si y sólo si $g_1 g_2^{-1} \in H$, para un determinado H (en nuestro caso, $H = n\mathbb{Z}$, la operación es la suma de enteros y el inverso de un entero m es $-m$).

En el caso de los enteros y los múltiplos de un entero, podemos incluso sumar estas "particiones". Por ejemplo, la suma de $1 + 3\mathbb{Z}$ consigo mismo es $2 + 3\mathbb{Z}$. En efecto, dado un entero k cuyo resto al dividir entre 3 es 1, $2k$ tiene resto 2 al dividir entre 3. Esto sugiere incluso que podemos operar con estas particiones de manera que aún somos capaces de preservar una estructura que otorga algo más de información sobre el conjunto de particiones.

Pero si seguimos con el ejemplo de los números enteros, estamos pasando por obvio una propiedad que es exclusiva al subconjunto de múltiplos de un entero. Utilizando los ejemplos de antes, da igual como sumemos, si $(-5)+8$ u $8+(-5)$, el resultado es siempre un múltiplo de 3. Esta propiedad del conjunto $3\mathbb{Z}$ se denomina *normalidad*, o decimos que el subgrupo $3\mathbb{Z}$ es un subgrupo *normal*. Esto no siempre es así.

Consideremos el conjunto $\{a, b\}$. Aquí, a y b representan caracteres, nada más. Definamos un grupo $F(\{a, b\})$ como sigue:

- Los elementos de $F(\{a, b\}$ son palabras escritas con los caracteres a, b, a^{-1} y b^{-1}, en cualquier order. Aquí, a^{-1} y b^{-1} son caracteres nuevos que hemos introducido. Por ejemplo,

  $$abbba^{-1}baab^{-1}bbb$$

  es un elemento de $F(\{a, b\})$.
- Imponemos una condición en $F(\{a, b\})$ de manera que decimos que una palabra se puede *reducir* si uno de los caracteres a o b sigue o biene precedido por uno de los caracteres a^{-1} o b^{-1}. Por ejemplo

  $$abb^{-1}aaa^{-1}b^{-1}bb \to aabab\,.$$

- Definimos una operación $\star$ en $F(\{a,b\})$, donde concatenamos dos palabras. Por ejemplo:

$$abbaba^{-1} \star bab = abbaba^{-1}bab\,.$$

$F(\{a,b\})$ es un grupo, denominado *grupo libre generado por dos elementos* (¿sabrías indicar cuál es el elemento neutro de este grupo?) Tomemos un subgrupo de $F(\{a,b\})$, por ejemplo, el subgrupo $F(\{a\})$ generado por a, es decir, palabras de la forma $a, a^2, a^3, \cdots, a^{-1}, a^{-2}, a^{-3}, \cdots$. Si cogemos por ejemplo la palabra $b \in F(\{a,b\})$, $ba^{-1}b \notin F(\{a\})$, ya que no hay manera de reducir la palabra $ba^{-1}b$. Por lo tanto, $F(\{a\})$ no es un subgrupo normal de $F(\{a,b\})$. En este caso, no tendría sentido considerar el cociente $F(\{a,b\})/F(\{a,b\})$ por las razones que hemos visto anteriormente.

2.3.1. *Cocientes y Aplicaciones Sobreyectivas (Avanzado).* Retomamos un poco las ideas del principio de la sección, donde hablamos de la relación entre aplicación inyectiva y subconjunto. La idea es sencilla: dado un conjunto X y una relación de equivalencia $\sim$, nos gustaría obtener una caracterización en términos de aplicaciones sobreyectivas y conjuntos cocientes. El resultado final debería ser algo en las líneas de:

- Dada una relación de equivalencia $\sim$ en X, podemos obtener una aplicación sobreyectiva $\pi\colon X \to X/\sim$.
- Al revés, dada una aplicación sobreyectiva $f\colon X \to Y$, f induce una biyección natural entre $X/\sim$ e Y.

Ataquemos la primera parte del objetivo. Sabemos que $X/\sim = \{[x] \mid x \in X\}$. La aplicación más natural posible entre X y $X/\sim$ se define como sigue

$$\begin{aligned} \pi\colon X &\to X/\sim \\ x &\mapsto [x]\,. \end{aligned}$$

Si empezamos ahora con una función sobreyectiva $f\colon X \to Y$, esta define una relación de equivalence como sigue:

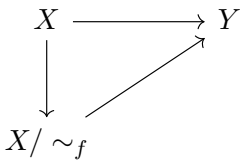
- Dos elementos x_1, x_2 están relacionados si y sólo si $f(x_1) = f(x_2)$.

La relación anterior, que denotamos como $\sim_f$, es claramente una relación de equivalencia. Más es cierto, sin embargo. Esta función define a su vez una aplicación

$$\overline{f}\colon X/\sim Y$$

dada por $[x] \mapsto f(x)$. $\overline{f}$ es inyectiva, pues dados $f(x_1) = f(x_2)$ en Y, por definición de $\sim_f$, x_1 y x_2 pertenecen a la misma clase de equivalencia en $X/\sim_f$. El hecho de que f sea sobreyectiva garantiza que la aplicación $\overline{f}$ sea biyectiva.

Además, la aplicación $\overline{f}$ commuta con $\pi\colon X \to Y$ en el sentido de que el diagrama



es *commutativo* ($\overline{f} \circ \pi = f$). En efecto, basta comprobar que, dado $x \in X$, tenemos

$$x \xrightarrow{\pi} [x] \xrightarrow{\overline{f}} f(x)\,.$$

Más es cierto, $\overline{f}$ es la única aplicación $X/\sim_f \to Y$ con esta propiedad (ejercicio).

2.4. **Grupos Cíclicos.** Grupos cíclicos son aquellos en los que todo elemento se puede escribir como la "potencia" de un determinado elemento. Por ejemplo, el grupo $\mathbb{Z}$ de los enteros todo entero k se puede escribir como $1 + \cdots + 1$ k veces si se trata de un entero positivo, o $1 - \cdots - 1$ si k es negativo. En este caso decimos que 1 es un *generador* del grupo $\mathbb{Z}$, y que por lo tanto $\mathbb{Z}$ es un grupo cíclico.

Definición 2.12 (Subgrupo generado por un elemento)**.** Sea G un grupo y $g \in G$ un elemento cualquiera. Denotamos por

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}$$

al *subgrupo generado por* g.

Por ejemplo, en $\mathbb{Z}$, el subgrupo generado por $2 \in \mathbb{Z}$ es

$$\langle 2 \rangle = \{2n \mid n \in \mathbb{Z}\} = 2\mathbb{Z}\,.$$

Definición 2.13 (Orden de un elemento)**.** Sea G un grupo y $g \in G$ un elemento. El *orden de* g se define como el menor entero positivo n tal que $g^n = 1$. Si no existe tal n decimos que g tiene *orden infinito*. Denotaremos por $o(g)$ al orden del elemento $g \in G$.

En el caso de los enteros, todo elemento tiene orden infinito, pues $nk \neq 0$ a no ser que k sea precisamente 0, el elemento neutro de $\mathbb{Z}$. Si consideramos en su lugar $\mathbb{Z}/5\mathbb{Z}$, por ejemplo, el elemento $[\overline{2}]$ tiene orden 5, pues

$$[\overline{2}] + [\overline{2}] + [\overline{2}] + [\overline{2}] + [\overline{2}] = [\overline{10}] = [\overline{0}]\,.$$

El elemento $[\overline{1}]$, sin embargo tiene orden 5, pues

$$[\overline{1}] + [\overline{1}] + [\overline{1}] + [\overline{1}] + [\overline{1}] = [\overline{5}] = [\overline{0}]\,.$$

Definición 2.14 (Grupo cíclico)**.** Sea G un grupo. Decimos que G es un grupo *cíclico* si existe un elemento $g \in G$ de manera que

$$G = \langle g \rangle\,.$$

El elemento g en la deifnición anterior se denomina *generador*. Si un generador de un grupo tiene orden infinito, decimos que G es cíclico infinito.

