Estructuras Algebraicas

Pablo Pallàs

31 de marzo de 2023

Índice

1. Generalidades sobre grupos **2**
1.1. Primeras definiciones 2
1.2. Subgrupos normales y grupos cociente 19
1.3. Homomorfismos y teoremas de isomorfía 26

2. Grupos cíclicos **35**
2.1. La función de Euler 35
2.2. Grupos cíclicos 38

3. Grupos de automorfismos **44**
3.1. Grupos de automorfismos y automorfismos internos 44
3.2. Producto directo y semidirecto 50

4. Acciones de grupos. Teoremas de Sylow **52**
4.1. Acciones de grupos sobre conjuntos 52
4.2. Teoremas de Sylow 60

5. Grupos de permutaciones **63**
5.1. Introducción y Teorema de Cayley 63
5.2. El homomorfismo índice y el grupo alternado 71
5.3. El teorema de Abel 73

6. Generalidades sobre anillos **75**
6.1. Introducción 75
6.2. Homomorfismos de anillos 88

7. Divisibilidad de anillos **94**
7.1. Dominio euclídeo 95
7.2. Dominio de ideales principales 96
7.3. Dominio de factorización única 100
7.4. Anillos de restos 105

8. Anillos de polinomios **108**

1. Generalidades sobre grupos

1.1. Primeras definiciones

Definición 1.1. *Un **grupo** es un conjunto no vacío G en el que está definida una operación binaria interna, que llamaremos $\cdot$*

$$\begin{array}{rccc} \cdot : & G \times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a \cdot b = ab \end{array}$$

con $a, b \in G$. Además, dicha operación binaria cumple:

I. *$\cdot$ es **asociativa**.*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G.$$

II. *G tiene **elemento neutro** para $\cdot$, que denotamos 1_G. Se tiene que*

$$a \cdot 1_G = 1_G \cdot a = a \quad \forall a \in G.$$

III. *Todos los elementos de G son invertibles para $\cdot$, es decir:*

$$\forall a \in G \quad \exists a^{-1} \text{ tal que } a \cdot a^{-1} = a^{-1} \cdot a = 1_G.$$

*Se dice que a^{-1} es el **inverso** de a.*

*Diremos que los elementos $a, b \in G$ conmutan si $a \cdot b = b \cdot a$. Si cada par de elementos de G conmutan se dice que el grupo G es **abeliano**.*

En ocasiones, escribiremos $(G, \cdot)$ para hablar de un grupo G cuando queramos destacar el hecho de que el conjunto G es un grupo con la operación binaria $\cdot$, que ya sabemos que llamaremos multiplicación.

Propiedades 1.1.1. *A partir de estos axiomas podemos deducir una serie de propiedades:*

1. *El elemento neutro de un grupo es único, en efecto, si existieran dos, digamos e_1 y e_2, entonces $e_1 = e_1 e_2 = e_2$, puesto que e_2 es neutro y e_1 también.*
2. *El inverso de cada elemento es también único. En efecto, sean b y c inversos de a. Entonces*

   $$b = b1_G = b(ac) = (ba)c = 1_G c = c$$

   Además, si $ab = 1_G$ entonces a es el inverso de b y b es el inverso de a, pues

   $$a^{-1} = a^{-1}1_G = a^{-1}(ab) = (a^{-1}a)b = 1_G b = b$$

   $$b^{-1} = 1_G b^{-1} = (ab)b^{-1} = a(bb^{-1}) = a1_G = a$$

3. *Cada elemento es el inverso de su inverso, esto es, $(a^{-1})^{-1} = a$. Consecuencia inmediata de las igualdades $aa^{-1} = a^{-1}a = 1_G$ y la unicidad del inverso.*
4. *Dados $a, b \in G$, se tiene $(ab)^{-1} = b^{-1}a^{-1}$ ya que*

   $$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1_G$$

5. *Dados $a, b, c \in G$ tales que $ab = ac$ se tiene que $b = c$, pues multiplicando por la izquierda ambos miembros de la igualdad inicial por a^{-1}, resulta*

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = c$$

Análogamente, si $ba = ca$ entonces $b = c$. Esta propiedad se llama ***propiedad cancelativa****.*

Ejemplo 1.1.1. *Algunos ejemplos:*

1. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la suma son grupos abelianos.*
2. *$\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con el producto también son grupos abelianos.*
3. *El conjunto $\mathfrak{M}_{m\times n}(\mathbb{R})$ de todas las matrices reales de tamaño $m \times n$ es un grupo abeliano con la adición de matrices.*
4. *El conjunto $\mathfrak{M}_n(\mathbb{R})$ de todas las matrices reales de tamaño $n\times n$ no es un grupo con la multiplicación de matrices, ya que no todas las matrices cuadradas son invertibles. En cambio, el conjunto*

$$GL_n(\mathbb{R}) = \{A \in \mathfrak{M}_n(\mathbb{R}) : det(A) \neq 0\}$$

de todas las matrices invertibles de tamaño $n\times n$ es un grupo con la multiplicación de matrices que, en general, no es abeliano. Llamaremos ***grupo general lineal*** *a dicho grupo.*

Consideremos ahora el siguiente conjunto

$$SL_n(\mathbb{R}) = \{A \in \mathfrak{M}_n(\mathbb{R}) : det(A) = 1\}$$

Es fácil comprobar que $SL_n(\mathbb{R})$ es un grupo con la multiplicación de matrices que, en general, no será abeliano. Lo llamaremos ***grupo especial lineal****.*

Aunque aún no conozcamos la noción de subgrupo, de contenido entre grupos, si que es evidente ver que en cuanto a conjuntos $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$.

A propósito del anterior, del grupo general lineal, sabemos que es un grupo abeliano con la operación multiplicación de matrices. Su elemento neutro es la matriz identidad, y se tiene

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow A^{-1} = \tfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

5. *El conjunto $G = \{1, i, -1, -i\}$ con la operación multiplicación es un grupo. En efecto, el elemento neutro es el 1, la operación es cerrada y todo producto de elementos pertenece a G, se cumple la propiedad asociativa y todo elemento tiene inverso: $1^{-1} = 1$, $(-1)^{-1} = -1$, $i^{-1} = -i$ y $(-i)^{-1} = i$.*
6. *Consideramos $C = \{z = a + bi \in \mathbb{C} : |z|^2 = a^2 + b^2 = 1\}$ el subconjunto de los números complejos formado por los elementos de la circunferencia de radio uno. Es un grupo con la operación multiplicación compleja. Si n es un entero positivo, el subconjunto de C formado por las n raíces n-ésimas de la unidad*

$$C_n = \{\xi^k : k = 0, \ldots, n-1\},$$

con $\xi = \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$ *es también un grupo con la multiplicación. En concreto es un tipo especial de grupo del que hablaremos más adelante.*

■

Además, en un grupo G no sólo vamos a poder multiplicar elementos, también subconjuntos (y lo que más tarde conoceremos como subgrupos). Así, dados dos subconjuntos $X, Y \subseteq G$, escribiremos

$$XY = \{xy : x \in X, y \in Y\} \subseteq G.$$

Por asociatividad, tenemos que si $Z \subseteq G$, entonces

$$(XY)Z = X(YZ).$$

También definimos

$$X^{-1} = \{x^{-1} : x \in X\}.$$

Proposición 1.2. *Tenemos:*

1. *La aplicación*

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array}$$

   es una biyección.

2. *Si $g \in G$, entonces las aplicaciones*

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & xg \end{array}$$

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gx \end{array}$$

   son biyectivas.

Demostración:

1. Veamos que es biyectiva. Si $x^{-1} = y^{-1}$, con $x, y \in G$, entonces $x = (x^{-1})^{-1} = (y^{-1})^{-1} = y$, y así es inyectiva. Ahora, si $z \in G$ tenemos que z es el inverso de z^{-1}, y así también es sobreyectiva.

2. Veamos que la aplicación

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & xg \end{array}$$

   es biyectiva, y con la otra será análoga. Sea $xg = yg$, entonces multiplicando por g^{-1} por la derecha tenemos que $x = y$ y así es inyectiva. Por otro lado, si tenemos un $z \in G$ entonces $zg^{-1}g = z$ y así es también sobreyectiva.

□

Siempre que estudiemos una estructura algebraica se darán definiciones, nociones generales y alguna propiedad sobre ella, pero sin duda una de las cuestiones más importantes será ver si esa estructura contiene o puede contener a subconjuntos que también estén dotados con la misma estructura. En el caso de los grupos sí ocurre y corresponde, como ya sabemos, a la noción de *subgrupo*. Este hecho es de especial relevancia para la *Teoría de Grupos*.

Definición 1.3. *Un subconjunto H de un grupo G se dice* ***subgrupo*** *de G (y se escribe $H \leq G$) si, con la misma operación que G, es un grupo.*

Esta definición nos proporciona una idea de lo que estamos hablando cuando nos referimos a un subgrupo, es algo así como un grupo más pequeño contenido en el grupo grande. A nivel cualitativo nos puede servir pero necesitaremos una forma de definir también, o mejor dicho de decidir, si un elemento $x \in G$ pertenece también a un subgrupo H. Para ello daremos algunas formas de caracterizar a los subgrupos. Una de ellas se desprende inmediatamente de la definición, y es que dados $x, y \in G$ entonces sabemos que $xy \in G$ y como H también es grupo con la misma operación de G ($\cdot$ en este caso, pero que omitimos su notación) entonces en caso de que $x, y \in H$ también $xy \in H$. Pero además de este hecho un subgrupo tiene que cumplir lo siguiente:

Propiedades 1.3.1. *Dado H un subgrupo de G, tenemos:*

1. *1_G pertenece a H y es su elemento neutro.*
2. *Si $x \in H$, entonces también $x^{-1} \in H$.*

Demostración:

1. Por definición H ha de tener elemento neutro, que llamaremos u. Es claro que $uu = u$. Sea $u^{-1} \in G$ el inverso de u en G. Entonces $u^{-1}(uu) = u^{-1}u = 1_G$, luego $(u^{-1}u)u = 1_G$, y así $1_G u = 1_G$. Esto quiere decir que $u = 1_G$.
2. Es simplemente consecuencia de lo anterior, si $x \in H$, existirá un $y \in H$ tal que $xy = 1_G \in H$, y de ahí se sigue.

□

Ejemplo 1.3.1. *Veamos los siguientes ejemplos:*

1. *Consideremos el subconjunto $H = \{1, -1\} \subseteq \mathbb{R}^*$ (y por tanto de $\mathbb{R}$). Claramente, H es un grupo con la multiplicación de números reales, pero no lo es con la adición de números reales, por tanto, H es subgrupo del grupo multiplicativo $\mathbb{R}^*$, pero no del grupo aditivo $\mathbb{R}$.*
2. *Anteriormente hemos visto que $G = \{1, i, -1, -i\}$ es un grupo con la multiplicación de números complejos, por tanto, G es un subgrupo del grupo multiplicativo $\mathbb{C}^*$.*
3. *El grupo aditivo $\mathbb{Z}$ es un subgrupo del grupo aditivo $\mathbb{Q}$, que a su vez es subgrupo del grupo aditivo $\mathbb{R}$ y éste lo es del grupo aditivo $\mathbb{C}$.*

De igual manera, el grupo multiplicativo $\mathbb{Q}^*$ es subgrupo del grupo multiplicativo $\mathbb{R}^*$ y éste lo es del grupo multiplicativo $\mathbb{C}^*$.

■

Así, una vez visto la noción de subgrupo veamos una forma de caracterizarlos bastante útil y la que se suele emplear:

Proposición 1.4. *Sea H un subconjunto no vacío de un grupo G. Entonces, tenemos las siguientes condiciones equivalentes:*

1. *H es subgrupo de G.*
2. *Para cada par de elementos $x, y \in H$ se tiene que $xy^{-1} \in H$*

Demostración:
1. $\Rightarrow$ 2. Dados dos elementos $x, y \in H$, sabemos que entonces $y^{-1} \in H$. El producto es una operación binaria interna en H, porque H es subgrupo. Así, como $x, y^{-1} \in H$, se tiene que $xy^{-1} \in H$.
2. $\Rightarrow$ 1. Sea $x \in H$. Ahora, si tomamos $y = x$ tenemos que

$$xx^{-1} \in H$$

y así $1_G \in H$, luego H tiene elemento neutro. Ahora, dado un $y \in H$, si tomamos $x = 1_G \in H$, tenemos que

$$y^{-1} = 1_G y^{-1} = xy^{-1} \in H$$

luego cada elemento de H tiene inverso en H. Finalmente, dados $x, y \in H$ ya sabemos que $z = y^{-1} \in H$, luego

$$xy = x(y^{-1})^{-1} = xz^{-1} \in H$$

y así la operación de G es una operación binaria interna de H. La asociatividad es evidente, pues lo es para cada terna de elementos de G.

□

Observación 1.4.1. *Tanto $\{1_G\}$ como G son siempre subgrupos. Llamaremos* ***subgrupos propios*** *de G a aquellos subgrupos distintos de $\{1_G\}$ y G.*

Veamos ahora un ejemplo interesante de subgrupo, en este caso los de $\mathbb{Z}$:

Ejemplo 1.4.1. *Supongamos que $m \in \mathbb{Z}$ con $m > 1$ y consideremos el conjunto*

$$m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$$

de todos los múltiplos de m. Claramente $m\mathbb{Z} \neq \emptyset$.

Supongamos que $a, b \in m\mathbb{Z}$, entonces $a = mx$ y $b = my$ para algunos $x, y \in \mathbb{Z}$. Ahora,

$$a - b = mx - my = m(x - y) \in m\mathbb{Z},$$

ya que $x - y \in \mathbb{Z}$.

Por tanto, por 1.4 tenemos que es subgrupo del grupo aditivo $\mathbb{Z}$. De hecho, los subgrupos de $\mathbb{Z}$ son todos de esa forma, con m un entero cualquiera.

■

Notar que en este caso hemos cambiado la notación empleada para la operación. En vez de escribir ab^{-1} hemos escrito $a - b$, esto es así porque $\mathbb{Z}$ es un grupo abeliano y para éstos se suele emplear este tipo de notación, que se conoce como aditiva.

Ya sabemos cómo son y cómo se caracterizan los subgrupos, ahora veremos cómo podemos obtenerlos a partir de ciertos conjuntos de elementos, que llamaremos generadores.

