Notas de Álgebra

Cristóbal Rivas

Notas para el curso de Álgebra Abstracta de la Universidad de Santiago de Chile.

Índice

1. Introducción a los grupos

1.1. Definición abstracta y primeros ejemplos

Una **operación** o regla de composición en un conjunto G es una función $op : G \times G \to G$ (en particular, para nosotros las operaciones son *cerradas* por definición). En lo sucesivo, para $x, y \in G$, anotaremos $op(x, y)$ simplemente como $x + y$ o $x \cdot y$ o simplemente xy dependiendo del contexto.

Definición 1.1. Un conjunto G dotado de una operación se dice **grupo** si la operación satisface las siguientes propiedades:

1. $\forall x, y, z \in G$, $(xy)z = x(yz)$ (la operación es asociativa).
2. Existe $e \in G$ tal que para todo $x \in G$ vale que $xe = ex = x$ (existe neutro).
3. Para todo $x \in G$ existe y tal que $xy = yx = e$ (existe inverso).

Observación 1.2. Note que un conjunto puede admitir varias reglas de composición, dependiendo de lo cual será o no un grupo. Para hacer explícita esta dependencia usualmente anotaremos (G, op).

Por ejemplo $(\mathbb{Z}, +)$ es un grupo, pero $(\mathbb{Z}, \cdot)$ no lo es (pues no tiene inversos), ni tampoco lo es $(\mathbb{Z}, op(n, m) = 0)$ (pues no tiene neutro).

Ejercicio 1.3. Sea $(G, \cdot)$ un grupo. Pruebe que el neutro es único, lo denotaremos por id. Pruebe también que si $x \in G$ entones existe un único $y \in G$ tal que $x \cdot y = id$. Al inverso de x lo denotaremos por x^{-1}.

Definición 1.4. Dado un grupo $(G, \cdot)$, decimos que $H \subseteq G$ es un **subgrupo** de G si H es no vacío y $h_1^{-1} \in H$ y $h_1 \cdot h_2 \in H$ para todo $h_1, h_2 \in H$. Anotamos $H \leq G$.

Observación 1.5. Note que si $(G, \cdot)$ es un grupo y $H \leq G$ es un subgrupo, entonces $(H, \cdot)$ también es un grupo. En efecto, como la operación en H es la misma que la de G se tiene que ella es asociativa. Por otro lado, H tiene inversos por definición de subgrupo y, como H es cerrado bajo el producto, también se tiene que H contiene al neutro $id = h \cdot h^{-1}$.

Ejemplo 1.6. Algunas familias de grupos

- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ y $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ son un grupos con la multiplicación. Mas aún, $(\mathbb{R}^*, \cdot) \leq (\mathbb{C}^*, \cdot)$.
- $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, equipado con la multiplicación, es un subgrupo de $(\mathbb{C}^*, \cdot)$. En efecto esto sigue de que el módulo de un número complejo cumple que
$$|z \cdot w| = |z| \cdot |w| \text{ y que } |z^{-1}| = |z|^{-1}.$$
- Ejercicio: pruebe que $\mathbb{Z}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ es un subgrupo de $(S^1, \cdot)$.

Note que todas estos grupos son grupos **Abelianos** o **conmutativos**, es decir $\forall a, b.$ se tiene $a \cdot b = b \cdot a$.

El siguiente es un ejemplo de un grupo que no es Abeliano.

Ejemplo 1.7 (El grupo simétrico)**.** Dado un conjunto X, denotaremos por $Biy(X)$ o S_X al conjunto de biyecciones $X \to X$. Notar que si $f, g \in Biy(X)$ entonces su composicion $f \circ g$ y su inversa f^{-1} también son biyecciones de X. De hecho, $(Biy(X), \circ)$ es un grupo puesto que la composición de funciones es asociativa y la función identidad $id : x \mapsto x$ cumple que $f \circ id = id \circ f = f$ para toda $f \in Biy(X)$.

El grupo $(Biy(X), \circ)$ se llama el **grupo simétrico sobre** X. Cuando X es un conjunto de n elementos, S_X usualmente se denota por S_n.

Ejercicio 1.8.

1. Pruebe que si $n \geq 3$ entonces S_n no es Abeliano.
2. Sea X un conjunto infinito. Pruebe que $Biy_0(X)$, el conjunto de biyecciones de soporte[1] finito, es un subgrupo de $(Biy(X), \circ)$.
3. Pruebe que el conjunto de $GL_n(\mathbb{R})$, el conjunto de matrices con entradas en $\mathbb{R}$ y con determinante $\neq 0$, es un grupo bajo la multiplicación matricial.

Ejercicio 1.9. Sean $(G, *_1)$ y $(H, *_2)$ dos grupos cualesquiera. Demuestre que $G \times H = \{(g, h) \mid g \in G,\ h \in H\}$ es un grupo bajo la operación

$$(g, h) * (g', h') := (g *_1 g', h *_2 h').$$

Ejercicio 1.10. Sea G un grupo y H_i una colección de subgrupos de G. Muestre que $\cap_i H_i$ también es subgrupo de G.

Ejercicio 1.11. Sea G un grupo y $S \subseteq G$ un subconjunto cualquiera. Denotamos por $\langle S \rangle$ a la intersección de todos los subgrupos de G que contienen a S. Muestre que

$$\langle S \rangle = \{g \in G \mid \exists n \in \mathbb{N},\ \exists\, s_1, \ldots, s_n \in S \cup S^{-1}\ :\ g = s_1 \cdot \ldots \cdot s_n\},$$

donde $S^{-1} = \{s^{-1} \mid s \in S\}$.

Tabla de Multiplicar: Una manera de visualizar una operación en un grupo es mediante su tabla de multiplicar[2]. Por ejemplo si $G = \{a, b, c\}$, su tabla de multiplicar es

	a	b	c
a	$a \cdot a$	$a \cdot b$	$a \cdot c$
b	$b \cdot a$	$b \cdot b$	$b \cdot c$
c	$c \cdot a$	$c \cdot b$	$c \cdot c$

[1] Recuerde que el soporte de una funcion $f : X \to X$ es el conjunto $sop(f) = \{x \in X \mid f(x) \neq x\}$.

[2] Note que una operación un grupo G está completamente determinada por su tabla de mutiplicación, puesto que su operación *es* la tabla de multiplicar.

Definición 1.12. Sea G un grupo y sea $g \in G$. Definimos las funciones multiplicar por g por la izquierda y por derecha:

$$L_g : G \to G \ , \ L_g : x \mapsto gx,$$

$$R_g : G \to G \ , \ R_g : x \mapsto xg.$$

Note que en la tabla de mutiplicar de G, la imagen de L_g es precisamente la fila de g y la imagen de R_g es precisamente la columna de g.

La siguiente proposición, aunque sencilla, es muy importante.

Proposición 1.13. *L_g y R_g son biyecciones de G.*

Demostración: Probamos solamente que L_g es biyección pues el argumento para R_g es análogo.

Sobreyectividad: basta notar que $L_g(g^{-1}x) = gg^{-1}x = x$.

Inyectividad: si $L_g(x) = L_g(y)$, entonces $gx = gy$. Si multiplicamos a izquierda por g^{-1} se tiene que $g^{-1}gx = g^{-1}gy$, lo que implica que $x = y$. □

Por ejemplo con ella podemos probar el

Teorema 1.14. *Salvo cambio de nombre, existe un único grupo con tres elementos.*

Demostración. Sea $G = \{a, b, c\}$. Lo que quiere decir este teorema es que hay una única manera de rellenar la tabla de multiplicar de G.

En efecto, uno de los elementos de G necesariamente es la identidad, digamos $a = id$, por lo que podemos al menos asegurar que la tabla de multiplicar se ve asi:

G	id	b	c
id	id	b	c
b	b	??	??
c	c	??	??

donde ?? indica que (aún) no sabemos que poner. Ahora, siguiendo la táctica del Sudoku, notamos que solo hay una forma de completar esta tabla de modo que no hayan filas ni columnas con letras repetidas (esto es, que L_b, L_c, R_b, R_c sean biyecciones):

G	id	b	c
id	id	b	c
b	b	c	id
c	c	id	b

□

Ejercicio 1.15. Demuestre que, salvo cambio de nombre, existe un único grupo con 5 elementos.

Terminamos esta sección introduciendo la buena notación para los elementos del grupo simétrico S_n e introduciendo el grupo Dihedral D_n como subgrupo de S_n.

El grupo simétrico: Consideremos $S_n = \{\text{biyecciones de } \{1, 2, \ldots, n\} \text{ en si mismo}\}$, bajo composición. [3]

Un **ciclo** en S_n es un arreglo de la forma $(\alpha_1, \ldots, \alpha_m)$ donde los $\alpha_i \in \{1, \ldots, n\}$ y no hay dos α_i repetidos. Por ejemplo $(3, 2, 4)$ es un ciclo en S_n para todo $n \geq 4$, pero $(2, 1, 2)$ no lo es.

Un ciclo $\sigma = (\alpha_1, \ldots, \alpha_m)$ en S_n representa una biyección de $\{1, \ldots, n\}$ si definimos $\sigma(\alpha_i) = \alpha_{i+1}$ para $i < m$, $\sigma(\alpha_m) = \alpha_1$, y $\sigma(i) = i$ para $i \in \{1, \ldots, n\} \setminus \{\alpha_1, \ldots, \alpha_m\}$. Por ejemplo, en S_4 el ciclo $(1, 4, 3)$ representa la biyección $1 \to 4 \to 3 \to 1$ y que fija el 2. Decimos que $\sigma = (\alpha_1, \ldots, \alpha_m)$ es la permutación cíclica de los α_i's.

Ejercicio 1.16. Verifique que con esta definición, un ciclo σ en S_n efectivamente es una biyección de $\{1, \ldots, n\}$. Verifique además que la biyección determinada por $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ es la misma que la determinada por $(\alpha_2, \ldots, \alpha_m, \alpha_1)$.

Diremos que los ciclos $(\alpha_1, \ldots, \alpha_m)$ y $(\alpha'_1, \ldots, \alpha'_\ell)$ **son disjuntos**, si $\alpha_i \neq \alpha'_j$ para todo i, j.

Dados dos ciclos $\sigma, \sigma' \in S_n$, su composición $\sigma \circ \sigma'$ es otro elemento de S_n (pues S_n es un grupo bajo composición), pero $\sigma \circ \sigma'$ no es necesariamente otro ciclo. Por ejemplo la composicón $(2, 3, 4) \circ (1, 5)$ no puede escribirse como un solo ciclo. Vamos a ver que todo elemento $\sigma \in S_n$ puede escribirse como una composición de una cantidad finita de ciclos, todos ellos disjuntos entre si.

Sea $\sigma \in S_n$ y $k \in \{1, \ldots, n\}$. La **órbita de k bajo** σ es el conjunto $Orb_\sigma(k) = \{k, \sigma(k), \sigma^2(k), \sigma^3(k), \ldots\}$. Note que $Orb_\sigma(k)$ es un conjunto finito de cardinalidad mayor o igual a 1. Si $Orb_\sigma(k) = \{1, \ldots, n\}$, entonces se tiene que σ puede ser representado por el ciclo $(k, \sigma(k), \ldots, \sigma^n(k))$. Por otro lado si $Orb_\sigma(k)$ es un subconjunto propio de $\{1, \ldots, n\}$, entonces $\sigma = (k, \sigma(g), \ldots, \sigma^n(k)) \circ \tilde{\sigma}$ donde $\tilde{\sigma}$ es una biyeccion del conjunto $\{1, \ldots, n\} \setminus Orb_\sigma(k)$. Puesto que la cardinalidad de $\{1, \ldots, n\} \setminus Orb_\sigma(k)$ es estrictamente menor que n, podemos aplicar inducción a $\tilde{\sigma}$ y suponer que $\tilde{\sigma}$ se escribe como composición de ciclos disjuntos $\tau_1 \circ \ldots \circ \tau_\ell$, y por lo tanto σ tambien se escribe como composición de ciclos.

Ejercicio 1.17. Demuestre que si σ y σ' son ciclos disjuntos entonces ellos **conmutan**, es decir $\sigma \circ \sigma' = \sigma' \circ \sigma$. Muestre también que si $\sigma = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ y $\beta = (\alpha_m, \ldots, \alpha_2, \alpha_1)$, entonces β es el inverso de σ en S_n (es decir $\beta \circ \sigma$ es la identidad de S_n).

Ejercicio 1.18. Sea $f \in S_n$. Demuestre que existen ciclos $\sigma_1, \ldots, \sigma_k$ $(k \leq n)$ disjuntos dos a dos tal que $f = \sigma_1 \circ \ldots \circ \sigma_k$.

El grupo Dihedral: El grupo Dihedral D_n es el grupo de simetrias del polígono regular P_n.

Por ejemplo D_3 es el subgrupo de simetrias del triangulo equilatero P_3. Además de la identidad, P_3 tiene dos tipos de simetrias: rotaciones y reflexiones, ver Figura 1.

Ejercicio 1.19. Verifique que el conjunto $\{id, R_{2\pi/3}, R_{4\pi/3}, \tau_2, \tau_2, \tau_3\}$ de la Figura 1 es cerrado bajo composición.

[3] Recomiendo ver el video en Youtube, www.youtube.com/watch?v=QTADYOCkKWg&t=35s.

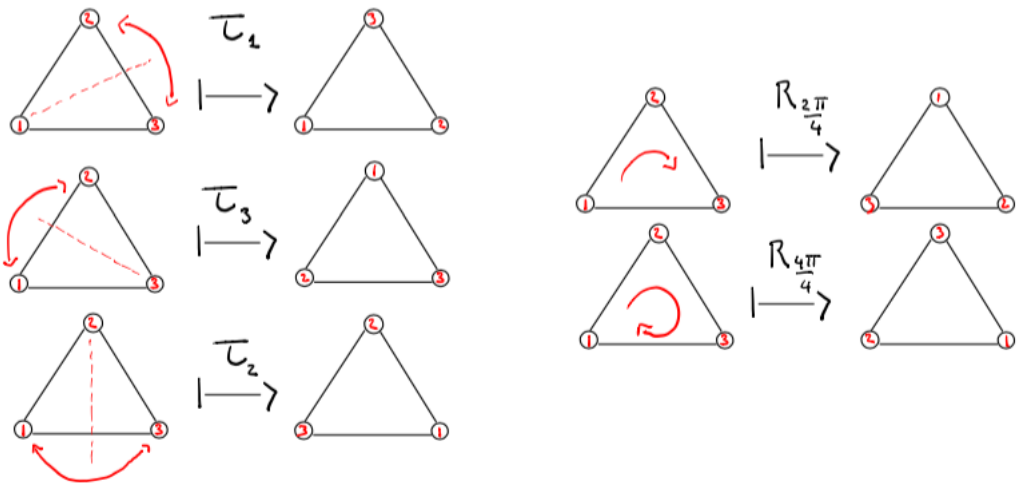


Figura 1: Rotaciones y reflexiones del triangulo.

Observación 1.20. Note que si etiquetamos los vértices de P_3, entonces toda simetría de P_3 induce una biyección de $\{1,2,3\}$. Reciprocamente toda biyección de $\{1,2,3\}$ induce una simetría de P_3. Por ejemplo $S_3 \ni (1,2,3) \leftrightarrow R_{2\pi/3} \in D_3$ o también $S_3 \ni (1,3) \leftrightarrow \tau_2 \in D_3$.

En particular se tiene que $D_3 \simeq S_3$.

Un ejemplo más interesante de grupo dihedral es D_4, el conjunto de simetrias del cuadrado P_4. En este caso, además de las rotaciones en $2\pi/4$, $4\pi/4$, $6\pi/4$ y $8\pi/4 = Id$, tenemos las reflexiones que se muestran en la Figura 2.

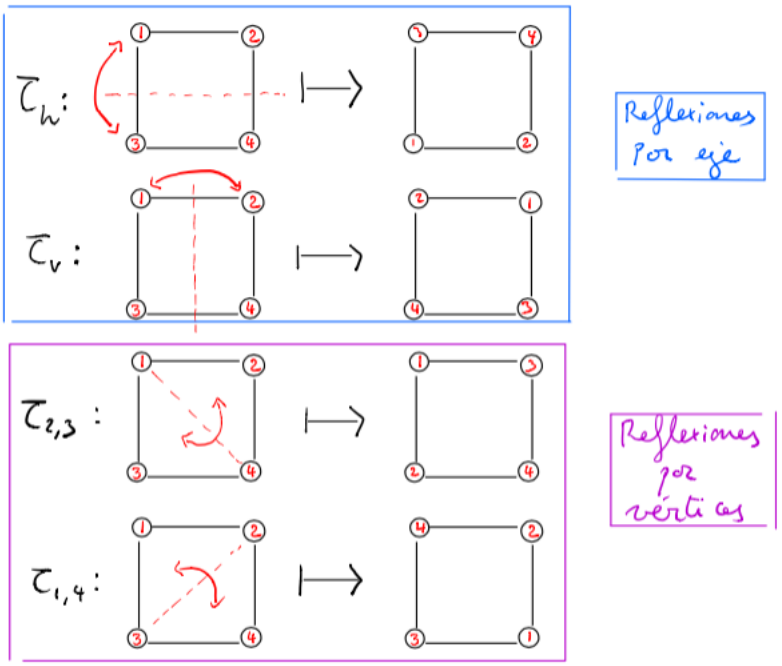


Figura 2: Reflexiones por eje y por vértice en el cuadrado.

El grupo D_4 es mas interesante que D_3 pues en este caso no es cierto que todo elemento de S_4 induzca una simetría de P_4. Por ejemplo el ciclo $(3,4) \in S_4$ no preserva la estructura del cuadrado, ver Figura 3.

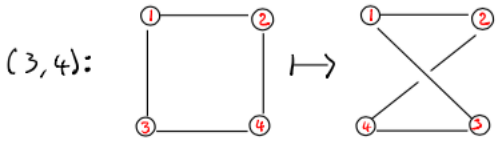


Figura 3: Un permutación de $\{1,2,3,4\}$ que no induce una simetría del cuadrado.

Ejercicio 1.21. Muestre que si $n \geq 4$, entonces D_n es un subgrupo propio de S_n. Mas aún:

1. Calcule la cardinalidad de S_n.
2. Calcule la cardinalidad de D_n.

1.2. Homomorfismos e isomorfismos

Entre otras cosas, en esta sección formalizaremos que queremos decir con *salvo cambio de nombre* en el Teorema 1.14. Primero introducimos la noción de homomorfismo, que es la clase de funciones que respeta la estructura de los grupos.

Definición 1.22. Sean G y H dos grupos cualesquiera. Una función $\psi : G \to H$ se dice **homomorfismo** si para todo $f, g \in G$ se tiene que

$$\psi(g \cdot f) = \psi(g) \cdot \psi(f).$$

Note que en la igualdad anterior, la operación a la izquierda de la igualdad es la operación de G mientras que la operación a la derecha de la igualdad es la operación en H. Por ello decimos que un homomorfismo $G \to H$ manda la estructura de G en la estructura de H.

La imagen de un homomorfismo $\psi : G \to H$ es $Im(\psi) = \{\psi(g) \mid g \in G\}$, y **el núcleo** de ψ (a veces también llamado **kernel**) es $Ker(\psi) = \{g \in G \mid \psi(g) = id_H\}$, donde id_H denota la identidad de H.

Note que $Im(\psi)$ es un subconjunto de H mientras que $Ker(\psi)$ es un subconjunto de G. De hecho tenemos

Proposición 1.23. *Sea $\psi : G \to H$ un homomorfismo. Entonces $Im(\psi)$ es un subgrupo de H y $Ker(\psi)$ es un subgrupo de G.*

Para probar esta proposición precisamos de un pequeño lema.

Lema 1.24. *Si $\psi : G \to H$ es un homomorfismo, entonces $\psi(id_G) = id_H$. Mas aún si $g \in G$ entonces $\psi(g^{-1}) = \psi(g)^{-1}$.*

Demostración: Sea $g \in G$. Puesto que ψ es un homomorfismo se tiene que $\psi(g) = \psi(g \cdot id_G) = \psi(g) \cdot \psi(id_G)$. Multiplicando a izquierda por $\psi(g)^{-1}$ encontramos que $id_H = \psi(id_G)$, lo que prueba la primera parte del lema.

Para ver la segunda parte notamos que $\psi(g) \cdot \psi(g^{-1}) = \psi(id_G) = id_H$. Esto dice que $\psi(g^{-1})$ es un inverso de $\psi(g)$. Luego, como los inversos son únicos (ver Ejercicio 1.3), concluimos que $\psi(g)^{-1} = \psi(g^{-1})$. □

Demostración de la Proposición 1.23: Probamos primero que $Im(\psi) \leq H$. Para ello hay que probar que si u y v están en $Im(\psi)$, entonces tanto uv como u^{-1} pertenecen a $Im(\psi)$. Como $u, v \in Im(\psi)$ existen $g, f \in G$ tal que $\psi(g) = u$ y $\psi(f) = v$. De este modo $uv = \psi(g)\psi(f)$ y como ψ es un homomorfismo concluimos que $uv = \psi(gf) \in Im(\psi)$. Finalmente gracias al Lema 1.24 sabemos que $u^{-1} = \psi(g^{-1}) \in Im(\psi)$.

Ahora probamos que $Ker(\psi)$ es un subgrupo de G. Si $f, g \in Ker(\psi)$ entonces $\psi(fg) = \psi(f)\psi(g) = id_H \cdot id_H = id_H$. Luego $fg \in Ker(\psi)$. Por otro lado por el Lema 1.24 tenemos $\psi(g^{-1}) = \psi(g)^{-1} = id_H^{-1} = id_H$. Luego $g^{-1} \in Ker(\psi)$, lo que dice que $Ker(\psi)$ es un subgrupo de G. □

Ejemplo 1.25. Los siguientes son ejemplos de homomorfismos.

- Sea $\lambda \in \mathbb{R}$ y $M_\lambda : \mathbb{R} \to \mathbb{R}$ la multiplicación por λ, es decir $M_\lambda(x) = \lambda x$. Entonces M_λ es un homomorfismo de $(\mathbb{R}, +)$ en si mismo pues

$$M_\lambda(a + b) = M_\lambda(a) + M_\lambda(b).$$

- Mas generalmente, un espacio vectorial es un grupo bajo la suma de vectores, y una función lineal $L : V \to W$ entre espacios vectoriales es un homomorfismo.

- Recuerde que $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ es un grupo bajo la multiplicación. Para $n \geq 1$, la función $\psi_n : S^1 \to S^1$ dada por $\psi(z) = z^n$, es un homomorphismo del círculo pues

$$\psi_n(a \cdot b) = (a \cdot b)^n = a^n \cdot b^n = \psi_n(a) \cdot \psi_n(b).$$

  La imagen de ψ_n es todo S^1 y su kernel es $\mathbb{Z}_n = \{z \in S^1 \mid z^n = 1\}$.

La siguiente propiedad de los homomorfismos es muy útil.

Ejercicio 1.26. Sea $\varphi : G \to H$ un homomorfismo de grupos. Pruebe que φ es inyectivo si y solo si $\ker(\varphi) = \{id_G\}$.

Definición 1.27. Un homomorfismo $\psi : G \to H$ biyectivo se dice **isomorfismo**. Un isomorfismo $\psi : G \to G$ se dice **automorfismo**. Dos grupos G y H se dicen **isomorfos** si existe un isomorfismo $G \to H$, y en tal caso anotamos $G \simeq H$.

La noción de isomorfía es lo que aludíamos en el Teorema 1.14 al decir *módulo cambio de nombre*. De hecho, con este lenguaje podemos re enunciar el Teorema 1.14 simplemente diciendo que, modulo isomorfismo, existe un único grupo con tres elementos.

Normalmente, en teoría de grupos se intenta comprender la clase de grupos módulo isomorfismo, es decir a grupos isomorfos se les trata como el mismo objeto. El siguiente ejemplo sin embargo muestra que pueden haber grupos que no se parecen demasiado *a priori* pero que resultan ser isomorfos.

Ejemplo 1.28. Los reales positivos $\mathbb{R}_+ = \{r \in \mathbb{R} \mid r > 0\}$ son un grupo bajo la multiplicación. Este grupo es isomorfo a los reales equipados con la suma. En efecto $log : \mathbb{R}_+ \to \mathbb{R}$ ciertamente es una función biyectiva que además es un homomorfismo pues

$$log(a \cdot b) = log(a) + log(b).$$

Ejercicio 1.29. Sea C el conjunto de matrices de la forma

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix},$$

con $x, y \in \mathbb{R}$.

1. Pruebe que C es un grupo bajo la suma de matrices y que $(C, +) \simeq (\mathbb{C}, +)$.
2. Pruebe que el conjunto de matrices en C con determinante $\neq 0$ es un grupo bajo la multiplicación de matrices y que dicho grupo es isomorfo a $(\mathbb{C}^*, \cdot)$.

Ejercicio 1.30. Puede ser

1. $(\mathbb{Q}, +)$ isomorfo a $(\mathbb{R}, +)$?
2. $(\mathbb{Q}, +)$ isomorfo a $(\mathbb{Z}, +)$?

Automorfismos por conjugación: Los grupos, en general, aceptan dos tipos de automorfismos: los automorfismos internos o automorfismos por conjugación y los automorfismos externos. La diferencia entre estos tipos de automorfismos es que los primeros estan implementados por elementos del mismo grupo mientras que los segundos no.

Definición 1.31. Sea G un grupo y $g \in G$. Definimos la **conjugación por** g como la función $C_g : G \to G$ definida por $C_g(f) = gfg^{-1}$.

Proposición 1.32. *$C_g : G \to G$ es un automorfismo.*

Demostración: Hay que probar que C_g es un homomorfismo que ademas es biyectivo.

Para ver que C_g es inyectivo notamos que si $C_g(f) = C_g(h)$ entonces $gfg^{-1} = ghg^{-1}$. Luego, necesariamente $f = h$. Para ver que C_g es sobreyectivo basta notar que $C_g(g^{-1}fg) = f$. Luego C_g es una función biyectiva.

La demostración de que C_g es un homomorfismo queda como ejercicio. □

El automorfismo identidad $Id : x \mapsto x$ siempre es un automorfismo interno pues $Id = C_{id}$. Este automorfismo a veces se le llama automorfismo *trivial* pues él no hace nada. Por otro lado, en muchas ocasiones los automorfismos de la forma C_g resultan ser triviales. Este es el caso, de los grupos Abelianos (es decir grupos que cumplen $a \cdot b = b \cdot a \ \forall a, b$), pues en dicho caso $C_g(f) = gfg^{-1} = fgg^{-1} = f$ para todo f.

El siguiente es un ejemplo donde las conjugaciones son no-triviales.

Ejemplo 1.33. Sea $GL_2(\mathbb{R})$ el conjunto de matrices 2x2 con entradas en $\mathbb{R}$ y determinante $\neq 0$. $GL_2(\mathbb{R})$ es un grupo bajo la multiplicación matricial. En los cursos de algebra lineal se nos enseña que si el polinomio caracteriztico de $M \in GL_2(\mathbb{R})$ tiene dos raices distintas, entonces existe $P \in GL_2(\mathbb{R})$ tal que PMP^{-1} es una matriz diagonal. Por ejemplo

$$PMP^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -3/2 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix}.$$

En particular, la conjucación por P es un automorfismo no trivial.

Ejemplo 1.34. Un ejemplo de un grupo donde todo automorfismo interno es trivial, es $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ con la suma de vectores (pues este grupo es Abeliano). Sin embargo, este grupo admite muchos automorfismos. En efecto, toda matriz 2x2 con coeficientes en $\mathbb{R}$ puede ser visto como una transformación lineal de $\mathbb{R}^2$ y por lo tanto $M : \mathbb{R}^2 \to \mathbb{R}^2$ es un homomorfismo. Mas aún, si ademas el determinante de M es distinto de 0 entonces M es es biyectiva y por lo tanto M es un automorfismo (externo) de $(\mathbb{R}^2, +)$.

El grupo de automorfismos de un grupo. Asi como el grupo dihedral aparece como el grupo de simetrias de un objeto geométrico, suele suceder que grupos interesantes aparecen como grupos de *simetrias* de otros grupos.

Si G es un grupo, denotamos por $Aut(G)$ la colección de automorfismos de G.

Proposición 1.35. *$Aut(G)$ es un grupo bajo la composición de funciones.*

Demostración: En efecto, si $\alpha, \beta \in Aut(G)$, entonces $\alpha \circ \beta(f \cdot g) = \alpha(\beta(f) \cdot \beta(g)) = \alpha(\beta(f)) \cdot \alpha(\beta(g))$ para todo $f, g \in G$. Luego $\alpha \circ \beta$ es un homomorfismo. Como además la biyectividad es una propiedad que se preserva por composición, se tiene que $\alpha \circ \beta \in Aut(G)$.