Ejemplo 2.15. Como hemos visto, $\mathbb{Z}$ es un grupo cíclico generado por el elemento $1 \in \mathbb{Z}$. Puesto que $n \cdot 1 \neq 0$ para cualquiera n entero positivo, $\mathbb{Z}$ es un grupo cíclico infinito.

En el caso de $\mathbb{Z}/5\mathbb{Z}$, $[\overline{1}]$ es claramente un generador, y por lo tanto $\mathbb{Z}/5\mathbb{Z}$ es un grupo cíclico finito, ya que $o([\overline{1}]) = 5$.

Nótese que $[\overline{2}]$ también es un generador de este grupo, pues

$$\begin{aligned}
[\overline{0}] &= [\overline{2}] + [\overline{2}] + [\overline{2}] + [\overline{2}] + [\overline{2}] \\
[\overline{1}] &= [\overline{2}] + [\overline{2}] + [\overline{2}] \\
[\overline{2}] &= [\overline{2}] \\
[\overline{3}] &= [\overline{2}] + [\overline{2}] + [\overline{2}] + [\overline{2}] \\
[\overline{4}] &= [\overline{2}] + [\overline{2}]
\end{aligned}$$

En otras palabras, un grupo cíclico puede tener varios generadores. Veremos más adelante que estos serán precisamente aquellos cuyo orden sea primo entre sí con el orden del grupo.

La propiedad *ser cíclico* se hereda al pasar al subgrupo. Dicho de otro modo, tenemos el siguiente resultado.

Proposición 2.16. *Todo subgrupo de un grupo cíclico es cíclico.*

Proof. Seag $H \trianglelefteq G$, donde $G = \langle g \rangle$ para un determinado $g \in G$. Para demostrar que H es cíclico tenemos que construir un generador de H de tal manera que $H = \langle h \rangle$. Si $H = \{e_G\}$, es decir, H consta sólo de un elemento, es trivialmente cíclico, así que podemos suponer que $H \neq \{e_G\}$.

Notad que, puesto que todo elemento de G es de la forma g^n para un cierto $n\mathbb{Z}$, en particular todos los elementos de H son de esa forma. Por lo tanto podemos escoger un entero $k \in \mathbb{Z}$ de manera que $g^k \in H$.

Continuar □

3. Acciones de Grupos sobre un Conjunto

Consideremos un conjunto X, y denotemos por $\mathrm{Func}(X)$ el conjunto de funciones $f\colon X \to X$. Conocemos un grupo, que denotamos como $\mathrm{Aut}(X)$, el grupo de automorfismos de X, que consiste en aquellas funciones de $\mathrm{Func}(X)$ que son invertibles.

Supongamos ahora que partimos de un grupo arbitrario G, y que queremos estudiar homomorfismos de la forma $\phi\colon G \to \mathrm{Aut}(X)$. Supopngamos que tal homomorfismo ϕ existe. ¿Qué información sobre $\mathrm{Aut}(X)$ podemos obtener de este hecho? Si tal ϕ existe, $\operatorname{im}\phi$, la imagen de ϕ será un subgrupo de $\mathrm{Aut}(X)$; además, $\phi(e_G) = \mathrm{id}_X$, pues la identidad es el elemento neutro en $\mathrm{Aut}(X)$. Además, dado que ϕ es un homomorfismo, tenemos también que

$$\phi(g_1 \cdot g_2)(x) = (\phi(g_1) \circ \phi(g_2)(x)\,.$$

En este ejemplo, decimos que ϕ define una *acción de* G *en* X.

La discusión anterior nos lleva a la siguiente definición:

Definición 3.1 (Acción de un Grupo sobre un Conjunto)**.** Sea G un grupo y X un conjunto. Una *acción de* G *sobre* X consiste en un homomorfismo de grupos

$$G \to \mathrm{Aut}(X)\,.$$

En particular, notad que dada una acción $\phi\colon G \to \mathrm{Aut}(X)$, podemos definir una aplicación

$$\begin{aligned}\Phi\colon G \times X &\to X\\ (g,x) &\mapsto \phi(g)(x)\,.\end{aligned}$$

Es más, por tratarse de un homomorfismo, podemos desglosar sus propiedades como sigue:

1) $\Phi(e_G, x) = x$ para todo $x \in X$. Esto se sigue del hecho de que ϕ es un homomorfismo de grupos, ya que, como antes
$$\Phi(e_G, x) = \phi(e_G)(x) = \mathrm{id}_X(x) = x\,.$$
2) $\Phi(g_1 \cdot g_2, x) = \Phi(g_1, \Phi(g_2, x))$. En efecto, desarrollando, tenemos que
$$\begin{aligned}\Phi(g_1 \cdot g_2, x) &= \phi(g_1 \cdot g_2)(x)\\ &= (\phi(g_1) \circ \phi(g_2)(x)\\ &= \phi(g_1)(\phi(g_2)(x))\\ &= \Phi(g_1, \Phi(g_2, x))\,.\end{aligned}$$

Notad que en $\mathrm{Aut}(X)$ podemos definir *dos* operaciones. Dados $f, g\colon X \to X$, podemos componer f con g o g con f. Denotemos por $\mathrm{Aut}^{\mathcal{C}^{\mathrm{op}}}(X)$ al grupo de automorfismos de X donde la operación está definida por $f \circ g$ para $f, g\colon X \to X$. Se puede comprobar que en este caso, un homomorfismo $\varphi\colon G \to \mathrm{Aut}^{\mathcal{C}^{\mathrm{op}}}(X)$ define una aplicación

$$\Psi\colon X \times G \to X\,.$$

A las acciones de grupos dadas por homomorfismos de la forma $G \to \mathrm{Aut}(X)$ se les denomina *acciones por la derecha*, y al contrario, a las acciones de grupos dadas por homomorfismos de la forma $G \to \mathrm{Aut}^{\mathcal{C}^{\mathrm{op}}}(X)$ se les denomina *acciones por la izquierda*.

Observación. Normalmente, y por agilizar la notación, escribiremos $g \cdot x$ en lugar de $\Phi(g, x)$, y $x \cdot g$ de igual manera para referirnos a acciones por la izquierda.

Ejemplo 3.2. Consideremos el grupo $\mathrm{SO}_2(\mathbb{R})$. Definimos una acción de $\mathrm{SO}_2(\mathbb{R})$ en $\mathbb{R}^2$ donde la operación consiste en multiplicar una matriz en $\mathrm{SO}_2(\mathbb{R})$ por un vector en $\mathbb{R}^2$ escrito como una columna. Esta operación define una acción por la derecha.

Ejemplo 3.3. Dado un grupo G, tenemos dos acciones sobre G sobre sí mismo (visto como un conjunto). Una de ellas consiste simplemente an aplicar la operación binaria en G, es decir, la acción es simplemente la operación de G

$$\cdot\colon G \times G \to G\,.$$

Otra acción posible es la acción por *conjugación*, donde definimos

$$G \times G \to G \;\; (g,h) \mapsto ghg^{-1}\,.$$

Nótese que en el caso en el que G es abeliano, esta acción es la acción trivial.