Definición 1.5. *Si S es un subconjunto no vacío de un grupo G, el conjunto*

$$\langle S\rangle = \{s_1^{h_1} \dots s_n^{h_n} : n \in \mathbb{N},\ s_i \in S,\ h_i \in \mathbb{Z},\ \ 1 \leq i \leq n\}$$

es un subgrupo de G que contiene a S, llamado ***subgrupo generado por*** *S.*

Si $\mathcal{F}$ es la familia de todos los subgrupos de G que contienen a S,

$$\langle S\rangle = \bigcap_{H\in\mathcal{F}} H$$

y, en particular, $\langle S\rangle \subseteq H$ para cada $H \in \mathcal{F}$.

Observación 1.5.1. *Un caso particular pero muy importante es aquel en que $S = \{a\}$ con $a \in G$. En tal caso escribimos $\langle a\rangle$. Y tenemos que,*

$$\langle a\rangle = \{a^k : k \in \mathbb{Z}\}$$

y se le llama ***subgrupo generado por a****.*

De hecho, a partir de este caso surgirán una tipo de grupos de sobra conocidos, los *grupos cíclicos*, que estarán generados por un sólo elemento, ya que el resto de elementos del grupo serán sus potencias.

Definición 1.6. *Un subconjunto no vacío S de un grupo G se llama* ***sistema generador*** *de G si $G = \langle S\rangle$. Un grupo G que posee un sistema finito de generadores se llama finitamente generado.*

Ya hemos definido lo que son los grupos abelianos, y hemos visto que ha de cumplirse la propiedad conmutativa. Esto en general no se tendrá en grupos no abelianos, pero sin embargo sí podremos encontrar subconjuntos de elementos que sí cumplan la propiedad conmutativa, es decir, que sus elementos conmutan. Además vamos a comprobar que a estos subconjuntos les vamos a poder dotar de estructura de grupo (en este caso subgrupo).

Definición 1.7. *Si H es un subgrupo de un grupo G, se llama* ***centralizador*** *de H en G a*

$$C_G(H) = \{x \in G : ax = xa\ \forall a \in H\}.$$

Al centralizador de G en G lo notaremos por $Z(G)$ y le llamaremos ***centro*** *de G. Así,*

$$Z(G) = \{x \in G : ax = xa\ \forall a \in G\}.$$

y como consecuencia se tiene que G es abeliano si y sólo si $G = Z(G)$. Además, el centro es un subgrupo de G. De hecho más en general todavía: se tiene que $C_G(H)$ es un subgrupo de G

Demostración: Demostraremos esto último. Como $1_G \in C_G(H)$, éste no es vacío. Sean $x, y \in C_G(H)$, $a \in H$. Como $x \in C_G(H)$, $ax = xa$. Como $y \in C_G(H)$, $a^{-1} \in H$, $a^{-1}y = ya^{-1}$. Por lo tanto,

$$a(xy^{-1}) = (ax)y^{-1} = (xa)y^{-1} = x(ay^{-1}) = x(ya^{-1})^{-1} = x(a^{-1}y)^{-1} = x(y^{-1}a) = (xy^{-1})a$$

luego $xy^{-1} \in C_G(H)$. Así, $C_G(H)$ es un subgrupo de G.

□

Más adelante daremos otras definiciones y llegaremos a estos subgrupos de otra forma a través de unos conceptos que veremos en los siguientes capítulos.

En el caso particular de que $H = \langle a \rangle$ con $a \in G$, entonces $x \in C_G(H) \Leftrightarrow xa = ax$. De hecho, cuando hablemos del centralizador del subgrupo generado por a en G escribiremos $C_G(a)$ en vez de $C_G(\langle a \rangle)$ y

$$C_G(a) = \{x \in G : ax = xa\}$$

y, es obvio que

$$Z(G) = \bigcap_{a \in G} C_G(a).$$

Además, $a \in Z(G) \Leftrightarrow C_G(a) = G$, ya que si $a \in Z(G)$ cada $x \in G$ cumple $ax = xa$, luego $G \subseteq C_G(a) \subseteq G$. Recíprocamente, si $C_G(a) = G$, cada $x \in G$ pertenece a $C_G(a)$, luego $ax = xa$ para cada $x \in G$ y así $a \in Z(G)$.

Ahora definiremos un concepto muy general, que no abarca sólo a subgrupos sino a todo subconjunto no vacío.

Definición 1.8. *Si S es un subconjunto no vacío de un grupo G y $a \in G$, se llama* ***conjugado*** *de S por a al conjunto*

$$S^a = \{axa^{-1} : x \in S\}$$

Diremos que $y \in S^a \Leftrightarrow a^{-1}ya \in S$. Ya que si $y \in S^a \Rightarrow y = axa^{-1} \Rightarrow a^{-1}ya = x$, $x \in S$.

Definición 1.9. *Si H es un subconjunto no vacío de un grupo G, se llama* ***normalizador*** *de H en G a*

$$N_G(H) = \{a \in G : H^a = H\},$$

que además es un subgrupo de G.

Demostración: Ya sabemos que $H^1 = H$, por lo que $1 \in N_G(H)$ y así $N_G(H)$ es no vacío. Por otro lado, si $a, b \in N_G(H)$, $H^{ab^{-1}} = (H^a)^{b^{-1}} = H^{b^{-1}}$ pues $a \in N_G(H)$. Además $H = H^1 = H^{bb^{-1}} = (H^b)^{b^{-1}} = H^{b^{-1}}$, ya que $b \in N_G(H)$. Tenemos entonces que $H^{ab^{-1}} = H$ luego $ab^{-1} \in N_G(H)$.

□

Ahora, antes de seguir notemos la siguiente observación, que es evidente y se refiere a dos propiedades sobre la intersección de subgrupos:

Observación 1.9.1. *Si tenemos una familia no vacía de subgrupos H_i de G, con $i \in I$, entonces la intersección*

$$H = \bigcap_{i \in I} H_i$$

también es subgrupo de G.

Además, para cada $a \in G$, tendremos que

$$H^a = \bigcap_{i \in I} H_i^a.$$

Esto quiere decir que si definimos un subgrupo como la intersección de una colección de subgrupos, su conjugado será también la intersección de los mismos subgrupos de la misma colección conjugados.

Antes ya habíamos dejado claro que no vamos a multiplicar sólo elementos de un grupo, también subconjuntos. Ahora que ya sabemos qué son los subgrupos podemos extender esta noción a ellos.

Definición 1.10. *Dados dos subgrupos H y K de un grupo G, se define*

$$HK = \{hk : h \in H, k \in K\}.$$

A este grupo lo llamaremos ***grupo producto****.*

Sin embargo, este producto no se suele comportar muy bien. En general, el producto de subgrupos no será subgrupo, para que lo sea tendrá que ocurrir lo siguiente:

Proposición 1.11. *HK es subgrupo de G si y sólo si $HK = KH$. Es claro que $H \subseteq HK$ y que $K \subseteq HK$.*

Demostración: Supongamos que HK es subgrupo de G. Si $x = hk \in HK$ entonces $k^{-1}h^{-1} = x^{-1} \in HK$, luego $k^{-1}h^{-1} = uv$ con $u \in H$, $v \in K$ y así $x = hk = (k^{-1}h^{-1})^{-1} = (uv)^{-1} = v^{-1}u^{-1} \in KH$ y esto prueba $HK \subseteq KH$.Sea ahora $y = kh \in KH$. Entonces $z = h^{-1}k^{-1} \in HK$, y como HK es subgrupo $y = kh = (h^{-1}k^{-1})^{-1} = z^{-1} \in HK$, y así $KH \subseteq HK$.

Recíprocamente, supongamos que $HK = KH$. Evidentemente HK es no vacío, pues $1 = 1 \cdot 1 \in HK$. Además, dados $x = h_1k_1$, $y = h_2k_2$, con $x, y \in HK$,$xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1k_3h_2^{-1}$, con $k_3 = k_1k_2^{-1} \in K$. Como $k_3h_2^{-1} \in KH = HK$, $k_3h_2^{-1} = h_3k$, con $h_3 \in H$, $k \in K$. Así, $xy^{-1} = h_1h_3k = hk \in HK$, con $h = h_1h_3 \in H$.

□

Veamos una aplicación de la proposición que acabamos de ver:

Ejemplo 1.11.1. *Sean m y n enteros no negativos, $H = m\mathbb{Z}$, $K = n\mathbb{Z}$ dos subgrupos de $\mathbb{Z}$. Como $\mathbb{Z}$ es abeliano es obvio que $H+K = K+H$, luego por el resultado anterior $H + K$ es subgrupo de $\mathbb{Z}$ (notar que aquí la operación es la suma).*

$H + K$ no es el subgrupo $\{0\}$ pues, $m = m + 0 \in H + K$. Y, como ya sabemos, existirá un $d \in \mathbb{Z}$ tal que $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, veamos que $d = mcd(m, n)$:

Como $m = m+0 \in m\mathbb{Z}+n\mathbb{Z} = d\mathbb{Z}$, d divide a m, y como $n = 0+n \in m\mathbb{Z}+n\mathbb{Z} = d\mathbb{Z}$, d divide a n. Además $d \in d\mathbb{Z} = m\mathbb{Z}+n\mathbb{Z}$ luego existen $a, b \in \mathbb{Z}$, tal que $d = ma+nb$. Entonces dado un c que divida a m y n:

$$m = cu,\ n = cv, u, u \in \mathbb{Z}$$

luego $d = (cu)a + (cv)b = c(ua + vb)$ y c divide a d. Esto prueba que $d = mcd(m, n)$.

En particular, dos números enteros m, n son primos entre sí si y sólo si

$$1 = am + bn \ \ a, b \in \mathbb{Z}.$$

En efecto, si $mcd(m, n) = 1$, es $m\mathbb{Z}+n\mathbb{Z} = 1\mathbb{Z}$ por lo visto ahora. Así, $1 \in m\mathbb{Z}+n\mathbb{Z}$. Recíprocamente, si $1 = am + bn$ y d es un divisor de m y n, tendremos $m = du$, $n = dv$, luego $1 = d(au + bv)$ y así $d = +1$ ó -1. Y como podemos asumir que $mcd(m, n)$ es positivo entonces $mcd(m, n) = 1$.

■

Otra noción importante de un grupo es el número de elementos que tiene, su cardinal si lo vemos como conjunto. Aunque no es exactamente lo mismo, veremos que en algunos grupos podremos tener todos los elementos que queramos pero el orden no será infinito, como es el caso de los *grupos cíclicos*. Además, también vamos a ver cómo extender este concepto a un sólo elemento cualquiera de un grupo G cualquiera, y tendrá una íntima relación con el subgrupo que genera.

Definición 1.12. *Sea G un grupo. Al número de elementos de un subgrupo finito H de G se le llama **orden** de H y lo denotamos por $o(H)$ ó también $|H|$. En particular, cuando G es finito, el número de elementos de G se llama **orden** de G y lo denotaremos $|G|$.. En caso contrario, diremos que G es un grupo infinito.*

*Dado un elemento $a \in G$ llamaremos **orden** de a, y lo denotaremos por $o(a)$, al número de elementos del subgrupo que genera, $\langle a \rangle$. Es decir, que $o(a) = |\langle a \rangle|$.*

Veamos algunas propiedades interesantes del orden y algunos resultados importantes:

Proposición 1.13. *Sea G un grupo y $a \in G$ un elemento de torsión (su subgrupo generado es finito). Entonces:*

1. *Existe $k \geq 1$ tal que $a^k = 1$.*
2. *El orden de a es el menor natural $n \geq 1$ tal que $a^n = 1$*
3. *Si $n = o(a)$, entonces $\langle a \rangle = \{1, a, \cdots, a^{n-1}\}$.*
4. *Si $n = o(a)$ y $k \in \mathbb{N}$, $a^k = 1$ si y sólo si k es múltiplo de n.(n divide a m).*

Demostración: Veamos punto por punto:

1. Como $\langle a \rangle$ es finito, la aplicación

$$\begin{array}{ccc} \mathbb{N}\backslash\{0\} & \longrightarrow & \langle a \rangle \\ m & \longmapsto & a^m \end{array}$$

no es inyectiva. Así, existen $r < s \in \mathbb{N}$ tales que $a^r = a^s$. Si $k = s - r$, $1 = a^0 = a^r a^{-r} = a^s a^{-r} = a^{s-r} = a^k$.

2. Sea n el menor natural que cumple $a^n = 1$, cuya existencia se deduce de lo que acabamos de demostrar. Si probamos que

$$\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$$

y que todos los miembros de la derecha son distintos, entonces tendremos que $o(a) = n$. Evidentemente el elemento de la izquierda de la igualdad contiene al de la derecha. Recíprocamente, si $x = a^k$, $k \in \mathbb{Z}$, dividimos por n y por el algoritmo de la división sabemos que:

$$k = qn + r,\ 0 \leq r \leq n - 1,$$

luego $x = a^{qn+r} = (a^n)^q a^r = 1^q a^r = a^r$, $0 \leq r \leq n-1$.Por último, si existieran $0 \leq r < s \leq n - 1$ tales que $a^r = a^s$, sería $a^{s-r} = a^s a^{-r} = a^r a^{-r} = a^0 = 1$, $s - r \leq n - 1 < n$, pero esto es absurdo porque n es el menor positivo tal que $a^n = 1$.

3. Demostrado al demostrar 2.

4. Si $m = np$ es múltiplo de n, $a^m = a^{np} = (a^n)^p = 1$. Recíprocamente, si m no es múltiplo de n, $m = np + r$, $1 \leq r \leq n - 1$, luego $a^m = a^{np+r} = (a^n)^p a^r = 1^p a^r = a^r \neq 1$ por 2.

□

Así, el subgrupo generado por un elemento $a \in G$ va a tener un número de elementos que va a estar marcado por su orden. Por lo tanto, queda claro que $o(a) = |\langle a \rangle|$.

Junto con el orden, veremos otra noción de suma importancia, que nos dará uno de lo resultados más útiles del capítulo. Pero antes de ello vamos a tener que definir unas relaciones de equivalencia concretas:

Definición 1.14. *Sea G un grupo y H un subgrupo de G. Llamaremos R_H y R^H a las siguientes relaciones en G:*

$$xR_H y \text{ si y sólo si } xy^{-1} \in H$$
$$xR^H y \text{ si y sólo si } x^{-1}y \in H$$

Tanto R_H como R^H son relaciones de equivalencia.