Por otro lado α^{-1}, la función inversa de α, es también una biyección que además es homomorfismo. En efecto se tiene que $\alpha(\alpha^{-1}(f \cdot g)) = f \cdot g$ y por otro lado -usando que α es homomorfismo- encontramos que

$$\alpha(\alpha^{-1}(f) \cdot \alpha^{-1}(g)) = \alpha(\alpha^{-1}(f)) \cdot \alpha(\alpha^{-1}(g)) = f \cdot g.$$

Puesto que α es inyectiva podemos deducir que $\alpha^{-1}(f \cdot g) = \alpha^{-1}(f) \cdot \alpha^{-1}(g)$. □

Ejercicio 1.36. Pruebe que la aplicación $C : G \to Aut(G)$ definida por $C(g) = C_g$ es un homomorfismo.

Ejercicio 1.37. Sea α un automorfismo de $(\mathbb{Z}, +)$.

1. Muestre que $\alpha(1)$ es igual a 1 o a -1.
2. Muestre que si $\alpha(1) = 1$ entonces $\alpha(n) = n$ para todo $n \in \mathbb{Z}$ (es decir α es el automorfismo identidad).
3. Concluya que $Aut(\mathbb{Z})$ es un grupo con dos elementos.
4. Exhiba un isomorfismo entre $Aut(\mathbb{Z})$ y $\mathbb{Z}_2$ (recuerde que $\mathbb{Z}_2 = \{1, -1\}$ bajo multiplicación).

Ejercicio 1.38. Pruebe que $Aut((\mathbb{Z}^2, +))$ es isomorfo a $(GL_2(\mathbb{Z}), \cdot)$, el grupo de matrices 2×2 con entradas en $\mathbb{Z}$ y determinante ± 1, bajo multiplicación de matrices.

1.3. Clases laterales, subgrupos normales y grupos cocientes

Uno de los conceptos mas importantes (y también mas dificiles de asimilar) en matemática es el de estructura cociente de una estructura dada. En esta sección veremos la noción de subgrupo *normal* y del grupo cociente inducido.

Para empezar, veremos que un subgrupo cualquiera de un grupo G induce en G una partición en *clases laterales*.

Definición 1.39. Sea G un grupo cualquiera, H un subgrupo de G y $g \in G$. Decimos que

$$gH = \{gh \mid h \in H\},$$

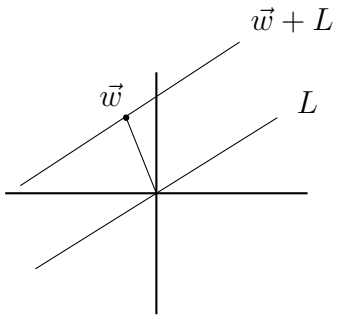
es la **clase lateral izquierda** de H por g.

Analogamente $Hg = \{hg \mid \in H\}$ es la **clase lateral derecha** de H por g. Note que si G es Abeliano, entonces $gH = Hg$.

Ejemplo 1.40. Consideremos $G = \mathbb{R}^2$ equipado con la suma de vectores y $L = \mathbb{R} \cdot \vec{v}$ un subespacio de dimensión 1. En particular L es un subgrupo de $\mathbb{R}^2$. Si $\vec{w} \in \mathbb{R}^2$, entonces la clase lateral de L por $\vec{w}$ es

$$\vec{w} + L = \{\vec{w} + \lambda \cdot \vec{v} \mid \lambda \in \mathbb{R}\},$$

la (única) recta paralela a L que pasa por $\vec{w}$.



Proposición 1.41. *Las clases laterales a izquierda (o a derecha) de un subgrupo H en G forman una* **partición** *de G. Mas aún, todas las partes de esta partición tienen la misma cardinalidad.*

Demostración: Para ver que una colección de subconjuntos de G –en este caso los subconjuntos de la forma gH con $g \in G$– forman una partición, hay que ver que

1. Su unión es todo G, es decir $G = \bigcup_{g \in G} gH$.
2. Las partes distintas son disjuntas, es decir $gH \cap fH \neq \emptyset$ implica $gH = fH$.

El punto 1. es claro pues para todo $g \in G$ vale que $g \in gH$. Para chequear el punto 2., notamos que si $x \in gH \cap fH$ entonces $x = gh_1 = fh_2$, donde h_1 y h_2 son elementos de H. De este modo se tiene que $g = fh_2h_1^{-1}$, y por lo tanto

$$gH = fh_2h_1^{-1}H = fH,$$

donde la última igualdad vale pues H es un subgrupo de G. Esto prueba que las clases laterales a izquierda forman una partición de G (el caso de particiones a derecha es análogo y queda para el lector).

Para terminar, hay que ver que dadas dos clases laterales gH y fH, siempre podemos encontrar una biyección entre ellas. Esto se logra pues la multiplicación a izquierda induce siempre una biyección de G. Concretamente consideramos

$$L_{fg^{-1}} : gH \to fH, \text{ dada por } L_{fg^{-1}} : x \mapsto fg^{-1}x.$$

Argumentando como en la Proposición 1.13, fácil ver que $L_{fg^{-1}} : gH \to fH$ es una biyección. □

Ejercicio 1.42. Muestre que si H es un subgrupo de G y f, g son dos elementos de G, entonces vale que $gH = fH \Leftrightarrow g^{-1}f \in H$. Note que esto en particular implica que $hH = H$ $\forall h \in H$.

Al conjunto de clases laterales izquierda (respectivamente derecha) de H en G lo denotaremos por G/H (respectivamente $H\backslash G$). Si $R = \{g_1, g_2, \dots, \}$ es un subconjunto de G que contiene exactamente un elemento por cada clase lateral izquierda de H, entonces decimos que R es **un conjunto de representantes** para G/H. Note que en este caso se tiene que $G = \bigcup_{g \in R} gH$.

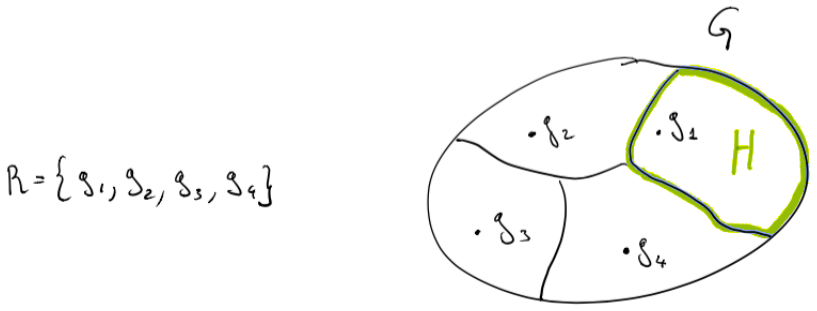


Figura 4: clases laterales de H en G y un conjunto R de representantes de clases.

La cardinalidad del conjunto G/H se le llama **indice** de H en G y lo denotaremos por $[G : H]$. Puesto que las clases laterales tienen todas la misma cardinalidad, podemos pensar al índice como *la cantidad de veces que cabe H en G*. En particular, si G es un grupo finito y $|G|$ denota su cardinalidad, entonces $|H|$ divide a $|G|$. En fórmula tenemos que

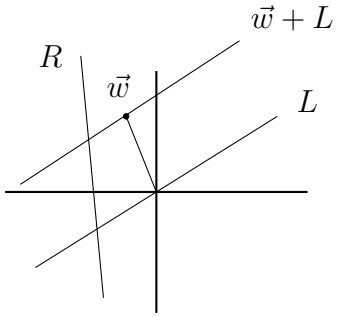
$$|G| = |H| \cdot [G : H]. \tag{1}$$

Hemos demostrado el

Teorema 1.43 (Lagrange[4])**.** *En un grupo finito, la cardinalidad de un subgrupo divide a la cardinalidad del grupo.*

[4]Es interesante notar que este teorema fue probado antes de la introducción del concepto de grupo, y, en su versión original, versaba asi: si a un polinomio dado de n variables se le permutan sus variables en todas las $n!$ formas posibles, entonces la cantidad de polinomios encontrados divide a $n!$.

Ejemplo 1.44. Con las notaciones del Ejemplo 1.40, se tiene que $\mathbb{R}^2/L$ es el conjunto de rectas paralelas a L. En este caso el índice de L en $\mathbb{R}^2$ es infinito, y un conjunto de representantes de clase laterales es, por ejemplo, una recta R transversal a todas las rectas paralelas a L.



Ejemplo 1.45 (Clases laterales en $\mathbb{Z}$)**.** Si $n_0 \in \mathbb{N}$, entonces el conjunto

$$n_0\mathbb{Z} = \{n_0 \cdot k \mid k \in \mathbb{Z}\},$$

es un subgrupo de $(\mathbb{Z}, +)$. Las clases laterales de $n_0\mathbb{Z}$ son de la forma $a + n_0\mathbb{Z}$, con $a \in \mathbb{Z}$, y sabemos (ver Ejercicio 1.42) que

$$a + n_0\mathbb{Z} = b + n_0\mathbb{Z} \text{ si y solo si } a - b \in n_0\mathbb{Z}.$$

Para calcular el índice de $n_0\mathbb{Z}$ en $\mathbb{Z}$, y de paso encontrar un conjunto de representantes, recordamos que por el algoritmo de la division podemos dividir a en n_0 para encontrar $d_a \in \mathbb{Z}$ y $r_a \in \{0, 1, \ldots, n_0 - 1\}$ tal que $a = n_0 d_a + r_a$. Puesto que $n_0 d_a \in n_0\mathbb{Z}$, esto nos dice que $a + n_0\mathbb{Z} = r_a + n_0\mathbb{Z}$, y por lo tanto encontramos que

$$a + n_0\mathbb{Z} = b + n_0\mathbb{Z} \text{ si y solo si } r_a - r_b \in n_0\mathbb{Z}.$$

Concluimos entonces que $\{0, 1, 2, \ldots, n_0 - 1\}$ es un conjunto de representantes de clases laterales de $n_0\mathbb{Z}$ en $\mathbb{Z}$, y por lo tanto $[\mathbb{Z} : n_0\mathbb{Z}] = n_0$.

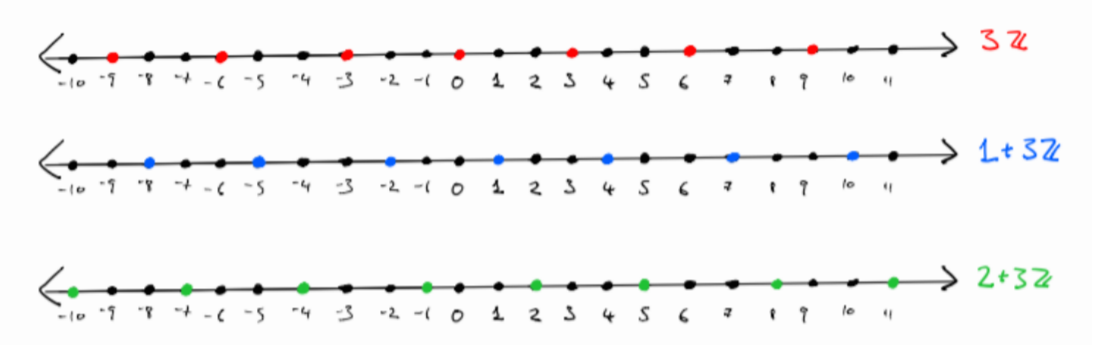


Figura 5: las 3 clases laterales de $3\mathbb{Z}$ en $\mathbb{Z}$.

Definición 1.46. Sea $g \in G$. Llamaremos **órden** de g, denotado $ord(g)$, al menor $n \in \mathbb{N} = \{1, 2, \ldots\}$ tal que $g^n = id$. Si tal entero no existe diremos que g tiene orden infinito. Note que la identidad de G es el único elemento de órden 1.

Ejercicio 1.47. Muestre que si G es un grupo finito cuya cardinalidad es un primo, entonces para todo $g \in G \setminus \{id\}$ vale que $G = \{g^n \mid n \in \mathbb{N}\}$.

Ejercicio 1.48. Sea G un grupo finito y $K \leq H \leq G$. Demuestre que $[G : K] = [G : H][H : K]$. (Ayuda: considere la partición dada por K como una subpartición de la partición dada por H.)

Subgrupos normales. Resulta natural preguntarse cuándo el conjunto de clases laterales de un subgrupo H en un grupo G *hereda la estructura del grupo*. Veremos que esto sucede precisamente cuando el subgrupo H es un subgrupo normal.

Definición 1.49. Diremos que un subgrupo H de G es **normal** si para todo $g \in G$ se tiene

$$gH = Hg.$$

En esta situación anotaremos $H \trianglelefteq G$.

Observación 1.50. Notar que en un grupo Abeliano, todos los subgrupo son normales.

Proposición 1.51. *Sea H un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

1. *H es normal en G.*
2. *H es invariante bajo conjugación. Es decir, para todo $h \in H$ y todo $g \in G$, se tiene que $ghg^{-1} \in H$.*

Mas aún, cuando H es un subgrupo normal de G, la opreación $(fH, gH) \mapsto fgH$ convierte a G/H en un grupo. Lo llamaremos el **grupo cociente**.

Demostración: Probamos primero que $1 \Rightarrow 2$. Para ello suponemos que H es un subgrupo normal de G, y elegimos $h \in H$ y $g \in G$. Como H es normal, se sigue que $gH = Hg$, y por lo tanto existe $h' \in H$ tal que $gh = h'g$. Concluimos entonces que $ghg^{-1} = h' \in H$ como buscabamos.

Ahora probamos que $2 \Rightarrow 1$. Para ello tomamos $g \in G$ y suponemos que H es un subgrupo de G que cumple la condición 2. En particular se tiene que

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

Multiplicando a derecha los extremos de esta igualdad por g, encontramos que $gH = Hg$.

Finalmente, probamos que si H es normal en G, entonces la operación

$$op : (fH, gH) \mapsto fgH$$

define una estructura de grupo en G/H. Para esto, lo primero y mas importante es verificar que la operación *está bien definida*, es decir que ella depende únicamente de las clases laterales fH y gH y no de su representantes f y g. Concretamente hay que verificar que si $g'H = gH$ y $f'H = fH$, entonces $fgH = f'g'H$.

Usando el Ejercicio 1.42 tenemos que $g^{-1}g'$ y $f^{-1}f'$ pertenecen a H y, como además H es normal, también se tiene que $f(f^{-1}f')f^{-1} = f'f^{-1} \in H$. En particular, el producto $g^{-1}g'\, f'f^{-1} \in H$. Nuevamente usando la normalidad de H encontramos que

$$g(g^{-1}g'\, f'f^{-1})g^{-1} = g'f'f^{-1}g^{-1} = (g'f')\,(gf)^{-1} \in H,$$

que por el concluimos que $g'f'H = gfH$ como queríamos.

Una vez chequeado que la operación está bien definida, es fácil ver ella es asociativa, que $H = idH$ es el neutro en G/H y que el inverso de gH es $g^{-1}H$. Esto muestra que G/H equipado con *op* es un grupo. □

Ejercicio 1.52. Pruebe que si $\varphi : G \to K$ es un homomorfismo, entonces su núcleo $Ker(\varphi) = \{g \in G \mid \varphi(g) = id\}$ es un subgrupo normal de G.

Ejercicio 1.53. Pruebe que $Biy_0(\mathbb{N})$, el conjunto de biyecciones $\mathbb{N} \to \mathbb{N}$ de soporte finito, es un subgrupo normal de $Biy(\mathbb{N})$.

Ejercicio 1.54. Sea $H \leq G$ y $N \lhd G$. Verifique que $HN = \{hn \mid h \in H, n \in N\}$ es un subgrupo de G. Vale lo mismo si solo se asume que $N \leq G$?.

Ejercicio 1.55. Pruebe que $Inn(G)$, el conjunto de automorfismos internos de un grupo G es un subgrupo normal de $Aut(G)$.

Enteros módulo n: Una de las instancias mas importantes de estructuras cocientes es $\mathbb{Z}/n\mathbb{Z}$, el conjunto de los enteros módulo n. En lo que sigue de estas notas, escribiremos simplemente $[a]_n$ para denotar la clase lateral $a + n\mathbb{Z}$. Si el contexto es claro, olvidaremos el subíndice n y escribiremos simplemente $[a] = a + n\mathbb{Z}$.

Fijemos $n \in \mathbb{N}$. Como $\mathbb{Z}$ es Abeliano, el subgrupo $[0] = n\mathbb{Z}$ es un subgrupo normal y la Proposición 1.51 nos dice que la aplicación

$$[n] + [m] = [n + m]$$

define una estructura de grupo en $\mathbb{Z}/n\mathbb{Z}$. El neutro es $[0]$ y el inverso de $[a]$ es $[-a]$. Mas aún, en el Ejemplo 1.45 vimos que toda clase $[a]$ admite un representante $r_a \in \{0, 1, \ldots, n-1\}$ y por lo tanto $\mathbb{Z}/n\mathbb{Z}$ es un grupo de cardinalidad n.

Ejercicio 1.56. Pruebe que $\mathbb{Z}/n\mathbb{Z}$ es isomorfo al grupo $\mathbb{Z}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ del Ejemplo 3.4.

Ejercicio 1.57. Muestre que en $\mathbb{Z}/15\mathbb{Z}$, el conjunto $5\mathbb{Z}/15\mathbb{Z} = \{[0]_{15}, [5]_{15}, [10]_{15}\}$ es un subgrupo.

Concluimos esta sección haciendo notar que todo subgrupo normal es necesariamente el núcleo de algún homomorfismo.

Observación 1.58. Dado K un subgrupo normal de G, podemos considerar la aplicación proyección: $\pi : G \to G/K$ definida por $\pi(g) = gK$. Es fácil ver que π es un homomorfismo y que $Ker(\pi)$ es precisamente el subgrupo K. En particular, hemos probado que todo subgrupo normal es el núcleo de algún homomorfismo.

Ejercicio 1.59. Dados $f, g \in G$, denotamos por $[f, g] = fgf^{-1}g^{-1}$ al *conmutador* de f y g. Denotamos por $[G, G]$ al subgrupo *generado* por los conmutadores $[f, g]$ con f y g en G. Demuestre que $[G, G]$ es un subgrupo normal y que $G/[G, G]$ es Abeliano.

1.4. Teoremas de isomorfismo

Suponga que $\varphi : G \to H$ es un homomorfismo de grupos. Sabemos que $Im(\varphi) = \{\varphi(g) \mid g \in G\}$ es un subgrupo de H y que $Ker(\varphi) = \{g \in G \mid \varphi(g) = id\}$ es un subgrupo normal de G (ver Proposicón 1.23 y Ejercicio 1.52). El siguiente teorema se conoce como el Primer Teorema del Isomorfismo y normalmente se utiliza para encontrar isomorfismos entre dos grupos dados.

Teorema 1.60. *Sea $\varphi : G \to H$ un homomorfismo. Entonces, $Im(\varphi) \simeq G/Ker(\varphi)$.*

Demostración: Sea $K = Ker(\varphi)$. Queremos ver que $G/K \simeq Im(\varphi)$. Para ello definimos $\overline{\varphi} : G/K \to H$ por $\overline{\varphi}(gK) = \varphi(g)$.

Lo primero que hay que verificar es que $\overline{\varphi}$ está bien definido, es decir que si $gK = fK$ entonces $\overline{\varphi}(gK) = \overline{\varphi}(fK)$. Para ello suponemos que $gK = fK$. Del Ejercicio 1.42 sabemos que esto equivale a que $f^{-1}g \in K$ y por lo tanto $g = fk$ para algún $k \in K$. Luego, aplicamos la definición, tenemos que

$$\overline{\varphi}(gK) = \varphi(g) = \varphi(fk) = \varphi(f)\varphi(k) = \varphi(f) = \overline{\varphi}(fK).$$

Luego verificamos que

- $\overline{\varphi}$ es un homomorfismo:

$$\overline{\varphi}(gK \cdot fK) = \overline{\varphi}(gfK) = \varphi(gf) = \varphi(g) \cdot \varphi(f) = \overline{\varphi}(gK) \cdot \overline{\varphi}(fK).$$

- El homomorfismo $\overline{\varphi}$ es inyectivo. Para ello, gracias al Ejercicio 1.26, basta chequeare $Ker(\overline{\varphi})$ solo contiene a la identidad de G/K.

  Veamos que este es el caso: supongamos que $\overline{\varphi}(gK) = id_H$. Por definición de $\overline{\varphi}$, esto dice que $\varphi(g) = id_H$, lo que implica que $g \in K = Ker(\varphi)$. Encontramos enotnces que $gK = K$ que es la clase lateral identidad en G/K. Luego $\overline{\varphi}$ es inyectivo.

- El homomorfismo $\overline{\varphi}$ es sobreyectivo sobre $Im(\varphi)$. Esto es claro pues $Im(\overline{\varphi}) = Im(\varphi)$.

Concluimos entonces que $\overline{\varphi} : G/K \to Im(\varphi)$ es un isomorfismo. □

Corolario 1.61. *Si $\varphi : G \to H$ es un homomorfismo sobreyectivo, entonces $G/Ker(\varphi)$ es isomorfo a H.*

Ejercicio 1.62. Pruebe que $\mathbb{Z}/n\mathbb{Z}$ es isomorfo al grupo $\mathbb{Z}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ del Ejemplo 3.4.

Los siguientes dos resultados se conocen comunmente como como el Segundo y el Tercer Teorema del Isomorfismo. Daremos la demostración de éstos en forma de pequeños ejercicios. Para empezar, recordamos que dado un subgrupo normal $N \lhd G$ y otro subgrupo $H \leq G$, podemos formar el grupo $HN := \{hn \mid h \in H,\ n \in N\}$.

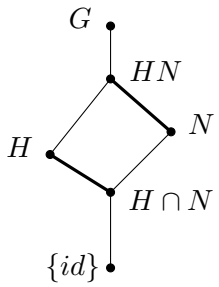
Ejercicio 1.63. Sea $N \lhd G$, $H \leq G$ y $HN := \{hn \mid h \in H,\ n \in N\}$.

1. Verifique que HN es un subgrupo de G y que $H \cap N$ es un subgrupo normal de H.

2. Muestre que si $N \cap H = \{id\}$ y la acción por conjugación de H en N es trivial, entonces $HN \simeq H \times N$.

3. Muestre que si $N \cap H = \{id\}$ y tanto N como H son subgrupos normales de G, entonces $HN \simeq H \times N$.

Ciertamente, HN es un subgrupo que contiene a H y a N pues, por ejemplo, todo elemento h de H puede escribirse como $h \cdot id \in HN$. Mas aún, N es un subgrupo normal de HN (¡pues lo es en G!) y por el ejercicio precedente $H \cap N$ es normal en H. El siguiente diagrama intenta visualizar esta situación:



Teorema 1.64. *Si $N \lhd G$ y $H \leq G$, entonces $H/(H \cap N) \simeq (HN)/N$.*

Demostración: Definimos $\varphi : H \to HN/N$ por $\varphi(h) = hN$ y verificamos que:

1. φ es un homomorfismo.

2. φ es sobreyectivo.

3. El núcleo de φ es $H \cap N$.

En particular, por el Corolario 1.61 concluimos que $H/(H \cap N) \simeq HN/N$. □

Teorema 1.65. *Sean N y H subgrupos normales de G tal que $N \subseteq H$. Entonces $G/H \simeq (G/N)/(H/N)$.*

Demostración: Definimos $\varphi : G/N \to G/H$ por $\varphi(gN) = gH$. Verificamos que:

1. φ está bien definida.

2. φ es un homomorfismo.

3. φ es sobreyectivo.

4. El núcleo de φ es $H/N = \{hN \mid h \in H\}$.

En particular, por el Corolario 1.61 concluimos que $G/H \simeq (G/N)/(N/H)$. □

Ejercicio 1.66. Complete las demostraciones de los Teoremas 1.64 y 1.65.

Concluimos esta sección con un par de aplicaciones: Tomemos, a modo de ejemplo, el grupo $G = \mathbb{Z}/30\mathbb{Z}$ y su subgrupo $N = 10\mathbb{Z}/30\mathbb{Z} = \{[0], [10], [20]\}$. Como G es Abeliano, N es un subgrupo normal y podemos tomar el cociente G/N.

¿cuántas clases laterales tiene N dentro de G?

Bien, el Teorema 1.65 nos dice que $G/N \simeq \mathbb{Z}/10\mathbb{Z}$, por lo que podemos conluir que N tiene 10 clases laterales en G.

Damos una segunda aplicación en forma de proposición.

Proposición 1.67. *No existe un homomorfismo sobreyectivo de* $\mathbb{Z}_{68}$ *en* $\mathbb{Z}_{12}$.

Demostración: Buscando una contradicción, suponemos que si existe un homomorfismo sobreyectivo $\varphi : \mathbb{Z}_{68} \to \mathbb{Z}_{12}$. En particular, por el Primer Teorema del Isomorfismo se tiene que $\mathbb{Z}_{68}/Ker(\varphi) \simeq \mathbb{Z}_{12}$ y por lo tanto se tiene que

$$\frac{|\mathbb{Z}_{68}|}{|Ker(\varphi)|} = |\mathbb{Z}_{12}|,$$

donde $|X|$ denota la cardinalidad del conjunto X (vea la ecuación (1) previa al Teorema 1.43). Pero esto implica que

$$68/12 = |Ker(\varphi)|,$$

lo que es imposible pues $68/12$ no es un número entero. □

1.5. Acciones de grupos

Tal vez el aspecto mas importante de los grupos es que son entidades que *mueven* cosas: los elementos de S_n mueven al conjunto $\{1, \ldots, n\}$ o el Dihedral D_n mueve al polígono P_n. En esta sección, recordamos la definición de acción de un grupo y damos dos acciones intrínsecas de un grupo en si mismo. Esto nos proposcionará un leguaje adecuado para abordar temas mas delicados en el siguiente capítulo.

Definición 1.68. Sea X un conjunto cualquiera y G un grupo. Una **acción** de G en X, es una aplicación $A : G \times X \to X$, que satisface:

1. $A(id, x) = x$ para todo $x \in X$.
2. Para todo $x \in X$ y para todo $f, g \in G$, vale que $A(fg, x) = A(f, A(g, x))$.

En esta situación anotamos $G \curvearrowright^A X$, y $A(g, x)$ es *la acción de* g *en* x.

Observación 1.69. Dada una acción $A : G \times X \to X$, es conveniente anotar $g.x$ en vez $A(g, x)$. De este modo las condiciones 1 y 2 se vuelven

1'. $id.x = x$ para todo $x \in X$.

2'. $f.(g.x) = (fg).x$ para todo $f, g \in G$ y todo $x \in X$.

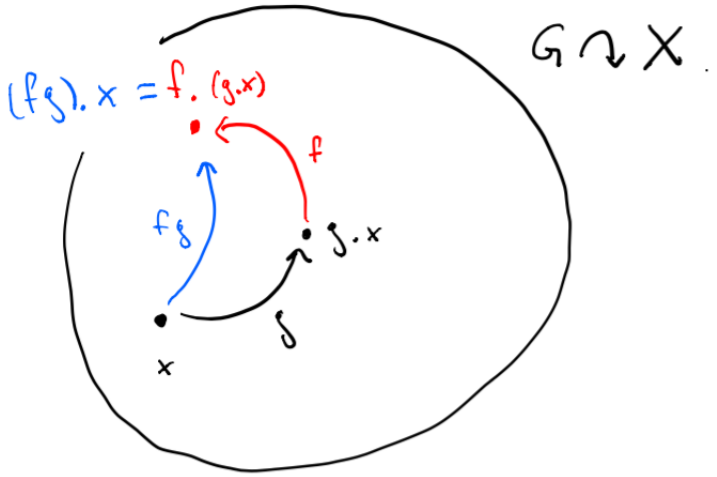


Figura 6: Representación gráfica de la condición $f.(g.x) = (fg).x$.

Ejemplo 1.70. $Sym(X)$, el grupo simétrico sobre un conjunto X, actúa naturalmente en X vía $g.x = g(x)$. En efecto para todo $x \in X$ se tienen que $id(x) = x$ y que $(g \circ f)(x) = g(f(x))$ para todo $f, g \in Sym(X)$.

Lo mismo ocurre con $Aut(G)$, el grupo de automorfismos de un grupo G, que actúa naturalmente en G por evaluación.

La siguiente proposición caracteriza las acciones de G en X en términos de homomorfismo de G en $Sym(X)$.