3.1. **Órbitas y Estabilizadores.** Partimos de un grupo G, un conjunto X y una acción de G sobre X

$$G \times X \to X\,.$$

Podemos estudiar dos conjuntos que surgen de manera natural al considerar acciones:

- ¿Qué elementos de G dejan fijo un elemento $x \in X$?
- ¿Qué elementos de G dejan fijos *todos* los elementos de X?

El primer conjunto se denomina *estabilizador de un elemento* $x \in X$, y se suele denotar como $\mathrm{Stab}_G(x)$. El segundo conjunto que denotamos $\mathrm{Fix}_G(X)$, es el conjunto de puntos fijos de la acción.

Definición 3.4 (Órbita de un Elemento)**.** Sea G un grupo, X un conjunto sobre el que G actúa por la izquierda, y fijemos un elemento $x \in X$. La *órbita de x bajo G* se define como el conjunto

$$\mathrm{Orb}_G(x) = \{y \in X \mid y = g \cdot x \text{ para un cierto } g \in G\} = \{g \cdot x \mid g \in G\}\,.$$

En otras palabras, la órbita de un elemento consiste en la imágen de los elementos de G actuando sobre dicho elemento.

Ejemplo 3.5. Siguiendo con el Ejemplo 3.2, tenemos que si $\overline{x} = (x_0, x_1) \in \mathbb{R}^2$

$$\mathrm{Orb}_G(\overline{x}) = \{A \cdot \overline{x} \mid A \in \mathrm{SO}_2(\mathbb{R}) \;.$$

Puesto que como vimos, $\mathrm{SO}_2(\mathbb{R})$ no deja de ser otra cosa que el grupo de matrices de traslaciones, pues toda matriz $A \in \mathrm{SO}_2(\mathbb{R})$ se puede representar como

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

para cierto $\theta \in \mathbb{R}$, el conjunto que obtenemos al aplicar dicha acción resultará en todas las posibles orientaciones de $\overline{x}$ en $\mathbb{R}^2$. Dicho de otro modo, obtendremos el conjunto de vectores de $\mathbb{R}^2$ con la misma longitud que $\overline{x}$. Es decir, $\mathrm{Orb}_G(\overline{x})$ es un círculo de radio $|x| = \sqrt{x_0^2 + x_1^2}$.

Observación. El conjunto $\mathrm{Stab}_G(x)$ es un subgrupo de G, pues la operación es cerrada en $\mathrm{Stab}_G(x)$, $e_G \cdot x = x$ por definición, y si g deja fijo a x, g^{-1} también lo deja fijo pues

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

Proposición 3.6 (Cardinal de una Órbita)**.** *Sea G un grupo y X un conjunto de manera que existe una acción de G sobre X. Tenemos que*

$$\mathit{Card}(\mathit{Orb}_G(x)) = [G : \mathit{Stab}_G(x)]\,,$$

es decir, el cadínal de una órbita viene dado por el índice del estabilizado de ese punto en el grupo G.

Proof. Para ver el resultado, es suficiente con demostrar que existe una biyección

$$G/\sim_H \to \mathrm{Orb}_G(x)\,,$$

donde $H := \mathrm{Stab}_G(x)$. Definimos tal aplicación como sigue,

$$g \cdot G \mapsto g \cdot x\,.$$

En primer lugar, veamos que esta aplicación está bien definida.

Si $g_1 \sim g_2$ quiere decir que $g_1^{-1} g_2 \in H = \mathrm{Stab}_G(x)$, pero por definición, tenemos que $(g^{-1} g_2) \cdot x = x$, luego en particular,

$$g_2 \cdot x = g_2 \cdot x\,.$$

Ahora bien, si $g_1 \cdot x = g_2 \cdot x$, siguiendo hacia atrás el argumento anterior, llegamos a la conclusión de que $g_1 \sim g_2$, y por lo tanto la aplicación así definida es inyectiva. Finalmente, todo elemento en $\mathrm{Orb}_G(x)$ es de la form $g \cdot x$ para un determinado $g \in G$, luego es sobreyectiva. □

Si consideramos X un conjunto finito, decimos que $R \subset X$ es un *representante* de las órbitas si podemos escribir

$$X = \bigcup_{x \in R} \mathrm{Orb}_G(x)$$

como unión disjunta de órbitas.

Observación. Debemos pensar en las órbitas de una acción sobre un grupo como una partición, del mismo modo que véiamos las clases de equivalencia como una partición del conjunto cociente. Esto es así dado que si $x, y \in X$ y $x \neq y$, entonces $\mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y) = \emptyset$. En efecto, supongamos que existe un elemento $z \in X$ de manera que $z \in \mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y)$. Entonces $z = g_1 \cdot x$ y $z = g_2 \cdot y$. Tenemos que bien $\mathrm{Orb}_G(x) \subset \mathrm{Orb}_G(y)$, o bien que ambas órbitas son disjuntas. Tenemos que si $w \in \mathrm{Orb}_G(x)$, es decir, $w = g_3 \cdot x$, $g_3 \in G$, entonces

$$g_3 \cdot g^{-1} \cdot g_2 \cdot y = g_3 \cdot g^{-1} \cdot z = g_3 \cdot x = w$$

luego $w \in \mathrm{Orb}_G(y)$.

3.2. **Ecuación de Clases.** Aquí veremos cómo relacionar el tamaño de un conjunto con el total de sus órbitas, y más en concreto, cuando el grupo G actúe sobre sí mismo por conjugación, veremos que el orden del grupo coincide con la suma total de los cardinales de las órbitas.

Proposición 3.7 (Fórmula de las Órbitas)**.** *Sea X un conjunto finito, $R \subset X$ un representante de las órbitas. Entonces,*

$$\mathit{Card}(X) = \sum_{x \in R} [G : \mathit{Stab}_G(x)]\,.$$

En particular, se deduce de la sección anterior que

$$\mathit{Card}(X) = \sum_{x \in R} \mathit{Card}(\mathit{Orb}_G(x))$$

Si aplicamos el anterior resultado al caso en el que $X = G$ sea finito y la acción de G sobre X sea por conjugación, tenemos que

$$\mathrm{ord}(G) = \sum_{x \in R} [G : \mathrm{Stab}_G(x)] \,.$$

Pero en particular,

$$\begin{aligned} \mathrm{Stab}_G(x) &= \{g \in G \mid g^{-1} \cdot x \cdot g = x\} \\ &= \{g \in X \mid g \cdot x = x \cdot g\} \\ &= C_G(x) \,, \end{aligned}$$

es decir, el estabilizador de un elemento coincide con su centralizador. Por lo tanto, $[G : \mathrm{Stab}_G(x)] = 1$ precisamente cuando $x \in C_G(x)$. Por lo tanto

$$\mathrm{ord}(G) = \mathrm{ord}(Z(G)) + \sum_{x \in R \setminus C_G(x)} [G : \mathrm{Stab}_G(x)] \,,$$

pues $\mathrm{ord}(Z(G)) = \sum_{x \in X} C_G(x)$. Esta última ecuación se conoce como *ecuación de clases*.

Observación. En particular, por el Teorema de Lagrange, cada uno de los sumandos $[G : \mathrm{Stab}_G(x)]$ divide al orden de G.

Ejercicio 3.8. Sea G un grupo de 143 elementos que actúa sobre un conjunto X de 108 elementos. Demostrar que X contiene un elemento cuyo estabiliador es G.