Demostración: Lo haremos para R_H (para R^H es análoga). Tenemos que ver que cumplen con las propiedades *reflexiva* (1), *simétrica* (2) y *transitiva* (3)

1. Si $x \in G$, $xx^{-1} = 1 \in H$ luego $xR_H x$.

2. Si $xR_H y$ entonces $xy^{-1} \in H$, luego $(xy^{-1})^{-1} \in H$, y esto es $yx^{-1} \in H$ así que $yR_H x$.

3. Si xR_Hy, y yR_Hz, entonces se tiene $xy^{-1} \in H$, $yz^{-1} \in H$ y así $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$ por lo que xR_Hz.

□

El haber definido estas relaciones de equivalencia nos va a permitir estudiar las clases que éstas mismas generan para llegar a unos conjuntos especiales que llamaremos *coclases* ó *clases laterales*. En ocasiones se hace al revés, primero se presentan las coclases y a partir de ahí estudiamos (normalmente en sus demostraciones) las relaciones que definen. En este caso se ha preferido partir de las relaciones de equivalencia e ir construyendo poco a poco éstos conjuntos. Así que:

Sea ahora $[x]_{R^H}$ la clase de equivalencia del elemento $x \in G$ definida por la relación R^H. Entonces

$$[x]_{R^H} = \{a \in G : xR^Ha\} = \{a \in G : x^{-1}a = h \in H\} = \{a \in G : a = xh,\ h \in H\} = xH.$$

En efecto, dado un $x \in G$, la clase de equivalencia de x respecto de R^H es xH, y la denominaremos *clase lateral a izquierda módulo H* ó *coclase izquierda*. Análogamente podemos hacer con R_H,

$$[x]_{R_H} = \{a \in G : xR_Ha\} = \{a \in G : ax^{-1} = h \in H\} = \{a \in G : a = hx,\ h \in H\} = Hx,$$

y tendremos que Hx es la *clase lateral a derecha módulo H* ó *coclase derecha*. Notar que en este último caso tomamos los h de la forma ax^{-1} cuando la relación R_H en realidad vendría a decir que h sería de la forma xa^{-1}, simplemente tomamos el inverso (que también está en H) ya que la relación es de equivalencia es igual da hacer xR_Ha que aR_Hx.

Proposición 1.15. *Sea $H \leq G$ y $x, y \in G$. Entonces:*

1. *$xH = H$ si y sólo si $x \in H$.*
2. *$xH = yH$ si y sólo si $x^{-1}y \in H$.*
3. *$xH \cap yH \neq 0$ si y sólo si $xH = yH$.*

Demostración:

1. Si $x \in H$ ya sabemos por 1.2 que $xH = H$. Recíprocamente, si $xH = H$ entonces $x = x1 \in xH = H$.
2. Sea $xH = yH$, entonces $y \in yH = xH$ luego $y = xh$ para algún $h \in H$. De aquí tenemos que $x^{-1}y = h \in H$. Recíprocamente, sea $x^{-1}y \in H$, luego $x^{-1}y = h \in H$ y se tiene que $y = xh$ y $x = yh^{-1}$. Sea $a \in xH$, entonces $a = xh'$, $h', \in H$. Ahora $a = xh' = yh^{-1}h' = y(h^{-1}h') \in yH$ ya que $h^{-1}h' \in H$. Así, $xH \subseteq yH$. Al revés es análogo. Así, $xH = yH$.
3. Sea $z \in (xH \cap yH)$. Entonces $z = xh \in xH$ y también $z = yh' \in yH$, luego $x^{-1}z \in H$ e $y^{-1}z \in H$. Como H es grupo, $(y^{-1}z)^{-1} = z^{-1}y \in H$

y $(x^{-1}z)(z^{-1}y) = x^{-1}y \in H$. Ahora, por el apartado anterior $xH = yH$. Recíprocamente es evidente.

□

Todo esto que acabamos de hacer es exactamente análogo con las coclases a derecha. Además notar que a partir de lo que acabamos de ver tenemos que:

1. $xR^H y$ si y sólo si $xH = yH$
2. $xR_H y$ si y sólo si $Hx = Hy$

Con esto, ya tenemos más que claro que las clases de equivalencia de estas relaciones, las coclases, van a definir una partición de G. Y también sabemos que podemos considerar los conjuntos de las clases de equivalencia (coclases) para formar los conjuntos cociente:

Definición 1.16. *A los conjuntos de estas clases los llamaremos G/R^H y G/R_H respectivamente. Son los **conjuntos cocientes** definidos por las relaciones de equivalencia R^H y R_H respectivamente. Es decir, podríamos definirlos así:*

$$G/R^H = \{xH : x \in G\}.$$

$$G/R_H = \{Hx : x \in G\}.$$

*Además sabemos que ambos conforman particiones de G. Es decir, que G es unión **disjunta** de clases de equivalencia:*

$$G = \bigcup_{x \in R} xH,$$

donde R es un conjunto de representantes de clases de equivalencia definidas por R^H. Además

$$|G| = \sum_{xH \in G/R^H} card\, xH.$$

Análogamente con R_H. Hablamos de cardinales y no órdenes porque hablamos de conjuntos y no de grupos.

Proposición 1.17. *Sea H un subgrupo de un grupo G. Entonces:*

$$card(G/R^H) = card(G/R_H).$$

Demostración: Veamos que la aplicación

$$\begin{array}{rccc} \Psi: & G/R^H & \longrightarrow & G/R_H \\ & xH & \longmapsto & Hx^{-1} \end{array}$$

es biyectiva.

1. Veamos primero que Ψ está *bien definida*, es decir, si $xH = yH$ entonces $Hx^{-1} = Hb^{-1}$. En efecto, si $xH = yH$, entonces tenemos que $xR^H y$, es decir que $x^{-1}y \in H$. Y como H es subgrupo de G, $(x^{-1}y)^{-1} \in H$, y como $(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1}$ se tiene que $y^{-1}R_H x^{-1}$ y por tanto $Hy^{-1} = Hx^{-1}$.

2. Veamos ahora que es *inyectiva*. Supongamos que $xH,\ yH \in G/R^H$. Si $\Psi(xH) = \Psi(yH)$, entonces $Hx^{-1} = Hy^{-1}$, luego $y^{-1}R_H x^{-1}$ y así $y^{-1}(x^{-1})^{-1} = (x^{-1}y)^{-1} \in H$ por lo que también $x^{-1}y \in H$, pero esto quiere decir que $xR^H y$ o lo que es lo mismo: que $xH = yH$. Así Ψ es inyectiva.

3. Veamos que es *suprayectiva*. Si $Hx \in G/R_H$, como $x^{-1}H \in G/R^H$ y $\Psi(x^{-1}H) = H(x^{-1})^{-1} = Hx$ tenemos que Ψ es suprayectiva.

Por lo tanto, Ψ es una aplicación biyectiva y así

$$card(G/R^H) = card(G/R_H).$$

□

Esta proposición nos permite establecer el concepto de *índice* de un subgrupo en un grupo como el número de elementos del conjunto formado por las clases laterales a izquierda (o derecha) del subgrupo.

Definición 1.18. *Decimos que H es un subgrupo de G de **índice infinito** si G/R_H (y por ello G/R^H) es un conjunto infinito.*

*Cuando G/R_H es finito, llamamos **índice** de H en G y lo denotamos $[G : H]$, al número de elementos de G/R_H (que además coincide con G/R^H). Es decir, definimos el índice como el número de coclases a derecha (ó a izquierda porque es el mismo). En este caso decimos que H es un subgrupo de G de índice finito ó que tiene índice finito en G. Por tanto tenemos que*

$$[G : H] = card(G/R_H) = card(G/R^H).$$

Además es claro que si G tiene orden finito, como la aplicación

$$\begin{array}{ccc} G & \longrightarrow & G/R_H \\ x & \longmapsto & Hx \end{array}$$

es suprayectiva, todo subgrupo de G es de índice finito.

Una consecuencia bastante clara de todo esto es que $[G : 1] = |G|$ y $[G : H] = 1$ si y sólo si $G = H$.

Ejemplo 1.18.1. *Veamos cómo se relacionan los subgrupos de $\mathbb{Z}$ con el mismo $\mathbb{Z}$ a través de sus respectivos índices:*

Sea $G = \mathbb{Z}$ y $H \neq \{0\}$ un subgrupo de $\mathbb{Z}$. Ya sabemos que H es de la forma $H = m\mathbb{Z}$, con m un entero positivo cualquiera. Como la operación en $\mathbb{Z}$ es la suma, las clases respecto de R_H, que son las mismas que respecto $R_{m\mathbb{Z}}$, serán de la forma

$$m\mathbb{Z} + x,\ x \in \mathbb{Z}.$$

Veamos que

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z} + 0, m\mathbb{Z} + 1, \ldots, m\mathbb{Z} + (m-1)\}.$$

Dado $x \in \mathbb{Z}$ obtenemos, por el algoritmo de la división,

$$x = qm + r,\ 0 \leq r \leq m - 1,$$

y así $x - r = qm \in m\mathbb{Z}$, luego $xR_{m\mathbb{Z}}r$, es decir, $m\mathbb{Z} + x = m\mathbb{Z} + r$, lo que prueba la igualdad. Además las clases son todas distintas, es decir, los elementos del segundo miembro son distintos, pues si $m\mathbb{Z} + k = m\mathbb{Z} + l$, $0 \leq k < l \leq m - 1$, entonces $lR_{m\mathbb{Z}}k$, y por tanto $l - k \in m\mathbb{Z}$, $1 \leq l - k < m$, y tenemos que $l - k = qm$, $q \in \mathbb{Z}$ lo cual implicaría que $l = qm + k > m$ si $q > 0$ ó $k = l - qm > m$ si $q < 0$ (y así $-q > 0$), lo cual es imposible.

Así, $[\mathbb{Z} : m\mathbb{Z}] = m$. Notar que $\mathbb{Z}$ es un grupo infinito cuyos subgrupos no nulos tienen índice finito.

■

Aunque hayamos usado en este caso la notación a derecha, normalmente usaremos la de izquierda, es decir, que lo anterior lo escribiremos como:

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}.$$

Observación 1.18.1. *De 1.2 tenemos que si G es un grupo, y H es un subgrupo de G entonces los conjuntos H, xH y Hx son biyectivos, es decir, tienen el mismo número de elementos. Por lo tanto tenemos que $card\,(xH) = |H| = card\,(Hx)$.*

Además también deducimos que, dado un $x \in G$, existe una biyección entre xH y Hx, aunque ésto no quiere decir que necesariamente tengan que ser iguales, pueden ser *distintos* y veremos más adelante que ocurre cuando se da la igualdad. Ahora ya tenemos todo lo necesario para ver el que es, con toda seguridad, el resultado más importante de los vistos hasta ahora.

Teorema 1.19 (*Teorema de Lagrange*)**.** *Sea G un grupo y H un subgrupo de G. Son equivalentes:*

1. *G es finito*
2. *$|H|$ es finito y H tiene índice finito en G. En tal caso,*

$$|G| = |H| \cdot [G : H]$$

En particular, en todo grupo finito el orden de cualquier subgrupo divide al orden del grupo.

Demostración: Veamoslo por doble impicación:

1. $\Rightarrow$ 2. Como

$$\begin{array}{ccc} H & \longrightarrow & G \\ x & \longmapsto & x \end{array}$$

es inyectiva la finitud de G implica la de H, y por 1.18 también lo es G/R_H.

2. $\Rightarrow$ 1. Como R_H es relación de equivalencia, G es unión *disjunta* de las clases de equivalencia como ya sabemos. Así, recordamos que

$$|G| = \sum_{Hx \in G/R_H} card\,(Hx).$$

Ahora, por **??**, $card\,(Hx) = card\,(H) = |H|$ tal y como vimos, luego

$$|G| = |H| \cdot card\, G/R_H = |H| \cdot [G : H],$$

y así G es finito, y se tiene la conocida *fórmula de Lagrange*.

□

Como consecuencia inmediata se tiene que si G grupo y H subgrupo de G son finitos, y es importante recalcar esto, entonces

$$[G : H] = \frac{|G|}{|H|}.$$

El *Teorema de Lagrange* es uno de los resultados más importantes en *Teoría de Grupos* y su sencillez lo convierte en una de las herramientas más útiles que servirá para demostrar resultados más complicados más adelante. Dos consecuencias sencillas pero útiles son las que siguen:

Corolario 1.19.1. *Si H y K son subgrupos finitos de un grupo G con $|H| = m$, $|K| = n$ y $mcd(m, n) = 1$, entonces $H \cap K = \{1_G\}$.*

Demostración: $H \cap K$ es subgrupo de H y de K, luego $|H \cap K|$ debe dividir a m y n. Como $mcd(m, n) = 1$, entonces $|H \cap K| = 1$ y así $H \cap K = \{1_G\}$.

□

Corolario 1.19.2. *Supongamos que G es un grupo finito. Si $a \in G$, entonces $o(a) \mid |G|$ y, en particular, $a^{|G|} = 1$.*

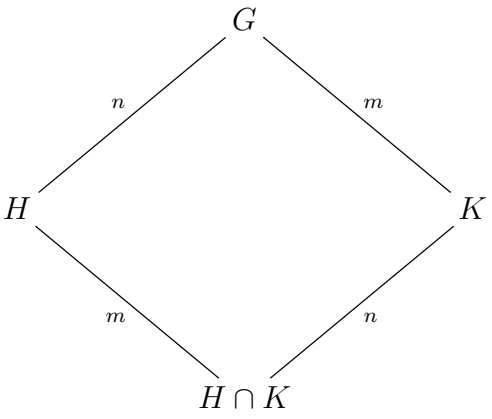
Demostración: Supongamos que $a \in G$ y que $o(a) = m$. Ya sabemos que $|\langle a\rangle| = m$ y como $\langle a\rangle$ es un subgrupo de G, por el teorema de Lagrange, $m \mid |G|$. Así $|G| = mq$ con $q \in \mathbb{Z}$, y por tanto:

$$a^{|G|} = a^{mq} = (a^m)^q = 1^q = 1.$$

□

En diagramas como el siguiente se nos presenta información útil para representar una serie de relaciones en un grupo, esquemas así serán utilizados con frecuencia. En éste podemos apreciar una serie de nodos, que son grupos y subgrupos, en este caso G y dos subgrupos suyos: H y K cualesquiera. Las líneas representan *contenido*, el subgrupo de abajo está contenido en el de arriba. En este caso $G = HK$ y lo

expresaremos como un diamante.