Proposición 1.71. *Las siguientes afirmaciones son equivalentes:*

1. *Existe una acción $G \curvearrowright X$.*

2. *Existe un homomorfismo $G \to Sym(X)$.*

Demostración: Dada una acción $G \curvearrowright^A X$, $(g, x) \mapsto g.x$, y dado $g \in G$, definimos $\phi_A(g)$ como la función de X a X dada por $\phi_A(g) : x \mapsto g.x$

Para empezar veamos que $\phi_A(g)$ es una biyección de X. Supongamos que $\phi_A(g)(x) = g.x = g.y = \phi_A(g)(y)$. Puesto que A es una acción podemos *multiplicar* la igualdad precedente por g^{-1} para obtener que $x = id.x = g^{-1}.(g.x) = g^{-1}.(g.y) = id.y = y$. Luego $\phi_A(g)$ es una inyección. Además ella es sobreyectiva pues $\phi_A(g)(g^{-1}.x) = x$. Luego $\phi_A(g)$ es una biyección de X. Podemos pensar entonces que $\phi_A : g \mapsto \phi_A(g)$ es una función de G en $Sym(X)$. Afirmamos que ϕ_A es un homomorfismo, es decir que $\phi_A(fg) = \phi_A(f) \circ \phi_A(g)$. En efecto para todo $x \in X$ vale que $\phi_A(fg)(x) := (fg).x = f.(g.x) = \phi_A(f)(\phi_A(g)(x))$. Hemos mostrado que toda acción de G en X induce un homomorfismo de G en $Sym(X)$.

Reciprocamente si $\phi : G \to Sym(X)$ es un homomorfismo, entonces la aplicación $A : (g, x) \mapsto \phi(g)(x)$ cumple que $A(id, x) = x$ para todo $x \in X$ y $A(f, A(g, x)) = A(fg, x)$ para todo $f, g \in G$. □

Definición 1.72. Sea $G \curvearrowright X$ una acción de un grupo G en un conjunto X. La **órbita** de $x \in X$ bajo G es el conjunto $Orb_G(x) = \{g.x \mid g \in G\}$, mientras que el **estabilizador** de $x \in G$ es el conjunto $Stab_G(x) = \{g \in G \mid g.x = x\}$. Mas aún, decimos que una acción es

- **fiel**, si para todo $g \in G \setminus \{id\}$ existe $x \in X$ tal que $g.x \neq x$.
- **libre** si para todo $g \in G \setminus \{id\}$ y para todo $x \in X$, se tiene que $g.x \neq x$.
- **transitiva** si para todo $x, y \in X$ existe $g \in G$ tal que $g.x = y$.

Observación 1.73. Note que $Stab_G(x)$ es un subgrupo de G. En efecto si $f, g \in Stab_G(x)$, entonces $(fg).x = f.(g.x) = x$ y $f^{-1}.x = f^{-1}.(f.x) = x$.

Ejercicio 1.74. Sea $G \curvearrowright^A X$ una acción y $\phi_A : G \to Sym(X)$ el homomorfismo asociado.

1. Muestre que la acción es fiel si y solo si ϕ_A es inyectivo.
2. Muestre que la acción es libre si y solo si $Stab_G(x) = \{id\}$ para todo $x \in X$.
3. Muestre que la acción es transitiva si y solo si $Orb_G(x) = X$ para todo $x \in X$.

Ejemplo 1.75. La acción natural de S_4 en $\{1, 2, 3, 4\}$ es fiel y transitiva, pero no es libre pues, por ejemplo, el elemento $(1, 3)$ fija al 2. El estabilizador de 2 en S_4 es, por definición, el conjunto de permutaciones de de $\{1, 2, 3, 4\}$ que fija al 2. En particular podemos identificar a $Stab_{S_4}(2)$ con el subgrupo de todas las permutaciones de $\{1, 3, 4\}$. Esto último certifica que $Stab_{S_4}(2)$ es isomorfo a S_3.

Ejercicio 1.76. Si X es un conjunto, denotamos por $\mathcal{F}(X, \mathbb{R})$ al conjunto de funciones de X a $\mathbb{R}$. Suponga que G es un grupo que actúa en X via $x \mapsto g.x$. Para $\varphi \in \mathcal{F}(X, \mathbb{R})$ y $g \in G$ definimos la función $g_*\varphi : X \to \mathbb{R}$ por $g_*\varphi : x \mapsto \varphi(g.x)$.

1. Pruebe que la aplicación $A : (g, \varphi) \mapsto g_*\varphi$ es una acción de G en $\mathcal{F}(X, \mathbb{R})$.
2. Bajo la acción $(g, \varphi) \mapsto g_*\varphi$, calcule es estabilizador en G de la función constante $\varphi(x) = 1$.
3. Si $x_0 \in X$, $\delta_{x_0} \in \mathcal{F}(X, \mathbb{R})$ es la función que en x vale 1 si $x = x_0$ y vale 0 en otro caso. Bajo la acción $(g, \varphi) \mapsto g_*\varphi$, calcule el estabilizador en G de δ_{x_0}.

Dos acciones naturales: Un grupo G puede actuar de muchas formas en un mismo espacio X. Particularmente importantes, son las acciones de un grupo G en si mismo. En este párrafo describiremos la acción por multiplicación y por conjugación de G en si mismo.

- **Acción por multiplicación (a izquierda):** Dado $x \in G$ (pensado como punto del espacio) y $g \in G$ (pensado como elemento que actúa), definimos $g.x = L_g(x) = gx$. Claramente $id.x = x$ y $(fg).x = (fg)x = f(gx) = f.(g.x)$ para todo $x, f, g \in G$, lo que dice que la multiplicación a izquierda es una acción de G en si mismo. Mas aún, si $g \neq id$ entonces $g.x \neq x$ para todo $x \in G$, lo que dice que la acción por multiplicación es una acción libre.

  Hemos encontramos el siguiente corolario.

Teorema 1.77 (Cayley, 1854)**.** *Todo grupo G es isomorfo a un subgrupo de algún grupo simétrico. Mas aún, si G es un grupo de cardinalidad $n \in \mathbb{N}$, entonces G es isomorfo a un subgrupo de S_n.*

Note que por (la prueba de) la Proposición 1.71, se tiene que la aplicación $L : G \to Sym(G)$ dado por $L : g \mapsto L_g$, es un homomorfismo inyectivo. A este homomorfismo se le conoce como **la representación regular izquierda** de G.

Ejercicio 1.78. *Muestre que todo grupo finito G admite una imagen isomorfa dentro de $GL_n(\mathbb{R})$, para algún n. (Ayuda: demuestre que S_n tiene una imagen isomorfa en $GL_n(\mathbb{R})$.)*

- **Acción por conjugación:** Dado $x \in G$ (pensado como punto del espacio) y $g \in G$ (pensado como elemento que actúa), definimos $g.x = C_g(x) = gxg^{-1}$. Claramente $id.x = x$ y $(fg).x = fgxf^{-1}g^{-1} = g.(f.x)$, lo que dice que la conjugación induce una acción de G en si mismo. Dos elementos se dicen **conjugados** si ellos estan en la misma órbita, y **la clase de conjugación** de $x \in G$ es la órbita de x bajo esta acción.

  Si bien en general, esta acción puede no ser fiel (por ejemplo si G es un grupo Abeliano, entonces esta acción es una acción trivial), veremos que de todas maneras ella entrega muchísima información sobre G.

Ejercicio 1.79. Dado n, calcule el menor m talque hay homomorfismos inyectivos $\mathbb{Z}_n \to S_m$ y $S_n \to S_m$. Compare con el Teorema de Cayley.

Asi como un subgrupo $H \leq G$ induce una partición de G, se tiene que una acción $G \curvearrowright X$ induce una partición de X.

Proposición 1.80. *Suponga que G actúa en un conjunto X. Entonces, las orbitas de G en X forman una partición X. Mas aún, dado $x \in X$, existe una biyección entre $Orb_G(x)$ y $G/Stab_G(x)$. En particular si G es un grupo finito de cardinalidad $|G|$, entonces $|Orb_G(x)|$ divide a $|G|$.*

Demostración: Suponga $G \curvearrowright X$. Para $x, y \in X$ anotamos $x \sim y$ si existe $g \in G$ tal que $g.x = y$. Note que $\sim$ es una relación de equivalencia: es refleja, pues $id.x = x$, es simétrica, pues si $g.x = y$ entonces $g^{-1}.y = x$ y es transitiva, pues si $g.y = y$ y $f.y = z$ entonces $fg.x = z$. Como la clase de equivalencia de x es precisamente la órbita de x, concluimos que las órbitas forman una partición de X.

Para ver que existe una biyección entre $Orb_G(x)$ y $G/Stab_G(x)$, notamos que

$$g.x = f.x \Leftrightarrow g^{-1}f \in Stab_G(x) \Leftrightarrow gStab_G(x) = fStab_G(x).$$

Esto conlleva que la aplicación $\psi : Orb_g(x) \to G/Stab_G(x)$ dada por $\psi(g.x) = gStab_G(x)$ sea una biyección bien definida. En particular, si G es un grupo finito de cardinalidad $|G|$, entonces

$$|G| = |Stab_G(x)| \cdot |G/Stab_G(x)| = |Stab_G(x)| \cdot |Orb_G(x)|,$$

donde la igualdad de la izquierda sigue del Teorema de Lagrange (Teorema 1.43). □

El Teorema de Lagrange (Teorema 1.43) nos dice que el orden de un subgrupo divide al orden del grupo ambiente. La afirmación recíproca, a saber que si n divide a $|G|$ entonces existe un subgrupo de cardinalidad n, si bien no es cierta en general, ella resulta ser cierta cuando el divisor es un número primo.

Teorema 1.81 (Cauchy, 1845)**.** *Si G es un grupo finito y p es un primo que divide a $|G|$, entonces existe $g \in G$ con $ord(g) = p$.*

Demostración: Sea p un primo que divide al orden del grupo G. Queremos demostrar que existe $g \neq id$ tal que $g^p = id$.

Denotamos por G^p al producto cartesiano $G \times \ldots \times G$ (p-veces) y hacemos $X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \ldots x_p = id\}$. Note que para fabricar un elemento de X, podemos elegir libremente las $p-1$ primeras entradas $x_1, \ldots, x_{p-1}$ y ajustamos la ultima de modo que $x_p = (x_1 \ldots x_{p-1})^{-1}$. Esto nos dice que $|X| = |G|^{p-1}$.

Para probar el teorema, vamos a hacer actuar un grupo cíclico de p elementos en X. Para ello consideremos $\sigma = (1, 2, \ldots, p) \in S_p$. Ciertamente $\langle\sigma\rangle$ es un subgrupo cíclico de p elementos en S_p, y podemos hacerlo actuar en X vía $\sigma^k.(x_1, \ldots, x_p) = (x_{\sigma^k(1)}, \ldots, x_{\sigma^k(p)})$.

Ahora, la Proposición 1.80 nos dice que las órbitas bajo la acción $\langle\sigma\rangle$ forman una partición de X, por lo que

$$|X| = |G|^{p-1} = \sum_{\text{órbitas}} |Orb_{\langle\sigma\rangle}(x)|, \tag{2}$$

y, mas aún, estas órbitas tienen cardinalidad 1 o p. La observación crucial es la siguiente: un punto $x \in X$ es fijo por la acción (es decir $Orb(x) = \{x\}$) si y solo si x es de la forma $(a, \ldots, a)$ con $a^p = 1$. Note que el vector $(id, \ldots, id) \in X$ es fijo por la acción. Concluimos que para demostrar el teorema, basta encontrar algún otro vector que sea fijo por la acción. En búsqueda de contradicción suponemos que $(id, \ldots, id)$ es el único vector fijo. Luego, podemos reescribir la ecuación (2) como

$$|X| = 1 + \sum_{\text{órbitas no fijas}} |Orb_{\langle\sigma\rangle}(x)|.$$

Pero esto es imposible pues el lado izquierdo de la igualdad es divisible por p, pero el lado derecho no (pues es de la forma 1+ cosas divisibles por p). Esta contradicción termina la demostración. □

La ecuación de clase de un grupo. Cuando $G \curvearrowright X$, la Proposición 1.80 nos dice que podemos contar la cardinalidad de X como suma de las cardinalidades de las distintas órbitas. La ecuación de clases de un grupo G es contar órbitas en el contexto de un grupo acuando en si mismo por conjugacion, es decir

$$|G| = \sum_{\text{Clases de conjugacion}} |C(g)|,$$

donde $C(g) = \{fgf^{-1} \mid f \in G\}$ denota la clase de conjugación de g en G.

Ejemplo 1.82. La ecuación de clase de un grupo Abeliano de cardinalidad n es $n = 1+1+\ldots+1$ n-veces. De hecho esta es una caracterización de la conmutatividad de un grupo.

Ejemplo 1.83. El grupo simétrico S_3 tiene 6 elementos:

$$S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}.$$

Claramente $C(id) = \{id\}$, por lo que la ecuación de clase de S_3 empieza $6 = 1+??$. Mas aún, calculando se tiene que $C((1,2)) = \{(1,2), (2,3), (1,3)\}$ y $C((1,2,3)) = \{(1,2,3), (1,3,2)\}$. De este modo la ecuación de clase de S_3 es $6 = 1 + 3 + 2$.

Ejercicio 1.84. Verifique que en S_3 se tiene que $C((1,2)) = \{(1,2), (2,3), (1,3)\}$ y $C((1,2,3)) = \{(1,2,3), (1,3,2)\}$.

Ejercicio 1.85. Calcule la ecuación de clase de D_4, el grupo de simetrias del cuadrado.

Estudiar la ecuación de clase de un grupo entrega bastante información sobre las posibles estructuras que el grupo puede admitir. Por ejemplo en la Sección 2.2 calcularemos la ecuación de clase de S_5 y usaremos esto para probar la simplicidad del grupo alternante A_5. El siguiente teorema muestra otro ejemplo donde la ecuación de clase resulta útil.

Teorema 1.86. Si G es un grupo de cardinalidad p^2, con p un primo, entonces G es Abeliano.

Para la prueba necesitamos un poco mas de lenguaje y un lema. Diremos que el **centro** de un grupo G es el conjunto $Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$. Si $g \in G$, el **centralizador** de g es $Centr(g) = \{f \in G \mid fg = gf\}$.

Ejercicio 1.87. Pruebe que $Centr(g)$ es un subgrupo de G y que $Z(G)$ es un subgrupo normal de G.

Lema 1.88. *Todo grupo G de orden p^n, con p un primo, tiene centro no trivial.*

Demostración: Consideramos la ecuación de clase un grupo G de cardinalidad p^n. Por la Proposición 1.80 tenemos que la cardinalidad de una clase de conjugación $C \subset G$, necesariamente divide a $|G| = p^n$. De este modo, puesto que $|C(id)| = 1$, se tiene que

$$p^n = |G| = 1 + \sum_{\text{clases de conjungación}} |C(g)|.$$

Puesto $|G|$ es divisible por p, concluimos que debe existir $g \neq id$ tal que $|C(g)| = 1$. Dicho g es un elemento central. □

Demostración del Teorema 1.86: Suponemos $|G| = p^2$. Por el Lema 1.88 se tiene que $Z(G)$ es no trivial. Debemos demostrar que $Z(G) = G$.

En búsqueda de contradicción, suponemos que $Z(G)$ no es todo G. Como la cardinalidad de $Z(G)$ divide a $|G|$, necesariamente tenemos que $|Z(G)| = p$. Sea $g \in G \setminus Z(G)$. Puesto que $Centr(g)$ en es subgrupo estrictamente mas grande que $Z(G)$, pues contiene a g y a $Z(G)$, concluimos que $|Centr(g)| = p^2$, lo que dice que g conmuta con todo elemento de G, es decir $g \in Z(G)$. Esto contradice nuestra elección de g. □

Ejercicio 1.89. Un grupo G se dice **soluble**, si existe una filtración finita

$$\{id\} = G_n \subseteq G_{n-1} \subseteq \ldots \subseteq G_0 = G,$$

tal que para todo $1 \leq i \leq n$ se tiene que G_i es un subgrupo normal de G_{i-1} y G_{i-1}/G_i es Abeliano. Por ejemplo si G es Abeliano, la filtración $\{id\} \subseteq G$ certifica que G es soluble. Muestre que todo grupo de orden p^n es soluble.

2. Algunos tópicos en teoría de grupos

2.1. El grupo $(\mathbb{Z}/p\mathbb{Z})^*$ y el protocolo de Diffie y Hellman

Vimos en el Ejercicio 1.37 que $Aut(\mathbb{Z}) \simeq \mathbb{Z}_2$. En esta sección describiremos el grupo de automorfismos de otro grupo sencillo, a saber el grupo $\mathbb{Z}/p\mathbb{Z}$ para p un número primo y veremos que él es isomorfo al grupo $(\mathbb{Z}/p\mathbb{Z})^*$ de enteros módulo p bajo *multiplicación*. A modo de aplicación de estas ideas, concluimos esta sección con una breve explicación del Protocolo de Diffie y Helman en criptografía.

Comenzamos con la identidad de Meziriac para números enteros, también conocida como de identidad de Bezout[5].

Definición 2.1. Dados $a, b \in \mathbb{Z}$ anotaremos MCM(a, b) su **mínimo común múltiplo**, es decir al menor entero positivo que es multiplo de a y b. Anotaremos por MCD(a, b) su **máximo común divisor**, es decir al mayor entero positivo que divide a a y b. Decimos que a y b son **coprimos**, si MCD$(a, b) = 1$. Note que 0 no es coprimo con nadie.

Ejercicio 2.2. Pruebe que MCD$(a, b) = 1$ si y solo si MCM$(a, b) = ab$. (Ayuda: use que todo número se descompone de manera *única* como producto de primos.)

Proposición 2.3 (Meziriac)**.** *Para $a, b \in \mathbb{N}$, coprimos, existe $x, y \in \mathbb{Z}$ tales que $1 = ax + by$.*

Demostración: Sea $D = \{ax + by \mid x, y \in \mathbb{Z}\}$. Observe que D es un subconjunto de $\mathbb{Z}$ con la propiedad que $d \in D \Leftrightarrow -d \in D$. Sea $d_0 = min\{d \in D \mid d > 0\}$. Queremos demostrar que $d_0 = 1$.

Supongamos en búsqueda de contradicción que $d_0 > 1$, digamos $d_0 = ax_0 + by_0$, para algún x_0 e y_0 en $\mathbb{Z}$.

Sea r_a el resto de dividir a por d_0, es decir $a = d_0 \cdot \ell + r_a$, con $\ell \in \mathbb{N}$ y $r_a \in \{0, 1, \ldots, d_0 - 1\}$. Puesto que $r_a = a - (ax_0 + by_0)\ell = a(1 - x_0\ell) + b(-y_0\ell)$ se tiene que r_a es un elemento de D. Pero como $0 \leq r_a \leq d_0 - 1$ y d_0 es el menor elemento positivo de D, concluimos que $r_a = 0$.

Analogamente r_b, el resto de dividir b en d_0, también cumple que $r_b = 0$.

Hemos encontrado entonces que d_0 divide tanto a a como a b, y como como estamos suponiendo que $d_0 > 1$, obtenemos que MCD$(a, b) \geq d_0 > 1$, contradiciendo que a y b son coprimos. □

Ejercicio 2.4. Adapte la prueba de la Proposición 2.3 para probar el siguiente enunciado: *Si a y $b \in \mathbb{N}$ son dos enteros cualesquiera, entonces existe $x, y \in \mathbb{Z}$ tal que $ax+by =$* MCD(a, b).

Definición 2.5. Para $n \in \mathbb{N}$, definimos $(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \ a$ y n son coprimos$\}$.[6]

Observación 2.6. Note que la definición precedente no depende del representante de clase, es decir que si $[a] = [a']$ en $\mathbb{Z}/n\mathbb{Z}$, entonces a es coprimo con n si y solo si a' es comprimo con n. Para ello notamos que $[a] = [a']$ implica que $a = a' + \ell n$ para

[5] Meziriac probó la identidad para números y Bezout para polinomios.

[6] Recuerde los elementos de $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ los denotamos por $[a] = a + n\mathbb{Z}$.

algún $\ell \in \mathbb{Z}$, y por lo tanto si k es un divisor común de n y a' entonces k también divide a a.

En particular, para p primo se tiene que $(\mathbb{Z}/p\mathbb{Z})^* = \{[1], \ldots, [p-1]\}$.

Gracias al Teorema de Meziriac podemos probar que $(\mathbb{Z}/p\mathbb{Z})^*$ admite una estructura natural de grupo.

Teorema 2.7. *Sea p un primo. Entonces $(\mathbb{Z}/p\mathbb{Z})^*$ es un grupo bajo el producto*

$$[a] \cdot [b] = [a \cdot b].$$

Demostración: Lo primero a chequear es que si $[a]$ y $[b]$ son elementos de $(\mathbb{Z}/p\mathbb{Z})^*$, entonces $[a \cdot b]$ también. Para ello hay que chequear que si a y b son coprimos on p entonces $a \cdot b$ tambien es coprimo con p. Esto sigue del hecho de que la descomposición en factores primos de un entero es *única* y, por lo tanto, si p no aparece en la descomosición de a ni de b entonces tampoco aparece en la descomposión de $a \cdot b$.

Luego chequeamos que la definición del producto $[a] \cdot [b]$ no depende de los representantes a y b. Para ello notamos que si $[a] = [a']$ y $[b] = [b']$, entonces $a = a' + \ell p$, y $b = b' + kp$. Luego,

$$[a \cdot b] = [a' \cdot b' + p(b' + a' + \ell k p)] = [a' \cdot b'] + [p(b' + a' + \ell k p)] = [a' \cdot b'] + [0],$$

y por lo tanto $[a \cdot b] = [a' \cdot b']$.

Finalmente, la asociatividad sigue pues la multiplicación dentro del corchete $[\cdot]$ es la multiplicación usual que es asociativa. El neutro ciertamente es $[1]$ y solo falta verificar que cada elemento tiene un inverso.

Para ello tomamos $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$. Como a y p son coprimos el Teorema de Meziriac nos asegura que existen $x, y \in \mathbb{Z}$ tal que $1 = a \cdot x + p \cdot y$. Mirando esta igualdad módulo p encontramos que

$$[1] = [a \cdot x] + [p \cdot y] = [a] \cdot [x].$$

□

Observación 2.8. Si bien hemos probado que todo elemento de $(\mathbb{Z}/p\mathbb{Z})^*$ tiene un inverso *multiplicativo*, no hemos dado una *receta* para encontrar dicho inverso. De hecho, para encontrarlo hemos usado el Teorema de Meziriac que es un teorema de existencia.

Observación 2.9. Podemos extender la multiplicación en $(\mathbb{Z}/p\mathbb{Z})^*$ a todo $\mathbb{Z}/p\mathbb{Z}$ simplemente definiendo $[0] \cdot [a] = [0 \cdot a] = [0]$. De este modo se tiene que multiplicación en $\mathbb{Z}/p\mathbb{Z}$ distribuye sobre la suma de $\mathbb{Z}/p\mathbb{Z}$ igual que en los números enteros usuales, es decir

$$[a] \cdot ([b] + [c]) = [a \cdot (b + c)] = ([a] \cdot [b]) + ([a] \cdot [c]).$$

Esto hace que podamos calcular alegremente en $\mathbb{Z}/p\mathbb{Z}$ como si de enteros se tratara. ¡La diferencia está en que ahora la multiplicación es invertible!

Ejercicio 2.10. Encuentre el inverso de $[5]$ en $(\mathbb{Z}/7\mathbb{Z})^*$, en $(\mathbb{Z}/11\mathbb{Z})^*$ y en $(\mathbb{Z}/13\mathbb{Z})^*$.

Automorfismos de $\mathbb{Z}/p\mathbb{Z}$: Dado un entero $k \in \mathbb{Z}$ definimos $M_k : \mathbb{Z} \to \mathbb{Z}$ por $M_k : n \mapsto k \cdot n$, la multiplicación por k. Si bien en general M_k no es una biyección de $\mathbb{Z}$, cuando miramos esta multiplicación módulo un primo p, ella si se vuelve una biyección.

Concretamente, dado $[k] \in \mathbb{Z}/p\mathbb{Z}$, definimos

$$M_{[k]} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \text{ por } M_{[k]} : [a] \mapsto [k] \cdot [a].$$

Nuestra primera observación es la

Proposición 2.11. *Sea p un primo. Si $[k] \neq [0]$ en $\mathbb{Z}/p\mathbb{Z}$, entonces $M_{[k]}$ es un automorfismo de $\mathbb{Z}/p\mathbb{Z}$.*

Demostración: Tenemos que ver que $M_{[k]}$ es un homomorfismo biyectivo. Para lo primero notamos que la condición $[k] \neq [0]$ equivale a decir que k y p son coprimos y luego, usando el Teorema 2.7, tenemos que

$$M_{[k]}([a] + [b]) = M_{[k]}([a + b]) = [k] \cdot [a + b] = [k \cdot a + k \cdot b] = M_{[k]}([a]) + M_{[k]}([b]).$$

Para ver que $M_{[k]}$ es biyectiva cuando $[k] \neq [0]$ observamos primero que $M_{[k]}$ es una función inyectiva. En efecto si $[k] \cdot [a] = [k] \cdot [b]$ entonces $[k \cdot a] = [k \cdot b]$ y por lo tanto $k \cdot a = k \cdot b + p\ell$ para algún $\ell \in \mathbb{Z}$. Esto nos dice que $k(a - b) = p\ell$ por lo que necesariamente $a - b$ es divisible por p (puesto que k no lo es). Esto útlimo equivale a decir que $[a - b] = 0$ lo que a su vez equivale a decir que $[a] = [b]$.

Finalmente como el conjunto $\mathbb{Z}/p\mathbb{Z}$ es un conjunto finito, concluimos que toda función inyectiva (por ejemplo $M_{[k]}$) es tambiés sobreyectiva. □

La proposición anterior nos dice que si $[k] \neq [0]$ entonces $M_{[k]} \in Aut(\mathbb{Z}/p\mathbb{Z})$. Concluimos la caracrerización de los automorfismos de $\mathbb{Z}/p\mathbb{Z}$ con

Proposición 2.12. $Aut(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$.

Demostración: Sea $M : (\mathbb{Z}/p\mathbb{Z})^* \to Aut(\mathbb{Z}/p\mathbb{Z})$ dada por $M : [k] \to M_{[k]}$. La Proposición 2.11 nos dice que M es una función bien definida. Afirmamos que M es en realidad un isomorfismo.

Para ver que M es un homomorfismo hay ver que $M([k] \cdot [k']) := M_{[k]\cdot[k']} = M_{[k]} \circ M_{[k']}$, donde $\circ$ denota la composición de funciones (que es la operación en $Aut(\mathbb{Z}/p\mathbb{Z})$). Esta igualdad se cumple pues, si a es un elemento cualquiera de $\mathbb{Z}/p\mathbb{Z}$, entonces

$$M_{[k]\cdot[k']}(a) = [(k \cdot k') \cdot a] = [k \cdot (k' \cdot a)] = M_{[k]}(M_{[k']}(a)).$$

Luego M es un homomorfismo.

Para ver que M es inyectivo calculamos su núcleo: si $M_{[k]} = Id$, donde $Id : x \mapsto x$, es el automorfismo identidad, entonces $M_{[k]}([1]) = [k]\cdot[1] = [1]$, y por lo tanto $[k] = [1]$ que es la identidad de $(\mathbb{Z}/p\mathbb{Z})^*$.

Finalmente debemos mostrar que M es un homomorfismo sobreyectivo, es decir que todo automorfismo $\alpha \in Aut(\mathbb{Z}/p\mathbb{Z})$ es, secretamente, la multiplicación por algún

$[k]$. Para ello tomamos $[k] := \alpha([1])$, y notamos que si $0 \leq a \leq p-1$, entonces $[a] = [1] + \ldots + [1]$ a-veces y por lo tanto

$$\alpha([a]) = \alpha([1] + \ldots + [1]) = [k] + \ldots + [k] = [k + \ldots + k] = [k \cdot a] = M_{[k]}([a]).$$

Como $[a]$ es arbitrario esto muestra que $\alpha = M_{[k]}$. □

Ejercicio 2.13. Demuestre que $Aut(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ para todo $n \in \mathbb{N}$.

El hecho de que $(\mathbb{Z}/p\mathbb{Z})^*$ sea un grupo bajo multiplicación se usa, en la actualidad, millones de veces al día para encriptar mensajes en internet y así mantener una comunicación segura entre partes muy distantes y que incluso pueden nunca antes haberse visto o intercambiado información. Los primeros en notar que las estructuras aritméticas (como por ejemplo $(\mathbb{Z}/p\mathbb{Z})^*$) pueden usarse con este propósito fueron Diffie y Hellman en 1976. En el siguiente párrafo damos una descripción breve del protocolo ideado por ellos.