Solución. Buecamos un elemento cuyo estabilizador sea G. En particular, puesto que $\mathrm{Card}(\mathrm{Orb}_G(x)) = [G : \mathrm{Stab}_G(x)]$, decir que un elemento tiene como estabilizador al propio grupo equivale a decir que su órbita contiene un único elemento.
Supongamos que es falso. Como $143 = 11 \cdot 13$, por el Teorema de Lagrange tenemos que el cardinal de las órbitas es o bien $1, 11, 13$ o 143. No es 1 puesto que estamos asumiendo que las órbitas de la acción tienen al menos 2 elementos. Tampoco puede ser 143, pues $\mathrm{Card}() = 108 < 143$. Por lo tanto quedan dos opciones, 11 o 13.
Denotemos por m el número de órbitas de 11 elementos y por n al número de órbitas de 13 elementos. Tenemos que

$$108 = 11 \cdot m + 13 \cdot n \,.$$

En particular, $1 \leq n \leq 8$. Ahora bien, $108 = 11 \cdot 9 + 9$, luego

$$108 = 11 \cdot +9 = 11 \cdot m + 13 \cdot n$$

implica que $11 \cdot m + 13 \cdot n = 11 \cdot (m + n) + 2 \cdot n = 11 \cdot 9 + 9$, luego $-2 \cdot n = 11 \cdot (m + n - 9) - 9$, es decir

$$9 \equiv 2 \bmod 11 \,,$$

lo que no ocurre para $1 \leq n \leq 8$, contradicción. □

4. Puntos Fijos

Como antes, sea $G \times X \to X$ una acción. Dado $g \in G$, recordad que los puntos fijos de g se definen como

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

Decimos que $u, v \in G$ son *conjugados* si existe $g \in G$ tal que

$$u \cdot g = g \cdot v \,.$$

Nótese que decir que u y v son conjugados equivale a decir que puedo obtener el uno del otro a través de conjugación. Podemos obtener una aplicación

$$\begin{aligned} \mathrm{Fix}(u) &\to \mathrm{Fix}(v) \\ x &\mapsto g \cdot x \end{aligned}$$

pues,

$$\begin{aligned} v \cdot (g \cdot x) &= (g \cdot v) \cdot x \\ &= (u \cdot g) \cdot x \\ &= g \cdot (u \cdot x) \\ &= g \cdot x \,. \end{aligned}$$

Denotaremos por $\mathrm{Fix}(G)$ al conjunto

$$\mathrm{Fix}(G) = \bigcap_{g \in G} \mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x \ \forall g \in G\}\,.$$

Ahora, ¿qué quiere decir que $\mathrm{Fix}(G) = \emptyset$? Es decir, ¿qué acciones de G sobre X no dejan *ningún* punto fijo?

Ejercicio 4.1. Sea G un grupo de 35 elementos que actúa sin puntos fijos sobre un conjunto X de 19 elementos. Calcular el número de órbitasa y el cardinal de cada una de ellas.

Solución. Como en el ejercicio anterior, supongamos que el enunciado es falso, es decir, $\mathrm{Fix}(G) \neq \emptyset$; $35 = 7 \cdot 5$, luego por Lagrange, $\mathrm{Card}(\mathrm{Orb}_G(x))$ divide a 35, lueg es $1, 5, 7$ o 35. Argumentando como antes, 1 no puede ser, pues si existe un órbita con un elemento, existe un elemento cuyo estabilizado sea todo el grupo G, y por tanto $g \cdot x = x$ para todo $g \in G$, luego $x \in \mathrm{Fix}(G)$, lo que no ocurre, y como $\mathrm{Card}(X) = 19 < 35$, tampoco existe un órbita de 35 elementos. Así, sea m el número de órbitas de 5 elementos y n el de 7. Tenemos que

$$19 = 5 \cdot m + 7 \cdot n\,.$$

En particular, $n = 1$ implica que $19 - 7 = 12 = 5m$ lo que es falso, y si $n = 2$, $m = 1$. Así, existe un órbita de 5 elementos y 2 órbitas de 7 elementos. □

4.1. **Grupo Simétrico.** Recordamos que el grupo simétrico S_n se define como el grupo de permutaciones sobre un conjunto de n elementos, con la operación de composición de permutaciones (al revés). Este grupo coincide con el grupo de biyecciones $\mathrm{Biy}(X)$.

Observación. $|S_n| = n!$. Hay n maneras de asignar el 1, $n - 1$ para el 2...

Teorema 4.2 (Teorema de Cayley)**.** *Todo grupo finito es isomorfo a un usbgrupo de S_n para cierto n.*

Proof. Intentamos buscar un isomorfismo. Puesto que $S_n = \mathrm{Biy}(X)$, donde $X = \{1, \dots, n\}$, si encontramos una aplicación

$$\phi\colon G \to \mathrm{Biy}(G)$$

cuyo núcleo sea el trivial, por el primer Teorema de Isomorfía tendremos que $G \cong \mathrm{im}\,\phi \trianglelefteq \mathrm{Biy}(G) = S_{|G|}$.

Definimos ϕ como

$$g \mapsto \overline{g}\,,$$

donde

$$\begin{aligned} \overline{g}\colon G &\to G \\ h &\mapsto h \cdot g\,. \end{aligned}$$

Veamos primero que ϕ es un homomorfismo. Dados $g_1, g_2 \in G$, tenemos que

$$\begin{aligned} \phi(g_1 \cdot g_2)(h) &= \overline{g_1 g_2}(h) = h(g_1 g_2) \\ &= (hg_1)g_2 \\ &= \overline{g_2}(hg_1) \\ &= \overline{g_2}(\overline{g_1}(h)) \\ &= (\phi(g_2) \circ \phi(g_1))(h)\,. \end{aligned}$$

Para ver que es inyectivo, observamos que $g \in \ker\phi$ quiere decir que $\phi(g)(h) = h$ para todo $h \in G$, es decir, $h \cdot g = h$, lo que implica que $g = e_G$. □

Definición 4.3 (Grupo Simple)**.** Un grupo G es *simple* si los únicos subgrupos normales de G son el subgrupo trivial y el total.

Ejercicio 4.4. Sea G un grupo finito y simple y H un subgrupo de G de manera que $[G : H] = p$ primo. Demostrar que p^2 no divide al orden de G y que p es el mayor divisor primo de $\mathrm{ord}(G)$.

Solución. Recordamos que si G es un grupo finito y $H \trianglelefteq G$, tenemos una acción canónica de G sobre $X = G/\sim_H$ dada por

$$\phi\colon G \to \mathrm{Biy}\left(G/\sim_H\right) ; g \mapsto \overline{g}$$

donde

$$\begin{aligned} \overline{g}\colon G/\sim_H &\to G/\sim_H \\ x \cdot H &\mapsto x \cdot H \cdot g\,. \end{aligned}$$

Esto es una acción, pues

$$\begin{aligned}\phi(g_1 \cdot g_2)(xH) &= (xH)(g_1 g_2)\\ &= (xHg_1)g_2\\ &= \overline{g}_2(xHg_1)\\ &= \overline{g_2}(\overline{g_1}(xH))\\ &= (\phi(g_2) \circ \phi(gf_1))(xH)\,.\end{aligned}$$

Ahora bien, $\ker\phi \trianglelefteq G$. Como G es simple, esto quiere decir que $\ker\phi = \{e_G\}$, es decir, ϕ tiene que ser inyectiva.
Además, si $[G : H] = n = \text{card}(X)$ es finito, por el primer Teorema de isomorfía podemos deducir que G es isomorfo a un subgrupo de S_n.
Volviendo a la solución, tenemos que G es simple, $[G : H] = p$ primo mayor que cero, luego G es isomorfo a un subgrupo de S_p. En particular, tenemos que

$$\text{ord}(G) \mid \text{ord}(S_p) = p!\,,$$

y como p es primo, p no divide a $(p-1)!$, luego p^2 no divide a $p!$.
Para la segunda parte, si q es un primo divisor de $\text{ord}(G)$, tenemos que $q|p!$, luego $q|p-j$ para algún j, ya que p es primo. En particular, $q \leq p - j \leq p$. □

No todas las acciones de un grupo sobre un conjunto son idénticas, y hay ciertas propiedades de las acciones que merecen una nomenclatura particular. Por ejemplo, decimos que una acción es *fiel* si la aplicación

$$G \to \text{Biy}(X)\ \ g \mapsto \overline{g}$$

que hemos deifnido antes es inyectiva.