Además si G es un grupo finito, entonces se va a cumplir que $n = [G : H] = [K : K \cap H]$ y $m = [G : K] = [H : H \cap K]$. Este diagrama nos va a proporcionar información también sobre los órdenes de los subgrupos, cuando veamos el orden del producto más adelante será interesante volver a revisarlo.

Ahora comprobaremos una propiedad que tiene la *fórmula de Lagrange*, la transitividad, es decir, que se puede aplicar sucesivamente sobre subgrupos que cumplen las condiciones expuestas en el teorema. En concreto, lo vamos a comprobar para un subgrupo contenido en otro.

Proposición 1.20 (*Transitividad del índice*)**.** *Sean G un grupo y H y K subgrupos de G tales que $H \subseteq K$. Entonces:*

1. *H es subgrupo de K*
2. *Si el índice de H en G es finito lo son también el índice de K en G y el de H en K y*
$$[G : H] = [G : K] \cdot [K : H] .$$

Esta propiedad se conoce como transitividad del índice.

Demostración: La aplicación $\varphi\colon G/R_H \longrightarrow G/R_K$ es sobreyectiva, luego la finitud de G/R_H implica la de G/R_K, esto es $m := [G : K]$ es finito. Sean $a_1, \ldots, a_m$ representantes de las clases de equivalencia de G/R_K, es decir,

$$G = \bigcup_{i=1}^{m} Ka_i.$$

la finitud de $[G : H]$ implica la de $[K : H]$ porque $[K : H]$ es el número de elementos de $K/R_H \subseteq G/R_H$.

Sean $n := [K : H]$ y $b_1, \ldots, b_n$ representantes de las clases de equivalencia de K/R_H, es decir

$$K = \bigcup_{j=1}^{n} Hb_j.$$

Sean $c_{ij} := b_j a_i \ \forall (i,j) \in I$, donde $I = \{(i,j) : 1 \leq i \leq m,\ 1 \leq j \leq n\}$. Entonces

$$G = \bigcup_{i=1}^{m} Ka_i = \bigcup_{i=1}^{m} (\bigcup_{j=1}^{n} Hb_j)a_i = \bigcup_{(i,j)\in I} Hb_j a_i = \bigcup_{(i,j)\in I} Hc_{ij}.$$

Por lo que $[G : H] = card(I) = mn = [G : K] \cdot [K : H]$.

□

Como su nombre indica, transitividad, podríamos literalmente haber aplicado, como se ha dicho antes, la *fórmula de Lagrange* dos veces, teniendo que

$$|G| = |K| \cdot [G : K],$$

$$|K| = |H| \cdot [K : H].$$

Al hablar de órdenes e índices, tratamos con elementos que conmutan, y sustituyendo se ve fácil el resultado, pero solamente es válido para el caso de grupos finitos, y a nosotros nos interesa probarlo en general.

Observación 1.20.1. *Sean $H_1, \ldots, H_t$ subgrupos de índice finito de un grupo G. Entonces, tenemos que $H = H_1 \cap \ldots \cap H_t$ es subgrupo de índice finito de G.*

El siguiente resultado es muy importante y será utilizado con frecuencia en problemas para hallar órdenes de productos y comprobar cuándo un grupo cualquiera se puede descomponer en un producto cartesiano (más tarde veremos que en teoría de grupos éste recibe un nombre distinto) de subgrupos suyos.

Proposición 1.21. *Sea G un grupo y H, K subgrupos de G de orden finito. Entonces,*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Demostración: Sean $h_1(H\cap K), \cdots, h_m(H\cap K)$ representantes de las clases laterales a izquierda de $H \cap K$ en H. Veamos que los elementos de HK son los $h_i k$, con $1 \leq i \leq m$, $k \in K$ y que todos son diferentes.

Por un lado está claro que $m = [H : H \cap K]$. Si $hk \in HK$, tendremos que $h = h_i x$, con un i cualquiera, y $x \in H \cap K$. Así, $hk = h_i xk = h_i(xk)$, con $xk \in K$. Ahora, supongamos que $h_i k = h_j k'$, con $1 \leq i, j \leq m$, $k, k' \in K$. Entonces, $h_j^{-1} h_i = k' k^{-1} \in H \cap K$. Como $h_i(H \cap K) \neq h_j(H \cap K)$ si $i \neq j$, necesariamente $i = j$. Así, $h_i k = h_i k'$ y multiplicando a izquierda por h_i^{-1} se tiene que $k = k'$. Por lo tanto, ha quedado claro que los elementos de HK son los $h_i k$ y que además son todos diferentes, luego

$$|HK| = [H : H \cap K]|K| = \frac{|H||K|}{|H \cap K|}.$$

□

De aquí se desprende que, evidentemente, si tenemos dos grupos disjuntos (es decir, que sólo comparten el elemento neutro) entonces $|HK| = |H||K|$. Esto es muy útil

cuando son dos subgrupos de un grupo cualquiera G tales que $G = HK$, es decir, cuando se da que el producto de dos subgrupos es un grupo.

Este es el resultado interesante que se avisó antes para revisar nuevamente el diagrama en diamante antes dibujado. Si lo observamos, teniendo en cuenta lo que acabamos de ver y que habíamos definido $G = HK$ un grupo finito, entonces necesariamente $|G| = |HK| = \dfrac{|H||K|}{|H \cap K|} = |H|[K : K \cap H]$ y de aquí $[G : H] = \dfrac{|G|}{|H|} = [K : K \cap H]$, tal y cómo habíamos visto. Análogamente con $[G : K]$.

1.2. Subgrupos normales y grupos cociente

En cualquier estructura algebraica, al trabajar con cualquier clase de objetos es importante encontrar relaciones de equivalencia tales que los conjuntos cocientes respecto a dichas relaciones admitan los diferentes tipos de estructuras que estudiamos de los objetos iniciales. Para los grupos, si H es un subgrupo de un grupo G, los cocientes G/R_H y G/R^H no admiten en general la estructura de grupo. Para que lo hagan han de cumplirse las siguientes condiciones:

Proposición 1.22. *Sean G un grupo y H un subgrupo de G. Las siguientes condiciones son equivalentes:*

1. *$Ha = aH$, $\forall a \in G$.*
2. *$H = H^a$ para cada $a \in G$. Es decir, $a^{-1}Ha = H \ \forall a \in G$.*
3. *$\forall a, b \in G$ tales que $ab \in H$ se verifica que $ba \in H$.*

Demostración: Hagamos una implicación circular:

1. $\Rightarrow$ 2. Si $y \in H^a$ entonces $aya^{-1} = h \in H$. Como $ay = ha \in Ha = aH$ existirá un $h' \in H$ con $ay = ah'$. Simplificando tenemos que $y = h' \in H$, luego $H^a \subseteq H$. Y aplicando el contenido que acabamos de probar para a^{-1} se tiene que $H^{a^{-1}} \subseteq H$, y así $H = (H^{a^{-1}})^a \subseteq H^a$, por lo tanto $H = H^a$.

2. $\Rightarrow$ 3. Como $ab \in H$ entonces $ba = a^{-1}(ab)a \in H^a = H$.

3. $\Rightarrow$ 1. Sea $x \in Ha$. Entonces, $x = ha$ con $h \in H$ y, por ello, $xa^{-1} = h \in H$. Por hipótesis $a^{-1}x = h' \in H$, y así $x = ah' \in aH$, demostrando el primer contenido $Ha \subseteq aH$.

Recíprocamente, si $x = ah \in aH$, resulta que $a^{-1}x = h \in H$, luego $xa^{-1} = h' \in H$, es decir, $x = h'a \in Ha$, demostrando con esto el contenido recíproco $aH \subseteq Ha$, y por lo tanto $aH = Ha$.

□

Como ya sabemos en general se tiene que, dado un $x \in H$, las coclases xH y Hx en general serán distintas. Sin embargo, cuando hablemos de subgrupos normales, N, se tendrá que $xN = Nx \ \forall x \in G$. Esta condición nos permitirá tomar el conjunto de las coclases a izquierda o a derecha (da igual) y construir sobre dicho conjunto un nuevo grupo, es decir, que podemos otorgarle una estructura de grupo.

A la hora de entender el desarrollo de la demostración anterior es importante entender el concepto del conjugado de un grupo por un elemento, en este caso un $a \in G$ cualquiera, que ya vimos en 1.8.

Definición 1.23. *Un subgrupo H de un grupo G que cumple cualquiera de las condiciones anteriores (y por tanto todas al ser equivalentes) se denomina* ***subgrupo normal****. Diremos que H es subgrupo normal de G y lo denotaremos de la forma $H \trianglelefteq G$. La primera de las condiciones anteriores equivale a decir que $R_H = R^H$.*

En particular, si H es normal tendremos que $G/R_H = G/R^H$, es decir que $xH = Hx$ $\forall x \in G$, y denotaremos ambos cocientes por G/H.

Notar que es evidente que *cualquier subgrupo de un grupo abeliano es normal.*

Observación 1.23.1. *Para probar que un subgrupo H es normal bastará ver que*

$$H^a \subseteq H,\ \forall a \in G.$$

Ya que, probado esto y aplicado a $a^{-1} \in G$, se tendrá que $H^{a^{-1}} \subseteq H$ y así

$$H = (H^{a^{-1}})^a \subseteq H^a \Longrightarrow H = H^a \text{ y } H \text{ es normal.}$$

Es decir, sólo hará falta probar un contenido del conjugado en el mismo subgrupo. La condición se traduce en que $aHa^{-1} \subseteq H$, $\forall a \in G$.

Ejemplo 1.23.1. *Sea $n > 0$ un entero y $O_n(\mathbb{R})$ un subgrupo de $GL_n(\mathbb{R})$ llamado subgrupo de las* ***matrices ortogonales*** *o simplemente* ***subgrupo ortogonal*** *de orden n con coeficientes en $\mathbb{R}$.*

$$O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : A^t A = I_n\}$$

donde A^t es la matriz traspuesta de A y I_n es la matriz identidad.

Veamos que $O_2(\mathbb{R})$, subgrupo formado por las matrices ortogonales de orden 2, no es subgrupo normal de $GL_2(\mathbb{R})$

$$\text{Sea } P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{R}), \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O_2(\mathbb{R}) \text{ y } P^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Simplemente multiplicando se tiene que

$$B = PAP^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}.$$

Y B no es ortogonal, ya que

$$B^t B = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -2 & -1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

■

Proposición 1.24. *Si G es un grupo y H un subgrupo de G con $[G : H] = 2$, entonces H es subgrupo normal de G.*

Demostración: Como $[G : H] = 2$, tanto G/R_H como G/R^H tienen 2 elementos. Entonces, dado un $a \in G$ puede ocurrir que:

1. Si $a \in H$. En tal caso, $a1^{-1} = a \in H$ y así aR_H1, luego $Ha = H1 = H$. Y como $a^{-1}1 = a^{-1} \in H$, entonces aR^H1 y así, $aH = 1H = H$. Por lo tanto,

$$aH = Ha.$$

2. Si $a \notin H$, $aH \neq H$. Como G/R^H tiene dos elementos, tendremos que $G = H \sqcup aH$ (unión disjunta). Pero si $a \notin H$, también se cumplirá $H \neq Ha$. Y como G/R_H también tiene dos elementos, tenemos $G = H \sqcup Ha$ (unión disjunta).

   Por lo tanto, $aH = G \setminus H = Ha$, y H es normal. Ésto se desprende de que G es unión disjunta de clases y que sólo existen dos, la del neutro y la del elemento $a \notin H$.

□

Observación 1.24.1. *En cualquier grupo G, los subgrupos $\{1_G\}$ y G son normales. Es claro, ya que dado un $a \in G$ tendremos que $a\{1_G\} = a = \{1_G\}a$. Esto último de hecho nos quiere decir que, en efecto $G/\{1_G\} = G$. Además, $aG = G = Ga$.*

Proposición 1.25. *Si G es un grupo, todo subgrupo $H \subseteq Z(G)$ es un subgrupo normal de G.*

Demostración: Recordar que el centro de G es

$$Z(G) = \{x \in G : ax = xa \ \ \forall a \in G\}$$

y es subgrupo de G tal y como vimos en 1.7.

Basta probar que $H^a \subseteq H$ para cada $a \in G$. Sea $x \in H^a$. Así $axa^{-1} = h \in H$, luego $x = a^{-1}ha$. Como $h \in H \subseteq Z(G)$, $ha = ah$ y así $x = a^{-1}ha = h \in H$.

□

Ejemplo 1.25.1. *En el siguiente ejemplo exploraremos dos de los grupos clásicos de matrices:*

Sea un $n \in \mathbb{N}$ no nulo, y el grupo $G = GL_n(\mathbb{R})$ de las matrices de orden n con coeficientes en $\mathbb{R}$ y determinante no nulo. Ya sabemos que G con la operación producto de matrices es un grupo.

Sea $H = \{A \in G : det(A) = 1\}$. Este grupo también lo vimos y es el grupo especial lineal. Se denota por $SL_n(\mathbb{R})$ y es subgrupo normal de G. En efecto:

Dados $A, B \in H$, como $BB^{-1} = I_n$, $det(B) \cdot det(B^{-1}) = 1$, luego $det(B^{-1}) = \frac{1}{det(B)} = 1$ y así

$$det(AB^{-1}) = det(A)det(B^{-1}) = 1 \cdot 1 = 1.$$

Esto demuestra que H es subgrupo de G. Para ver que es normal veamos que cumple la últimas de las condiciones vistas.

Si $A, B \in G$ y $AB \in H$ significa que $det(AB) = 1$. Entonces

$$det(BA) = det(B) \cdot det(A) = det(A) \cdot det(B) = det(AB) = 1,$$

luego $BA \in H$.