El protocolo de Diffie y Hellman. Cuando información importante viaja a través de canales fácilmente interceptables (por ejemplo, ondas de radio viajando por el aire, bits viajando por internet o cartas viajando por el correo tradicional) lo normal es querer encriptar dichos mensajes para así ocultar su verdadero contenido.

Ya en la antigua Roma, Julio Cesar encriptaba sus cartas usando un sencillo decalaje en su alfabeto[7] (ver Figura 7) y dicha práctica se popularizó y complejizó con el correr de los siglos encontrando uno de sus puntos mas sofisticados en la máquina Enigma usada por los Alemanes en la Segunda Guerra[8].

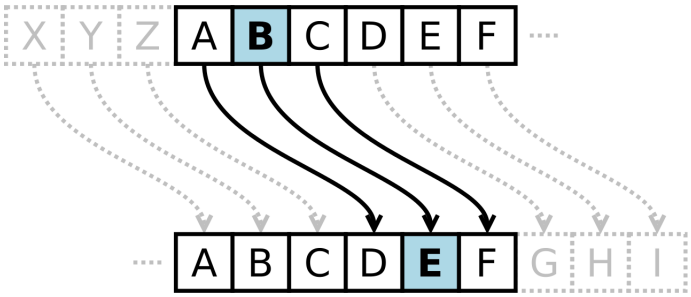


Figura 7: Un ejemplo de cifrado de Cesar. (imagen sacada de Wikipedia)

Todos estos métodos de cifrado tienen una cosa en común: el interlocutor y receptor tiene que estar de acuerdo *a priori* en cual va a ser la regla de cifrado. A este tipo de cifrado se les llama cifrados de Clave Privada. El problema con estos cifrados es que una vez que suficiente información es interceptada, se pueden usar métodos estadísticos para intentar adivinar el verdadero contenido de los mensajes.[9]

La novedad del protocolo de Diffie y Hellman es que permite crear reglas de encriptación de manera rápida, segura, y sobre todo sin acordarlas de antemano.

[7] Recomiendo ver Cifrado César en Wikipedia.

[8] Vea máquina Enigma en Wikiedia.

[9] Recomiendo ver la película Codigo Enigma, que relata el afán (y logro) de los Británicos para romper el cifrado de Enigma usado por los Alemanes.

Mas aún, el protocolo para crear la clave de encriptación sucede de forma *pública* y, aún asi, solamente los interesados obtendrán el secreto que les permitirá encriptar y desencriptar sus mensajes. Es por esto que estos tipos de cifrado se llaman de Clave Pública.

La *clave* de este protocolo está en la solución al siguiente dilema: ¿Cómo pueden dos personas obtener un *secreto* entre ellas, aún cuando ellas no compartan información previa y, mas aún, toda su conversación este siendo escuchada por una tercera persona?

En la práctica, este secreto S será un número (o una clase de números) que se usará para encriptar futuros mensajes[10]. La principal observación de Diffie y Hellman es que en el grupo $(\mathbb{Z}/p\mathbb{Z})^*$ es fácil tomar potencias, pero dificil encontrar raices y que esto se puede explotar para *fabricar* secretos. El siguiente ejercicio intenta transmitir esta disonancia.

Ejercicio 2.14. Sea $G = (\mathbb{Z}/11\mathbb{Z})^*$. Note que este grupo tiene 10 elementos.

1. Calcule la clase de $[2^n]$ para $n = 6, 8, 14, 42, 2021$. (Ayuda: use que $[2]^{10} = [1]$)
2. Escriba $[7]$ y $[9]$ como potencias de $[2]$, digamos $[7] = [2^a]$ y $[9] = [2^b]$ con $a, b \in \{1, 2, \ldots, 10\}$. Luego calcule $[2^{a\cdot b}] = [2^a]^b = [2^b]^a$. ¿Puede encontrar a y b sin escribir *todas* las potencias de 2?

El lector notará que cualquier elemento de $(\mathbb{Z}/11\mathbb{Z})^*$ se puede escribir como potencia de $[2]$, y por lo tanto se tiene que $(\mathbb{Z}/11\mathbb{Z})^*$ es cíclico. Esto último es un hecho general que usaremos para describir el protocolo y que demostraremos mas delante en este texto cuando estudiemos teoría de cuerpos (ver Proposición 3.49).

Proposición 2.15. *Si p es primo, entonces el grupo $G = (\mathbb{Z}/p\mathbb{Z})^*$ es cíclico.*

EL PROTOCOLO:

El Instituto Nacional de Estándares y Tecnología (NIST por su sigla en inglés) fija un primo p bien grande y fija también un generador g de $(\mathbb{Z}/p\mathbb{Z})^*$. Esta información es pública. El primo p puede cambiar (por ejemplo si la capacidad de procesamiento de los computadores aumenta muchísimo), pero en general permanece invariable.

Paso 1: Yo y mi interlocutor elegimos cada uno un numero entre 1 y $p-1$. Yo elijo a y mi interlocutor elige b. Estos números son secretos y por ningún motivo voy a decirlo en voz alta.

Paso 2: Yo calculo g^a y se lo comunico a mi interlocutor. El hace lo mismo y me manda g^b. Este paso bien podría ser interceptado por una tercera persona, llamémosla P.

Paso 3: Yo y mi interlocutor podemos calcular $S = g^{ab} = (g^b)^a = (g^a)^b$. Esta es nuestra clave secreta.

[10]Un ejemplo de juguete: podemos pensar que un *mensaje* es una sucesión de números (elegir alguna biyección entre letras y números) y el número S se usa para multiplicar la sucesión.

Observación 2.16. Si bien la tercera person P puede, en teoría, calcular S, en la práctiva esto es muy lento computacionalmente hablando. En efecto NIST elige el primo p de modo que calcular a a partir de g^a demore aproximadamente la edad del Universo, mientras que calcular g^a dados g y a demora a penas una fracción de segundo. Formalmente, lo que está pasando es que los algoritmos que disponemos para calcular g^a, dados g y a, son muy muy rápidos comparados con los algoritmos que disponemos para calcular a dados g y g^a.

Esto hace que el número S en la práctica sea un secreto infranqueable que además puede ser cambiado en un tris.

2.2. Simplicidad del grupo alternante

Un grupo G se dice **simple** si no admite cocientes otros que G y el grupo trivial $\{id\}$. Esta clase de grupos es especialmente interesante pues conforman las piezas irreductibles dentro de la teoría de grupos. Ejemplos de grupos simples son los grupos cíclicos $\mathbb{Z}/p\mathbb{Z}$ con p primo, pero ellos son demasiado sencillos y están lejos de capturar toda la riqueza de la teoría. En esta sección introduciremos A_n, el grupo de permutaciones alternantes del conjunto $\{1, \ldots, n\}$, y veremos que dicho grupo es un grupo simple si $n \geq 5$.

El signo de una permutación. Queremos definir el *signo* de una permutación $\sigma \in S_n$. Para ello definimos el polinomio en n-variables $P(x_1, \ldots, x_n) = \Pi_{i<j}(x_i - x_j)$. Notar que cada pareja de índices (i, j) aparece una única vez en la pitatoria que define a P. Definimos la función $sgn_n : S_n \to \{-1, 1\}$ por

$$sgn_n(\sigma) = \frac{P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{P(x_1, \ldots, x_n)}.$$

Observación 2.17. Dado $\sigma \in S_n$, la definición de su signo no depende realmente de n pues $sgn_n(\sigma) = sgn_{n+1}(\sigma)$. Es por ello que en lo que sigue olvidaremos el subíndice n en la función sgn.

Ejercicio 2.18. Calcule $sgn((1,2))$, $sgn((2,3))$ y $sgn((1,2,3))$.

La idea de la función *signo* es que detecta cuantas veces se da vuelta algún factor en la pitatoria de P. El punto crucial, es que dicha cantidad es independiente de los nombres que tengan los índices y por lo tanto se tiene

$$sgn(\sigma) = \frac{P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{P(x_1, \ldots, x_n)} = \frac{P(x_{\sigma\tau(1)}, \ldots, x_{\sigma\tau(n)})}{P(x_{\tau(1)}, \ldots, x_{\tau(n)})},$$

para toda permutación $\tau \in S_n$. Con esto, podemos mostrar que sgn es un homomorfismo:

$$sgn(\sigma\tau) = \frac{P(x_{\sigma\tau(1)}, \ldots, x_{\sigma\tau(n)})}{P(x_{\tau(1)}, \ldots, x_{\tau(n)})} \cdot \frac{P(x_{\tau(1)}, \ldots, x_{\tau(n)})}{P(x_1, \ldots, x_n)} = sgn(\sigma) \cdot sgn(\tau).$$

Hemos mostrado la

Proposición 2.19. *$sgn : S_n \to \mathbb{Z}_2$ es un homomorfismo de grupos (recuerde que $\mathbb{Z}_2 = \{-1, 1\}$ con la multiplicación usual).*

Definimos A_n, **el grupo alternante**, como $A_n = Ker(sgn : S_n \to \mathbb{Z}_2)$.

Observación 2.20 (Criterio para el signo)**.** Es fácil ver que el signo de una transposición $\tau = (a, b) \in S_n$ es -1. Puesto que *sgn* es un homomorfismo, si $\tau_1, \ldots, \tau_\ell$ son transposiciones en S_n, el signo de su producto $sgn(\tau_1 \circ \ldots \circ \tau_\ell) = (-1)^\ell$.

Ejercicio 2.21. Muestre que todo $\sigma \in S_n$ se puede escribir como un producto de transpociciones. Use esto para probar que el signo de un ciclo $(\alpha_1, \ldots, \alpha_k)$ es $(-1)^{k-1}$.

Descomposición en ciclos y conjugación. Hemos visto que todo $\sigma \in S_n$ puede escribirse como producto de ciclos disjuntos. Si bien esta escritura no es única, pues los ciclos disjuntos conmutan, ella caracteriza las clases de conjugación de los elementos de S_n.

Proposición 2.22. *Las clases de conjugacion en S_n están dadas por la descomposicion en ciclos disjuntos. Mas precisamente, dos permutaciones σ y σ' en S_n son conjugadas si y solo si ellas se escriben con el mismo número de ciclos disjuntos, cada uno del mismo largo.*

Demostración: Si bien el enunciado es un poco confuso, la demostración es cristalina. La observación crucial es la siguiente: Si τ es un elemento cualquiera de S_n y $\sigma = (\alpha_1, \ldots, \alpha_k)$ es un ciclo, entonces

$$\tau\sigma\tau^{-1} = (\tau(\alpha_1), \ldots, \tau(\alpha_k)). \tag{3}$$

En particular esto dice que dos ciclos son conjugados si y solo si ellos tienen el mismo largo. Para el caso general, basta notar que si $S_n \ni \sigma = \sigma_1 \ldots \sigma_\ell$, donde los σ_i son ciclos disjuntos, entonces

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \ldots (\tau\sigma_\ell\tau^{-1}),$$

donde los ciclos $(\tau\sigma_i\tau^{-1})$ son disjuntos dos a dos. □

La Proposición 2.22 nos ayuda a calcular la ecuación de clase de S_n pues ella dice que simplemente tenemos que contar cuantas formas de escribir elementos hay. Por ejemplo en S_5 hay

- 10 transposiciones (i.e. elementos de la forma (ab)), pues una transposición esta determinada por una pareja en $\{1, \ldots, 5\}$, y (elegir 2 entre 5)=10.
- 20 elementos de la forma (abc): 2 veces (3 entre 5), pues hay dos maneras de orientar un trío $\{a, b, c\}$.
- 15 elementos de la forma $(ab)(cd)$. Pues 15= (2 entre 5) por (2 entre 3) dividido en 2, esto último para no contar dos veces cada elemento (los ciclos disjuntos conmutan).

- 20 elementos de la forma $(abc)(cd)$: 20= 2 veces (3 entre 5) pues una vez elegido y orientado el trio $\{a, b, c\}$ no quedan mas elecciones.
- $24 = 4 \cdot 3 \cdot 2$ ciclos largos (i.e. elementos de la forma $(abcde)$). Pues, permutando ciclicamente nuestro ciclo, podemos suponer que él empieza con a, para la segunda letra tenemos 4 opciones para la tercera 3 para la cuarta 2 y la quinta esta determinada.
- $30 = 5 \cdot 6$ elementos de la forma $(abcd)$. Pues es 5 veces la cantidad de ciclos largos en S_4 y, argumentando como en el item previo, se tiene que con $\{a, b, c, d\}$ se pueden fabricar 6 ciclos de largo 4.

De este modo la ecuación de clase de S_5 es

$$|S_5| = 120 = 1 + 10 + 20 + 15 + 20 + 24 + 30.$$

Simplicidad de A_5. Puesto que A_5 es el núcleo de $sgn : S_5 \to \mathbb{Z}_2$, se tiene que A_5 es un subgrupo de índice 2 en S_5 y por lo tanto $|A_5| = 60$. Para ver que A_5 es simple calcularemos su ecuación de clase y veremos que ella fuerza que los únicos subgrupos normales sean A_5 e $\{id\}$.

La primera observación es que hay varias clases de connjugación de S_5 que no perteneces a A_5. Usando el Ejercicio 2.21 es facil ver que solo tenemos que investigar las clases de conjugación de elementos (escritos en ciclos disjuntos) de la forma

$$(ab)(cd),\ (abc),\ (abcde).$$

El siguiente ejercicio nos ayuda:

Ejercicio 2.23. Suponga que G es un grupo finito que actúa transitivamente en un conjunto finito X. Suponga que $N \lhd G$ es un subgrupo de índice 2. Muestre que si la acción de N en X no es transitiva, entonces N parte a X en exactamente dos orbitas, ambas con la misma cardinalidad.

Con esto podemos calcular la ecuación de clase de A_5.

- Los elementos de la forma $(ab)(cd)$ forman una única clase de conjugación en A_5, puesto que 15 no es divisible por 2.
- Los elementos de la forma (abc) forman una única clase de conjugación en A_5 puesto que para cualquier $\tau \in S_n$, si (de) es disjunto de (abc) vale que

  $$\tau(abc)\tau^{-1} = \tau(de)(abc)(de)\tau^{-1} = (\tau(de))\ (abc)\ (\tau(de))^{-1}.$$

  En particular, toda conjugación de (abc) en S_5 puede ser implementada por un elemento de A_5.
- Los elementos de la forma $(abcde)$ se dividen en dos clases de conjugación en A_5. Por ejemplo (12345) no es conjugado a (21345) en A_5.

De este modo encotramos que la ecuación de clase de A_5 es

$$|A_5| = 60 = 1 + 20 + 15 + 12 + 12.$$

Terminamos la prueba de la simplicidad de A_5 con la

Proposición 2.24. *Suponga que G tiene la ecuación de clase*

$$|G| = 60 = 1 + 20 + 15 + 12 + 12.$$

Entonces G es simple.

Demostración: La demostración tiene dos ingredientes. El primero es el Teorema de Lagrange (Teorema 1.43), que dice que $|N|$ tiene que dividir a $|G| = 60 = 2^2 \cdot 3 \cdot 5$. El segundo ingrediente es que, por ser N un subgrupo normal de G, entonces las clases de conjugación en G o bien estan totalmente contenidas en N o bien son disjuntas de N, y por lo tanto $|N|$ tiene que escribirse como suma de 1 (pues N contiene a la identidad) mas 12 o 15 o 20 o una combinación de estos.

Es fácil ver que estas dos condiciones fuerzan que $|N|$ sea igual a 1 o 60. □

Ejercicio 2.25. Muestre que las permutaciones $K_4 = \{id, (12)(34), (13)(24), (14)(23)\}$ es un subgrupo normal de A_4. Muestre además que $K_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Simplicidad de A_n, para $n \geq 6$. Terminamos esta sección demostrando la simplicidad de A_n para $n \geq 6$. Nuestra demostración es por inducción siendo la simplicidad de A_5 el caso inicial. [11]

Sea $N \lhd A_n$. Queremos demostrar que N coincide con A_n o bien $N = \{id\}$.

Nuestra primera observación es que que podemos identificar A_{n-1} con $Stab_{A_n}(n)$, el estabilizador de n en A_n. De hecho, módulo un cambio de nombre, se tiene que $Stab_{A_n}(i) \simeq A_{n-1}$ para todo $i \in \{1, \ldots, n\}$ y por lo tanto $Stab_{A_n}(i)$ es un grupo simple.

Ciertamente $N \cap Stab_{A_n}(i)$ es normal en $Stab_{A_n}(i)$, luego la hipótesis inductiva nos dice que la intersección de N con $Stab_{A_n}(i)$ es o bien trivial o bien coincide con $Stab_{A_n}(i)$. Esto último es fácil de descartar:

Ejercicio 2.26. Sea $n \geq 4$ y suponga que N es un subgrupo normal de A_n que contiene a $Stab_{A_n}(1)$. Muestre que necesariamente $N = A_n$.

Así, necesariamente tenemos que $N \cap Stab_{A_n}(i) = \{id\}$ para todo i. Esto dice que si $\sigma \in N \setminus \{id\}$, entonces σ mueve cada punto de $\{1, \ldots, n\}$.

Sea $\tau \in A_n$. Puesto que $n \geq 6$, podemos elegir $\tau \in A_n$ tal que τ fija i y $\sigma(i)$ y, ademas, τ **no conmuta** con σ (para ello basta elegir τ de modo que τ no preserve las orbitas de σ, ver Ejercicio 2.27). De este modo tenemos que $\tau\sigma\tau^{-1}\sigma^{-1}$ es un elemento no trivial de N que fija $\sigma(i)$, lo que contradice que N intersecta trivialmente los estabilizadores. □

Ejercicio 2.27. Sea $\sigma, \tau \in S_n$ dos transformaciones que conmutan y sean x, y dos elementos de $\{1, \ldots, n\}$. Muestre que x e y están en la misma órbita bajo σ (es decir, $\sigma^k(x) = y$ para algún k) si y solo si $\tau(x)$ y $\tau(y)$ están en la misma órbita bajo σ.

[11] Los grupos simples suelen agruparse en familias con el caso de los grupos alternantes. Sin embargo, este no es siempre es caso pues existen los grupos finitos simples *esporádicos*. La clasificación de los grupos finitos simples se completó en la década del 80.

2.3. Un grupo simple infinito

Hemos visto en §2.2 que los grupos alternantes A_n, $n \geq 5$, son grupos simples. En esta sección estudiaremos el grupo $S_\infty = Sym_0(\mathbb{Z})$, de permutaciones de soporte finito de $\mathbb{Z}$, y mostraremos que el grupo A_∞ de permutaciones pares de $\mathbb{Z}$ es un grupo simple e infinito. Este tipo de objetos simples infinitos son importantes pues nos dicen que la teoría de grupos no es una teoría que pueda entenderse cabalmente mirando solo sus representaciones finitas.

Para empezar notemos que si identificamos a S_{2n+1} con $Sym(\{-n, \ldots, n\})$, entonces podemos escribir $S_\infty = Sym_0(\mathbb{Z})$ como la unión creciente de los S_{2n+1}. En fórmula

$$S_\infty = \bigcup_{n \in \mathbb{N}} S_{2n+1}.$$

De ello se desprende que el signo de cada $\sigma \in S_\infty$ está bien definido, por lo que podemos definir $A_\infty = Ker(sgn : S_\infty \to \{-1, 1\})$ el subgrupo de S_∞ de permutaciones pares. Ciertamente A_∞ tiene índice 2 en S_∞ por lo que A_∞ es un grupo infinito.

En lo que sigue adaptaremos un argumento de Higman para probar el siguiente teorema.

Teorema 2.28. *A_∞ es un grupo simple.*

Observación 2.29. Note que en S_∞ y en A_∞ las clases de conjugación son infinitas, por lo que no hay una ecuación de clase para aprovechar. Por ello la presente demostración no usa esa herramienta. De hecho, la simplicidad de A_∞ es independiente de la simplicidad de A_n.

Antes de ir a la demostración necesitamos un poco de vocabulario.

Definición 2.30. Dado un grupo G y $f, g \in G$ denotamos por $[f, g] = fgf^{-1}g^{-1}$ al **conmutador** de f y g. Denotamos por $G^{(1)} = [G, G]$ al subgrupo *generado* por los conmutadores $[f, g]$ con f y g en G. El subgrupo $[G, G]$ se llama **subgrupo derivado** o **subgrupo conmutador**.

Ejercicio 2.31. Demuestre que $[G, G]$ es un subgrupo **caracteristico** de G, es decir, que $\varphi([G, G]) = [G, G]$ para todo $\varphi \in Aut(G)$ (en particualr $[G, G]$ es un subgrupo normal).

Ejercicio 2.32. Muestre que si N es un subgrupo normal de G y K es un subgrupo caracteriztico de N, entonces K es un subgrupo normal de G.

Ejercicio 2.33. Demuestre que $G/[G, G]$ es un grupo Abeliano. Mas aún, muestre que si G/N es un cociente Abeliano de G, entonces $[G, G] \subseteq N$.

Ejercicio 2.34. Demuestre que $A_\infty = [S_\infty, S_\infty]$ (Ayuda: la contención $[S_\infty, S_\infty] \subseteq A_\infty$ sigue del hecho que *sgn* es un homomorfismo, para la otra contención saque ideas de la prueba del Lema 2.35).

El argumento principal en la demostración del Teorema 2.28 es el siguiente lema.

Lema 2.35. *Sea $N \neq \{id\}$ un subgrupo normal de S_∞. Entonces N contiene a $[S_\infty, S_\infty]$.*

Demostración: Sean $a, b \in S_\infty$ y $n \in N \setminus \{id\}$. Basta demostrar que $[a, b]$ pertenece al subgrupo normal generado por n (es decir, $[a, b]$ se puede escribir como producto de conjugados de n). Como es de esperar, la Proposición 2.22 será de gran utilidad.

Comenzamos por demostrar que N, por ser normal y no trivial, contiene elementos que permutan ciclicamente intervalos (finitos pero) arbitrariamente largos de $\mathbb{N}$. Para ello descomponemos $n \in N \setminus \{id\}$ en producto de ciclos disjuntos: $n = \sigma_1 \dots \sigma_k$. Usando la Proposición 2.22 (mas precisamente la ecuación (3) en su demostración), podemos conjugar n por $\tau_1 \in S_\infty$ de modo que $\tau_1\sigma_1\tau_1^{-1}, \dots, \tau_1\sigma_{k-1}\tau_1^{-1}$ tengan soporte en los enteros negativos, pero $\tau_1\sigma_k\tau_1^{-1}$ tenga soporte en los enteros positivos. De hecho, podemos elegir τ_1 de modo que $\tau_1\sigma_k\tau_1^{-1} = (1, 2, \dots, j)$ (algún $j \geq 2$). Repetimos el argumento con $\tau_2 \in S_\infty$ de modo que $\tau_2\sigma_1\tau_2^{-1}, \dots, \tau_2\sigma_{k-1}\tau_2^{-1}$ tengan soporte en los enteros negativos, pero $\tau_2\sigma_k\tau_2^{-1} = (j, j+1, \dots, j+(j-1))$. De este modo encontramos que

$$\begin{aligned} N \ni (\tau_1 n \tau_1^{-1})(\tau_2 n \tau_2^{-1}) &= \beta \cdot (1, 2, \dots, j) \cdot (j, j+1, \dots, j+(j-1)) \\ &= \beta \cdot (1, 2, \dots j + (j-1)), \end{aligned}$$

donde $\beta \in S_\infty$ tiene soporte en los enteros negativos. Repitiendo este proceso cuantas veces sea necesario, encontramos $m \in N$, un elemento que permuta ciclicamente un intervalos arbitrariamente grande de $\mathbb{N}$.

Con esto podemos escribir $[a, b]$ como producto de conjugados de $n \in N$. Para simplificar el argumento supondremos que los soportes de a y de b están contenidos en los enteros positivos (el caso general queda de ejercicio). Digamos $sop(a) \cup sop(b) \subseteq \{1, \dots, k\}$. Elegimos $m \in N$ un elemento que permuta cíclicamente el intervalo $\{1, \dots, j\}$ con $j \geq 2k + 1$. En particular se tiene que $m^k(sop(a) \cup sop(b))$ es disjunto de $sup(a) \cup sop(b)$.

Ejercicio 2.36. Muestre que $sop(m^k a m^{-k}) = m^k(sop(a))$.

Puesto que elementos de S_∞ con soporte disjunto necesariamente conmutan, concluimos que $m^k a m^{-k}$ conmuta con b y con a. En particular se tiene que

$$[[a, m^k], b] = a m^k a^{-1} m^{-k} b m^k a m^{-k} a^{-1} b^{-1} = a b a^{-1} b^{-1}.$$

La demostración termina observando que $[[a, m^k], b]$ pertenece a N. Para ello basta usar dos veces el siguiente ejercicio.

Ejercicio 2.37. Sea N un subgrupo normal de un grupo G. Muestre que si $n \in N$ y $g \in G$, entonces $[g, n] \in N$. □

Ejercicio 2.38. Adapte el argumento de la prueba del Lema 2.35 para el caso a y b con soporte arbitrario.

Ejercicio 2.39. Adapte el argumento del Lema 2.35 para mostrar la siguiente afirmación: *Si N es un subgrupo normal de $[S_\infty, S_\infty]$, entonces N contiene al* doble conmutador $[[S_\infty, S_\infty], [S_\infty, S_\infty]]$.
(Ayuda: basta notar que los τ_i de la prueba pueden tomarse en $[S_\infty, S_\infty]$).

Ejercicio 2.40. Muestre que el doble conmutador $[[S_\infty, S_\infty], [S_\infty, S_\infty]]$ no es el grupo trivial.

Con esto podemos terminar la prueba del Teorema 2.28. Sea $G := S_\infty$. Como $G^{(2)} := [[S_\infty, S_\infty], [S_\infty, S_\infty]]$ es un subgrupo caracteriztico de $G^{(1)} := [S_\infty, S_\infty]$, se tiene $G^{(2)}$ es un subgrupo normal de G (Ejercicio 2.32). Como $G^{(2)}$ no es el grupo trivial, el Lema 2.35 nos dice que $G^{(2)} = G^{(1)}$. Finalmente, esta ultima igualdad, junto con el Ejercicio 2.39 nos dice que si N es un subgrupo normal no trivial de $G^{(1)}$, entonces $N = G^{(1)}$, es decir $G^{(1)}$ es un grupo simple. □

2.4. Estructura de grupos Abelianos finitos

Sea p un primo. Decimos que un grupo finito G es un **p-grupo** si $|G| = p^\alpha$ para algún $\alpha \geq 1$. En esta sección veremos que un grupo Abeliano finito se descompone como producto directo de sus p-grupos maximales. Este teorema de estructura ciertamente tambin sigue de los Teoremas de Sylow que veremos mas adelante, pero en el caso Abeliano el argumento es mucho mas nítido (y sirve como motivación de los Teoremas de Sylow) puesto que en este caso la aplicación $g \mapsto g^n$ es un homomorfismo de grupos.

Comenzamos con una observación sobre grupos finitos generales. Diremos que el **exponente** de un grupo G, que denotaremos por $Exp(G)$, es el menor entero n tal que $g^n = id$ para todo $g \in G$. Ciertamente cuando G es un grupo finito se tiene que $Exp(G)$ divide a $|G|$ (vea Teorema 1.43 (Lagrange)). Mas aún, si $|G| = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$ es la descomposición prima de $|G|$ (es decir, $2 \leq p_1 < p_2 < \ldots < p_\ell$ y $1 \leq \alpha_i$) entonces por el Teorema 1.81 (Cauchy) se tiene que $Exp(G) = p_1^{r_1} \cdots p_\ell^{r_\ell}$ con $1 \leq r_i \leq \alpha_i$.

El siguiente lema caracteriza el exponente de un grupo finito como el mínimo múltiplo común (MCM) de los órdenes de los elementos.

Lema 2.41. *Suponga que G es un grupo finito. Entonces $Exp(G) = \text{MCM}\{ord(g) \mid g \in G\}$.*

Demostración: Sea $K = \text{MCM}\{ord(g) \mid g \in G\}$. Claramente $g^K = id$ para todo $g \in G$ por lo que $Exp(G) \leq K$ por definición.