Diremos que una acción es transitiva si dados $x, y \in X$, existe un $g \in G$ de manera que

$$g \cdot x = y\,.$$

Observación. En particular, si una acción es transitiva, existe un única órbita.

Diremos que una acción es *libre* si $g \cdot x = x$ implica que $g = e_G$, es decir, si solamente la identidad deja fijo.a $x \in X$ para cada x.

Ejercicio 4.5. Sea H un subgrupo de un grupo G con índice $k > 1$ y de manera que $\text{ord}(G)$ no divide a $k!$. Demostrar que H contiene un grupo normal no trivial.

Solución. Como antes, será suficiente con comprobar que la aplicación

$$G \to \text{Biy}(X)\ \ g \mapsto \overline{g}\,,$$

donde $X = G/\sim_H$ y

$$\begin{aligned}\overline{g}\colon G &\to G\\ H \cdot x &\mapsto (H \cdot x)g\end{aligned}$$

no es inyectiva, pues si lo fuese, G sería isomorfo a la imagen de dicha aplicación, que es un subgrupo de $\text{Biy}(X)$, luego $\text{ord}(G)|\text{ord}(\text{Biy}(X)) = k!$, lo que no ocurre por hipótesis. □

Por el Teorema de Lagrange, sabemos que el orden de todo subgrupo de un grupo tiene que dividir al orden del grupo. Esto sin embargo no garantiza que existan subgrupos para cualquier divisor de $\text{ord}(G)$. El siguiente resultado es un resultado parcial a este problema.

Teorema 4.6 (Teorema de Cauchy)**.** *Sea G un grupo finito y p primo de manera que $p|ord(G)$. El número de subgrupos de G de orden p es congruente 1 mod p.*
En particular, existe un elemento $g \in G$ de orden p.

Ejercicio 4.7. Sea p un número primo y k un entero mayor que 1 y menor que p. Demostrar que todo grupo de orden pk no es simple.

Solución. Por Cauchy tenemos que existe un subgrupo $H \trianglelefteq G$ con $\text{ord}(H) = p$. Por otro lado, $[G : H] = k$. y por el Ejercicio anterior, tenemos que H contiene un subgrupo normal no trivial. □

5. Producto Semidirecto

Esta sección trata de la construcción del producto semidirecto y la idea detrás, usos, ejemplos, etc. La idea es entender el producto semidirecto como una "factorización" de un grupo en un producto de subgrupos. Como sabemos, para que el producto de dos subgrupos de G sea un grupo, al menos uno de los dos factores tiene que ser normal en G. En este caso, entender la estructura de G equivaldría a entender la estructura de los subgrupos que forman dicha factorización, lo que a priori es un problema algo más sencillo.

Empezamos definiendo la noción de *sucesión corta de grupos*.

Definición 5.1 (Sucesión Corta)**.** Una *sucesión corta de grupos* es una sucesión de grupos y homomorfismos de grupos de la forma

$$1 \longrightarrow K \xrightarrow{f} G \xrightarrow{g} H \longrightarrow 1 \tag{2}$$

que es *exacta*. Esto quiere decir lo siguiente:

- f es un homomorfismo inyectivo.
- g es un homomorfismo sobreyectivo.+
- $\ker g = \operatorname{im} f$.

En el diagram anterior, los homomorfismos $1 \to K$ y $H \to 1$ son la inclusión del elemento neutro en K y la proyección de H sobre el único elemento de 1.

Observación. La noción de *exactitud* se puede hacer algo más precisa como sigue: dados tres grupos G_1, G_2, G_3, y homomorfismos $f_1 \colon G_1 \to G_2$ y $f_2 \colon G_2 \to G_3$, la sucesión

$$G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3$$

es exacta si $\ker g = \operatorname{im} f$. Así, una sucesión

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \cdots$$

es exacta cada sucesión de la forma

$$G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1}$$

es exacta para cada i.

Ejemplo 5.2. Las siguientes sucesiones de grupos son exactas:

$$1 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2 \longrightarrow 1$$

$$1 \longrightarrow \mathbb{Z}/2 \xrightarrow{\cdot 2} \mathbb{Z}/4 \longrightarrow \mathbb{Z}/2 \longrightarrow 1$$

donde en ambos casos, $\cdot 2$ denota multiplicación por 2 y la otra aplicación es reducción módulo 2.

Definición 5.3. Dados dos grupos H y K, decimos que G es una *extensión de H por K* si podemos construir una sucesión corta de la forma (2).

En general, dados dos subgrupos H y K, clasificar las posibles extensiones de H por K es un problema complicado sin restringir la clase de grupos a los que nos atenemos. Por ejemplo, podríamos requerir que H sea en cierto sentido *similar* a G. ¿Cómo de similar? Requiriendo la existencia de un homomorfismo

$$s \colon H \to G$$

de manera que $f \circ s = 1_H$. En lo que sigue, supondremos que K es un subgrupo normal de G.

Definición 5.4 (Sección/Sucesión Split)**.** Un homomorfismo $f \colon G \to H$ es *split* si existe $s \colon H \to G$ como en la discusión anterior. Decimos que tal s es una *sección*. Si en (2) requerimos que $g \colon G \to H$ sea split, decimos que (2) es una *sucesión split*.

Observación. Requerir la existencia de una sección para un homomorfismo de grupos $f \colon G \to H$ implica que f es sobreyectiva y que s es un homomorfismo inyectivo. En efecto, dado $h \in H$, denotemos por $s \colon H \to G$ la sección. Entonces $f(s(h)) = h$, luego f es sobreyectiva. Dados $h_1, h_2 \in H$, si $i(h_1) = i(h_2)$, se sigue que $f(i(h_1)) = f(i(h_2))$, y como $f \circ i = 1_H$, esto a su vez implica que $h_1 = h_2$.

La existencia de una sección es una propiedad bastante restrictiva, que tiene como consecuencia el hecho de que podemos interpretar H con el subgrupo $s(H) \trianglelefteq G$. Además, en sucesiones de la forma (2), podemos identificar H con el cociente G/K, de manera que la existencia de una sección nos permite "ver" el cociente G/N como un subgrupo de G.

En este sentido, tras identificar $s(H)$ con H, podemos entender tanto a K como a H como subgrupos de G con intersección trivial. Pues todo $k \in K$ es la identidad en H bajo la identificación

$$H \sim G/K\,.$$

Así, si H es normal, obtenemos una descomposición de G como $G = HK$.