■

Definición 1.26. *Si H y K son subgrupos de un grupo G decimos que K es un* ***subgrupo conjugado*** *de H si existe $a \in G$ tal que $K = H^a$.*

El siguiente resultado vendrá bien tenerlo en cuenta cuando demos los *Teoremas de Sylow* en capítulos posteriores:

Proposición 1.27. *Sean H y K subgrupos de un grupo G:*

1. *Si K es conjugado de H, entonces H es conjugado de K, y diremos que H y K son conjugados.*
2. *Si Σ es la familia de subgrupos conjugados de H (distintos) y $N = N_G(H)$ es el normalizador de H en G, la aplicación*

$$\begin{array}{rccc} \varphi\colon & G/R_N & \longrightarrow & \Sigma \\ & Na & \longmapsto & H^a \end{array}$$

   es biyectiva.
3. *En particular, si $N_G(H)$ tiene índice finito en G, el número de conjugados de H en G es $[G : N_G(H)]$.*

Demostración:

1. Es evidente, pues si $K = H^a$, $K^{a^{-1}} = (H^a)^{a^{-1}} = H$.
2. Comencemos por demostrar que φ está bien definida:

   Si $Na = Nb$, entonces $ab^{-1} \in N$, luego $H^{ab^{-1}} = H$ y así $H^b = (H^{ab^{-1}})^b = H^a$. Veamos ahora que es inyectiva:

   Si $H^a = H^b$ se tiene $H^{ab^{-1}} = (H^b)^{b^{-1}} = H$, luego $ab^{-1} \in N$ y $Na = Nb$. Como la sobreyectividad es evidente, queda demostrado.
3. Es claro ya que
$$card\, \Sigma = card(G/R_N) = [G : N]\,.$$

□

Proposición 1.28. *Sea $N \trianglelefteq G$, sean $H, K \leq G$ tales que $H \trianglelefteq K$. Entonces NH es subgrupo normal de NK.*

Demostración: Primeramente veamos que $NH = HN$ y así NH es subgrupo de G:

En particular NH es subgrupo de NK, pues $NH \subseteq NK$. Pero si $x \in NH$ se escribirá $x = nh$, $n \in N$, $h \in H$. Así $x \in Nh = hN \subseteq HN$, la igualdad $Nh = hN$ se tiene por ser N subgrupo normal de G. Esto prueba el contenido $NH \subseteq HN$. El

otro es análogo. De igual forma se prueba que $NK = KN$, luego NK es subgrupo de G, y así es grupo. Ahora veamos la normalidad:

Usaremos la primera de las condiciones definidas. Veamos que si $a \in NK$, entonces $a(NH) = (NH)a$. Como $a \in NK$ se escribirá $a = nk$, $n \in N$, $k \in K$. Si $x \in a(NH) = a(HN)$ se tendrá $x = ahn_1$, $h \in H$, $n_1 \in N$. Como $x \in (ah)N = N(ah)$ por ser N subgrupo normal de G, tendremos entonces $x = n_2ah = n_2nkh$, $n_2 \in N$. Como $kh \in kH = Hk$ por ser H subgrupo normal de K, $x = n_2nh_1k$, $h_1 \in H$, o también, $x = n_2nh_1n^{-1}nk = n_2nh_1n^{-1}a$. Ahora $h_1n^{-1} \in HN = NH$, con lo que se tiene $h_1n^{-1} = n_3h_2$, $n_3 \in N$, $h_2 \in H$. Finalmente, $x = n_2nn_3h_2a \in (NH)a$. Y así $a(NH) \subseteq (NH)a$. Para el otro contenido se procede de igual forma.

□

Definición 1.29. *Decimos que un grupo G es **simple** si sus únicos subgrupos normales son $\{1_G\}$ y G. Los ejemplos más sencillos de grupos simples son los de orden primo.*

Observación 1.29.1. *Así, si p es un número primo y G un grupo de orden p, los únicos subgrupos de G son $\{1_G\}$ y G. En particular, G es simple.*

Esto se sigue del hecho que si H es un subgrupo de G, su orden debe dividir a p por el Teorema de Lagrange. Y como p es primo, ó bien $|H| = 1$ y así $H = \{1_G\}$, ó bien $|H| = p$ y así $H = G$.

Notar que la normalidad no es una propiedad *transitiva*, es decir , puede existir un grupo G y subgrupos suyos H y K con $H \subseteq K$, H subgrupo normal de K, y K subgrupo normal de G, pero H no ser subgrupo normal de G.

Definición 1.30. *Si H es un subgrupo de un grupo G, se llama **corazón** de H a*

$$K(H) = \bigcap_{a \in G} H^a.$$

Además, $K(H)$ es un subgrupo de G, en particular es un subgrupo normal de G.

Demostración: Basta probar que $K(H)^b \subseteq K(H)$ para cada $b \in G$:

Sea $x \in K(H)^b$, tenemos que ver que $x \in H^a$ para cada $a \in G$. Pero $bxb^{-1} \in K(H) \subseteq H^{ab^{-1}}$, luego $ab^{-1}(bxb^{-1})(ab^{-1})^{-1} \in H$, y por lo tanto $axa^{-1} \in H$ y $x \in H^a$.

□

Como consecuencia de esto se tiene que, dado un $N \subseteq H$ subgrupo normal de G, entonces $N \subseteq K(H)$, ya que, para cada $a \in G$,

$$N = N^a \subseteq H^a, \text{ y así } N \subseteq \textstyle\bigcap_{a \in G} H^a = K(H).$$

Es decir, hallar el corazón de un subgrupo nos dará una forma de encontrar un subgrupo normal, lo cual es muy útil porque normalmente encontrarlos no es tarea sencilla. Aún así, hallar el corazón tampoco será sencillo.

Teorema 1.31 (*Teorema de Poincaré*)**.** *Si G posee un subgrupo de índice finito, también posee un subgrupo normal de índice finito.*

Demostración: Probemos que si H es un subgrupo de índice finito, $K(H)$, que es normal, tiene índice finito. Como $[G:H]$ es finito, también lo es

$$[G:N_G(H)] = \frac{[G:H]}{[N_G(H):H]},$$

luego sabemos que H tiene un número finito de conjugados. Y como $K(H)$ es la intersección de los conjugados de H, y hay una cantidad finita de éstos, para probar que $[G:K(H)]$ es finito basta (ya que la intersección de subgrupos de índice finito es subgrupo de índice finito) demostrar que cada H^a es subgrupo de G de índice finito. De hecho probaremos la igualdad

$$[G:H] = [G:H^a]\,.$$

Para eso es suficiente demostrar que la aplicación

$$\begin{array}{ccc} G/R_{H^a} & \longrightarrow & G/R_H \\ H^a x & \longmapsto & Hax \end{array}$$

es biyectiva. Está bien definida, y es inyectiva, pues $H^a x = H^a y$ equivale a que $xy^{-1} \in H^a$, y así $axy^{-1}a^{-1} \in H$, o lo que es lo mismo, $ax(ay)^{-1} \in H$ y esto es $Hax = Hay$. Además es sobreyectiva, puesto que $Hy = Hax$ con $x = a^{-1}y \ \ \forall y \in G$.

□

Ahora buscaremos subgrupos H tales que G/R_H tenga, de modo natural, estructura de grupo. Estos subgrupos serán los normales.

Proposición 1.32. *Sean G un grupo y H un subgrupo normal de G. El* ***grupo cociente*** $G/H = G/R_H = G/R^H$ *tiene estructura de grupo con la operación*

$$\begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (aH, aH) & \longmapsto & abH. \end{array}$$

El elemento neutro es $H = 1H$. Además, si H es subgrupo de G de índice finito, $|G/H| = [G:H]$.

Demostración: Ya sabemos que cuando H es normal, los conjuntos cocientes G/R_H y G/R^H coinciden, y los denotaremos por G/H. El único punto problemático, y donde se hace uso de la normalidad de H, es cuando hay que comprobar que la operación está bien definida, es decir, que no dependa de los representantes a y b elegidos.

1. Sea pues $aH = xH$, $bH = yH$, comprobemos que $abH = xyH$, es decir que $(ab)^{-1}xy \in H$, y así $b^{-1}a^{-1}xy \in H$. Como $aH = xH$, $a^{-1}x = h \in H$. Como $bH = yH$, $b^{-1}y = h' \in H$. Por ello, $b^{-1}a^{-1}xy = b^{-1}hy = b^{-1}yy^{-1}hy = h'y^{-1}hy$. Si $z = y^{-1}hy$, resulta que $z \in H^y = H$ por ser H normal. Por lo que, $b^{-1}a^{-1}xy = h'z \in H$.

2. Además la operación es asociativa, pues

$$aH((bH)(cH)) = (aH)(bcH) = (a(bc))H = ((ab)c)H = ((ab)H)(cH) = ((aH)(bH))cH.$$

3. Como

$$(aH)H = (aH)(1H) = (a1)H = (aH) \text{ y}$$
$$H(aH) = (1H)(aH) = (1a)H = aH,$$

la clase H es el elemento neutro.

4. Dado $aH \in G/H$ se verifica

$$(aH)(a^{-1}H) = (aa^{-1}H) = 1H = H,$$

$$(a^{-1}H)(aH) = (a^{-1}aH) = 1H = H,$$

y así $a^{-1}H$ es el inverso de aH. Es decir

$$(aH)^{-1} = a^{-1}H.$$

5. Finalmente, si H tiene índice finito en G,

$$|G/H| = card(G/R_H) = [G : H].$$

□

Es decir, si tenemos un grupo G y un subgrupo H que es normal, entonces el cociente G/H es también un grupo. Los subgrupos normales son los adecuados para dotar a un cociente de estructura de grupo. Una vez visto esto, sólo nos queda estudiar cómo son los subgrupos de un grupo cociente G/H.

Demostración: Si K es un subgrupo de G que contiene a H, H es subgrupo normal de K por serlo de G. Entonces tiene sentido considerar el grupo cociente K/H. Evidentemente $K/H \subseteq G/H$ y es subgrupo de G/H, puesto que dados $aH, bH \in K/H$, $a, b \in K$ se tiene $(aH)(bH)^{-1} = (aH)(b^{-1}H) = ab^{-1}H \in K/H$, ya que al ser K subgrupo de G, $ab^{-1} \in K$.

Recíprocamente, sea M un subgrupo de G/H, y llamemos

$$K = \{x \in G : xH \in M\}.$$

Veamos que K es un subgrupo de G que contiene a H y que $M = K/H$.

Desde luego, si $h \in H$ se tiene que $hH = H$, que pertenece a M pues M es subgrupo y H es el neutro de G/H. Esto prueba que $h \in K$ y con ello que $H \subseteq K$. Dados $x, y \in K$ tenemos $xH, yH \in M$ de donde $xy^{-1}H = (xH)(y^{-1}H) = (xH)(yH)^{-1} \in M$ por ser M subgrupo. Esto quiere decir que $xy^{-1} \in K$. Por lo tanto K es subgrupo de G.

Veamos que se cumple la igualdad $M = K/H$. Dado $xH \in K/H$, es $x \in K$ y por tanto $xH \in M$. En el otro sentido, si $xH \in M$, entonces $x \in K$, luego $xH \in K/H$. Es inmediato que si K_1 y K_2 son subgrupos de G que contienen a H y $K_1/H = K_2/H$, entonces $K_1 = K_2$.

□

Por lo tanto, hemos demostrado que la aplicación

$$\begin{array}{ccc} K & \longrightarrow & K/H \\ x & \longmapsto & xH. \end{array}$$

es una biyección entre los subgrupos de G que contienen a H y los subgrupos de G/H. Este resultado se conoce como ***Teorema de la correspondencia***. Además la biyección preserva la normalidad y por lo tanto tenemos que:

Proposición 1.33. *K es subgrupo normal de G si y sólo si K/H es subgrupo normal de G/H.*

Demostración: Sea $K \trianglelefteq G$. Dados aH, bH con $(aH)(bH) \in K/H$, entonces $(ab)H \in K/H$, es decir, $ab \in K$. Como K es normal, y $ab \in K$, deducimos que $ba \in K$, luego $(bH)(aH) = (ba)H \in K/H$, y así K/H es normal. Para el recíproco es análogo.

□

Ejemplo 1.33.1. *Dado un entero positivo m, el subgrupo $H = m\mathbb{Z}$ del grupo $\mathbb{Z}$ es desde luego normal, por ser $\mathbb{Z}$ abeliano. Como la notación es aditiva, la operación en el cociente vendrá dada por*

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ (a + m\mathbb{Z}, b + m\mathbb{Z}) & \longmapsto & a + b + m\mathbb{Z}. \end{array}$$

Además el grupo cociente $\mathbb{Z}/m\mathbb{Z}$ es de orden m. y sabemos que

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}$$

siendo todos sus elementos distintos. Finalmente es claro que $\mathbb{Z}/m\mathbb{Z} = \langle 1 + m\mathbb{Z} \rangle$. Además definiremos un grupo abeliano concreto que estudiaremos más adelante, y que veremos que es muy interesante:

$$\mathbb{Z}_m^* = \{a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} : mcd(a, m) = 1\},$$

con la operación

$$\begin{array}{ccc} \mathbb{Z}_m^* \times \mathbb{Z}_m^* & \longrightarrow & \mathbb{Z}_m^* \\ (a + m\mathbb{Z}, b + m\mathbb{Z}) & \longmapsto & ab + m\mathbb{Z}. \end{array}$$

■

1.3. Homomorfismos y teoremas de isomorfía

Ya sabemos lo que son los grupos, cómo se subdividen y si estos subconjuntos heredan la estructura de grupo (subgrupos), cúantas de estas subestructuras hay y bajo qué condiciones podemos hablar de un *cociente* que herede la estructura de grupo. A continuación vamos a ver cuándo dos grupos son "iguales", y de qué manera podemos establecer esta igualdad *algebraica*, es decir, cuándo podemos decir que dos grupos tienen la misma estructura y que, salvo los nombres que les demos a sus elementos, son el mismo. De ésto se ocupan los conocidos *Teoremas de Isomorfía*, para los cuales tendremos antes que presentar y definir qué son los homomorfismos, las aplicaciones que conservan la estructura.

Definición 1.34. *Una aplicación* $f\colon G_1 \longrightarrow G_2$ *entre dos grupos* G_1 *y* G_2 *se llama* ***homomorfismo de grupos*** *si*

$$f(ab) = f(a)f(b) \text{ para cada } a, b \in G_1.$$

Además, nuevamente recordar que, al igual que al comienzo del capítulo lo comentamos en general, a la hora de denotar homomorfismos, la operación que definamos en el grupo de salida y/o grupo de llegada (ya sea la aditiva + o la multiplicativa $\cdot$) se omitirá cuando no haya lugar a dudas y se especificará cuando convenga.