Para la recíproca basta notar que para todo $g \in G$, $Exp(G)$ es un múltiplo de $ord(g)$. En particular $K \leq Exp(G)$ por definición. □

En lo que queda de esta sección G denotará un grupo Abeliano finito. Igual que antes, la factorización prima de su cardinalidad será $|G| = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$ y la factorización prima de su exponente será $Exp(G) = p_1^{r_1} \cdots p_\ell^{r_\ell}$ con $1 \leq r_i \leq \alpha_i$. Dado d un entero cualquier, denotamos por E_d al homomorfismo

$$E_d : G \to G, \quad g \mapsto g^d.$$

Al kernel de E_d lo denotamos G_d y a la imagen de E_d la denotamos por $E_d(G)$. Note que el Teorema de Cauchy implica que d es comprimo con $|G|$ exactamente cuando $G_d = \{id\}$. De especial importancia para nosotros es el caso $d = p_i^{r_i}$ pues en este caso el homomorfismo E_d descompone al grupo G es producto directo. Mas precisamente tenemos

Lema 2.42. El primo p_i no divide a $|E_{p_i^{r_i}}(G)|$. Mas aún, $G \simeq G_{p_i^{r_i}} \times E_{p_i^{r_i}}(G)$.

Demostración: Veamos primero que p_i $(1 \leq i \leq \ell)$ no divide a $|E_{p_i^{r_i}}(G)|$. Supongamos en búsqueda de contradicción que si lo divide. Luego, por el teorema de Cauchy (Teorema 1.81) existe $g \in E_{p_i^{r_i}}(G)$ tal que $g^{p_i} = id$. Pero $g = h^{p_i^{r_i}}$ para algún $h \in G$. En particular, $ord(h) = p_i^{r_i+1}$, lo que no puede ser.

Ahora probamos que $G \simeq G_{p_i^{r_i}} \times E_{p_i^{r_i}}(G)$. Para empezar notamos que el teorema del isomorfismo (Teorema 1.60) tenemos que $G/G_{p_i^{r_i}} \simeq E_{p_i^{r_i}}(G)$. En particular $|G| = |G_{p_i^{r_i}}| \cdot |E_{p_i^{r_i}}(G)|$. Por otra parte, como p_i no divide a $|E_{p_i^{r_i}}(G)|$ se tiene que

$$G_{p_i^{r_i}} \cap E_{p_i^{r_i}}(G) = \{id\}.$$

Concluimos la prueba gracias al

Ejercicio 2.43. Suponga que G es un grupo cualquiera y que N y H son subgrupos normales de G tal que $N \cap H = \{id\}$. Entonces $HN \simeq H \times N$. □

El lema previo nos entrega el siguiente

Corolario 2.44. El subgrupo $G_{p_i^{r_i}}$ tiene cardinalidad $p_i^{\alpha_i}$ y el subgrupo $E_{p_i^{r_i}}(G)$ tiene cardinalidad $|G|/p_i^{\alpha_i}$.

En particular, podemos iterar el argumento ℓ-veces para encontrar el siguiente teorema de estructura de grupos Abelianos.

Teorema 2.45. *Sea G un grupo Abeliano de cardinalidad $p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$ y de exponente $Exp(G) = p_1^{r_1} \cdots p_\ell^{r_\ell}$. Entonces $G \simeq G_{p_1^{r_1}} \times \ldots \times G_{p_\ell^{r_\ell}}$, donde $G_{p_i^{r_i}} = Ker(E_{p_i^{r_i}})$ tiene cardinalidad $p_i^{\alpha_i}$ y exponente $p_i^{r_i}$.*

Una consecuencia que nos será útil mas adelante es el siguiente corolario.

Corolario 2.46. *Si G es un grupo Abeliano finito, entonces existe $g \in G$ tal que $Exp(G) = ord(g)$.*

Demostración: Supongamos $Exp(G) = p_1^{r_1} \cdots p_\ell^{r_\ell}$. Por el Teorema 2.45 tenemos que $G \simeq G_{p_1^{r_1}} \times \ldots \times G_{p_\ell^{r_\ell}}$, donde cada $G_{p_i^{r_i}}$ tiene exponente $p_i^{r_i}$.

Para empezar, afirmamos que existe $g_i \in G_{p_i^{r_i}}$ tal que $ord(g_i) = p_i^{r_i}$. En efecto por el Lema 2.41 sabemos que existe $h \in G$ tal que $ord(h) = p_i^{r_i} \cdot q$ con q coprimo con p_i. Esto implica que $h^q \in G_{p_i^{r_i}}$ tiene orden $p_i^{r_i}$.

Para terminar notamos que $g = g_1 \cdot g_2 \cdots g_\ell$ tiene orden $Exp(G)$. □

2.5. Los teoremas de Sylow (1870)

Los teoremas de Sylow son una herramienta fundamental a al hora de comprender las posibles estructuras de grupo en un conjunto de cardinalidad dada. Una noción importante a la hora de enunciar (y probar) los teoremas de Sylow es la de p-grupo.

Definición 2.47. Sea p un primo. Decimos que un grupo (no necesariamente finito) es un p-grupo si todo elemento $g \in G$ tiene orden alguna potencia de p. Notar que en caso de que G sea un grupo finito esto implica (por el Teorema de Cauchy) que $|G| = p^n$.

Proposición 2.48. *Sea G un p-grupo finito acutando en un espacio finito X. Entonces vale*

$$|X| \equiv |Fix_X(G)| \pmod{p},$$

donde $Fix_X(G) := \{x \in X \mid G.x = x\}$ es el conjunto de puntos fijos por G.

Dem: En efecto, sabemos que en general $|X| = \sum_{\text{orbitas}} |Orb_G(x)|$, y que la cardinalidad de una órbita divide a la del grupo. Luego, en un p-grupo la cardinalidad de una orbitas es o bien 1 (y este caso es precisamente cuando la órbita es fija) o bien divisible por p. La proposición sigue pasando modulo p. □

Teorema 2.49 (Sylow I)**.** *Sea p un primo y G un grupo finito digamos de cardinalidad $p^k m$, donde p no divide a m. Entonces, existe $H \leq G$ con $|H| = p^k$. A un tal H lo llamamos un p-subgrupo de Sylow.*

Dem: Probaremos algo mas fuerte, a saber, que *para todo $i \leq k$ existe un $H \leq G$ con $|H| = p^i$.* La prueba es por inducción.

Comenzamos invocando el Teorema de Cauchy, que nos dice que G contiene un subgrupo de orden p. Llamemoslo H_1. Ahora, tomemos $i < k$ y supongamos como hypotesis de inducción que existe H_i un subgrupo de orden p^i. Consideramos la accion por traslacion a izquierda de H_i en G/H_i, las clases laterales de H_i. La Proposición 2.48 nos dice que

$$|G/H_i| \equiv |Fix_{G/H_i}(H_i)| \pmod{p}.$$

Como $i < k$, la parte izquierda es divisible por p. Mas an, como H_i fija su propia clase lateral se tiene que deben existir al menos p clases laterales que son fijas por H_i. Pero que H_i fije una clase lateral gH_i, quiere decir que

$$hgH_i = gH_i \ \ \forall h \in H_i,$$

lo que equivale a decir que

$$g^{-1}hg \in H_i \ \ \forall h \in H_i,$$

es decir $g \in Norm_G(H_i) = \{g \in G \mid gH_ig^{-1} = H_i\}$ el normalizador de H_i. Concluimos entonces que

$$Fix_{G/H_i}(H_i) = \{gH_i \mid g \in Norm_G(H_i)\}.$$

Pero ciertamente $\{gH_i \mid g \in Norm_G(H_i)\} = Norm_G(H_i)/H_i$, por lo tanto $\mid Norm_G(H_i)/H_i \mid$ es divisible por p. Ahora, como $H_i \lhd Norm_G(H_i)$, nuevamente por el Teorema de Cauchy, sabemos que existe $\overline{H} \leq Norm_G(H_i)$ subgrupo de cardinalidad p. Tomando la imagen inversa, encontramos $H \leq G$ tal que $H_i \leq H$ y $[H : H_i] = p$. Luego $H_{i+1} = H$ tiene cardinalidad p^{i+1}. □

Teorema 2.50 (Sylow II)**.** *Sean P y Q dos p-subgrupos de Sylow de un grupo finito G. Entonces, P y Q son conjugados.*

Dem: Considere la accion por multiplicacion a izquierda de Q en G/P. La Proposición 2.48 nos dice que

$$|G/P| \equiv |Fix_{G/P}(Q)| \pmod{p}.$$

Puesto que el lado izquierdo no es divisible por p, concluimos que existe algun punto fijo $gP \in G/P$ para la acción de Q. Esto dice que para todo $q \in Q$, $qgP = gP$, de donde sigue que $g^{-1}qg \in P$ para todo $q \in Q$. Concluimos entonces que $g^{-1}Qg \subset P$. La igualdad sigue de la finitud de P y Q. □

Corolario 2.51. *Sea G es un grupo finito, p un primo que divide a $|G|$ y P un p-Sylow de G. Entonces vale que $P \lhd G$ si y solo si P es el unico p-Sylow de G.*

Teorema 2.52 (Sylow III)**.** *Para p primo, sea $n_p \in \mathbb{N}$ la cantidad de p-subgruops de Sylow en un grupo finito G, digamos $|G| = p^k m$, donde p no divide a m. Entonces*

1. *$n_p = 1 \pmod p$,*
2. *n_p divide a m,*
3. *$n_p = [G : Norm_G(P)]$, donde P es cualquier p-subgrupo de Sylow.*

Dem: Probamos 1). Sea P un p-subgruop de Sylow. Considere la accion por conjugación de P en $Syl_p(G)$, el conjunto de todos los p-subgrupos de Sylow. Nuevamente por la Proposición 2.48, tenemos que

$$n_p = |Syl_p(G)| \equiv |Fix_{Syl_p(G)}(P)| \pmod p.$$

Afirmamos que el unico p-Sylow fijo por P es P. En efecto, si $Q \in Syl_p(G)$ es fijo por P, tenemos que $P \leq Norm_G(Q)$. Pero Q es un subgrupo normal de $Norm_G(Q)$. Pero, por otro lado, por el Teorema de Sylow II aplicado a $Norm_G(Q)$, tenemos que P y Q son conjugados dentro de $Norm_G(Q)$, lo que contradice la normalidad de Q en $Norm_G(Q)$. Esto prueba que $Q = P$. Concluimos entonces que $|Fix_{Syl_p(G)}(P)| = 1$, y por ende que $n_p \equiv 1 \pmod p$.

Para probar 3), consideramos la accion por conjugación de G en $Syp_p(G)$. Pro el Teorema de Sylow II, esta accion tiene una sola orbita. Luego tenemos que

$$n_p = |Syl_p(G)| = [G : Stab_G(P)].$$

Pero para esta accion, el estabilizador de P claramente es $Norm_G(P)$. Luego $n_p = [G : Norm_G(P)]$.

El punto 2) sigue inmediatamente del 3). En efecto

$$m = [G : P] = [G : Norm_G(P)][Norm_G(P) : P] = n_p[Norm_G(P) : P].$$

Comparar con un diagrama. □

Grupos de cardinalidad $p \cdot q$: En este párrafo usamos los resultados de Sylow para probar el

Teorema 2.53. *Si $p \leq q$ son dos numeros primos tales que p no divide a $q - 1$, entonces todo grupo de cardinalidad $p \cdot q$ es Abeliano. Si además $p \neq q$, entonces el grupo es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_q$.*

Observación 2.54. La hipótesis de que p no divida a $q-1$ es necesaria pues, por ejemplo, S_3 es un grupo de cardinalidad $2 \cdot 3$ que no es un grupo Abeliano.

Demostración del Teorema 2.53: El caso $p = q$ fue tratado en el Teorema 1.86, por lo que supondremos que $p < q$.

Para la prueba usamos la Proposición **??**.

Por Sylow I existen H_p un p-Sylow y H_q un q-Sylow. Por Sylow III, $n_q = 1$, o sea $H_q \lhd G$. Observamos que $H_q \cap H_p = \{id\}$, lo que implica que $H_q H_p = G$. De este modo, para ver que $G \simeq H_q \times H_p$, basta probar que $\alpha : H_p \to Aut(H_q)$, el automorfismo inducido por conjugación, es trivial. Pero, si α no fuera trivial, tendriamos que su imagen tiene cardinalidad p, que por hypotesis no divede a $q-1$, la cardinalidad de $Aut(H_q) \simeq (\mathbb{Z}/q\mathbb{Z})^*$. □

2.6. Fabricando nuevos grupos

Producto semi-directo de grupos. Sean H y G grupos y $\alpha : G \to Aut(H)$ un homomorfismo. Denotamos por α_g al automorfismo $\alpha(g)$ y definimos $H \rtimes_\alpha G$, el producto semi-directo de H por G via α como sigue: El conjunto subyacente a $H \rtimes_\alpha G$ es $H \times G$ y la estructura (i.e. operación) de grupo viene dada por

$$(h, g)(h', g') := (h\alpha_g(h'), gg').$$

Proposición 2.55. *$H \rtimes_\alpha G$ es un grupo.*

Demostración: Por definición la operación de $H \rtimes_\alpha G$ es cerrada. Para chequear la asociatividad notamos que puesto que α es homomorfismo se tiene que $\alpha_{gg'} = \alpha_g \circ \alpha_{g'}$ y por tanto

$$\begin{aligned}[(h, g) \cdot (h', g')] \cdot (h'', g'') &= (h\alpha_g(h'), gg') \cdot (h'', g'') \\ &= (h\alpha_g(h')\alpha_{gg'}(h''), gg'g'') \\ &= (h, g) \cdot (h'\alpha_{g'}(h''), g'g'') = (h, g) \cdot [(h', g') \cdot (h'', g'')].\end{aligned}$$

Del mismo modo se tiene que el neutro de $H \rtimes G$ es (id_H, id_G) y el inverso de (h, g) es $(h, g)^{-1} = (\alpha_{g^{-1}}(h^{-1}), g^{-1})$. □

Observación 2.56. Notamos que $H \rtimes_\alpha G$ contiene copias isomorfas de H y G, a saber, (H, id) e (id, G). Mas aún, esta copia de H es normal en $H \rtimes G$ y la acción por conjugación de (la copia) de G recupera el automorfismo α. Mas precisamente se tiene que

$$(id, g)\,(h, id)\,(id, g)^{-1} = (\alpha_g(h), id).$$

En particular, si la imagen de α es trivial, entonces $H \rtimes_\alpha G \simeq H \times G$.

El siguiente ejercicio muestra que la descomposición en producto semi-directo aparece en la naturaleza (compare con Ejercicio 1.63).

Ejercicio 2.57. Muestre que si $N \lhd G$ y $H \leq G$ son tales que $H \cap N = \{id\}$, entonces $NH \simeq N \rtimes_\alpha H$, donde α es el homomorfismo de H en $Aut(N)$ inducido por la conjugacion de H en N.

Observación 2.58. En muchos casos tomaremos $N \rtimes_\alpha C$ con C un subgrupo cíclico, digamos generado por $c \in C$. En este caso, puesto que el homomorphismo $\alpha : C \to Aut(N)$ está completamente determinado por la imagen del generador, se sueleescribir $N \rtimes_{\alpha(1)} C$ para referirse a $N \rtimes_\alpha C$.

Por ejemplo, usualmente la descomposición en producto semi-directo del grupo de Heissemberg discreto se denota por $\mathcal{H} \simeq \mathbb{Z}^2 \rtimes_A \mathbb{Z}$ donde $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Ejercicio 2.59. Sea $\mathcal{H}$ es grupo de matrices 3x3, triangulares superiores con unos en la diagonal. Muestre que $\mathcal{H} \simeq \mathbb{Z}^2 \rtimes_A \mathbb{Z}$ donde $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Ejemplo 2.60. El ejemplo mas pequeño (en cardinalidad) de descomposicón no trivial en producto semi-directo es $N \rtimes H$ con $N \simeq \mathbb{Z}_3$ y $H \simeq \mathbb{Z}_2$.

En efecto en este caso $Aut(\mathbb{Z}_3) \simeq \mathbb{Z}_3^* \simeq \mathbb{Z}_2$ es no trivial y existe un incrustamiento de $\mathbb{Z}_2$ en $Aut(\mathbb{Z}_3)$. Por ejemplo podemos definir $\alpha(1)$ como la inversión de $\mathbb{Z}_3$: $[n] \mapsto [-n]$. De este modo $\mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_2$ es un grupo no Abeliano.

Por otro lado, si en el grupo simétrico S_3 tomamos $N = \langle (123) \rangle$ y $H = \langle (12) \rangle$, se tiene que $N \lhd S_3$ y $(12)(123)(12) = (132) = (123)^{-1}$, por lo que el Ejercicio 2.57 implica

$$S_3 \simeq \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_2.$$

En general no es fácil decidir cuándo dos estructuras en producto semi-directo son isomorfas. De hecho, es posible que productos semi-directos sean isomorfos a productos directes, vea Ejercicio 2.65. Podemos sin embargo, dar algunas condiciones suficientes para tener la isomorfía.

Definición 2.61. Para $i = 1, 2$, sean $\alpha_i : H \to Aut(N)$ dos homomorfismos. Decimos que α_1 y α_2 son **conjugados** si existe $\psi \in Aut(N)$ tal que $\psi \circ \alpha_1(h) = \alpha_2(h) \circ \psi$ para todo $h \in H$.

Proposición 2.62. *Si $\alpha, \beta : H \to Aut(N)$ son dos homomorfismos conjugados, entonces $N \rtimes_\alpha H \simeq N \rtimes_\beta H$.*

Demostración: Sea $f \in Aut(N)$ tal que $f \circ \alpha_h = \beta_h \circ f$ para todo $h \in H$. Definimos $\varphi : N \rtimes_\alpha H \to N \rtimes_\beta H$ por

$$\varphi : (n, h) \mapsto (f(n), h).$$

Puesto que f es un automorfismo se tiene que φ es una biyección, por lo que solo hay que mostrar que φ es un homomorfismo. Para ello notamos que

$$\begin{aligned} \varphi((n,h) \cdot (n',h')) &= \varphi((n\alpha_h(n'), hh')) \\ &= (f(n)f(\alpha_h(n')), hh') \\ &= (f(n)\beta_h(f(n')), hh') \\ &= (f(n), h) \cdot (f(n'), h') = \varphi((n,h)) \cdot \varphi((n',h')). \end{aligned}$$

Por lo tanto φ es un isomorfismo. □

Un segundo criterio para la isomorfía es

Proposición 2.63. *Sea $f \in Aut(H)$ y $\alpha : H \to Aut(N)$ un homomorfismo. Entonces $N \rtimes_\alpha H \simeq N \rtimes_{\alpha \circ f} H$.*

Demostración: En efecto en este caso $\varphi : N \rtimes_{\alpha\circ f} H \to N \rtimes_\alpha H$ dado por

$$(n, h) \mapsto (n, f(h))$$

es un isomorfismo, pues claramente es biyectivo y es también un homomorfismo pues

$$\begin{aligned}\varphi((n,h)\cdot(n',h')) &= \varphi((n\alpha_{f(h)}(n'), hh')) \\ &= (n\alpha_{f(h)}(n'), f(hh')) \\ &= (n, f(h))\cdot(n', f(h')) = \varphi((n,h))\cdot\varphi((n',h')).\end{aligned}$$

□

Ejemplo 2.64. Sea $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_2)$. Claramente $A^3 = Id$ por lo que podemos formar los grupo $G_1 = (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_A \mathbb{Z}_3$ y $G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{A^2} \mathbb{Z}_3$.

Se sigue, tanto de la Proposición 2.62 como de la Proposición 2.63, que los grupos G_1 y G_2 son isomorfos. En efecto, basta notar que A y A^2 son conjugados en $GL_2(\mathbb{Z}_2) = Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ (por ejemplo por la transformación que permuta los elementos de la base canónica), o que $x \mapsto x^2$ es un automorfismo de $\mathbb{Z}_3$.

Concluimos la sección con con un ejercicio que muestra que un producto semidirecto bien puede ser secretamente un producto directo.

Ejercicio 2.65. Sea S_3 el grupo simétrico, $n = (1, 2) \in S_3$ una transposición y $C_n \in Aut(S_3)$ la conjugación por n. Muestre que $S_3 \rtimes_{C_n} \mathbb{Z}_2 \simeq S_3 \times \mathbb{Z}_2$.

Producto en corona. Dados G y H grupos, definimos H^G como el conjunto de *funciones* de soporte finito[12] de $f : G \to H$. Note que H^G es un grupo bajo el producto punto a punto $(f_1 \cdot f_2)(x) = f_1(x) \cdot f_2(x)$. Mas aún, este grupo es isomorfo a $\bigoplus_{g\in G} H$ con el producto coordenada a coordenada.

Ejercicio 2.66 (Representación de Koopman)**.** Sean G y H grupos, y H^G como arriba.

1. Muestre que para todo $g \in G$, la aplicación $\sigma_g : H^G \to H^G$ dada por $\sigma_g(f) : x \mapsto f(g^{-1}x)$ es un automorfismo de H^G.
2. Muestre que $\sigma : G \to Aut(H^G)$ dada por $g \mapsto \sigma_g$ es un homomorfismo. A este homomorfismo (asi como algunas de sus variantes) se le conoce como la representación de Koopman.

Definimos el **producto en corona** de H por G como $H \wr G := H^G \rtimes_\sigma G$, donde σ es la representacón de Koopman del Ejercicio 2.66. Claramente $H \wr G$ es un grupo que contiene a G y a H^G (y por lo tanto también contiene a H).

El producto en corona es útil para fabricar ejemplos patológicos de grupos finitamente generados. En efecto tenemos

[12]En este caso, por soporte de $f : G \to H$ debemos entender $\{g \in G \mid f(g) \neq id_H\}$.

Ejercicio 2.67. Sean G y H grupos finitamente generados no triviales.

1. Muestre que si G es infinito, entonces H^G no es finitamente generado.
2. Muestre sin embargo que $H \wr G$ es finitamente generado.

Ejemplificamos esta construcción con un grupos famoso.

Ejemplo 2.68 (El grupo de farolero)**.** El grupo $G = \mathbb{Z}_2 \wr \mathbb{Z}$ se conoce como el grupo del farolero (*lamplighter group*, en inglés). La razón es que este grupo admite una acción que recuerda la labor de los antiguos faroleros que prendian y apagaban las farolas de las calles.

Concretamente sea $X = \mathbb{Z} \times \{0, 1\}$. Podemos pensar que un elemento de X es una calle con farolas ($\mathbb{Z}$) donde algunas de sus farolas estn encendidas (i.e. etiquetadas con 1) o apagadas (i.e. etiquetadas con 0). Note que $\mathbb{Z}_2^{\mathbb{Z}}$ se identifica naturalmente con el subconjunto de X consistente en las configuraciones con solo un número finito de farolas encendidas. En particular (bajo la topología adecuada) $\mathbb{Z}_2^{\mathbb{Z}}$ es un subconjunto *denso* de X y por lo tanto la acción por multipliación de $\mathbb{Z}_2^{\mathbb{Z}}$ en si mismo se extiende a una acción de $\mathbb{Z}_2^{\mathbb{Z}}$ en X.

Por ejemplo, si denotamos por $e_i : \mathbb{Z} \to \mathbb{Z}_2$ la función que vale 0 en toda entrada distinta de i y $e_i(i) = 1$, entonces la acción de $e_i \in \mathbb{Z}_2^{\mathbb{Z}}$ en X es precisamente cambiar el estado de la farola i-esima.

Por otro lado el factor $\mathbb{Z}$ de $G = \mathbb{Z}_2 \wr \mathbb{Z}$ actúa por precomposición. Asi, si denotamos por c el generador de $\mathbb{Z}$ se tiene que $c.e_i = e_{i+1}$. De este modo, el elemento $(e_0, c) \in \mathbb{Z}_2 \wr \mathbb{Z}$, y sus potencias, lo identificamos al farolero que va caminando por la calle prendiendo o apagando las farolas que ve pasar.

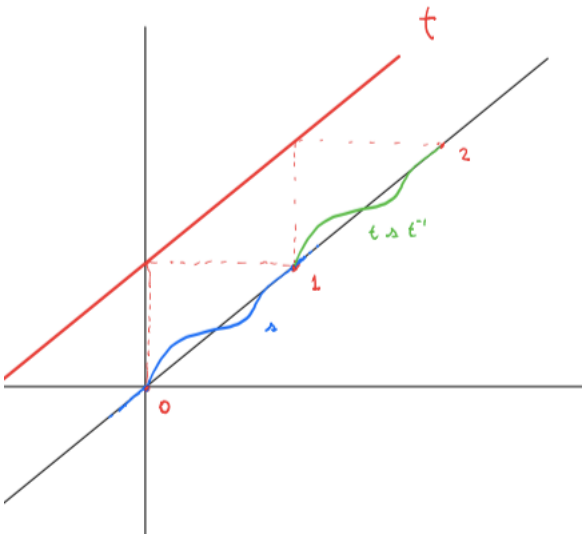


Figura 8: Representación por homeomorfismos de la recta del grupo $\mathbb{Z} \wr \mathbb{Z}$. En azul el homeomorfismo s y en verde el su conjugado $t \circ s \circ t^{-1}$.

Ejercicio 2.69 ($\mathbb{Z} \wr \mathbb{Z}$ como homeomorfismos de $\mathbb{R}$)**.** Denotamos por $\mathsf{Homeo}(\mathbb{R})$ al grupo de homeomorfismos de $\mathbb{R}$. Sea $t \in \mathsf{Homeo}(\mathbb{R})$ la traslación $t(x) = x + 1$ y $s \in \mathsf{Homeo}(\mathbb{R})$ un homeomorfismo no trivial soportado dentro de $(0, 1)$. Sea $W = \langle t, s \rangle$ el grupo de homeomorfismos generado por t y s. Muestre que $W \simeq \mathbb{Z} \wr \mathbb{Z}$. (Ayuda, use el Ejercicio 2.57.)

2.7. Clasificación de grupos de orden 12

Sea G un conjunto de orden 12. En esta sección clasificamos todas las posibles estructuras de grupo posibles en G (modulo isomorfismo).

Sea H_2 el 2-Sylow y H_3 el 3-Sylow de G. Oservamos que n_3 puede ser 1 o 4, y si es 4, entonces solo cabe un unico 2-Sylow.

- Luego, siempre hay un Sylow normal, y por ende siempre vale que $G = H_3H_2$. Asi, en general se tiene que

$$G \simeq H_2 \rtimes H_3 \text{ o bien } G \simeq H_3 \rtimes H_2.$$

El punto crucial es entender $Aut(H_p)$, el grupo de automorfismos de un Sylows dado.

Caso $H_2 \lhd G$**:** Este caso se divide en dos casos:

1. $H_2 \simeq \mathbb{Z}_4$: En este caso tenemos que H_3 conmuta con H_2, luego $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$. En efecto, basta probar que $Aut(\mathbb{Z}_4)$ no contiene elementos de orden 3. Esto ultimo es fácil si notamos que $\varphi(1)$ puede ser 1 o 4. Luego $\varphi^2(1) = 1$. Por lo tanto

$$G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3.$$

2. $H_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$: Para entender $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$, la observacion crucial es que $\mathbb{Z}_2 \times \mathbb{Z}_2$ es un espacio vectorial sobre $\mathbb{Z}_2$ y un automorfismo de $\mathbb{Z}_2 \times \mathbb{Z}_2$ corresponde a una transformación lineal de este.