Observación. Dada una extensión split de H por K como antes, dicha extensión induce acciones de H en K.

Recordamos que una acción de H sobre K es la misma información que un homomorfismo

$$\phi\colon H \to \mathrm{Biy}(K)(=\mathrm{Aut}(K))\,.$$

Dada una extensión de H por K, hacemos que H actúe sobre K por conjugación, es decir, para cada $h \in H$, definimos $\phi(h) = \phi_h\colon K \to K$ como

$$\phi_h(k) = hkh^{-1}\,.$$

Esto es posible dada la existencia de una sección $s\colon H \to G$ y la identificación que hemos descrito anteriormente.

Dado $k \in K$, los automorfismos de K de la forma

$$\begin{aligned}\phi_k\colon K &\to K\\ x &\mapsto kxk^{-1}\end{aligned}$$

se les denomina *automorfismos interiores*. Estos forman un subgrupo normal de $\mathrm{Aut}(K)$, de manera que podemos definir el cociente

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

$\mathrm{Out}(K)$ se denomina el group de *automorfismos exteriores*.

Si G es una extensión (no necesariamente split) de H por K, la normalidad de K implica que existe siempre un homomorfismo

$$\phi\colon G \to \mathrm{Aut}(K)$$

cib $\phi(g) = \phi_g$ definido por conjugación como antes. En particular, los elementos de k son enviados a los automorfismos interiores de K, de manera que la acción define un homomorfismo

$$\Phi\colon G/K = H \to \mathrm{Out}(K)\,.$$

De esta manera, podemos entender una sección $s\colon H \to G$ como un objeto que nos permite resolver el problema de encontrar una acción $\phi\colon H \to \mathrm{Aut}(K)$ de manera que el

$$\begin{array}{ccc} & & \mathrm{Aut}(K) \\ & \overset{\phi}{\nearrow} & \big\downarrow{\scriptstyle \pi} \\ H & \xrightarrow{\Phi} & \mathrm{Out}(K) \end{array}$$

commute, es decir, $\pi \circ \phi = \Phi$.

Para resumir, hemos introducido la noción de sucesión split como existencia de una sección. El producto semidirecto de H y K se define como la extensión de H por G. Por otro lado, hemos visto que tenemos una acción canónica una acción de H sobre K

$$\phi\colon H \to \mathrm{Aut}(K)$$

si G es tal producto semidirecto.

Ejemplo 5.5. Consideremos las sucesiones del Ejemplo 5.2. La primera de ellas no es split. Si existiese una sección para la primera, necesitaríamos encontrar un homomorfismo inyectivo $s\colon \mathbb{Z}/2 \to \mathbb{Z}$, pero no hay ninguno.

Para la segunda, necesitaríamos un homomorfismo $s\colon \mathbb{Z}/2 \to \mathbb{Z}/4$, que tampoco existe.

Ejemplo 5.6. Sean K, H dos grupos cualesquiera y consideremos

$$1 \longrightarrow K \longrightarrow K \times H \longrightarrow H \longrightarrow 10$$

donde ls homomorfismos son $k \mapsto (k, e_H)$ y $(k, h) \mapsto h$. Definimos

$$\begin{aligned}s\colon H &\to K \times H\\ h &\mapsto (e_K, h)\,.\end{aligned}$$

Claramente $f \circ s = e_H$, pues

$$h \mapsto (e_K, h) \mapsto h\,.$$

Es más, la acción $\phi\colon H \to \mathrm{Aut}(K)$ es trivial, ya que

$$\phi_h(k,1) = (k, hh^{-1}) = (k,1)\,.$$

Esto se debe a que H es normal en G. De hecho, tenemos que esto sólo puede suceder cuando H es normal en G.

Proposición 5.7. *G una extensión split de H por K con $H \trianglelefteq G$ si y sólo si $G \cong K \times H$.*

Ejemplo 5.8. Consideremos el grupo dihédrico D_n de orden $2n$. Definimos

$$1 \longrightarrow \mathbb{Z}/n \longrightarrow D_n \longrightarrow \mathbb{Z}/2 \longrightarrow 1$$

Donde el generador $\overline{1} \in \mathbb{Z}/n$ de orden n se envía a la rotación $\rho \in D_n$, y el segundo homomorfismo envía una simetría de D_n su determinante.

Esta sucesión es split, ya que podemos definir $s\colon \mathbb{Z}/2 \to D_n$ como la aplicación que envía $\overline{1}$ a la reflexión σ.

En este caso, el homomorfismo

$$\phi\colon \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/n)$$

viene definido por $\phi_{\overline{1}}(k) = \overline{n-k}$, pues

$$\phi_1(\rho) = \sigma\rho\sigma = \rho^{-1}\,.$$

5.1. **Existencia y Unicidad.** Hemos visto como reconstruir H y K a través de una extensión split de H por K. Ahora nos preguntamos qué ocurre al revés, es decir, dados K y H, cómo podemos construir todas las extensions split de H por K?

Definición 5.9. Sea

$$1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$$

una sucesión exacta corta y $\theta\colon H \to \mathrm{Aut}(K)$ un homomorfismos. Decimos que G es un *producto semidirecto de K y H a través de θ* si existe una sección $s\colon H \to G$ de manera que la acción por conjugación

$$\begin{aligned} \phi\colon H &\to \mathrm{Aut}(K) \\ h &\mapsto \phi(h)(k) = hkh^{-1} \end{aligned}$$

coincide con θ.

Teorema 5.10 (Existencia y Unicidad)**.** *Sean K y H dos grupos y $\theta\colon H \to Aut(K)$. El producto semidirecto de K y H a través de θ existe y se nota como $K \rtimes_\theta H$. Más aún, este producto es único.*

6. Teoremas de Sylow

Recordad que el Teorema de Cauchy afirma que si G es un grupo abeliano y p un número primo que divide al orden de G, G posee un elemento de orden p, y en particular, el subgrupo $H = \langle `\rangle$ tiene orden p. Los Teoremas de Sylow son una generalización de este resultado, que se puede ver también como un recíproco al Teorema de Lagrange (el orden de todo subgrupo de G tiene que dividir al orden de G). Como veremos, consecuencias de estos resultados incluyen criterios de normalidad y simplicidad.

Empezamos con la definición de *p-grupo* y *p-subgroupo.*

Definición 6.1. Sea G un grupo y p un número primo:

1) Un grupo de orden p^k donde $k \geq 1$ se denomina *p-grupo.* Un subgrupo de orden p^k para un cierto $k \geq 1$ se denomina *p-subgrupo.*
2) Si $ord(G) = p^n m$ donde p no divide a m, un subgrupo de orden p^n se denomina *p-subgrupo de Sylow* de G.