Propiedades 1.34.1. *Consideremos un homomorfismo* $f\colon G \longrightarrow H$*. Entonces algunas propiedades sobre los homomorfismos de grupos que serán importantes tenerlas en cuenta:*

1. $f(1_G) = 1_H$ *ya que* $1_H f(1_G) = f(1_G) = f(1_G 1_G) = f(1_G)f(1_G) \Longrightarrow 1_H = f(1_G)$.
2. $f(a^{-1}) = (f(a))^{-1}$ *para cada* $a \in G$*, puesto que*

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_G) = 1_H,$$
$$f(a^{-1})f(a) = f(a^{-1}a) = f(1_G) = 1_H.$$

3. $o(f(x))$ *divide al orden de* x*. En efecto, si* $o(x) = m$ *como* $x^m = 1_G$ *se tiene que* $1_H = f(1_G) = f(x^m) = f(x)^m$ *y así* $o(f(x))$ *divide a* m*.*
4. *Si* Y *es un subgrupo de* H*,*

$$f^{-1}(Y) = \{x \in G : f(x) \in Y\}$$

es un subgrupo de G*. Además si* Y *es subgrupo normal de* H*,* $f^{-1}(Y)$ *lo es de* G*.*

En efecto, si $x, y \in f^{-1}(Y)$*, entonces* $f(x), f(y) \in Y$*, de donde* $f(xy^{-1}) = f(x)f(y)^{-1} \in Y$*, luego* $xy^{-1} \in f^{-1}(Y)$*. Para probar la normalidad de* $f^{-1}(Y)$ *usamos la última de las condiciones: Si* $ab \in f^{-1}(Y)$ *se sigue que* $f(a)f(b) = f(ab) \in Y$ *y como* Y *es normal,* $f(ab) = f(b)f(a) \in Y$*. Por lo tanto* $ba \in f^{-1}(Y)$*.*

5. *Si además consideramos otro homomorfismo* $g\colon H \longrightarrow Z$ *entonces,*

$g \circ f\colon G \longrightarrow Z$ *también es homomorfismo, pues*

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

■

Definición 1.35. *Dado un homomorfismo* $f\colon G_1 \longrightarrow G_2$ *entre dos grupos* G_1 *y* G_2*, llamaremos* ***núcleo de f*** *a*

$$Kerf = \{a \in G_1 : f(a) = 1_{G_2}\}.$$

Y de igual forma, llamaremos ***imagen de f*** *al conjunto*

$$Imf = \{f(x) : x \in G_1\}.$$

Todas estas propiedades y definiciones respecto a los homomorfismos también ser verán más adelante para la otra estructura algebraica que estudiaremos, los anillos. Notar que además, el núcleo de f es un subgrupo de G, en particular $Kerf \trianglelefteq G_1$. En efecto, dados $a, b \in Kerf$,

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1_{G_2}1_{G_2} = 1_{G_2}$$

y así $Kerf$ es subgrupo de G_1. Para ver que es normal es suficiente probar que $(Kerf)^a \subseteq Kerf\ \forall a \in G_1$. Si $x \in (Kerf)^a$ resulta que $a^{-1}xa \in Kerf$, y así

$$f(a^{-1}xa) = 1_{G_2} \Rightarrow f(a)^{-1}f(x)f(a) = 1_{G_2} \Rightarrow f(a)f(x) = 1_{G_2}f(a) = f(a) = f(a)1_{G_2}.$$

Simplificamos y queda $f(x) = 1_{G_2}$, luego $x \in Kerf$.

La imagen también es un subgrupo de G_2 pues dados $a = f(x)$, $b = f(y)$, con $a, b \in Imf$, $ab^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in Imf$.

Que el núcleo de un homomorfismo sea un subgrupo normal es de especial importancia para un par de resultados que veremos a continuación, de hecho esta observación nos puede llevar a pensar que *todo subgrupo normal es el núcleo de un homomorfismo de grupos.*

Propiedades 1.35.1. *Sea $f\colon G_1 \longrightarrow G_2$ un homomorfismo entre dos grupos G_1 y G_2:*

1. *f es inyectiva si y sólo si $Kerf = \{1_{G_1}\}$.*

   Demostración: *Supongamos que f es inyectiva. Sea $a \in Ker\, f$, entonces $f(a) = 1 = f(1)$. Luego $a = 1$ y $Ker\, f = \{1_{G_1}$.*

   Recíprocamente, sea $Kerf = \{1_{G_1}\}$. Sea $f(a) = f(b)$. Entonces $f(ab^{-1}) = f(a)f(b)^{-1} = 1$, así $ab^{-1} \in Ker\, f = 1$. Así $a = b$ y f es inyectiva.

2. *Si f es inyectiva y $x \in G_1$ es un elemento de orden m, entonces $o(f(x)) = m$.*

   Demostración: *Sea $k = o(f(x))$. Entonces $f(x)^k = 1_{G_2}$, luego $f(x^k) = 1_{G_2}$ y así $x^k \in Kerf = \{1_{G_1}\}$. Por lo tanto, $x^k = 1_{G_1}$, luego k es múltiplo de m. Y como $o(f(x))$ divide a m por una de las propiedades anteriores, tenemos que $k = m$.*

3. *f es sobreyectiva (o suprayectiva) si y sólo si $Imf = G_2$*

   Demostración: *Supongamos que f es sobreyectiva, por tanto $f(G_1) = G_2$ y así $Imf = G_2$. Recíprocamente, si $Imf = G_2$ entonces $f(G_1) = G_2$ y así f es sobreyectiva.*

■

De entre todos los homomorfismos que podemos establecer entre dos grupos, son especialmente importantes dos de ellos:

- Si H es un subgrupo de un grupo G, la ***inclusión***

$$\begin{array}{rccc} i\colon & H & \longrightarrow & G \\ & x & \longmapsto & x \end{array}$$

es un homomorfismo inyectivo puesto que $i(xy) = xy = i(x)i(y)$ y $x \in Kerf$ implica que $i(x) = 1_G$, es decir, $x = 1_G = 1_H$.

- Si H es un subgrupo normal de un grupo G, la ***proyección***

$$\begin{array}{rccc} \pi\colon & G & \longrightarrow & G/H \\ & x & \longmapsto & xH \end{array}$$

es un homomorfismo sobreyectivo. La sobreyectividad es obvia y para ver que es homomorfismo:

$$\pi(xy) = xyH = (xH)(yH) = \pi(x)\pi(y).$$

Lo llamaremos ***proyección canónica***.

Definición 1.36. *Sea $f\colon G_1 \longrightarrow G_2$ un homomorfismo entre dos grupos G_1 y G_2, diremos que f es un **monomorfismo** si f es inyectiva y **epimorfismo** si f es sobreyectiva.*

A partir de lo que ya sabemos de grupos cocientes, subgrupos normales y lo que acabamos de ver del núcleo de un homomorfismo (que es subgrupo normal del grupo de partida) y en concreto estos dos últimos homomorfismos podemos, ahora sí, dar un significado alternativo a lo que conocemos por subgrupo normal:

Proposición 1.37. *Todo subgrupo normal es el núcleo de un homomorfismo de grupos.*

Demostración: Sea N un subgrupo normal de un grupo G. Vamos a construir un homomorfismo φ y un grupo H tales que $N = Ker\,\varphi$ y $H = G/N$. Sabemos que

$$\forall a \in G, b \in N,\ aba^{-1} \in N \Longleftrightarrow \forall a \in G,\ aN = Na.$$

Además, si N es subgrupo normal de G, podemos definir el grupo cociente

$$H = G/N = \{aN : a \in G\} = \{Na : a \in G\},$$

con la operación

$$\begin{array}{rccc} G/N \times G/N & \longrightarrow & G/N \\ (aN, bN) & \longmapsto & abN \end{array}$$

que en 1.32 ya definimos y comprobamos que estaba bien definida, que era cerrada, que cumplía la asociatividad, la existencia del elemento neutro y la existencia del elemento inverso. Así que ahora sea la aplicación

$$\begin{array}{rccc} \varphi\colon & G & \longrightarrow & H \\ & a & \longmapsto & aN. \end{array}$$

Es claro que φ es homomorfismo puesto que es una proyección:

$$\varphi(ab) = abN = (aN)(bN) = \varphi(a)\varphi(b).$$

Entonces

$$Ker\,\varphi = \{a \in G : \varphi(a) = aN = N\} = \{a \in G : a \in N\} = N.$$

□

Una vez presentadas las principales propiedades de los homomorfismos y dos de los más importantes como son la inclusión y la proyección canónica vamos a ver un resultado que será fundamental para entender los homomorfismos en general y así poder llegar a discernir cuándo dos grupos son *algebraicamente* equivalentes.

Proposición 1.38 (*Descomposición canónica de un homomorfismo*)**.** *Sean dos grupos G_1, G_2 y $f\colon G_1 \longrightarrow G_2$ un homomorfismo entre ellos. Entonces existe un homomorfismo biyectivo*

$$\bar{f}\colon G_1/Kerf \longrightarrow Imf$$

que hace conmutativo el siguiente diagrama,

$$\begin{array}{ccc} G_1 & \xrightarrow{\quad f \quad} & G_2 \\ {\scriptstyle \pi}\downarrow & & \uparrow{\scriptstyle i} \\ G_1/Kerf & \xrightarrow{\quad \bar{f} \quad} & Imf \end{array}$$

donde i y π son los homomorfismos presentados anteriormente. Notar que $Kerf$ es subgrupo normal y por eso podemos definir el cociente. Además la conmutatividad del diagrama significa que:

$$f = i \circ \bar{f} \circ \pi.$$

Demostración: La última condición nos indica como actúa $\bar{f}$:

$$f(x) = (i \circ \bar{f} \circ \pi)(x) = i(\bar{f}(\pi(x))) = \bar{f}(\pi(x)) = \bar{f}(xKerf).$$

Y con eso definimos $\bar{f}$. Veamos ahora que:

(i). $\bar{f}$ está bien definida ya que si $xKerf = yKerf$, entonces

$$\begin{gathered} x^{-1}y \in Kerf \Longrightarrow 1_{G_2} = f(x^{-1}y) = f(x)^{-1}f(y) \text{ y así} \\ f(x) = f(y) \Longrightarrow \bar{f}(xKerf) = \bar{f}(yKerf). \end{gathered}$$

(ii). $\bar{f}$ es homomorfismo ya que

$$\bar{f}((xKerf)(yKerf)) = \bar{f}(xyKerf) = f(xy) = f(x)f(y) = \bar{f}(xKerf)\bar{f}(yKerf).$$

(iii). $\bar{f}$ es inyectiva ya que si $xKerf \in Ker\bar{f}$ entonces

$f(x) = \bar{f}(xKerf) = 1_{Imf} = 1_{G_2} \Longrightarrow x \in Kerf$ y así $xKerf = Kerf$, que es el elemento neutro de $G_1/Kerf$ y así $\bar{f}$ es inyectiva.

(iv). $\bar{f}$ es sobreyectiva ya que cada elemento de Imf es de la forma

$$Imf \ni g = f(x) = \bar{f}(xKerf) \text{ para cierto } x \in G_1.$$

Además la conmutatividad del diagrama es obvia, pues $\bar{f}$ se ha definido para que lo sea.

□

Así, ya estamos en condiciones de presentar la *igualdad algebraica* entre dos grupos cualesquiera.

Definición 1.39. *Un homomorfismo biyectivo entre dos grupos se llama* ***isomorfismo****. Cuando exista un isomorfismo* $f\colon G_1 \longrightarrow G_2$ *diremos que los grupos* G_1 *y* G_2 *son* ***isomorfos****, y escribiremos* $G_1 \simeq G_2$.

Observación 1.39.1. *Algunas observaciones con respecto al concepto de isomorfismo de grupos:*

1. *Si* $f\colon G_1 \longrightarrow G_2$ *es isomorfismo, también lo es* $f^{-1}\colon G_2 \longrightarrow G_1$ *, o, dicho de otra forma, si* $G_1 \simeq G_2$ *entonces* $G_2 \simeq G_1$.

   Demostración: *Como la inversa de toda aplicación biyectiva es biyectiva, basta comprobar que* f^{-1} *es homomorfismo de grupos.*

   Si $a, b \in G_2$, *y* $f^{-1}(a) = x$, $f^{-1}(b) = y$, *entonces*

   $$f(x) = a,\ f(y) = b \Longrightarrow f(xy) = f(x)f(y) = ab,$$

   y así, $xy = f^{-1}(ab)$, *por lo que* $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$.

2. *Si* $G_1 \simeq G_2$ *y* G_1 *es abeliano, también lo será* G_2

   Demostración: *Sean* $x, y \in G_2$ *y* $f\colon G_1 \longrightarrow G_2$ *isomorfismo. Como* f *es sobreyectiva, existirán* $a, b \in G$ *tales que* $x = f(a)$, $y = f(b)$. *Entonces*

   $$xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx.$$

Notemos que si G_1 es un grupo cualquiera, entonces $G_1 \simeq G_1$ puesto que que la aplicación identidad $f\colon G_1 \longrightarrow G_1$ es claramente un isomorfismo. Ya sabemos que si $G_1 \simeq G_2$ entonces $G_2 \simeq G_1$, y además si tenemos un tercer grupo G_3 y $G_1 \simeq G_2$, $G_2 \simeq G_3$, entonces $G_1 \simeq G_3$ ya que la composición de isomorfismos también es isomorfismo. Por lo tanto, si consideramos el conjunto de todos los grupos, la relación binaria $\simeq$ es de equivalencia.

Como hemos podido ver, la propiedad de ser abeliano se conserva en isomorfismos. Será común ir viendo más propiedades que se conservan, y las llamaremos *invariantes bajo isomorfismo*. Es decir, dos grupos isomorfos tienen, por así decirlo, «las mismas propiedades» y lo único en lo que se diferencian será en los símbolos utilizados para representar los elementos y operaciones. Es decir, son en esencia el mismo grupo.

A continuación presentaremos uno de los grandes resultados de la *Teoría de Grupos*, que establece uno de los isomorfismos más útiles y conocidos. En este caso debería ser presentado como corolario pero, por cuestiones estéticas y haciendo honor a su importancia, lo haremos como teorema:

Teorema 1.40 (***Primer Teorema de Isomorfía***)**.** *Si* $f\colon G_1 \longrightarrow G_2$ *es un homomorfismo entre dos grupos* G_1 *y* G_2, *los grupos* $G_1/Kerf$ *e* Imf *son isomorfos. Es decir*

$$G_1/Kerf \simeq Imf.$$

Demostración: Por la *descomposición canónica.* $\bar{f}\colon G_1/Kerf \longrightarrow Imf$ es un isomorfismo como ya se ha visto.

□

Como observación interesante es importante tener en cuenta que si tenemos dos grupos finitos *isomorfos*, (importante que sean finitos) entonces han de tener el mismo orden pues la aplicación que los relaciona es biyectiva.