   Observamos que un automorfismo φ *manda base en base*. Luego si escribimos $\mathbb{Z}_2 \times \mathbb{Z}_2$ como $\langle a \rangle \times \langle b \rangle$ entonces $\varphi(a)$ puede ser a o b o $a + b = (a, b)$ y $\varphi(b)$ puede ser cualquiera de los otros dos elementos no nulos de $\mathbb{Z}_2 \times \mathbb{Z}_2$. Luego $|Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6$. Es mas, el analisis anterior muestra que $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3$. Luego, modulo conjugacion (i.e. cambio de base) existe un unico automorfismo α de $\mathbb{Z}_2 \times \mathbb{Z}_2$ de orden tres. Luego, en este o bien G es Abeliano, o bien

$$G \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\alpha \mathbb{Z}_3.$$

   Ahora, bien podría ser que este caso contuviera una o mas clases de isomorfimso. Por ejemplo,

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_A \mathbb{Z}_3 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{A^2} \mathbb{Z}_3,$$

   donde identificamos $\alpha(1) = A$, con

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

   Esto se isomorfismo tiene, en este caso particular, dos explicaciones.

a) $M_2 : x \mapsto 2x$ es un automorfismo de $\mathbb{Z}_3$. Luego (Id, M_2) es un isomorfismo.

b) A y A^2 con **conjugados** en $GL_2(\mathbb{Z}_2)$. Mas generalmente tenemos

Proposición 2.70. *Para $i = 1, 2$, sea $\alpha_i : G \to Aut(H)$ dos homomorfismos* **conjugados***, es decir existe $\psi \in Auth(H)$ tal que $\psi \circ \alpha_1(g) = \alpha_2(g) \circ \psi$ para todo $g \in G$. Entonces $H \rtimes_{\alpha_1} G \simeq H \rtimes_{\alpha_2} G$ via $(h, g) \mapsto (\psi(h), g)$.*

Caso $H_3 \lhd G$: En este caso $Aut(\mathbb{Z}_3) \simeq \mathbb{Z}_3^* \simeq \mathbb{Z}_2$ admite una imagen no trivial de $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1. Si $H_2 \simeq \mathbb{Z}_4$, entonces existe un unico homomorfismo $\mathbb{Z}_4 \to Aut(\mathbb{Z}_3) \simeq \mathbb{Z}_2$ (multiplicar por 2!!). Luego G es Abeliano o

$$G \simeq \mathbb{Z}_3 \rtimes_{(2)} \mathbb{Z}_4. \text{ (explicar notacion).}$$

2. Si $\alpha : H_2 \to \mathbb{Z}_3*$ es no trivial, entonces $G \simeq H_3 \rtimes_\alpha H_2$ (basta comparar las cardinalidades).

   a) Si $H_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces nuevamente modulo cambiode base en $\mathbb{Z}_2 \times \mathbb{Z}_2$ existe un unico homomorfismo de $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 = Aut(\mathbb{Z}_3)$, a saber. matar una coordenada. En este caso o bien G es Abeliano o bien

$$G \simeq \mathbb{Z}_3 \rtimes_\alpha (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq (\mathbb{Z}_3 \rtimes_{(2)} \mathbb{Z}_2) \times \mathbb{Z}_2.$$

En conclusion: hay 5 clases de isomorfia para grupos de orden 12. Veremos ahora a que grupos *concretos* de orden 12 corresponden estas descomposiciones abstractas.

Aparte de los grupos Abelianos, tenemos los siguientes grupos de orden 12.

$$A_4\,,\ D_6\,,\ S_3 \times \mathbb{Z}_2.$$

A_4: En este caso el 2-Sylow es normal e isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ (luego hay 4 3-Sylow (verlos)). La unica opcion es

$$A_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3.$$

D_6: En este caso el subgrupo $\langle R^2 \rangle \simeq \mathbb{Z}_3$ es normal, luego el es el unico 3-Sylow y hay 3 2-Sylows. Los 2-Sylow son de la forma $\langle R^3, \tau \rangle$ con τ cualquier reflexion (ver que las reflexiones son 2 clases de conjugacion). Asi, aparecen naturalmente 6 2-Sylows!! (lo que no puede ser), pero en realidad estamos contando dos veces cada uno: ver que pasa al hacer $R^3\tau$ (cambio de base!).

$$D_4 \simeq (\mathbb{Z}_3 \times \mathbb{Z}_2) \rtimes_{(-1)} \mathbb{Z}_2 \simeq (\mathbb{Z}_3 \rtimes_{(-1)} \mathbb{Z}_2) \times \mathbb{Z}_2 \simeq S_3 \times \mathbb{Z}_2.$$

El caso $G \simeq \mathbb{Z}_3 \rtimes_{(2)} \mathbb{Z}_4$ no es un grupo conocido.

2.8. Simplicidad de A_5 usando Sylow

En esta tarea vamos a usar los Teoremas de Sylow para probar que A_5, el subgrupo alternante de S_5 es simple. Recuerde que $A_5 = Ker(sgn)$ es el subgrupo de permutaciones pares y por lo tanto $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$.

Si p es un primo, denotamos por P_p a un p-Sylow y por n_p, la cantidad de p-Sylows en A_5.

A) Calentamiento

1. Muestre que todo 3-ciclo (i.e. una permutación de la forma (abc)) vive en A_5, y que lo mismo ocurre para todo 5-ciclo.
2. Muestre que $P_5 \simeq \mathbb{Z}/5\mathbb{Z}$ y $P_3 \simeq \mathbb{Z}/3\mathbb{Z}$.
3. Muestre que $n_3 \in \{1, 4, 10\}$ y $n_5 \in \{1, 6\}$.
4. Muestre que, para A_5, se tiene que $n_3 = 10$ y $n_5 = 6$.

B) Suponga, en busqueda de una contradicción, que $N \lhd A_5$ es un subgrupo normal no trivial.

1. Suponga que 5 divide a $|N|$.
   a) Muestre que N contiene a todos los 5-Sylows. Concluya que entonces $|N| \geq 24 = 6 \cdot (5 - 1)$.
   b) Muestre que si $|N| \geq 24$, entonces se tiene que $|N| = 30$.
   c) Muestre que si $|N| = 30$ entonces N contiene a todos los 3-Sylows.
   d) Concluya finalmente que entonces N contiene mas de 30 elementos y por lo tanto $N = A_5$.
2. Suponga que 3 divide a $|N|$.
   a) Muestre $|N|$ contiene a todos los 3-Sylows, y por lo tanto $|N| \geq 21$. Concluya entonces que $|N| = 30$.
   b) Concluya, como antes, que $N = A_5$.

C) Remate: note que solo falta analizar el caso $|N|$ es 4 o 2.

1. Caso $|N| = 4$.
   a) Muestre $H = \{id, (12)(34), (13)(24), (14)(23)\}$ es un 4-Sylow (en particular, muestre que H es un subgrupo de A_5).
   b) Muestre que H **no** es un subgrupo normal de A_5. Concluya que el caso $|N| = 4$ es imposible.
2. Caso $|N| = 2$. Muestre que en este caso $N = \langle (ab)(cd) \rangle$ (escritura en ciclos disjuntos). Muestre que en tal caso, N no puede ser normal en A_5.

2.9. El grupo libre y el lema del ping pong

Presentaciones de grupo: Una presentación de un grupo es una expresion de la forma

$$\Big\langle a_1,\ a_2, \ldots \mid r_1,\ r_2, \ldots \Big\rangle, \tag{4}$$

donde cada r_i es una *palabra* en las *letras* $a_1, a_2, \ldots$. Por definición el grupo con presentacion (4) es el grupo

$$G = F(a_1,\ a_2, \ldots)/N(r_1,\ r_2, \ldots),$$

donde $F(a_1, a_2, \ldots)$ es el **grupo libre** sobre los a_i's y $N(r_1,\ r_2, \ldots) := \langle\langle r_1,\ r_2, \ldots\rangle\rangle$, es el subgrupo normal generado por los r_i's. Los a_i se llaman **generadores** y los r_i se llaman **relaciones** pues, en el cociente, cada palabra que puede ser escrita como producto de relaciones representa el elemento trivial de G.

Decimos que un grupo es **finitamente presentable** si admite una presentacion con finitos generadores y finitas relaciones.

Construcción del grupo libre: Construiremos F_2 y quedara de ejercicio el caso general.

Sea $W(x, y)$ el conjunto de todas las palabras en x, y, x^{-1} e y^{-1}. Este conjunto es cerrado bajo yuxtaposicion: $(u, v) \mapsto u*v$. Además, $W(x, y)$ posee un neutro para esta operación, a saber, ϵ, la palabra vacía. El problema es que $W(x, y)$ no tiene inversos. Para hacer aparecer los inversos, debemos cocientar por una relacion de equivalenca adecuada. Quisieramos que $xx^{-1} = x^{-1}x = \epsilon$, lo mismo para y e y^{-1}.

Introducimos la siguente relación de equivalencia. Decimos que dos palabras u y v estan relacionadas: $u \sim v$ si v se puede obtener de u usando una cantidad finita de los siguientes cambios:

1. Insertar xx^{-1}, $x^{-1}x$, yy^{-1} o $y^{-1}y$ al comienzo, al final o entremedio de las letras de u.

2. Borrar xx^{-1}, $x^{-1}x$,yy^{-1} o $y^{-1}y$.

Veamos que $\sim$ es una relacion de equivalencia. Claramente $u \sim u$. Ademas $u \sim v$ implica $v \sim u$ pues los movimientos 1 y 2 son inversos uno del otro. Finalmente $u \sim v$ y $v \sim w$ implica que puedo pasar por un numero finito de movimientos de u a v y luego de v a w, lo que prueba que $u \sim w$. Además, notamos que esta relacion se lleva bien con la yuxtaposicion. Precisamente se tiene que

$$u \sim v\,,\ u' \sim v' \Rightarrow u * u' \sim v * v'. \tag{5}$$

Denotamos por $\bar{u}$, la clase de equivalencia de u. Tenemos

Proposición 2.71. *$W(x, y)/\sim$ es un grupo bajo la operación $\bar{u}\bar{v} := \overline{u\,v}$. Denotaremos a este grupo por F_2, el grupo libre a dos generadores.*

Dem: Por definicion, la operación es cerrada, y no depende del representante por (5).

La asociatividad sigue de la asociatividad de la yuxtaposición.

el neutro es $\bar{\epsilon}$.

el inverso sigue tb. □

Hemos construido el grupo libre F_2. Como ejercicio queda la construcción del grupo libre en n generadores.

Convencion: De ahora en mas, a los elementos de un grupo libre, por ejemplo $F(a_1, a_2, \ldots)$, los designaremos por palabras en $a_i^{\pm 1}$, y no por su clase de equivalencia. Tendremos el cuidado eso si, de identificar palabras en una misma clase de equivalencia, por ejemplo $a_1 a_1^{-1} a_2 = a_2$.

El grupo F_2 posee una interesante propiedad que es la razón de porque el apodo *libre*.

Teorema 2.72. *Sea G un grupo que admite un sistema generador con dos elementos. Entonces, existe $\varphi : F_2 \to G$, un homomorfismo sobreyectivo. En particular $G \simeq F_2/ker(\varphi)$.*

El teorema sigue directamente del siguiente

Lema 2.73. *Sea F_2 el grupo libre sobre $\{x, y\}$. Sea G un grupo cualquiera y $f : \{\bar{x}, \bar{y}\} \to G$ una función. Entonces, existe homomorfismo $\varphi : F_2 \to G$ que extiende a f, esto es $\varphi(\bar{x}) = f(\bar{x})$ y $\varphi(\bar{y}) = f(\bar{y})$.*

Dem de Lema 2.73: Vamos a definir φ en una palabra de $W(x, y)$, y ver que esto tiene las propiedades que necesitamos.

Sea $w = w(x, y)$ una palabra cualquiera en las letras $x^{\pm 1}$ e $y^{\pm 1}$. Definimos $\varphi(w)$ simplemente como $w(f(\bar{x}), f(\bar{y}))$, es decir, la misma palabra pero en las letras $f(\bar{x})^{\pm 1}$ y $f(\bar{y})^{\pm 1}$. Observamos lo siguiente: Si $w \sim w'$ entonces $\varphi(w) = \varphi(w')$.

En efecto $w \sim w'$ implica que puedo pasar de una a la otra mediante un numero finito de cambios 1 y/o 2 descritos mas arriba. Luego basta probar que $\varphi(w) = \varphi(w')$ en el caso que un solo cambio me lleva de w a w'. Y esto es muy facil pues en cualquier grupo $f(\bar{x}) f(\bar{x})^{-1}$ representa siempre el elemento trivial.

Esto nos dice que en realidad φ esta definida en $F_2 = W(x, y)/\sim$: $\varphi(\overline{w(x, y)}) = w(f(\bar{x}), f(\bar{y}))$. Esta definicion ciertamente extiende a f pues $\varphi(\bar{x}) = f(\bar{x})$, $\varphi(\bar{y}) = f(\bar{y})$.

Veamos que φ es homomorfismo.

$$\varphi(\overline{u(x,y)}\ \overline{v(x,y)}) = \varphi(\overline{u(x,y) * v(x,y)}) = u(f(x), f(y))\, v(f(x), f(y)) = \varphi(\overline{u(x,y)})\varphi(\overline{v(x,y)}).$$

□

Observación 2.74. $F_1 \simeq \mathbb{Z}$.

Observación 2.75. Claramente F_2 se mete en F_n para $n \geq 2$. Pero un teorema de Schreier dice que F_n se mete en F_2 para todo n. Por ejemplo en F_2 el grupo generado por a, bab^{-1} y b^2ab^{-2} es isomorfo a F_3.

Ejercicio 2.76. (Tarea) Decimos que una palabra es reducida si no contiene $\ell\ell^{-1}$ con $\ell \in \{x^{\pm 1}, y^{\pm 1}\}$. Pruebe que para todo $w \in W(x,y)$, existe $w' \sim w$ con w' reducida.

Lema 2.77. *Sean $A^+, A^-, B^+, B^- \subseteq X$ subconjuntos disjuntos y $a, b \in Sym(X)$ tales*

$$a(X \setminus A^-) \subseteq A^+, a^{-1}(X \setminus A^+) \subseteq A^-,$$

$$b(X \setminus B^-) \subseteq B^+, b^{-1}(X \setminus B^+) \subseteq B^-.$$

Entonces, $\langle a, b\rangle \simeq F_2$.

Demostración: Basta probar que toda palabra reducida en a y b (y sus inversos) actua no trivialmente en X. □

Ejemplo 2.78. Matricies hyperbólicas actuando en $\mathbb{R}P^1$. O parabolicas.

Ejemplo 2.79. F_2 actuando sobre si mismo por traslaciones.

Ejemplo 2.80. Aunque el grupo sea libre, no siempre hay un ping-pong evidente. Por ejemplo

$$a = \begin{pmatrix} \frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 \\ -\frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{2\sqrt{2}}{3} \\ 0 & -\frac{2\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}$$

generan un grupo libre. (hablar de la paradoja de Banach y Tarski)

3. Anillos y Cuerpos

3.1. Definiciones y Ejemplos

Definición 3.1. Un conjunto A dotado de dos operaciones (cerradas) $+$ y $*$, se llama **anillo** si el triple $(A, +, *)$ satisface:

1. A con la operación $+$ es un grupo conmutativo. En particular existe un neutro al que llamaremos 0.
2. A es un monoide bajo $*$. Es decir, $*$ es asociativa, y existe un neutro que llamaremos 1.
3. $*$ distribuye sobre $+$, es decir $a*(b+c) = a*b+a*c$ y $(b+c)*a = b*a+c*a$.

En el caso que $*$ sea conmutativa, diremos que $(A, +, *)$ es un **anillo conmutativo**.

Ejercicio 3.2. Pruebe que las siguientes afirmaciones valen en un anillo $(A, +, *)$.

a) Para todo $a \in A$, $a * 0 = 0 = 0 * a$.

b) Si $0 = 1$ entonces A tiene solo un elemento. En este caso decimos que A es el anillo cero.

Definición 3.3. Diremos que $(A, +, *)$ es un **cuerpo** si $(A, +, *)$ es un anillo que además cumple que

4. Para todo $a \in A \setminus 0$ existe $b \in A$ tal que $a * b = 1 = b * a$.

   [Note que en este caso $(A \setminus \{0\}, *)$ es un grupo.]

Ejemplo 3.4. Los siguientes son ejemplos básicos de anillos.

- $(\mathbb{Z}, +, \cdot)$ (suma y producto usual) es un anillo.
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ (suma y producto usuales) son cuerpos.
- Si X es un conjunto, entonces $\mathcal{F}(X, \mathbb{R}) = \{f : X \to \mathbb{R}\}$ con suma y producto dadas por $(f + g)(x) = f(x) + g(x)$ y $(f * g)(x) = f(x) \cdot g(x)$ es un anillo.
- $M_n(\mathbb{R})$, las matrices n por n con coeficientes en $\mathbb{R}$, con producto usual de matrices y suma por coordenadas es un anillo.
- $\mathbb{R}[x]$, los polinomios con coeficientes en $\mathbb{R}$, es un anillo con su suma y multiplicación usual.

Ejercicio 3.5. Suponga que $(A, +, *)$ es un anillo. Demuestre que

1. $A[x]$, los polinomios con coeficientes en A, tiene una estructura *natural* de anillo.
2. $M_n(A)$, matrices n por n con coeficientes en A, con producto matricial y suma por coordenadas es un anillo.

Ejercicio 3.6 (Los enteros módulo n)**.** Vimos que $\mathbb{Z}/n\mathbb{Z} = \{[i] := i + n\mathbb{Z} \mid i \in \mathbb{Z}\}$ es un grupo bajo $[a] + [b] = [a + b]$. Definimos $[a] * [b] = [a \cdot b]$.

1. Demuestre que entonces $(\mathbb{Z}/n\mathbb{Z}, +, *)$ es un anillo.

2. Demuestre que si $n = p$ es un número prinmo, entonces $(\mathbb{Z}/p\mathbb{Z}, +, *)$ es un cuerpo.

(Ayuda: vea la Sección 2.1)

Ejemplo 3.7 (Los cuateriones de Hamilton[13])**.** Sean i, j, y k entidades abstractas que cumplen que $i^2 = j^2 = k^2 = ijk = -1 \in \mathbb{R}$. Note que esto implica que

$$k = ij,\ i = jk,\ j = ki,$$

y que $xy = -yx$ para todo $x, y \in \{i, j, k\}$ con $x \neq y$. Los cuaterniones es el conjunto

$$\mathcal{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

equipado con la suma *por coordenadas*,

$$(a + bi + cj + dk) \oplus (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k,$$

y el producto al estilo polinomios:

$$\begin{aligned}(a + bi + cj + dk) * (a' + b'i + c'j + d'k) = {} & a \cdot a' + (a \cdot b')i + (a \cdot c')j + (a \cdot d')k \\ & \oplus (b \cdot a')i + (b \cdot b')i^2 + (b \cdot c')ij + (b \cdot d')ik \\ & \oplus (c \cdot a')j + (c \cdot b')ji + (c \cdot c')j^2 + (c \cdot d')jk \\ & \oplus (d \cdot a')k + (d \cdot b')ki + (d \cdot c')kj + (d \cdot d')k^2.\end{aligned}$$

Note que por las identidades de arriba, esta multiplicación es cerrada.

Ejercicio 3.8. Demuestre que $(\mathcal{H}, \oplus, *)$ es un cuerpo.

Definición 3.9. Sea $(A, +, \cdot)$ un anillo. Decimos que $B \subseteq A$ es un **subanillo** de A si B equipado con $+$ y $\cdot$ es un anillo. Además, si $S \subset A$ denotamos por $\langle S \rangle$ a la intersección de todos los subanillos de A que contienene a S. Llamamos a $\langle S \rangle$ el **anillo generado** por S.

Ejercicio 3.10. Los Enteros Gaussianos, denotados $\mathbb{Z}[i]$, son el subanillo de $\mathbb{C}$ generado por $S = \{1, i\}$. Verifique que $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Definición 3.11. Sean A y B dos anillos. Decimos que $\varphi : A \to B$ es un **homomorfismo de anillos** si $\varphi(a + a') = \varphi(a) + \varphi(a')$ y $\varphi(a * a') = \varphi(a) * \varphi(a')$, y $\varphi(1_A) = 1_B$. Decimos que dos anillos son **isomorfos** si existe un homomorfismo biyectivo entre ellos.

El **nucleo** o **kernel** de un homomorfismo de anillos $\varphi : A \to B$, es el conjunto $Ker(\varphi) = \{a \in A \mid \varphi(a) = 0_B\}$.

[13] Los cuaterniones son el primer ejemplo de un cuerpo no conmtutativo. De hecho, ahora sabemos que los cuaterniones son el cuerpo mas grande que contiene a $\mathbb{R}$.

Ejercicio 3.12. Suponga que $\varphi : A \to B$ es un homomorfismo de anillos.

1. Demuestre que $Im(\varphi)$, la imagen de φ, es un subanillo de B.
2. Demuestre que si C es un subanillo de B, entonces $\varphi^{-1}(C)$, el conjunto de preimagenes de C, es un subanillo de A.

Ejercicio 3.13. Sea M_2 el conjunto de matrices con coeficientes complejos de la forma

$$\begin{pmatrix} a+bi & c+di \\ a-bi & -c+di \end{pmatrix}.$$

1. Verifique que M_2 con suma por coordenadas y producto matricial es un anillo.
2. Pruebe que este anillo M_2 es isomorfo a los cuaterniones $\mathcal{H}$ del Ejemplo 3.7.

Concluimos esta sección introduciendo el anillo de series formales.

Ejemplo 3.14. Dadoun anillo $(A, +, \cdot)$ definimos el **anillo de series formales con coeficientes en** A como el conjunto

$$A[[X]] = \{(a_n)_{n\in\mathbb{N}} \mid a_n \in A\},$$

equipado con la suma

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}},$$

y el producto

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = \left(\sum_{i+k=n} a_i \cdot b_k\right)_{n\in\mathbb{N}}.$$

Note que el anillo A es isomorfo al subanillo de $A[[X]]$ dado por los elementos del la forma $(a, 0, 0, \dots)$ con $a \in A$. Mas aún, si definimos $X = (0, 1, 0, \dots) \in A[[X]]$, entonces el anillo generado por A y por X es isomorfo al anillo de polinomios con coeficientes en A.

3.2. Ideales y anillos cocientes

En esta sección revisamos la noción de anillo cociente. Para simplificar la notación, la multiplicación $a * b$ de elementos en un anillo la denotaremos simplemente por $a\,b$ o $a \cdot b$.

Dado un subconjunto I de un anillo A, diremos que I **absorve** por izquierda (respectivamente, por derecha) si para todo $a \in A$ se tiene que $aI := \{ai \mid i \in I\} \subseteq I$ (respectivamente $Ia \subseteq I$).

Ejercicio 3.15. Suponga que $\varphi : A \to B$ es un homomorfismo de anillos. Demuestre que $Ker(\varphi) := \{a \in A \mid \varphi(a) = 0_B\}$ absorve por derecha y por izquierda.

Definición 3.16. Sea $(A, +, \cdot)$ un anillo e I un subconjunto de A. Decimos que I es un **ideal a izquierda** (resp. a derecha) si $(I, +)$ es un subgrupo de $(A, +)$ que absorve por izquierda (resp. por derecha). Decimos que el subgrupo I es un **ideal bilatero**, si absorve por derecha e izquierda.

Cuando la multiplicación en A sea conmutativa, omitiremos el apellido *izquierdo* o *derecho* y simplemente diremos que I es un ideal.

En general, un anillo A siempre admite al menos dos ideales: A y $\{0\}$. Nos referiremos a estos ideales como ideales *triviales*.

Observación 3.17. Un ideal de un anillo A no es necesariamente un subanillo pues para nosotros los subanillos contienen al 1. En efecto, si un ideal a izquierda I contiene al 1, entonces $a \cdot 1 = a$ pertenece a I para todo a, y en particular $I = A$.

Ejercicio 3.18. Sea $\varphi : A \to B$ un homomorfismo de anillos y sea J un ideal a izquierda de B. Demuestre que $\varphi^{-1}(J)$, el conjunto de preimagenes de J, es un ideal de A.

Ejercicio 3.19. Muestre que la intersección arbitraria de ideales (bilateros, izquierdos o derechos) es también un ideal (bilatero, izquierdo o derecho respectivamente).

Ejercicio 3.20. Sea $M_2(\mathbb{R})$ el anillo de matrices 2 x 2 con entradas en $\mathbb{R}$. Muestre que el subconjunto de matrices de la forma

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix},$$

con a y b en $\mathbb{R}$, es un ideal izquierdo pero no un ideal derecho de $M_2(\mathbb{R})$.

Los ideales bilateros, son precisamente los objetos por los cuales podemos cocientar un anillo para obtener otro.

Proposición 3.21. *Si I un ideal bilatero de A, entonces $A/I := \{a + I \mid a \in A\}$ hereda la estructura de anillo de A.*

Dem: Sea I un ideal bilatero de A. Por simplicidad, anotaremos $[a] = a + I$. Puesto que $(A, +)$ es un grupo Abeliano e I es un subgrupo, tenemos que I es un subgrupo normal de A y por lo tanto la sume $[a] + [b] := [a + b]$ convierte a A/I en un grupo Abeliano.

Definimos la multiplicación en A/I por $[a]\cdot[b] = [a\cdot b]$. Note la propiedad absorbente de los ideales hace que ésta operación est bien definida (vea Ejercicio 3.22) y que $[1] = [1_A]$ funciona como neutro de A/I. Mas aún, la asociatividad y la distrubucion de $\cdot$ sobre $+$ sigue de la asociatividad y distributividad en A. Luego A/I es un anillo. □

Ejercicio 3.22. Sea A un anillo e I un ideal bilatero de A. Para $a \in A$, denotamos $a + I$, la clase lateral de a módulo I, como $[a]$. Pruebe que la operación $[a] \cdot [b] = [a \cdot b]$ no depende del representante de clase.

Ejercicio 3.23. Demuestre que todo ideal bilatero de un anillo A es el nucleo de algún homomorfismo. (Ayuda: considere la aplicación $a \mapsto [a]$ de A en A/I).

Ejercicio 3.24. Sea $\varphi : A \to B$ un homomorfismo de anillos. Muestre que $Im(\varphi)$ es isomorfa al anillo $A/Ker(\varphi)$.

La siguiente observación caracteriza a los cuerpos como los anillo que solo admiten ideales triviales.

Teorema 3.25. *Un anillo no trivial A es un cuerpo si y solo si sus unicos ideales, tanto a izquierda como a derecha, son los triviales.*

Dem: Sea I un ideal izquierdo de un cuerpo k que contiene un elemento $a \neq 0$. Luego $1 = a^{-1}a \in I$, lo que implica que $I = k$. Esto muestra que en un cuerpo solo los únicos ideales izquierdos son los triviales. La demostración para el caso de ideales derechos es análoga.

Reciprocamente, suponga que A es un anillo no trivial cuyos únicos ideales, tanto izquierdos como derechos, son los ideales triviales $\{0\}$ y A. Sea $b \in A \setminus \{0\}$. Queremos probar que b es invertible. Para ello consideramos

$$Ab = \{ab \mid a \in A\},$$

y notamos que Ab es un ideal izquierdo de A: factorizando se ve que Ab es un grupo bajo la suma, y claramente absorve a izquerda. En particular, puesto que A solo contiene ideales triviales a izquierda y $Ab \neq \{0\}$, se tiene que existe $a \in A$ tal que $ab = 1$.

Análogamente considerando bA encontramos que existe a' tal que $ba' = 1$. Finalmente notamos que $a = aba' = a'$. Luego A es un cuerpo. □

3.3. Ideales maximales

Alerta: En esta sección y en adelante, salvo que explícitamente digamos lo contrario, **la multiplicación en nuestros anillos será siempre conmutativa**. En particular todos los ideales son biláteros.

Vamos a usar el Teorema 3.25 para ver que todo anillo admite un cociente que es un cuerpo. Para ello precisamos de la siguiente noción.

Definición 3.26. Un ideal I de un anillo A se dice **maximal** si $I \neq A$ y el único ideal distinto de I que contiene a I es A.

Ejemplo 3.27. Es fácil ver que un subgrupo de $\mathbb{Z}$ de la forma $k\mathbb{Z} = \{k \cdot n \mid n \in \mathbb{Z}\}$ es un ideal dentro de $\mathbb{Z}$. Mas aún, un breve cálculo nos muestra que $k\mathbb{Z} \supseteq \ell\mathbb{Z}$ si y solo si k divide a ℓ.

Por otra parte, el Teorema de Meziriac (mas precisamente el Ejercicio 2.4) nos dice que si I es un ideal en $\mathbb{Z}$, y $a, b \in I$, entonces su máximo común divisor, MCD(a, b), pertenece a I. Con esto podemos probar la siguiente proposición

Proposición 3.28. *Todo ideal de $\mathbb{Z}$ es de la forma $k\mathbb{Z}$ para algún $k \in \mathbb{N}$.*

Demostración: Sea I un ideal. Claramente $\mathbb{Z} = 1\mathbb{Z}$, por lo que podemos asumir que I es un ideal propio, es decir ni 1 ni -1 pertenecen a I. Sea $d > 0$ el elemento positivo de I mas pequeno. Queremos demostrar que $d\mathbb{Z} = I$. Para ello tomamos $a \in I$ otro elemento positivo cualquiera. Si d divide a a entonces claramente $a \in d\mathbb{Z}$. Si d no divide a a, entonces, como observamos mas arriba, $\text{MCD}(d, a) \in I$. Pero en este caso $0 < \text{MCD}(d, a) < d$, lo que contradice la elección de d. □

En particular, los ideales maximales de $\mathbb{Z}$ son aquellos de la forma $p\mathbb{Z}$ con p un número primo.