Por fijar la notación de aquí en adelante,

$$\mathrm{Syl}_p(G) = \text{ conjunto de } p\text{-subgrupos de Sylow de } G$$

y

$$n_p(G) = \text{ número de } p\text{-subgrupos de Sylow de } G\,.$$

El Primer Teorema de Sylow dice como sigue:

Teorema 6.2 (Primer Teorema de Sylow)**.** *Cualesquiera dos p-subgrupos de Sylow son conjugados. Esto quiere decir que existe $g \in G$ de manera que $gH = Kg$ para cualesquiera p-subgrupos de Sylow H, K de G.*

Proof. La demostración consistre en construir $g \in G$ en particular. Sean H y K los dos p-subgrupos de Sylow, $\sim_K$ denote la relación por congruencia y el conjunto cociente $X = G/\sim_K$ (nótese que a priori K no tiene por que ser normal, por lo que X es un conjunto, no necesariamente un grupo). Consideremos la acción de H sobre X definida por

$$\phi\colon H \to \mathrm{Biy}(X)$$
$$h \mapsto \overline{h}$$

donde

$$\overline{h}(K \cdot g) = K \cdot (gh)\,.$$

Como G es un grupo finito,

$$\mathrm{card}(X) = \frac{\mathrm{ord}(G)}{\mathrm{ord}(K)} = \frac{p^n m}{p^n} = m\,.$$

De esta manera, podemos reescribir la ecuación de órbitas como

$$m = \mathrm{card}(X) = \sum_{K\cdot g \in R} [H : \mathrm{Stab}_H(Kg)]\,.$$

Ahora, si no existe $g \in G$ de manera que $H = \mathrm{Stab}_H(Kg)$, tenemos que para todo $g \in G$, el índice $[H : \mathrm{Stab}_H(Kg)]$ es múltiplo de p, que no ocurre, ya que por hipótesis p no divide a m. Así, sea $g \in G$ tal que $H = \mathrm{Stab}_H(kg)$. Para dicho g,

$$Kg = \overline{h}(Kg) = K(gh)$$

para todo $h \in H$, es decir, $ghg^{-1} \in K$ para todo $h \in H$.
Por otro lado, sabemos que dado $H \trianglelefteq G$, $\mathrm{ord}(H) = \mathrm{ord}(gHg^{-1})$. En nuestro caso, $gHg^{-1} \subset K$. Pero como

$$\mathrm{ord}(gHg^{-1}) = \mathrm{ord}(H) = \mathrm{ord}(K)\,,$$

tenemos que $K = gHg^{-1}$, es decir, K y H son conjugados. □

Ejemplo 6.3. Sea G un grupo finito con $\mathrm{ord}(G) = p^n m$ donde p no divide a m y H un p-subgrupo de Sylow de G. Por el primer Teorema de Sylow, los p-subgrupos de Sylow de G son los conjugados con H. Así H es normal si y sólo si todos los conjugados con H coinciden.

En particular, un subgrupo p-subgrupo de Sylow es normal si y solo si es el unico p-subgrupo de Sylow de G. De esta manera, un criterio de simplicidad de un grupo se puede formular como sigue:

Un grupo finito G no es simple si posee un unico p-subgrupo de Sylow para cualquier $p|ord(G)$.

Corolario 6.4. *Sea p un número primo, G un grupo finito cuyo orden es múltiplo de p. Definimos*

$$N = \bigcap_{H \in Syl_p(G)} H\,.$$

N es un subgrupo normal de G.

Proof. Por el Primer Teorema de Sylow, los elementos de $\mathrm{Syl}_p(G)$ son conjugados dos a dos. Así, dado $K \in \mathrm{Syl}_p(G)$ cualquiera,

$$\mathrm{Syl}_p(G) = \{g^{-1}Kg \mid g \in G\}\,.$$

De esta manera, para todo $x \in G$,

$$\begin{aligned} x^{-1}Nx &= x^{-1}\left(\bigcap_{H\in \mathrm{Syl}_p(G)} H\right)x \\ &= \bigcap_{H\in \mathrm{Syl}_p(G)} (x^{-1}Hx) \\ &= \bigcap_{g\in G} x^{-1}(g^{-1}Kg)x \\ &= \bigcap_{g\in G} (gx)^{-1}K(gx) \\ &= \bigcap_{z\in G} z^{-1}Kz \\ &= \bigcap_{H\in \mathrm{Syl}_p(G)} H \\ &= N\,. \end{aligned}$$

□

Teorema 6.5 (Segundo Teorema de Sylow)**.** *Sea G un grupo finito de orden $p^n m$ donde p es primo y p no divide a m. Fijados índices $0 \leq i \leq n-1$ y $H_i \trianglelefteq G$ de orden p^i, existe un subgrupo H_{i+1} de G de orden p^{i+1} tal que*

$$H_i \trianglelefteq H_{i+1}\,,$$

es decir, H_i es normal en H_{i+1}.
En particular, existen subgrupos $H_1, \ldots, H_n$ de G de órdenes $p, p^2, \ldots, p^n$ respectivamente, tales que H_i es normal en H_{i+1}.

Proof. La segunda parte se sigue de la primera donde empezamos con $H_0 = \{e_H\}$ de orden $p^0 = 1$. Así, por la primera parte, existe H_1 subgrupo de G de orden p de manera que $\{e_H\}$ es normal en H_1, y así sucesivamente.

Para demostrar la primera parte utilizamos inducción. El caso base se corresponde con $H_0 = \{e_G\}$. Por el Teorema de Cauchy sabemos que existe $H_1 \trianglelefteq G$ de orden p, de manera que $H_0 \trianglelefteq H_1$.

Sea ahora $0 < i < n$ y H_i un subgrupo de G de orden p^i. Como

$$[G : H_i] = p^{n-i}m \in p\mathbb{Z}$$

se sigue que $[N_H(H_i) : H_i]$ es múltiplo de p. En efecto, consideremos en G la relación $\sim_{H_i}$ de congruencia y el conjunto $X = G/\sim_{H_i}$. Definimos como siempre la acción de H_i sobre X mediante $h \mapsto \overline{h}$ donde

$$\begin{aligned} \overline{h}\colon X &\to X \\ H_i g &\mapsto H_i(gh)\,. \end{aligned}$$

La ecuación de órbitas se lee

$$[G : H] = \mathrm{card}(X) = \sum_{H_i g \in R} [H_i : \mathrm{Stab}_{H_i})H_i g]$$

□

Terminamos esta seccion con el Tercer Teorema de Sylow. Si los dos Teoremas de Sylow anteriores aportaban informacion sobre la estructura de los p-subgrupos de Sylow, este proporciona informacion sobre el numero de dichos subgrupos. Este ultimo Teorema tiene consecuencias importantes a la hora de decidir sin un grupo es, por ejemplo, simple o no: si de alguna manera somos capaces de encontrar que el numero de p-subrupos para un determinado p es unico, dicho subgrupo sera normal, y por tanto G no seria simple.

Teorema 6.6 (Tercer Teorema de Sylow)**.** *Sean p un numero primo y G un grupo finito cuyo orden se escribe como $ordG = p^n m$, donde m y n son eneteros positivos y p no divide a m. Entonces, el numero n_p de p-subgrupos de Sylow de G cumple las siguientes relaciones:*

(1) $n_p = [G : n_G(H)]$ para cada p-subgrupo de Sylow H de G.
(2) n_p divide a m y $n_p - 1$ es multiplo de p.

Ejercicio 6.7. Existe algun grupo simple de orden 5625?

Solución. Empezamos buscando una descomposicion en factores primos de 5625 y vemos que

$$5635 = 5^4 \cdot 3^2 \, .$$

Asi, por el Tercer Teorem de Sylow sabemos que el numero de 5-subgrupos de Sylow de un grupo de order 5625 tiene que dividir a $3^2 = 9$, luego dicho numero n pertenece al conjunto $\{1, 3, 9\}$. Como ademas, $n-1$ es multiplo de 5, concluimos que $n = 1$. Por tanto, G posee un 5-subgrupo de Sylow de orden 5^4, que es normal, y por tanto G no puede ser simple. □

Ejercicio 6.8. Sea G un grupo de orden 2013.

(1) Cuantos subgrupos de order 671 tiene G? Es ciclico alguno de ellos?
(2) Suponemos que G no es ciclico. Calcular el numero de elementos de orden 3 en G.