Ejemplo 1.40.1. *Veamos algunos ejemplos:*

1. *Vamos a calcular los homomorfismos* $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$.

   Sea f *uno de estos homomorfismos, y* $f(1) = a$*, con* $a \in \mathbb{Z}$*, entonces tendremos que para cada entero positivo* n*:*

   $$f(n) = f(\underbrace{1 + \ldots + 1}_{n}) = f(1)\underbrace{+ \ldots +}_{n} f(1) = na$$

   mientras que si n *es negativo,* $m = -n$ *será positivo y así* $f(n) = f(-m) = -f(m) = -(ma) = (-m)a = na$*. Y como* $f(0) = 0a$*, tenemos que* $f(n) = na$ *para cada* $a \in \mathbb{Z}$*.*

   Esta aplicación es homomorfismo, ya que

   $$f(n + m) = (n + m)a = na + ma = f(n) + f(m).$$

   Así, los homomorfismos de $\mathbb{Z}$ *en* $\mathbb{Z}$ *son las aplicaciones* ($a \in \mathbb{Z}$)

   $$\begin{array}{rccc} f_a\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & na \end{array}$$

2. *La aplicación*

   $$\begin{array}{rccc} f\colon & (GL_n(\mathbb{R}), \cdot) & \longrightarrow & (\mathbb{R}^*, \cdot) \\ & A & \longmapsto & detA \end{array}$$

   es un epimorfismo (un homomorfismo sobreyectivo) de grupos con núcleo $SL_n(\mathbb{R})$ *y así, por el Primer Teorema de Isomorfía,*

   $$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

   En efecto, $f(AB) = det(AB) = detA \cdot detB = f(A)f(B)$*, luego* f *es homomorfismo. Es evidente que* $Kerf = SL_n(\mathbb{R})$ *por definición. Finalmente, si* $a \in \mathbb{R}^*$*, la matriz*

   $$A = (a_{ij} : 1 \leq i \leq n,\ 1 \leq j \leq n)$$

   definida por

   $$a_{ij} = \begin{cases} 0 \; si \; i \neq j \\ a \; si \; i = j = 1 \\ 1 \; si \; i = j > 1 \end{cases}$$

   cumple $detA = a1^{n-1} = a$*, probando la sobreyectividad de* f*.*

3. *Sea $x \in \mathbb{R}$ y*

$$\begin{array}{rccc} f\colon & (\mathbb{R},+) & \longrightarrow & (\mathbb{C}^*,\cdot) \\ & x & \longmapsto & e^{2\pi x i}, \end{array}$$

como $e^{2\pi x i} = \cos 2\pi x + i \sin 2\pi x = 1$ si $x \in \mathbb{Z}$, deducimos que $Ker f = \mathbb{Z}$. Y como, para cualquier $x \in \mathbb{R}$, el valor absoluto o módulo del número complejo $e^{2\pi x i} = \cos 2\pi x + i \sin 2\pi x$ es $\sqrt{\cos^2 2\pi x + \sin^2 2\pi x} = 1$, tenemos que $Im f = S^1 = \{z \in \mathbb{C} : |z| = 1\}$ (indicaremos el módulo con $|\cdot|$). Así, por el Primer Teorema de Isomorfía:

$$(\mathbb{R}/\mathbb{Z},+) \simeq (S^1,\cdot).$$

4. *Sea G un grupo abeliano y*

$$\begin{array}{rccc} f\colon & G & \longrightarrow & G \\ & x & \longmapsto & x^2 \end{array}$$

una aplicación que es homomorfismo ya que

$$f(xy) = (xy)^2 = xyxy = xxyy = x^2y^2 = f(x)f(y).$$

Observar que

$$Ker f = \{x \in G : x^2 = 1\}$$

que estará formado por 1 y todos los elementos de orden 2 de G en caso de que existan. Por ejemplo si $G = \mathbb{R}^*$, entonces $x^2 = 1$ equivale a $(x+1)(x-1) = 0$, y así $ker f = \{+1, -1\}$. A este grupo lo denotaremos $\mathcal{U}_2$ y será interesante cuando veamos el grupo simétrico y anillos.

Notar que en general f no es inyectiva, sólo lo será si el orden de G es impar.

Demostración: *Suponer que $|G| = 2k+1$ impar, sea $x \in ker f$. Así $x^2 = 1$ y también $x^{2k+1} = 1$, por ser el orden de G. Entonces*

$$x = x1 = x1^k = x(x^2)^k = x^{2k+1} = 1$$

y así f es inyectiva.

Recíprocamente, veamos que si $|G| = 2k$ es par, sea o no G abeliano, f no es inyectiva. Para cada $x \in G$ llamaremos $A_x = \{x, x^{-1}\}$. Además los A_x constituyen una partición de G pues como cada $x \in A_x$, la igualdad

$$G = \bigcup_{x \in G} A_x$$

es obvia, además si $A_x \cap A_y \neq \emptyset$ entonces $x \in \{y, y^{-1}\}$ ó $x^{-1} \in \{y, y^{-1}\}$.

Para el primer caso, si $x = y$ entonces $x^{-1} = y^{-1}$ y $A_x = A_y$, y si $x = y^{-1}$ entonces $x^{-1} = y$ y nuevamente $A_x = A_y$. Análogamente para el segundo caso.

Es claro que $A_1 = \{1\}$, pues $1^{-1} = 1$. Si el resto de los A_x (supongamos que hay p de ellos) tuviese dos elementos, entonces

$$2k = |G| = card A_1 + 2p = 2p + 1.$$

Y como éste último es impar sería absurdo. Luego ha de existir $1 \neq a \in G$ *tal que* $card A_a = 1$. *Esto significaría que* $a^{-1} = a$, *y así* $f(a) = a^2 = aa^{-1} = 1 = f(1)$. *Luego* f *no es inyectiva.*

Esto se puede reformular diciendo que: «Todo grupo finito de orden par posee algún elemento de orden 2».

■

Teorema 1.41 (***Segundo Teorema de Isomorfía***)**.** *Sean* N *y* H *subgrupos normales de un grupo* G, *tales que* $N \subseteq H$. *Entonces* H/N *es subgrupo normal de* G/N *y*

$$(G/N)/(H/N) \simeq G/H.$$

Demostración: Consideremos la aplicación

$$\begin{array}{rccc} f\colon & G/N & \longrightarrow & G/H \\ & aN & \longmapsto & aH \end{array},$$

que está bien definida, pues si $aN = bN$ entonces $ab^{-1} \in N \subseteq H$, luego $aH = bH$.

Como $f((aN)(bN)) = f(abN) = abH = (aH)(bH) = f(aN)f(bN)$, f es homomorfismo. Cada $aH \in G/H$ es de la forma $aH = f(aN)$ y así f es sobreyectiva y, por lo tanto, epimorfismo.

Por último, $aN \in Kerf \Longleftrightarrow aH = f(aN) = H$, pero esto quiere decir que

$$Kerf = \{aN \in G/N : a \in H\} = H/N.$$

Y por el *Primer Teorema de Isomorfía*, $(G/N)/Kerf \simeq Imf$, y como $Imf = G/H$, por ser f sobreyectiva, y $Kerf = H/N$ se tiene

$$(G/N)/(H/N) \simeq G/H.$$

□

Teorema 1.42 (***Tercer Teorema de Isomorfía***)**.** *Sean* H *y* N *subgrupos de un grupo* G, *con* N *subgrupo normal de* G. *Entonces:*

1. $H \cap N$ *es subgrupo normal de* H.
2. HN *es subgrupo de* G.
3. N *es subgrupo normal de* HN.
4. $HN/N \simeq H/(H \cap N)$.

Demostración:

1. Veamos que se cumple la última de las condiciones de normalidad. Sean $a, b \in H$ tales que $ab \in H \cap N$. Entonces $ab \in N$, $a, b \in G$. Como N es subgrupo normal de G, $ba \in N$. Además $ba \in H$, ya que $b, a \in H$, luego $ba \in H \cap N$.

2. Tenemos que probar que $HN = NH$ (como ya sabemos de la primera sección). Si $x \in HN$, existen $h \in H$, $n \in N$ tales que $x = hn$. En particular: $x \in hN =$

$Nh \subseteq NH$, ya que N es normal. Esto prueba que $HN \subseteq NH$ y el otro contenido es análogo.

3. De un resultado anterior.

4. Definimos

$$\begin{array}{rccc} f\colon & H & \longrightarrow & HN/N \\ & h & \longmapsto & hN \end{array}$$

que evidentemente es un homomorfismo. Veamos que $Imf = HN/N$. Dado $xN \in HN/N$ será $x = hn$, $h \in H$, $n \in N \Longrightarrow x^{-1}h = n^{-1}h^{-1}h = n^{-1} \in N$, luego $xN = hN = f(h)$.

Veamos que $Kerf = H \cap N$. $x \in Kerf$ quiere decir que $x \in H$ y $xN = N$, es decir, $x \in H$, $x \in N$ y, por lo tanto, $x \in H \cap N$. Así, por el Primer Teorema de Isomorfía,

$$H/Kerf \simeq Imf \Longrightarrow H/(H \cap N) \simeq HN/N.$$

□

Notar que para demostrar lo primero también se podría haber visto que $H \cap N$ es el núcleo de algún homomorfismo, en concreto del que se expone en el último apartado.

Notar también que en algunos libros de texto el segundo y tercer teoremas de isomorfía aparecen intercambiados, realmente da igual si el segundo es el tercero o viceversa pero es importante que una vez fijados sigan así durante el resto del texto.

2. Grupos cíclicos

2.1. La función de Euler

Definiremos y estudiaremos un concepto conocido como *función de Euler*, la presentamos ahora porque es una función muy interesante que será útil más adelante con el estudio de ciertos grupos. También suele definirse en *anillos*, y tiene importantes aplicaciones en dichas estructuras algebraicas; sin embargo, no es necesario definir un *anillo*, se puede perfectamente hacer sobre un *grupo abeliano finito* aunque más adelante también la definiremos sobre anillos.

Comenzaremos definiendo un conjunto sobre el que definiremos todo lo que veremos en adelante, sea m un entero positivo y denotemos

$$\mathbb{Z}_m^* = \{a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} : mcd(a, m) = 1\},$$

y consideremos la operación binaria

$$\begin{array}{rcl} \mathbb{Z}_m^* \times \mathbb{Z}_m^* & \longrightarrow & \mathbb{Z}_m^* \\ (a + m\mathbb{Z}, b + m\mathbb{Z}) & \longmapsto & ab + m\mathbb{Z}. \end{array}$$

Veamos primero que, con esta operación, $\mathbb{Z}_m^*$ es un grupo abeliano.

La operación está bien definida ya que: si $a + m\mathbb{Z} = a' + m\mathbb{Z}$ y $b + m\mathbb{Z} = b' + m\mathbb{Z}$, tendremos que $a = a' + mu$, $b = b' + mv$, con $u, v \in \mathbb{Z}$ y así

$$ab = a'b' + m(b'u + a'v + muv).$$

Luego $ab - a'b' \in m\mathbb{Z}$ y por tanto $ab + m\mathbb{Z} = a'b' + m\mathbb{Z}$. Esto demuestra que la definición no depende de los representantes.

Ahora veamos que es interna: si $mcd(a, m) = mcd(b, m) = 1$, entonces $mcd(ab, m) = 1$. Usando la *Identidad de Bézout* tenemos que

$$1 = ua + vm,\ 1 = u'b + v'm,\ u, v, u', v' \in \mathbb{Z}.$$

Por lo que,

$$1 = (ua + vm)(u'b + v'm) = uu'ab + (auv' + bvu' + mvv')m = u''ab + v''m,$$

$$\text{con } u'' = uu' \text{ y } v'' = auv' + bvu' + mvv'.$$

Y de nuevo, por la *Identidad de Bézout*, $mcd(ab, m) = 1$ como queríamos ver.

Para ver el resto de axiomas de grupo hay que tener en cuenta que la asociatividad es obvia y también está claro que $1 + m\mathbb{Z}$ es el elemento neutro. También es inmediato que $\mathbb{Z}_m^*$ es abeliano. Y para el inverso: para cada $a + m\mathbb{Z}$, como $mcd(a, m) = 1$, se tiene que

$$1 = au + mv,\ u, v \in \mathbb{Z}, \text{ y así}$$

$$1 + m\mathbb{Z} = (au + m\mathbb{Z}) + (mv + m\mathbb{Z}) = (a + m\mathbb{Z})(u + m\mathbb{Z}),$$

por lo que $u+m\mathbb{Z}$ es el inverso de $a+m\mathbb{Z}$. Es decir, para cada $a+m\mathbb{Z} \in \mathbb{Z}_m^*$ existe un inverso, éstos elementos se denominan *invertibles* y en teoría de anillos se denotan como *unidades*, conformando así el *grupo de unidades módulo m*. Sin embargo como ya hemos visto, no es necesario definir ni hablar de anillos, podemos hacerlo sobre grupos abelianos finitos. Y así lo haremos.

Por lo tanto podemos definir la *función de Euler* como:

$$\begin{array}{rccc} \phi\colon & \mathbb{N} \setminus \{0\} & \longrightarrow & \mathbb{N} \setminus \{0\} \\ & m & \longmapsto & \phi(m) \end{array}$$

que a cada natural positivo m le hace corresponder el orden $\phi(m)$ del grupo $\mathbb{Z}_m^*$. Una forma alternativa de entender a la *función de Euler* es a partir de la definición, como una función que a cada natural le asigna el número de naturales más pequeños que él con los que es *coprimo*. Vamos a dar un procedimiento para calcularla viendo como actúa sobre cada natural positivo:

- Si p es primo, $\phi(p) = p-1$, pues cada natural $1 \leq a \leq p-1$ cumple $mcd(a, p) = 1$.
- Si p es un número primo y m un natural positivo,

$$\phi(p^m) = p^{m-1}(p - 1).$$

Esto se desprende del hecho de que los naturales $1 \leq a \leq p^m$ que no son primos con p^m son

$$p, 2p, 3p, \ldots, p^{m-1}p.$$

Así que hay p^{m-1} que no son primos con p, por lo que

$$\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1).$$

- Si m y n son primos primos entre sí, $\phi(mn) = \phi(m)\phi(n)$. Para ver esto se trata de encontrar una biyección

$$\mathbb{Z}_{mn}^* \longrightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*,$$

ya que el primer miembro tiene $\phi(mn)$ elementos, y el segundo $\phi(m)\phi(n)$. Y, ¿cúal es esta biyección?, bien pues aquí la tenemos

$$f\colon \quad a + mn\mathbb{Z} \longrightarrow (a + m\mathbb{Z}, a + n\mathbb{Z}).$$

Es claro que, si $mcd(a, mn) = 1$, se tendrá

$$mcd(a, m) = mcd(a, n) = 1.$$

Además, si $a \in mn\mathbb{Z}$, también $a \in m\mathbb{Z}$ y $a \in n\mathbb{Z}$. Esto prueba que f está bien definida.