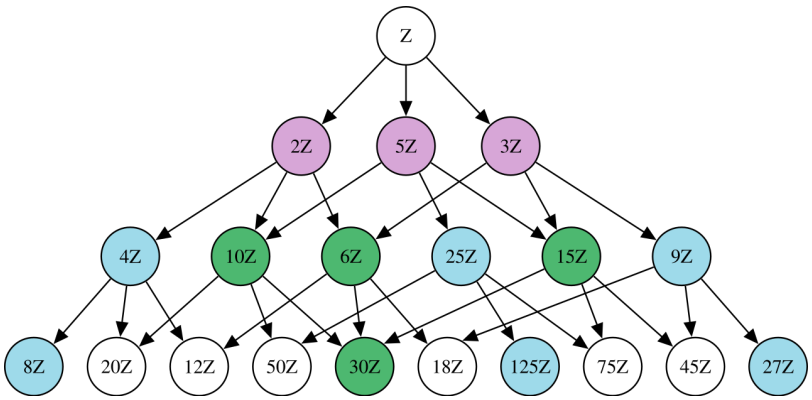


Figura 9: Una porción de la familia de ideales en $\mathbb{Z}$. La flechas denotan contención. (imagen sacada de Wikipedia).

Proposición 3.29. *Sea A un anillo e I un ideal maximal. Entonces A/I es un cuerpo.*

Demostración: Sea I un anillo maximal de A. Por la Proposición 3.21 tenemos que A/I es un anillo. Afirmamos que los únicos ideales de A/I son los triviales. Para verificar esto usaremos la proyección

$$\pi : A \to A/I,\ a \mapsto a + I$$

es un homomorfimos de anillos.

En efecto si $\tilde{J}$ es un ideal no trivial de A/I, entonces $\pi^{-1}(J) = \{a \in A \mid a+I \in \tilde{J}\}$ es un ideal de A que contiene a I (vea Ejercicio 3.18), pero que es distinto de I y de A. Esto niega la maximalidad de I. □

Ejercicio 3.30. Pruebe la recíproca del teorema anterior, a saber que si A/I es un cuerpo (no trivial), entonces I es un ideal maximal.

Ahora probamos que los anillos siempre admiten ideales maximales y por lo tanto siempre admiten a un cuerpo como cociente.

Teorema 3.31. *Todo ideal $I \neq A$ de un anillo A esta contenido en un ideal maximal de A. En particular todo anillo contiene ideales maximales.*

Para la demostración, precisamos del *Axioma de Elección*. Usaremos, eso si, una formulación equivalente de este axioma que se conoce bajo el nombre de *El Lema de Zörn*. La prueba de la equivalencia entre este lema y el Axioma de Elección excede el alcance de estas notas, pero puede ser encontrada en cualquier libro de teoría de conjuntos.

Para enunciar el Lema de Zörn necesitamos un poco de vocabulario: Un **orden parcial** en un conjunto X es una relación $\preceq$ que para todo $x, y, z \in X$ cumple lo siguiente:

1. $x \preceq x$,
2. $x \preceq y$ e $y \preceq z$ implica $x \preceq z$,
3. $x \preceq y$ e $y \preceq x$ implica $x = y$.

La relación $\preceq$ es se dice **orden total** si además cumple

4. Para todo $x, y \in X$ vale que $x \preceq y$ o $y \preceq x$.

Sea $(X, \preceq)$ es un conjunto dotado de un orden parcial. Decimos que $m \in X$ es **maximal** si $m \preceq x$ implica $x = m$. Decimos que $\mathcal{C} \subseteq X$ es una **cadena**, si $(\mathcal{C}, \preceq)$ es un conjunto totalmente ordenado.

Lema 3.32 (Zörn)**.** *Sea X un conjunto dotado con un orden parcial $\preceq$. Suponga que toda cadena $\mathcal{C} \subseteq X$ admite una* **cota superior***, es decir existe $x_{\mathcal{C}} \in X$ tal que $c \preceq x_{\mathcal{C}}$ para todo $c \in \mathcal{C}$. Entonces existe $m \in X$ maximal.*

En otras palabras el Lema de Zörn nos dice que para encontrar elementos maximales, debemos chequear que todas las cadenas tengan una cota superior. El tipico ejemplo de un conjunto con un orden parcial es $\mathcal{P}(\mathbb{R})$, el conjunto de los subconjuntos de $\mathbb{R}$, dotado de la inclusión. Ciertamente en este caso $\mathbb{R}$ es un elemento maximal.

Un ejemplo mas sutil donde se aplica este lema es el Teorema 3.31.

Demostracón del Teorema 3.31: Sea I un ideal propio de un anillo A. Denotaremos por X al conjunto de todos los ideales propios de A que contienen a I. Dotamos a X del orden parcial inducido por la inclusión. Claramente un elemento maximal de X es un ideal maximal de A que contiene a I. Luego, basta con que chequeemos que toda cadena en X admite una cota superior.

Sea $\mathcal{C} \subseteq X$ una cadena. Es claro que $\bigcup_{J \in \mathcal{C}} J$ es un ideal de A que contiene a I (la unión creciente de ideales es un ideal). Solo queda por chequear que $\bigcup_{J \in \mathcal{C}} J$ no es todo A. Para ello notamos que si $\bigcup_{J \in \mathcal{C}} J = A$, entonces $1 \in \bigcup_{J \in \mathcal{C}} J$, luego, existe $J \in \mathcal{C}$ tal que $1 \in J$. Pero ya vimos que esto implica que $J = A$, lo que contradice que J es un ideal propio de A. □

Ejercicio 3.33. Sea X un conjunto cualquiera y $\mathcal{F}(X, \mathbb{R})$ el conjunto de todas las funciones de X a $\mathbb{R}$. Vimos en el Ejemplo 3.4 que $\mathcal{F}(X, \mathbb{R})$ es un anillo. Sea $Y \subseteq X$.

1. Demuestre que $I_Y = \{f \in \mathcal{F}(X, \mathbb{R}) \mid f(x) = 0 \ \forall x \in Y\}$ es un ideal de $\mathcal{F}(X; \mathbb{R})$.
2. Demuetre que si Y es un singleton, digamos $Y = \{x_0\}$, entonces I_Y es un ideal maximal de $\mathcal{F}(X, \mathbb{R})$.
3. Muestre que si Y es un singleton, entonces $\mathcal{F}(X, \mathbb{R})/I_Y$ es isomorfo como anillo a $\mathbb{R}$.

3.4. Dominios de Integridad y Dominios Euclideanos

Hemos visto que cuando cortamos un anillo A por un ideal maximal I, el cociente A/I es un cuerpo. En el caso de $A = \mathbb{Z}$, los ideales generados por números primos son ideales maximales (de hecho la reciporca también vale, ver Proposición 3.43), y es por ello que nos interesamos en la noción de *número primo* en contextos mas generales.

El contexto que nos imponemos es el de **Dominios de Integridad**. Decimos que un anillo conmutativo A es un dominio de integridad, si cada vez que $a \cdot b = 0$ se tiene que a o b es igual a 0. Note, por ejemplo, que el anillo de los enteros $\mathbb{Z}$ es un Dominio de Integridad, pero no así cualquiera de sus cocientes $\mathbb{Z}/n\mathbb{Z}$.

Una propiedad muy cómoda de los Dominios de Integridad, es que en ellos **hay cancelación**, es decir que si $a \neq 0$ entonces vale que

$$ab = ac \Rightarrow b = c.$$

En efecto, si $ab = ac$ entonces $a(b - c) = 0$, y como $a \neq 0$ se tiene que $b = c$.

Vocabulario: Sea $(A, +, \cdot)$ un Dominio de Integridad. Denotamos por A^* al subconjunto de elementos invertibles o **unidades** de A. Note que A^* es un grupo bajo la multiplicación (pero no bajo la suma). Dados $a, b \in A$, decimos que a **divide a** b si existe $c \in A$ tal que $b = ac$. En tal caso anotamos $a \,|\, b$.

Note que dado $a \in A$, los divisores de a contiene siempre a las unidades A^* y a $a \cdot A^*$, los elementos asociados a a, pues basta escribir $a = (ae)e^{-1}$. Estos son los divisores *triviales* de a.

Definición 3.34. Sea $(A, +, \cdot)$ un anillo Dominio de Integridad.

1. Decimos que $a \in A \setminus A^*$ es **irreducible** si $[\, a = bc \,] \Rightarrow [\, b \text{ o } c \in A^*]$.

   Esto es, *nadie no trivial divide a a.*

2. Decimos que a es **primo** si a divide a bc implica a divide a b o a c.

   Esto es, *a es persistente bajo descomposiciones.*

Observación 3.35. En $\mathbb{Z}$ la noción de primo e irreducible coinciden. Usualmente decimos que $p \in \mathbb{Z}$ es primo si satisface el punto 1 de la definición de arriba. El hecho que p tambien cumple la definición 2 de arriba se debe a que en $\mathbb{Z}$, la descomposición en factores primos es única salvo reordenamiento y multiplicación por ± 1.

Ejercicio 3.36. Sea A un Dominio de Integridad. Dado $a \in A$, denotamos por $(a) := \{ab \mid b \in A\}$ el ideal generado por $a \in A$.

1. Muestre que $(a) \subseteq (b)$ si y solo si b divide a a.
2. Muestre que $(a) = (b)$ si y solo si a y b son asociados.
3. Muestre que si a es primo en A, entonces $A/(a)$ no tiene divisores de 0.
4. Suponga que en A todo ideal es principal. Muestre que a es irreducible en A si y solo si (a) es un ideal maximal.

La siguiente proposición dice que en un Dominio de Integridad los elementos primos necesariamente son irreducibles.

Proposición 3.37. *En un dominio de integridad que todo primo es irreducible.*

Demostración: Sea A un Dominio de Integridad y supongamos que $a \in A$ es primo. Para chequear que a es irreducible, suponemos que $a = bc$ y notamos que por primidad, a divide a b o a c. Digamos a divide a c. Luego

$$a = bc = b(da),$$

y como hay cancelación se tiene que $1 = bd$, es decir b es invertible. □

Si bien en la mayoría de los ejemplos que veremos se tendrá que todo elemento se puede descomponer en irreducibles, en muchos de estos ejemplos la descompisicón en irreducibles no es única. Esto equivale a decir que en estos ejemplos no todos los irreducibles son primos. El siguiente es un caso concreto de esta situación.

Ejemplo 3.38. Sea $\mathbb{Z}[\sqrt{-5}]$ el sub anillo de $\mathbb{C}$ generado por 1 y $\sqrt{-5}$.

Ejercicio 3.39. Muestre que $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

Ahora, en $\mathbb{C}$, y por lo tanto también en $\mathbb{Z}[\sqrt{-5}]$, disponemos de la **norma** de un elemento, $N(a+bi) = |a+bi| = \sqrt{a^2+b^2}$, y sabemos que la norma es multiplicativa, es decir

$$N(zw) = N(z)N(w).$$

Por otra parte el Ejercicio 3.39 muestra que $\mathbb{Z}[\sqrt{-5}]$ es un subconjunto discreto de $\mathbb{C}$ y por lo tanto la norma alcanza un mínimo en $\mathbb{Z}[\sqrt{-5}] \setminus \{0\}$, que en este caso es 1. En particular, **las unidades de $\mathbb{Z}[\sqrt{-5}]$ son los elementos de norma 1**, es decir $\mathbb{Z}[\sqrt{-5}]^* = \{1, -1\}$.

Si seguimos inspeccionando lo valores que la norma puede tomar en $\mathbb{Z}[\sqrt{-5}]$ encontramos que despues de 1 aparece 2, $\sqrt{5}$, y cosas mas grandes. En particular (note que $2 \leq \sqrt{5}$) se tiene que si $z \in \mathbb{Z}[\sqrt{-5}]$ tiene una descomposición no trivial, entonces $N(z) \geq 4$. Asi, por ejemplo, 2 y 3 son irreducibles en $\mathbb{Z}[\sqrt{-5}]$ como también lo son $1 + \sqrt{-5}$ y $1 - \sqrt{-5}$ (pues su norma $\sqrt{6}$ es menor que 4).

Pero

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

lo que nos dice que la descomposicón en irreducibles no es única y por lo tanto $\mathbb{Z}[\sqrt{-5}]$ es un anillo donde *los irreducibles no son primos.* Decimos que $\mathbb{Z}[\sqrt{-5}]$ **no es un Dominio de Factorizacion Única**.

Vamos a introducir una clase de anillos donde las nociones de irreducible y primo si son equivalentes. Estos serán anillos donde podremos implementar el *algoritmo de la división de Euclides.*

Definición 3.40. Un Dominio de Integridad A se dice **Dominio Euclideano**si admite una valuación discreta, es decir una función $\nu : A \setminus \{0\} \to \mathbb{N}$ tal que

1. Para todo $a, b \in A \setminus \{0\}$, vale que $\nu(a) \leq \nu(ab)$.

2. Para todo $a, b \in A \setminus \{0\}$ existen q y $r \in A$ tal que $a = bq + r$ con $r = 0$ o $\nu(r) < \nu(b)$.

El ejemplo canónico de un Dominio Euclideano es $\mathbb{Z}$ con el valor absoluto como valuación. Otro ejemplo importante es $k[x]$, los polinomios con coeficientes en un cuerpo conmutativo (por ejemplo $k = \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$, etc), con *el grado*[14] como valuación. Note que para que el algoritmo de la división de polinomios funcione, se precisa de forma crucial que k sea un cuerpo. De hecho, veremos en la Proposición 3.44 mas adelante, que $\mathbb{Z}[x]$, lo polinomios con coeficientes en $\mathbb{Z}$, no es un Dominio Euclideano.

Observación 3.41. En un Dominio Euclideano A con valuación ν, los elementos invertibles de A son precisamente los elementos que realizan el mínimo de ν.

En efecto, sea $n_0 = \min \nu(A \setminus \{0\})$. Si b es invertible entonces siempre vale que $\nu(b) \leq \nu(bb^{-1}a) = \nu(a)$, luego $\nu(b)$ es mínimo. Reciprocamente si $\nu(a) = n_0$, entonces al dividir 1 por a se tiene que $1 = ba + r$, con $r = 0$, lo que dice que a era invertible.

El siguiente es otro ejemplo de un Dominio Euclideano (comparar con Ejemplo 3.38).

Ejemplo 3.42 (El anillo de enteros Gaussianos)**.** El anillo de los enteros Gaussianos es el conjunto $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ bajo suma y multiplicaicón compleja. Vamos a ver que en este ejemplo N^2, el cuadrado de la norma compleja, funciona como una valuación.

Para empezar notamos $\mathbb{Z}[i]$ es un conjunto discreto en $\mathbb{C}$ y que el minimo de la norma en $\mathbb{Z}[i] \setminus \{0\}$ es 1. Mas aún $N^2(zw) = N^2(z)\, N^2(w)$, por lo que N^2 satisface trivialmente punto 2. de la Definición 3.40.

Ahora chequeamos el punto 1 de la Definición 3.40. Sean a y b dos enteros Gaussianos no nulos. Sea z el numero complejo a/b. Si $z \in \mathbb{Z}[i]$ entonces tenemos que $a = zb + 0$ y estamos listos.

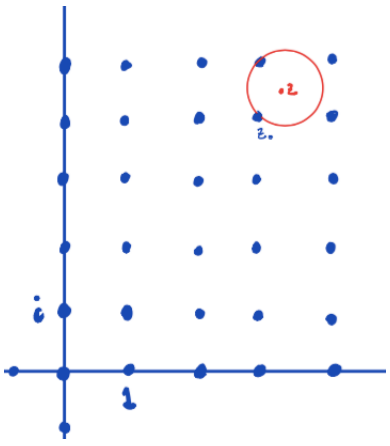


Figura 10: Una porción de los enteros Gaussianos $\mathbb{Z}[i]$ dentro de $\mathbb{C}$. z_0 es el entero *mas cercano* a z.

[14]Recuerde que si $p(x) = a_n x^n + \ldots + a_0$, es un polinimio cualquiera, entonces su grado es $gr(p(x)) = \max\{i \mid a_i \neq 0\}$.

En caso que z no sea un entero Gaussiano, tomamos z_0 el entero Gaussiano mas proximo a z en $\mathbb{C}$ (aqui hay una pequeña a sutileza pues la elección puede no ser única. En este caso elegimos uno de los (a lo mas) cuatro enteros Gaussianos posibles. Ver Figura 10). En particular, tenemos que $N(z - z_0) < 1$, y se tiene que

$$a = zb = z_0b - z_0b + zb = z_0b + b(z - z_0).$$

Sea $r = b(z-z_0)$. Como $a = z_0b+r$, en particular se tiene que $r = a-z_0b \in \mathbb{Z}[i]$. Mas aun, $N^2(r) = N^(b)N^2(z-z_0) < N^2(b)$, lo que dice que $\mathbb{Z}[i]$ es un Dominio Euclideano.

Con la noción de Dominio Euclideano podemos generalizar la Proposición 3.28. Diremos que ideal I en un anillo A es **principal** si $I = (a) := a \cdot A$ para algún $a \in A$. Un anillo donde todo ideal es principal se dice llama **dominio de ideales principales**.

Proposición 3.43. *Todo ideal en un Dominio Euclideano es principal.*

Demostración: (ir comparando con el caso $A = \mathbb{Z}$) Sea I un ideal en un Dominio Euclideano A, y sea $f : A \to \mathbb{N}$ su valuación. Sea $a \in A$ un elemento realizando el minimo de $f(I \setminus \{0\})$. Sea $b \in I$. Dividiendo b en a obtenemos que $b = ac + r$ con $f(r) < f(a)$ o $r = 0$. Pero como $r = b - ca \in I$, se deduce que $r = 0$, lo que a su vez implica que $I = a \cdot A$. □

Con esto es fácil mostrar que $\mathbb{Z}[x]$ no es un Dominio Euclideano.

Proposición 3.44. $\mathbb{Z}[x]$ *contiene ideales que no son principales. En particular,* $\mathbb{Z}[x]$ *no es un Dominio Euclideano.*

Demostración: Consideremos $I = (2, x)$ el ideal generado por 2 y x en $\mathbb{Z}[x]$. Es decir, I es la intersección de todos los ideales en $\mathbb{Z}[x]$ que contienen 2 y a x (ver Ejercicio 3.19). En búsqueda de contraricción suponemos que existe $p(x) \in \mathbb{Z}[x]$ tal que $I = (p(x)) = p(x)\mathbb{Z}[x]$.

De una parte, mirando el grado, y puesto que $2 \in (p(x))$, se tiene que necesariamente $gr(p(x)) = 0$, es decir $p(x)$ es una constante.

Por otra parte, I no es todo $\mathbb{Z}[x]$, pues, por ejemplo, I esta contenido en el ideal J formado por los polinomios cuyo coeficiente constante es par. En particular concluimos que $p(x) = 2$ o -2.

Pero esto no puede ser pues $x \notin (2)$. Esta contradicción prueba que I no es un ideal principal. □

Ejercicio 3.45. Pruebe que $\mathbb{R}[x, y]$, los polinomios en dos variables (que conmutan) es un anillo sin divisores de cero. Pruebe que él no es un Dominio Euclideano.

Ejercicio 3.46. (Enteros de Eisenstein) Sea $w \in \mathbb{C}$ una raíz cubica de la unidad $\neq 1$. Sea $\mathbb{Z}[w]$ el anillo generado por 1 y w en $\mathbb{C}$.

1. Muestre que $\mathbb{Z}[w] = \{a + bw \mid a, b \in \mathbb{Z}\}$ (Ayuda: use que $w^2 + w - 1 = 0$).
2. Pruebe además que $\mathbb{Z}[w]$ es un Dominio Euclideano con la valuación $f(a + bw) = a^2 - ab + b^2$. (Ayuda: f coincide con la norma usual al cuadrado)

Concluimos esta sección mostrando que en un Dominio Euclideano todo irreducible es primo.

Teorema 3.47. *Sea A es un dominio de ideales principales (por ejemplo A un Dominio Euclideano). Entonces se tiene que*

1. *todo irreducible en A es primo en A.*

2. *Si p es irreducible en A, entonces (p) es un ideal maximal de A.*

Demostración: Primero probamos las afirmación 1. Sea $p \in A \setminus A^*$ un irreducible, y sean $a, b \in A$ tal que $p|ab$. Queremos demostrar que p divide a a o a b.

Supongamos, en búsqueda de contradicción, que p no divide a a ni a b. Luego se tiene que $(p) \subsetneq (a, p) = (c)$ y $(p) \subsetneq (b, p) = (d)$ para algún $c, d \in A$. Note que esto implica, por ejemplo, que $p = ck$ y -por ser p irreducible- o bien c o bien k tiene que ser una unidad de A. Pero k no puede ser una unidad puesto que $(p) \subsetneq (c)$, por lo que concluimos que c y (analogamente) d son unidades.

Con esto podemos llegar a una contradicción. En efecto, como $(c) = (a, p)$ se tiene que que $c = k_1 a + k_2 p$ y analogamente $d = \ell_1 b + \ell_2 p$. Luego $cd \in (ab, ap, bp, p^2) \subseteq (p)$, lo que no puede ser puesto que (p) es un ideal propio.

Ahora probamos la afirmación 2. Sea p un irreducible y suponga que J es un ideal que contiene a p. Puesto que $J = (b)$ es principal, se tiene que b divide a p. Pero como p es irreducible se tiene que o b es invertible, en cuyo caso $J = A$, o bien b es asociado a p, en cuyo caso $J = (p)$. □

Concluimos esta sección notando si k es un cuerpo, entonces no cualquier grupo Abeliano puede aparecer como grupo de unidades bajo la multiplicación. Para empezar tenemos el

Ejercicio 3.48. Sea k un cuerpo y $p(x) \in k[x]$ un polinomio. Muestre que $a \in k$ es una raiz de $p(x)$ (i.e. $p(a) = 0$) si y solo si $(x - a)$ divide a $p(x)$ en $k[x]$ (i.e. existe $q(x) \in k[x]$ tal que $p(x) = (x - a) \cdot q(x)$). En particular, un polinomio $p(x) \in k[x]$ de grado n tiene a los sumo n raíces.

Con esto podemos mostrar la

Proposición 3.49. *Sea k un cuerpo (conmutativo) y $G \leq k^*$ un subgrupo del grupo multiplicativo de k. Si G es finito, entonces G es cíclico.*

Demostración: Recuerde que el órden de un elemento $g \in G$, denotado $ord(g)$, es el menor entero $j \geq 1$ tal que $g^j = 1$. Recuerde también que el exponente de un grupo G, denotado $Exp(G)$, es el menor entero j tal que $g^j = 1$ para todo $g \in G$. Finamente recuerde por el Corolario 2.46, sabemos que en un grupo Abeliano finito G existe g tal que $Exp(G) = ord(g)$.

Luego, para probar que G es cíclico basta demostrar que $Exp(G) = |G|$. Para ello consideramos el polinomio $p(x) = x^{Exp(G)} - 1$. Claramente $p(x)$ tiene grado $Exp(G)$, pero se anula en todo $g \in G$. Luego, el Ejercicio 3.48 implica que $Exp(G) = |G|$. □

3.5. El cuerpo de fracciones de un Dominio de Integridad

Pregunta (Mal'cev): Cuándo un anillo se realiza como un subanillo de un cuerpo?

Esta pregunta en general es muy difícil y materia de investigación actual. Sin embargo en el caso de que A sea un anillo conmutativo la respuesta se reduce a la presencia o ausencia de divisores de 0.

En efecto notamos que si A es un anillo conmutativo que si tienen divisores de 0, entonces A no puede ser un subanillo de un cuerpo k (pues los cuerpos no tienen divisores de 0). La reciproca, a saber que todo Dominio de Integridad se realiza como sub anillo de un cuerpo, es el contenido del siguiente teorema.

Teorema 3.50. Sea A un Dominio de Integridad. Entonces existe k un cuerpo (conmutativo) tal que A se incrusta en k.

Dem: Construimos el *cuerpo de fracciones de A*. Indicaremos solo los pasos principales dejando al lector la verificación de los detalles.

Sea $X = A \times A$. En X introducimos la siguiente relacion de equivalencia:

$$(a, b) \sim (c, d) \Leftrightarrow ad = cb.$$

Veamos que esto es una relacion de equivalencia:

- Es refleja.
- Es simetrica (conmutatividad!)
- Es transitiva (usamos que hay cancelacion).

En $X/\sim$ definimos las siguientes operaciones.

$$(a, b) + (c, d) = (ad + cb, bd)$$

$$(a, b)(c, d) = (ac, bd).$$

Estas definiciones no dependen del representante (verificar).

Afirmamos que $k = X/\sim$ es un cuerpo. Lo llamamos el cuerpo de fracciones de A: $Frac(A)$.

- El neutro aditivo es $(0, 1)$,
- El inverso aditivo es fácil.
- Neutro multiplicativo $(1, 1)$.
- El inverso multiplicativo fácil.
- Se tiene que ambas operaciones son asociativas.
- Se tiene que la multiplicación distribuye sobre la suma.

Finalmente notamos que $a \mapsto (a, 1)$ es un homomorfismo (de anillos) que inyecta A en $Frac(A)$. □

Corolario 3.51. *El cuerpo de fracciones de un Dominio de Integridad A, es el menor cuerpo Abeliano que contiene a A. Mas precisamente, para todo cuerpo Abeliano k tal que $A \hookrightarrow k$, se tiene que $Frac(A) \hookrightarrow k$.*

Dem: Sea $\varphi : A \to k$ una inyeccion de A en k. Definimos $\varphi((a,b)) = \varphi(a)\varphi(b)^{-1}$. Basta ver que es un homomorfismo (pues es no trivial):

$$\varphi((a,b)(c,d)) = ac(bd)^{-1}$$

$$\varphi((a,b)+(c,d)) = \varphi((ad+bc,bd)) = (ad+bc)(bd)^{-1} = ab^{-1} + cd^{-1}.$$

□

3.6. Extensiones de anillos y cuerpos

En esta sección nos interesamos en los subcuerpos de $\mathbb{C}$. Ciertamente, cualquier subcuerpo de $\mathbb{C}$ contiene al 1 y por lo tanto al cuerpo que él genera: $\mathbb{Q}$. El objetivo principal de esta sección discutir las noción de número algebraico y número trascendente. Veremos el argumento de Liouville para mostrar existencia de números trascendentes (i.e. que no se anulan en ningún polinomio con coeficientes en $\mathbb{Q}$) y por otra parte veremos que los número algebraicos forman un cuerpo, que denotaremos por $\overline{\mathbb{Q}}$, el menor cuerpo algebraicamente cerrado que contiene a $\mathbb{Q}$.

Definición 3.52. Dados un anillo subanillo A de un anillo B y un conjunto $S \subseteq B$, denotamos por $A[S]$ al subanillo de B generado por A y S y por $A(S)$. Claramente

$$A[S] = \{\sum_{i=1}^{n} a_i s_{i,1} \dots s_{i,k} \mid k, n \in \mathbb{N}, s_{i,j} \in S, a_i \in A\}.$$

En paricular si $S = \{b\}$ se tiene que $A[b] = \{a_0 + a_1 b + a_2 b^2 + \ldots + a_n b^n \mid n \in N, a_i \in A\}$. Claramente $A[S]$ es un anillo, y, por ejemplo, los enteros Gaussianos $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Definición 3.53. Dados K y F dos cuerpos, decimos que K es una **extension** de F si $F \subset K$ como subcuerpo. Decimos que un elemento $a \in K$ es **algebraico** sobre F, si existe un polinomio $p(x) \in F[x]$ tal que $p(a) = 0$. Si no existe tal polinomio, entonces decimos que a es **transcendente** sobre F.

Dado $p(x) \in F[x]$ un polinomio de grado n, decimos que $p(x)$ es mónico si el coeficiente que acompaa a x^n es 1. Dado $a \in K$ algebraico sobre F, el **polinomio minimal** de a sobre F es el polinomio mónico $p(x) \in F[x]$ de menor grado tal que $p(a) = 0$. Denotamos este polinomio por $min(F, a)$.

Ejemplo 3.54. Todo número racional es anulado por un polinomio mónico en $\mathbb{Q}[x]$. Los números i, $\sqrt{2}$, $\omega_p = e^{2\pi i/p}$ son algebraicos sobre $\mathbb{Q}$ pues ellos se anulan en x^2+1, x^2-2, y x^p-1.

Como x^2+1 y x^2-2 son irreducibles en $\mathbb{Q}[x]$ (ejercicio), ellos corresponden a los polinomios minimales asociados a i y $\sqrt{2}$. Por otro lado x^p-1 no es irreducible pues es divisible por $x-1$. Veremos mas adelante que el polinomio minimal asociado a ω_p es $x^{p-1} + x^{p-2} + \ldots + x + 1$.