Solución. (1) Empezamos factorizando 2013 y vemos que

$$2013 = 3 \cdot 11 \cot 61 \, .$$

Asi, por el Tercer Teorema de Sylow sabemos que, como el numero de 11-subgrupos de 61-subgrupos de G dividen a $61 \cdot 3 = 183$ y $11 \cdot 3 = 33$, respectivamente. Ademas, dichos numeros n_{11} y n_{61} son congruentes con 1 moduloe 11 y 61. En particular, $n_{61} \in \{1, 3, 11\}$ y $n_{11} \in \{1, , 61\}$. Estas dos condiciones implican que $n_{11} = n_{61} = 1$.

En particular, si consideramos $H = H_{11} \cdot H_{61}$, puesto que 11 y 61 son primos entre si, H es un subgrupo de G de orden $61 \cdot 11 = 671$. Ademas, tenemos que la aplicacion

$$H_{61} \times H_{11} \to H_{61} \cdot H_{11}$$
$$(x, y) \mapsto x \cdot y$$

es un isomorfismo de grupos. Asi, como 61 y 11 son primos,

$$H \cong H_{61} \times H_{11} \cong \mathbb{Z}_{61} \times \mathbb{Z}_{11} \cong \mathbb{Z}_{671} \, ,$$

y por tanto G posee un subgrupo ciclico de orden 671.

Finalmente, calculemos el numero de subgrupos de orden 671. Supongamos que existe otro, K. Por el Teorema de Cauchy el grupo K posee algun subgrupo de orden 11 y algun subgrupo de orden 61. Estos son subgrupos de GH que son precisamente H_{11} y H_{61}. De esta forma, K contiene a H, y como el orden de ambos grupos es el mismo, concluimos que $K = H$, de manera que hay un unico subgrupo de orden 671.

(2) Por el Tercer Toerema de Sylow, el numero n_3 de subgrupos de orden 3 divide a $671 = 11 \cdot 61$, luegp $n_3 \in \{1, 11, 61\}$. Ademas, $n_3 - 1$ tiene que ser multiplo de 3, luego podemos descartar que el numero de 3-subgrupos sea 11. Si $n_3 = 1$, el grupo G poseeria un subgrupo normal de orden 3. Argumentando como antes, tendriamos que $G \cong H_{671} \cdot H_3 \cong \mathbb{Z}_{2013}$, que es ciclico, contra la hipotesis. De esta forma, el numero de de 3-subgrupos es 61. Cada uno de estos subgrupos tiene dos elementos de orden 3, el grupo G tiene un total de $51 \cdot 2 = 122$ elementos de orden 3.

□

7. Teorema de Estructura de los Grupos Abelianos Finitos

Esta breve seccion presenta el Teorema de Estructura de Grupos Abelianos Finitos. Ese resultado nos dice como descomponer cualquier grupo abeliano finito en una suma directa de subgrupos ciclicos cuyo orden es la potencia de un cierto primo.

Teorema 7.1 (Teorema de Estructura)**.** *Sea G un grupo abeliano finito. Existen enteros positivos $m_1, \cdots, m_r$ tales que cada m_i divide a m_{i-1} para $2 \leq i \leq r$, y un isomorfismo*

$$G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \, .$$

Ademas, dicha descomposicion es unica. Los elementos $m_1, \ldots, m_r$ se denominan coeficientes de torsion de G.

Ejercicio 7.2. Utilizando el Teorema de Estructura vamos a calcular el numero de grupos abelianos de orden $48 = 2^4 \cdot 3$. Para ello, descompongamos uno de llos en sus coeficientes de torsion, $\mu = (m_1, \ldots, m_r)$. Sabemos que cada m_i divide a m_{i-1}

Dejo aquí una lista de ejercicios para que vayáis intentando. Los ejercicios marcados

Ejercicio 10.1. Denotamos por $\mathbb{T}$ al conjunto de los números complejos con módulo 1, es decir

$$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}\,.$$

i) Demuestra que $\mathbb{T}$ es un grupo abeliano con la multiplicación.

ii) * Sea $\mathrm{SO}_2(\mathbb{R})$ el grupo lineal especial de matrices 2×2 con coeficientes en $\mathbb{R}$. Construye explícitamente un isomorfismo

$$\mathbb{T} \xrightarrow{\cong} \mathrm{SO}_2(\mathbb{R})\,.$$

(Pista: utiliza la fórmula de Euler).

iii) Denotemos por $\mathrm{U}(n)$ el el grupo de matrices unitarias $n \times n$. Una matriz cuadrada con coeficientes en $\mathbb{C}$ se dice que es *unitaria* si $UU^* = U^*U = I$, donde U^* denota la matriz transpuesta conjugada de U. Deduce del apartado anterior que $\mathrm{U}(1) \cong \mathbb{T}$.

iv) Consideremos los groups $(\mathbb{Z}, +)$ y $(\mathbb{R}, +)$. Justifica que $(\mathbb{Z}, +)$ sea un subgrupo normal de $(\mathbb{R}, +)$ y describe las clases de equivalencia del grupo cociente $\mathbb{R}/\mathbb{Z}$.

v) ** Construye un homomorfismo $\mathbb{R} \to \mathbb{T}$ y utiliza el Primer Teorema de Isomorfía para demostrar que

$$\mathbb{R}/\mathbb{Z} \cong \mathbb{T}\,.$$

(Pista: mira la pista de ii))

Ejercicio 10.2. Sea G un grupo. Dados $g, h \in G$, definimos

$$g, h = g^{-1}h^{-1}gh\,.$$

Denotamos por $[G, G]$ el subgrupo de G generado por todos los elementos de la forma $[g, h]$ para $g, h \in G$.

i) Demuestra que $[G, G]$ es un subgrupo normal de G.

ii) Demuestra que $G/[G, G]$ es un grupo abeliano. Este grupo se suele denotar G^{ab}.

iii) * Demuestra que, en general, dado $N \trianglelefteq G$, G/N es abeliano si y sólo si $[G, G] \trianglelefteq N$.

iv) * Demuestra que todo subgrupo de G que contiene a $G/[G, G]$ es un subgrupo normal de G.

v) ** Considera el homomorfismo sobreyectivo $\pi\colon G \to G/[G, G]$. Demuestra que π satisface la siguiente propiedad:

- Dado $f\colon G \to H$ un homomorfismo donde H es abeliano, existe único homomorfismo $F\colon G/[G, G] \to H$ de manera que $f = F \circ \pi$.

vi) * Demuestra que $\mathrm{GL}_n(\mathbb{R})^{\mathrm{ab}}$ es isomorfo a $(\mathbb{R} \setminus \{0\}, \cdot)$ mediante el siguiente argumento:

(a) Construye una aplicación

$$\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}$$

cuyo núcleo sea $\mathrm{SL}_n(\mathbb{R})$. (Pista: álgebra lineal).

(b) Utiliza el Primer Teorema de Isomorfía y uno de los apartados anteriores para deducir que

$$[\mathrm{GL}_n(\mathbb{R}), \mathrm{GL}_n(\mathbb{R})] \trianglelefteq \mathrm{SL}_n(\mathbb{R})\,.$$

(La otra implicación también es cierta, aunque la demostración es bastante más complicada, así la daremos por supuesta.)

(c) Concluye el resultado aplicando el Primer Teorema de Isomorfía.

vii) ** Calcula $G/[G, G]$ cuando $G = F(\{a, b\})$.