Observación 3.55. Note que, dado $a \in K$, $ev_a : F[x] \to K$ definida por $ev_a(t(x)) = t(a)$ es un homomorfismo de anillos. De hecho, $min(F, a)$ se puede definir como el generador mónico del kernel del homomorfismo $ev_a : F[x] \to K$.

En efecto, si $p(x) = min(F, a)(x)$ entonces $p(x) \in Ker(ev_a)$. Por otro lado, como en $F[x]$ todo ideal es principal pues F es un cuerpo, se tiene que $q(x)$, el generador mónico de $Ker(ev_a)$ tiene que dividir a $p(x)$, es decir $p(x) = q(x)r(x)$. En particular se tiene que $0 = p(a) = q(a)r(a)$, luego $r(a) = 0$ o $q(a) = 0$. Pero como $p(x)$ es el polinimio minimal de a, se tiene que $q(a)) = 0$ y $r(x)$ es una constante. Concluimos que que $p(x) = q(x)$ (modulo una unidad).

Observación 3.56. Dado un anillo K que es una extension de un cuerpo F, se tiene que K es un F-espacio vectorial: podemos sumar elemntos de K y ponderarlos por F visto como escalares. La dimension de este K como F-espacio vectorial la denotamos por $[K : F]$. (notar que esto **no** es igual al índice de K/F como grupos bajo $+$.)

Por ejemplo $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ tiene dimension 2 sobre $\mathbb{Q}$: una base es $\{1, \sqrt{2}\}$.

Observación 3.57. Note que $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ es en realidad un cuerpo (y no solamente un anillo). Por ejemplo $(a + bi)^{-1} = ...$ (resolver con un sistema de ecuaciones). De hecho tenemos la siguiente proposición.

Proposición 3.58. Si $a \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$, entonces $\mathbb{Q}[a]$ es un cuerpo y $[\mathbb{Q}[a] : \mathbb{Q}] = gr(min(\mathbb{Q}, a)(x))$.

Demostración: (Esta prueba es general) Sea K una extension de F y $a \in K$ algebraico. La imagen del homomorfismo de anillos $ev_a : F[x] \to K$ coincide con $F[a]$. Su núcleo es el ideal generado por $p(x) := min(F, a)(x)$, ver Observación 3.55. Luego

$$F[a] \simeq F[x]/(p(x)). \tag{6}$$

Afirmamos que el ideal $(p(x))$ es un ideal maximal de $F[x]$ (y por lo tanto $F[a]$ es cuerpo por Proposición 3.29). En efecto, suponga que J es un ideal maximal que contiene a $(p(x))$. Sabemos que J es un ideal principal, es decir, $J = (q(x))$ para algún $q(x)$ que podemos suponer que es monico y de grado ≥ 1. Concluimos que $p(x) = q(x)t(x)$. Puesto que $0 = p(a) = q(a)t(a)$ tenemos que o bien $q(a)$ o $t(a)$ es 0. Pero $p(x)$ es el polinomio de menor grado que se anula sobre a, en particular concluimos que $gr(p(x)) = gr(q(x))$ y que $t(x)$ es una constante. En particular $(p(x)) = (q(x))$ es maximal y $F[a] \simeq F[x]/(p(x))$ es un cuerpo.

Para ver la dimension de la extensión basta ver que $\{1, a, \ldots, a^{n-1}\}$ es una base de $F[a]$, donde $n = gr(min(F, a)(x))$. La independencia lineal es sigue de la minimalidad del grado de $min(F, a)$ y la generación sigue de la ecuación (6). □

La prueba nos entrega una manera de fabricar muchos cuerpos. Recordar que $p(x) \in F[x]$ es **irreducible** si en cada descomposicion $p(x) = q(x)t(x)$ se tiene que $q(x)$ o $t(x)$ es invertible (i.e. es un escalar).

Corolario 3.59. *Si F es un cuerpo y $p(x) \in F[x]$ es irreducible, entonces $(p(x))$ es un ideal maximal. En particular $F[x]/(p(x))$ es cuerpo que contiene una copia isomorfa de F.*

Ejercicio 3.60. Sea $w^3 = 1$, $\mathbb{C} \ni w \neq 1$. En $K = \mathbb{Q}[w]$ calcule el inverso de w y de $1 + w$.

Ejercicio 3.61. Sea $F_3 = \mathbb{Z}/3\mathbb{Z}$ es cuerpo con 3 elementos. Pruebe que $x^2 + x + 2 \in F_3[x]$ es un polinomios irreducible. Concluya que F_3 admite una extensión finita que es un cuerpo.

Teorema 3.62. *Los números algebraicos sobre $\mathbb{Q}$ forman un cuerpo que denotamos por $\overline{\mathbb{Q}}$. Este cuerpo $\overline{\mathbb{Q}}$ es numerable, en particular existen (muchos) números trascendentes.*

Presisamos el siguiente

Lema 3.63. (a) Si K es una extension de F tal que $[K : F] < \infty$, entonces todo $b \in K$ es algebraico sobre F.

(b) Si $F \leq K \leq L$ son extensiones de cuerpos, entonces $[L : F] = [L : K] \cdot [K : F]$.

Demostración: En efecto $1, b, \ldots, b^n$ eventualmente se vuelve un conjunto linealmente dependiente. Eso dice que existe una combinacion lineal $a_0 + a_1 b + \ldots + a_n b^n = 0$ con los $a_i \in F$. Luego b es algebraico.

Para demostrar (b) usamos bases. Tomamos $\mathcal{V} = \{v_1, \ldots, v_n\}$ una base de L sobre K y $\mathcal{U} = \{u_1, \ldots, u_m\}$ una base de K sobre F. Afirmamos que $\mathcal{B} = \{u_i v_j \mid 1 \leq i \leq m\,,\ 1 \leq j \leq n\}$ es una base de L sobre F. En efecto todo $\ell \in L$ se puede escribir como K-combinación de elementos de $\mathcal{V}$ y a su vez cada escalar de ésta combinación se escribe como combinación de elementos de $\mathcal{U}$. Esto muestra que $\mathcal{B}$ es un conjunto generador de L sobre F. Para ver que $\mathcal{B}$ es también un conjunto linealmente independiente suponemos que $0 = \sum_{i,j} \alpha_{i,j} u_i v_j$ de donde se deduce que $0 = \sum_j \left(\sum_i \alpha_{i,j} u_i\right) v_j$, lo que dice que $\sum_i \alpha_{i,j} u_i = 0$ para cada j, lo que implica que los $\alpha_{i,j}$ son todos 0. □

Dem del Teo: Para ver la numerabilidad de $\overline{\mathbb{Q}}$, basta ver que $\mathbb{Q}[x]$ es numerable y que cada polinomio tiene finitas raices.

Para ver que $\overline{\mathbb{Q}}$ es un cuerpo tomamos a y b en $\overline{\mathbb{Q}}$. Como a y b son algebraicos sobre $\mathbb{Q}$ se tiene que $\mathbb{Q}[a]$ es un cuerpo y, además, b es tambien algebraico sobre $\mathbb{Q}[a]$. En particular $\mathbb{Q}[a][b]$ es un cuerpo que contiene a a y b y, por el lema previo, dicho cuerpo esta contenido en $\overline{\mathbb{Q}}$. Luego $a+b$ y $ab \in \overline{\mathbb{Q}}$, lo que implica que $\overline{\mathbb{Q}}$ es un cuerpo. □

Ejercicio 3.64. *Sea $F \subset L \subset K$ extensiones de cuerpo. Pruebe que si K/L y L/F son algebraicos, entonces K/F es algebriaco. En particular, todo polinomio en $\overline{\mathbb{Q}}[x]$ tiene al menos una raiz en $\overline{\mathbb{Q}}$.*

Si bien el argumento previo muestra que la mayoria de los numeros son trascendentes, dicha prueba no entrega ningun numero trascendente explícito. Actualmente se sabe por ejemplo que π y e son trascendentes, pero la prueba es dificil. Un ejemplo explicito (previo al argumento de Cantor!) fue fabricado por Liouville.

Teorema 3.65 (Liouville 1844)**.** *El número $L = \sum_{k \geq 0} 10^{-k!}$ es trascendente.*

Precisamos el siguiente

Lema 3.66. *Si α es un numero irracional y algebraico, entonces existe $n \geq 1$ y $C > 0$ tal que $|\alpha - p/q| \geq C/q^n$ para todo $p/q \in \mathbb{Q}$.*

El lema nos dice que los irracionales algebraicos no se aproximan muy bien por racionales. La demostracion del Teorema de Liouville consiste en mostrar que L es irracional y si se aproxima bien racionales.

Demostración del Teorema de Liouville: Es claro que L no es racional pues su expansion decimal no es periodica. Mas aún, si hacemos

$$p/q = \sum_{k=0}^{r} 10^{r!-k!}/10^{r!},$$

entonces

$$|\alpha - p/q| = |\alpha - \sum_{k=0}^{r} 10^{-k!}| \leq \sum_{k=r+1}^{\infty} 10^{-k!} \leq 2/10^{(r+1)!}.$$

Como dicha desigualdad vale para todo $r \in \mathbb{N}$, se sigue que α no satisface la conclusion del Lema previo. En efecto suponga que si cumple la conclusion para algun C y n, entonces para todo r se tendrá

$$C/10^{r!\cdot n} = C/q^n \leq |\alpha - p/q| \leq 2/10^{(r+1)!},$$

lo que no vale para todo r. Concluimos entonces que α no puede ser algebraico. □

Demostración del Lema 3.66: Suponga que α es irracional y $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ es un polinomio de grado n tal que $f(\alpha) = 0$.

Tomamos $M = \text{máx}\{|f'(x)| \mid x \in [\alpha - 1, \alpha + 1]\}$, donde f' es la derivada, y $\alpha_1, \ldots, \alpha_m$ las otras posibles raices reales de $f(x)$. Sea $C < \text{mín}\{1, 1/M, |\alpha - \alpha_1|, \ldots, |\alpha - \alpha_m|\}$. En búsqueda de contradicción suponemos que existe $p/q \in \mathbb{Q}$ tal que

$$|\alpha - p/q| \leq C/q^n.$$

Puesto que $C/q^n \leq C$ concluimos que $p/q \in [\alpha - 1, \alpha + 1]$, que p/q no es raiz de $f(x)$ y, mas aún, que no hay ninguna raíz de $f(x)$ entre α y p/q.

Por otro lado, por el teorema del valor medio, tenemos que para algún x_0 entre α y p/q se tiene que

$$-f(p/q) = f(\alpha) - f(p/q) = f'(x_0)(\alpha - p/q).$$

En particular $f'(x_0) \neq 0$ y $|\alpha - p/q| = \left|\frac{f(p/q)}{f'(x_0)}\right|$. Pero

$$|f(p/q)| = \left|\sum_{i=0}^{n} c_i p^i q^{-i}\right| = \frac{1}{q^n}\left|\sum_{i=0}^{n} c_i p^i q^{n-i}\right| \geq \frac{1}{q^n},$$

donde la última desigualdad sigue de que la ultima suma es un entero distinto de 0 (acá usamos que $f \in \mathbb{Z}[x]$ y $f(p/q) \neq 0$). Asi, podemos concluir que

$$|\alpha - p/q| = \left|\frac{f(p/q)}{f'(x_0)}\right| \geq \frac{1}{q^n M} > \frac{C}{q^n} \geq |\alpha - p/q|.$$

Contradiccion. □

3.7. Irreducibilidad de polinomios en $\mathbb{Q}[x]$

Hemos visto que en un anillo de polinomios $k[x]$, los ideales maximales son ideales generados por polinomio irreducible. En esta sección revisaremos algunos criterios de irreducibilidad para polinomios en $\mathbb{Q}[x]$ y probaremos que hay muchos (i.e. infinitos) irreducibles en $\mathbb{Q}[x]$. Como hemos visto, esto nos provee de una cantidad infinita de cuerpos intermedios entre $\mathbb{Q}$ y $\mathbb{C}$.

Nuestro primer resultado importante será que la irreducibilidad en $\mathbb{Q}[x]$ equivale a irreducibilidad en $\mathbb{Z}[x]$ (salvo en el caso de las constantes). Luego, veremos criterios concretos de irreducibilidad en $\mathbb{Z}[x]$.

Definición 3.67. Un polonimio $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Q}[x]$ se dice **primitivo** si sus coeficientes son enteros, si el maximo comun divisor de sus coeficientes es 1 y si a_n es positivo.

Lema 3.68 (Gauss)**.** Un entero (*i.e.* polinomio de grado cero) es un primo en $\mathbb{Z}[x]$ si y solo si es un entero primo. En particular

1. Un primo $p \in \mathbb{Z}$ divide a $p(x)q(x)$ si y solo si divide a uno de ellos.

2. El producto de elementos primitivos en $\mathbb{Q}[x]$ es primitivo.

Dem: Claramente, si $n \in \mathbb{Z}$ no es entero primo entonces n no es primo en $\mathbb{Z}[x]$.

Para el reciproco tomamos $p \in \mathbb{Z}$ un entero primo. Queremos demostrar que p es un primo en $\mathbb{Z}[x]$. Para ello, en busqueda de contradiccion, suponemos que p divide a $q(x)r(x)$, pero no a $q(x)$ ni $r(x)$. Entonces hay coeficientes r_{i_0} y q_{j_0} que no son divisibles por p. Elegimos dichos coeficientes i_0 y j_0 lo mas chico posible. El coeficiente de $x^{i_0+j_0}$ en $q(x)r(x)$ es

$$\sum_{i+j=i_o+j_o} r_i q_j = r_{i_0} q_{j_0} + \sum_{i+j=i_0+j_0\,,\, i\neq i_0} r_i q_j.$$

Pero la ultima sumatoria es divisible por p, pues en cada sumando aparece un $i < i_0$ o un indice $j < j_0$. Por otro lado p divide a $p(x)r(x)$, lo que implica que p divide a la suma de la izquierda. Concluimos que p divide a $r_{i_0} q_{j_0}$, lo que entrega la contradicción deseada.

Las afirmaciones 1 y 2 siguen inmediatamente. □

Teorema 3.69 (Gauss)**.** *Sea $f_0(x)$ un polinomio primitivo y $g(x)$ un polinomio con coeficientes enteros. Si $f_0(x)$ divide a $g(x)$ en $\mathbb{Q}[x]$, entonces tambien lo divide en $\mathbb{Z}[x]$. Ademas, si $f(x)$, $g(x) \in \mathbb{Z}[x]$ tienen un divisor comun no constante en $\mathbb{Q}[x]$, entonces tienen un divisor comun no constante en $\mathbb{Z}[x]$. En particular, si un polinomio no constante $f(x)$ es irreducible en $\mathbb{Z}[x]$, tambien lo es en $\mathbb{Q}[x]$.*

Para la prueba necesitamos el siguiente

Lema 3.70. *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio no constante. Luego, $f(x) = c f_0(x)$ con c un racional y $f_0(x)$ un polinomio primitivo. Esta descomposición es unica. Mas aun, c es un entero si y solo si $f(x)$ tiene coeficientes enteros, en cuyo caso c corresponde al máximo comun divisor de los coeficientes de $f(x)$.*

Dem: Primero multiplicamos $f(x)$ por un entero d de modo que los coeficientes de $f_1(x) = df(x)$ sean entero. Luego extraemos el máximo comun divisor de los coeficientes de $f_1(x)$ y ajustamos el signo de modo que $f_1(x) = cf_0$ tenga coeficiente lider positivo. Asi obtenemos que $f(x) = \frac{c}{d} f_0(x)$ como queriamos.

La unicidad de esta descomposición sigue pues si $f_0(x)$ y $f_0'(x)$ son polinomios primitivos tales que $cf_0(x) = c' f_0'(x)$, entonces existe un entero d tal que $dc\, f_0(x) = dc'\, f_0'(x)$ tiene coeficientes enteros. Ahora, por ser f_0 y f_0' primitivos, se tiene que si un entero n divide a $dcf_0(x)$ entonces dicho entero tiene que dividir a dc.

Concluimos que un primo p divide $dc\, f_0(x) = dc'\, f_0'(x)$, si y solo si divide a dc y a dc'. Esto dice que los divisores primos de dc son los mismos que los de dc', lo que implica que $dc = dc'$, lo que a su vez implica $f_0(x) = f_0'(x)$. Luego la unicidad de la descomposicion.

La ultima afirmacion sigue de lo hecho hasta ahora. □.

Dem del Teorema de Gauss: Suponga que $g(x) = f_0(x)q(x) \in \mathbb{Z}[x]$ con $f_0(x)$ primitivo y $q(x)$ un polinomio con coeficientes racionales. Veremos que $q(x)$ tiene coefiientes enteros. Por el lema previo podemos escribir $g(x) = cg_0(x)$ y $q(x) = c'q_0(x)$, con $g_0(x)$ y $q_0(x)$ primitivos. Luego $g(x) = cg_0(x) = c' f_0(x)q_0(x)$. Por el Lema de Gauss se tiene que $f_0(x)q_0(x)$ es primitivo, y por la unicidad de dicha descomposición se tiene que $g_0(x) = f_0(x)q_0(x)$ y $c = c'$. Pero c era entero pues $g(x)$ lo era, luego $q(x) = cq_0(x) \in \mathbb{Z}[x]$.

La segunda afirmación sigue de la primera. En efecto si $h(x) \in \mathbb{Q}[x]$ divide a dos polinomios con coeficientes enteros $f(x)$ y $g(x)$, entonces su polinomio primitivo asociado $h_0(x)$ tambien divide a f y g en $\mathbb{Q}[x]$. Luego, por la primera afirmacion, $h_0(x)$ tambien divide a $f(x)$ y $g(x)$ divide en $\mathbb{Z}[x]$. Asi, $h_0(x)$ es divisor comun de $f(x)$ y $g(x)$ en $\mathbb{Z}[x]$. □

Antes de pasar a criterios concretos de irreducibilidad, veremos que, aunque $\mathbb{Z}[x]$ no sea un Dominio de Ideales principales, de todas maneras se tiene que $p(x) \in \mathbb{Z}[x]$ es irreducible si y solo si es primo.

Corolario 3.71. Todo irreducible de $\mathbb{Z}[x]$ es primo (la reciproca vale en general).

Demostración: Sea $p(x) \in \mathbb{Z}[x]$ un polinomio irreducible. Eventualmente multiplicando por -1, podemos suponer que el coeficiente lider de $p(x)$ es positivo, es decir, $p(x)$ es primitivo. Es claro que si $p(x)$ es constante entonces $p(x)$ es irreducible si y solo si $p(x)$ es un entero primo. Luego, solo hay que analizar el caso en que $p(x)$ no sea constante.

Suponga que $p(x)$ divide a $q(x)r(x)$. Queremos demostrar que $p(x)$ divide a $q(x)$ o a $r(x)$, para lo cual miramos todo con ojos de $\mathbb{Q}[x]$ (que es un DIP!!). Primero notamos que $p(x)$ por ser primitivo y no constante, $p(x)$ es irreducible en $\mathbb{Q}[x]$ por el Teorema de Gauss. Luego, como $\mathbb{Q}[x]$ es un DIP, se tiene que $p(x)$ divide, en $\mathbb{Q}[x]$, a $q(x)$ o a $r(x)$. Digamos $p(x)$ divide a $q(x)$. Pero, nuevamente por el Teorema de Gauss, tenemos que $p(x)$ divide a $q(x)$ en $\mathbb{Z}[x]$. □

Dos criterios de irreducibilidad en $\mathbb{Z}[x]$. Hemos visto, entre otras cosas, que los irreducibles de $\mathbb{Q}[x]$ corresponden de manera canónica a irreducibles en $\mathbb{Z}[x]$. Ahora

damos dos criterios muy utiles de irreducibilidad.

Para enunciar el primero, dado p un entero primo, y $F_p = \mathbb{Z}/p\mathbb{Z}$, el cuerpo con p elementos. Definimos $\psi_p : \mathbb{Z}[x] \to F_p[x]$, por

$$\psi_p(a_n x^n + \ldots + a_0) = \bar{a}_n x^n + \ldots + \bar{a}_0,$$

donde $\bar{a}_i$ es el residuo p. Queda como ejercicio verificar que ϕ_p es un homomorfismo de anillos.

Proposición 3.72. *Sea p un primo y $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ un polinomio con coeficiente lider no divisible por p. Si $\bar{f} = \psi_p(f)$ es irreducible en $F_p[x]$, entonces f es irreducible en $\mathbb{Q}[x]$.*

Dem: Sea f como en la proposición. Probaremos que si f es reducible, entonces $\bar{f}$ tambien.

Si $f = gh$ es una factorizacion no trivial en $\mathbb{Q}[x]$, en particular, el grdo de g y h es positivo. Ademas, podemos suponer por el Teorema 3.69 que dicha factorizacion ocurre en $\mathbb{Z}[x]$.

Como ψ_p es un homomorfismo y $\bar{a}_n \neq 0$, tenenmos que $\bar{f} = \bar{g}\bar{h}$, y $gr(f) = gr(\bar{f}) = gr(\bar{g}) + gr(\bar{h})$. Esto implica que $gr(g) = gr(\bar{g})$ y $gr(h) = gr(\bar{h})$, lo que dice que la factorizacion en $F_p[x]$ era no trivial □

Lema 3.73 (Criterio de Eisenstein)**.** Sea $f(x) = a_n x^n + \ldots + a_0$ un polinomio con coeficientes entros. Sea p un entero primo. Suponga que los coeficientes de $f(x)$ satisfacen lo siguiente

- p no dicide a a_n,
- p divide a $a_{n-1}, \ldots, a_0$,
- p^2 no divide a a_0.

Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Por ejemplo $x^4 + 5x^3 + 5x^2 + 5$ y $x + 2$ son irreducibles.

Dem: Sea $f(x) = a_n x^n + \ldots + a_0$ un polinomio satisfaciendo las hypotesis, en particular $f(x)$ no es constante. Denotamos por $\overline{f}(x)$ su residuo modulo p. Se tiene que $\overline{f}(x) = \bar{a}_n x^n \neq 0$. Si $f(x)$ fuera reducible en $\mathbb{Q}[x]$ entonces por el Teorema 3.69, se tiene que $f(x)$ se factoriza en polinomios no constantes en $\mathbb{Z}[x]$, digamos $f(x) = g(x)h(x)$, donde $b(x) = b_r x^r + \ldots + b_0$, $h(x) = h_k x^k + \ldots + h_0$. Psando modulo p esto queda $\bar{f}(x) = \bar{g}(x)\bar{h}(x) = \bar{a}_n x^n$. Esto implica que

$$\bar{g}(x) = \bar{b}_r x^r \quad \text{y} \quad \bar{h}(x) = \bar{h}_k x^k,$$

es decir, p divide a todos los coeficientes, salvo el primero, de g y h. Pero esto implica que a_0 es divisible por p^2, lo que contradice las hypotesis. Luego f era irreducible. □

Ejemplo 3.74. El polinomio $x^n - p$, con $p \in \mathbb{Z}$ un primo, es irreducible.

Damos ahora una aplicación: para un primo p, definimos

$$\Phi_p(x) = x^{p-1} + x^{p-1} + \ldots + x + 1$$

el polinomio se *ciclotómicos*. Note que $\Phi_p(x)(x-1) = x^p - 1$, luego toda raiz de $\Phi_p(x)$ es una raiz de la unidad.

Mas aun, $\Phi_p(x)$ es irreducible en $\mathbb{Q}[x]$. En efecto si hacemos el cambio de variable $x = y + 1$, se tiene que

$$\Phi_p(y+1)(y+1-1) = (y+1)^p - 1 = y^p + a_{p-1}y^{p-1} + \ldots + a_2y^2 + py + 1 - 1,$$

donde cada a_i es divisible por p. Luego, $\Phi(y+1) = y^{p-1} + a_{p-1}y^{p-2} + \ldots + a_2y + p$, es irreducible por el criterio de Eisenstein.

3.8. El grupo de Galois de una extensión de cuerpos

Sean K y L dos extensiones de un cuerpo F. Un **F-automorfismo** de K a L es un homomorfismo de anillos $\tau : K \to L$ que τ fija a F punto a punto. En particular, τ es F-lineal e inyectivo. Se sigue que si $K = L$ y $[K : F] < \infty$, entonces τ es un isomorfismo de cuerpos.

Definición 3.75. Sea K un cuerpo que extiende a F. El **grupo de Galois** de K/F es $Gal(K/F) = \{\tau : K \to K \mid \tau \text{ es un } F\text{-automorfismo}\}$. Ciertamente $Gal(K/F)$ es un grupo bajo composición.

Ejemplo 3.76. Sea $\tau : \mathbb{C} \to \mathbb{C}$, $\tau(z) = \overline{z}$, la conjugación compleja (i.e. $\tau(x + iy) = x - iy$). Se tiene que $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$ y $\overline{z + w} = \overline{z} + \overline{w}$, luego τ es un $\mathbb{R}$-automorfismo de $\mathbb{C}$.

Proposición 3.77. Sea $a \in K$ algebraico sobre F, $p(x) = min(F, a)(x) \in F[x]$, y $\tau \in Gal(F[a]/F)$. Entonces τ queda completamente determinado por su acción en a, y, mas aún, $\tau(a)$ es una raiz de $p(x)$.

Demostración: Sabemos que $B = \{1, a, \ldots, a^{n-1}\}$ es una base de $F[a]$ como F-espacio vectorial, donde $n = gr(min(F, a)(x))$. Suponga que $\alpha \in Gal(F[a]/F)$ cumple que $\alpha(a) = \tau(a)$. Afirmamos que α y τ coinciden sobre B, y por lo tanto son iguales. En efecto, $\alpha(a^j) = \alpha(a)^j = \tau(a)^j = \tau(a^j)$. Luego τ esta determinado por su acción en a.

Para terminar afirmamos que $p(\tau(a)) = 0$. En efecto se tiene que $p(x) = x^n + \beta_{n-1}x^{n-1} + \ldots + \beta_0$, con $\beta_i \in F$. Luego, $0 = \tau(0) = \tau(p(a)) = p(\tau(a))$, por ser τ un F-homomorfismo. □

Lema 3.78. Sea τ un F-automorfismo de K/F, $a \in K$ algebraico y $f(x) \in F[x]$ tal que $f(a) = 0$, entonces $f(\tau(a)) = 0$. En particular, $min(a, F) = min(\tau(a), F)$.

Dem: $0 = \tau(f(a)) = f(\tau(a))$. De esto se sigue que $min(a; F)$ divide a $min(\tau(a), F)$. La otra division se sigue usando τ^{-1} o la irreducibilidad. □

Ejemplo 3.79. La proposición anterior es útil para calcular el grupo de Galois de una extensión algebraica. Por ejemplo, si $K = \mathbb{Q}[\sqrt[3]{2}]$, entonces $Gal(K/\mathbb{Q})$ es trivial.

En efecto 1, $\sqrt[3]{2}$, $\sqrt[3]{2}^2$ es una base de $K/\mathbb{Q}$. Además, el polinomio minimal de $\sqrt[3]{2}$ es $p(x) = x^3 - 2$, y sus otras raices complejas son $\sqrt[3]{2}\,\omega$ y $\sqrt[3]{2}\,\omega^2$, donde $\omega^3 = 1$ y $\omega \neq 1$. Afirmamos que ni $\sqrt[3]{2}\,\omega$ ni $\sqrt[3]{2}\,\omega^2$ viven en K, lo que implica que $Gal(K/\mathbb{Q})$ es trivial. En efecto si $\sqrt[3]{2}\,\omega \in K$ se tiene, multiplicando por $\sqrt[3]{2}$, que $\omega \in K$. Conlcuimos que K contiene a $\mathbb{Q}[\omega]$. Pero el polinomio minimal de ω es $x^2 + x + 1$ y luego $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2$. Lo que no puede ser pues $[K : \mathbb{Q}] = 3$.

Ejercicio 3.80. Pruebe la siguiente generalización de la proposición anterior: Si $a_1, \ldots, a_n \in K$ son algebraicos sobre F, entonces la acción de $\tau \in Gal(F[a_1, \ldots, a_n]/F)$ esta totalemente determinada por la acción de τ sobre $a_1, \ldots, a_n$.

Corolario 3.81. Si K/F es una extension finita, entonces $Gal(K/F)$ es finito.

Dem: Como la extension es finita, $K = F(a_1, \ldots, a_n)$ con los a_i algebraicos. Por ende un automorphismo permuta las raices de cada $min(a_i, F)$, luego $([K : F]!)^{[K:F]}$ es una cota (muy grosera) para la cardinalidad de $Gal(K/F)$. □