También es inyectiva: si $a + m\mathbb{Z} = b + m\mathbb{Z}$ y $a + n\mathbb{Z} = b + n\mathbb{Z}$, resulta que $a - b$ es múltiplo de m y de n. Y como m y n son primos entre sí, deducimos que $a - b$ es múltiplo de mn, luego $a + mn\mathbb{Z} = b + mn\mathbb{Z}$.

Es sobreyectiva. Sea $(x + m\mathbb{Z}, y + n\mathbb{Z}) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Como m y n son primos entre sí, por la *Identidad de Bézout* tenemos que existen $u, v \in \mathbb{Z}$ tales que $um + vn = 1$. Sea entonces

$$a = yum + xvn.$$

Veamos que si $a + mn\mathbb{Z} \in \mathbb{Z}_{mn}^*$, entonces $f(a + mn\mathbb{Z}) = (x + m\mathbb{Z}, y + n\mathbb{Z})$ probando así la sobreyectividad:

Si $mcd(a, mn) \neq 1$, existirá un primo p que dividirá a ambos. Como p es primo y divide a mn, divide a uno de ellos, digamos m. Entonces también divide a

$$a - yum = xvn,$$

y por ello ha de dividir a x, v o n. Como $mcd(m, x) = mcd(m, n) = 1$, se sigue que p divide a v. En tal caso dividirá a

$$um + vn = 1,$$

lo cual es absurdo. Por lo tanto, $a + mn\mathbb{Z} \in \mathbb{Z}_{mn}^*$. Como

$$a - x = yum + x(vn - 1) = yum - xum \in m\mathbb{Z},$$

$$a - y = xvn + y(um - 1) = xvn - yvn \in n\mathbb{Z},$$

y así tenemos que

$$f(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z}) = (x + m\mathbb{Z}, y + n\mathbb{Z}).$$

- Finalmente, y como consecuencia de lo definido anteriormente tenemos que, sabiendo que todo natural positivo m puede descomponerse en factores primos por el *Teorema fundamental de la Aritmética*, $m = p_1^{a_1} \dots p_k^{a_k}$, resulta

$$\phi(m) = \phi(p_1^{a_1} \dots p_k^{a_k}) = p_1^{a_1-1} \dots p_k^{a_k-1}(p_1 - 1) \dots (p_k - 1).$$

Así, hemos podido definir la *función de Euler*, y la vamos a enunciar como teorema:

Teorema 2.1. *Dado un natural positivo m y el grupo abeliano $\mathbb{Z}_m^*$, formado por todas las clases cuyo representante es coprimo con m, entonces existe una función que llamaremos* ***función de Euler*** *y la definiremos como:*

$$\begin{array}{rccl} \phi\colon & \mathbb{N} \setminus \{0\} & \longrightarrow & \mathbb{N} \setminus \{0\} \\ & m & \longmapsto & \phi(m) = \phi(p_1^{a_1} \dots p_k^{a_k}) = p_1^{a_1-1} \dots p_k^{a_k-1}(p_1 - 1) \dots (p_k - 1) \end{array}$$

que a cada m le hace corresponder el orden $\phi(m)$ del grupo $\mathbb{Z}_m^*$.

2.2. Grupos cíclicos

Ya hemos podido presentar las principales propiedades y resultados sobre grupos: su estructura, la de los subgrupos, cocientes, aplicaciones entre ellos, etc. Lo que veremos ahora es un tipo concreto de grupo, los más sencillos de todos, que son aquellos que están generados por un sólo elemento: los conocidos como *grupos cíclicos*. Para esta sección será útil recordar la conocida como *función de Euler*, a la que le he dedicado unas páginas en la sección anterior.

Definición 2.2. *Diremos que un grupo G es* ***cíclico*** *si existe un elemento $a \in G$ tal que $G = \langle a \rangle$, es decir, si está generado por un sólo elemento $a \in G$. En tal caso diremos que a es un generador de G. Escribiremos*

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Notar que esto último es sólo si el grupo G es multiplicativo, en caso de ser aditivo tendríamos

$$G = \langle a \rangle = \{na : n \in \mathbb{Z}\}.$$

Como ejemplo sencillo de grupo cíclico es el grupo $\mathbb{Z}$ de los número enteros, ya que $\mathbb{Z} = \langle 1 \rangle$. También $\mathbb{Z}_n$ es grupo cíclico, en este caso generado por la clase de equivalencia del 1, $[1]_n$. Al grupo cíclico $\mathbb{Z}_n$ lo llamaremos ***grupo de restos módulo n*** y, como ya sabemos, consta de n elementos, que son:

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\},$$

donde $[0]_n = 0 + n\mathbb{Z}$, $[1]_n = 1 + n\mathbb{Z}$, ..., $[n-1]_n = (n-1) + n\mathbb{Z}$. Se llama grupo (en realidad es un anillo) de restos módulo n porque a cada clase pertenecen varios elementos: todos los que al dividir por n den el resto que tenga como representante. Es decir, a la clase del 0 pertencerán todos los elementos que al dividir entre n tengan como resto 0, a la clase del 1 los que al dividir entre n den como resto 1, y así hasta $n - 1$.

Además como consecuencia también sencilla de ver tenemos:

Proposición 2.3. *Un grupo finito G es cíclico si y sólo si existe $a \in G$ tal que $o(a) = |G|$.*

Demostración: En efecto, si $G = \langle a \rangle$, $|G| = o(\langle a \rangle) = o(a)$(el orden de un elemento a coincide con el orden del subgrupo generado por a). Recíprocamente, si $a \in G$ y $o(a) = |G|$, $\langle a \rangle$ es un subconjunto de G con tantos elementos como G, luego

$$\langle a \rangle = G.$$

□

Proposición 2.4. *Si p es un número primo y G es un grupo de orden p, entonces G es cíclico.*

Demostración: Sea $a \in G$, con $a \neq 1$. Por el *Teorema de Lagrange* $o(a)$ divide a p, como $o(a) \neq 1$, será entonces $o(a) = p$ y así G es cíclico.

□

Proposición 2.5. *Sea G un grupo, $x \in G$ un elemento de orden n y k un entero positivo entre 1 y n. Entonces $o(x^k) = n/d$, con $d = mcd(n, k)$.*

Demostración: Veamos que n/d es el menor entero positivo tal que $(x^k)^{n/d} = 1$.

Para comenzar,

$$(x^k)^{n/d} = (x^n)^{k/d} = 1^{k/d} = 1$$

ya que d divide a k por ser $d = mcd(n, k)$ y que el orden de x es n.

Por otra parte, si t es un entero positivo tal que $(x^k)^t = 1$, entonces kt es múltiplo de n, es decir que existe un t' entero positivo tal que $kt = nt'$. De aquí, puesto que d divide a k y a n,

$$\left(\frac{k}{d}\right) t = \left(\frac{n}{d}\right) t',$$

luego $\left(\frac{n}{d}\right)$ divide a $\left(\frac{k}{d}\right) t$. Pero como n/d y k/d son primos entre sí, necesariamente (n/d) divide a t, como queríamos demostrar. (n/d es el menor entero positivo tal que $(x^k)^{n/d} = 1$).

□

Y, como consecuencia de este resultado tenemos el siguiente corolario (ya que recordamos que el orden de un elemento coincide con el orden de su subgrupo generado).

Corolario 2.5.1. *Sea G un grupo, $x \in G$ un elemento de orden n y k un entero positivo entre 1 y n. Si $mcd(n, k) = d$, entonces $\langle x^k \rangle$ es un subgrupo de orden n/d.*

Proposición 2.6. *Supongamos que $G = \langle x \rangle$ es un grupo cíclico. Si H es un subgrupo de G, entonces $H = \{1\}$ ó $H = \langle x^k \rangle$, con k el menor entero positivo tal que $x^k \in H$.*

Demostración: Si $H = \{1\}$ no hay nada que probar. Sea $H \neq \{1\}$ y veamos que $H = \langle x^k \rangle$, con k el menor entero positivo tal que $x^k \in H$.

Es claro, por ser el producto una operación interna en H, que $\langle x^k \rangle \in H$.

Ahora, dado $x^p \in H$, comprobemos que $x^p \in \langle x^k \rangle$, es decir, que p es múltiplo de k. Podemos suponer que $p \geq 0$ pues p será múltiplo de k si y sólo si lo es $-p$. Por el algoritmo de la división, al dividir p entre k existirán enteros no negativos q, r , $0 \leq r < k$, tales que $p = kq + r$. Entonces,

$$x^p = x^{kq+r} = (x^k)^q x^r, \text{ por tanto } x^r = x^p (x^k)^{-q} \in H$$

pero por la elección de k (el menor entero positivo tal que $x^k \in H$) necesariamente $r = 0$. Esto implica que $x^p = (x^k)^q \in \langle x^k \rangle$.

□

Es decir, lo que acabamos de comprobar nos demuestra que *todo subgrupo de un grupo cíclico es también cíclico*, ó bien el subgrupo trivial ó bien el generado por una potencia del elemento generador del grupo.

Así pues, sabemos que todo subgrupo de un grupo cíclico es también cíclico, pero de qué forma son concretamente estos subgrupos nos lo dirá el siguiente resultado:

Proposición 2.7. *Sea G un grupo cíclico, $n = |G|$. Para cada divisor m de n existe un único subgrupo de G de orden m. Además este subgrupo es cíclico.*

Demostración: Sea $a \in G$ tal que $G = \langle a \rangle$. En primer lugar, si $n = kl$, $\langle a^k \rangle$ es un subgrupo de orden l, ya que $o(a^k) = \dfrac{n}{mcd(k,n)} = \dfrac{n}{k} = l$ por 2.5.

Probemos la proposición. Como m divide a n, existe un natural d tal que

$$n = dm.$$

Por lo que acabamos de ver al comienzo de la demostración $H = \langle a^d \rangle$ tiene orden m. Veamos que es el único subgrupo de orden m. Sea K otro subgrupo de G de orden m. Sea k el menor entero positivo tal que $a^k \in K$ (que existe puesto que $K \subset G = \langle a \rangle$).

Si $a^p \in K$, p es múltiplo de k ya que, si dividimos p entre k tenemos, por el algoritmo de la división, que

$$p = kq + r,\ 0 \leq r < k, \text{ luego } a^r = a^{p-kq} = a^p (a^k)^{-q} \in K$$

pero por la elección de k (el menor entero positivo tal que $a^k \in K$), ha de ser necesariamente $r = 0$, y así

$$p = qk, \text{ es decir, } p \text{ es múltiplo de } k.$$

De esto se deduce que $n = sk$, con $s \in \mathbb{N}$, ya que $a^n = 1 \in K$, además

$$K = \langle a^k \rangle$$

porque para cada $x = a^p \in K$ se tiene que $x = (a^k)^p \in \langle a^k \rangle$.

Ahora, $m = |K| = o(a^k) = n/k$, con lo que $k = n/m = d$ y así $K = \langle a^d \rangle = H$.

Luego, $\langle a^d \rangle$ es el único subgrupo de G de orden m. Como además es cíclico, hemos acabado.

□

Por lo tanto, dado un grupo cíclico finito $G = \langle x \rangle$ de orden n, los subgrupos serán de la forma $\langle x^{n/m} \rangle$, con m un divisor de n.

Corolario 2.7.1. *Sea G un grupo finito. G no tiene subgrupos propios si y sólo si $|G|$ es primo. Por lo tanto, un grupo simple abeliano finito es de orden primo.*

Demostración: Si $|G|$ es un primo, entonces G no tiene subgrupos propios por el *Teorema de Lagrange.*

Recíprocamente, supongamos que G no tiene subgrupos propios. Sea $1 \neq x \in G$. Entonces $G = \langle x \rangle$. Si p es un número primo que divide a $|G|$, entonces sabemos que G va a tener un subgrupo H de orden p. Por lo tanto, $G = H$ tiene orden p.

□

Como ya hemos visto, tanto para grupos en general como para grupos cíclicos en particular, existen ciertos elementos que dan lugar ó que generan el grupo, y los denominamos *generadores.* A la hora de definirse un grupo cíclico cualquiera suele darse además el elemento que lo genera y puede parecer que este elemento es único, así que es natural preguntarse si pueden o no existir más generadores. Así, en caso de que los haya, el siguiente resultado nos ayudará a encontrar todos *generadores* de un grupo cíclico G cualquiera, es decir aquellos elementos x tales que $G = \langle x \rangle$.

Proposición 2.8. *Sea $G = \langle x \rangle$ un grupo cíclico finito de orden n, y sea k un entero positivo entre 1 y n. Entonces x^k es un generador de G si y sólo si $mcd(n, k) = 1$.*

Demostración: Si $mcd(n, k) = 1$, entonces $|\langle x^k \rangle| = n/1 = n$ luego $\langle x^k \rangle$ es un grupo, subgrupo de G, con el mismo número de elementos de G, por lo que necesariamente es el propio G y así x^k un generador.

Recíprocamente, supongamos que $mcd(n, k) > 1$, entonces resulta $|G| = |\langle x^k \rangle| = \dfrac{n}{mcd(n, k)} < n$, lo cual es absurdo.

□

Por ejemplo, si tenemos un grupo $G = \langle x \rangle$ cíclico de orden 9, sus generadores son x, x^2, x^4, x^5, x^7 y x^8.

Ejemplo 2.8.1. *Como hemos visto al principio, si tenemos $n \in \mathbb{Z}$, con $n > 1$ y consideramos el grupo aditivo $\mathbb{Z}_n$, tenemos que $\mathbb{Z}_n = \langle [1] \rangle$ (aquí hemos escrito $[1]$ en lugar de $[1]_n$ por cuestiones estéticas). Esto se comprueba fácilmente ya que*

$$0\,[1] = [0],\ 1\,[1] = [1],\ 2\,[1] = [2],\ \ldots,\ (n-1)\,[1] = [n-1]\,.$$

Y como acabamos de ver, en función del n escogido, $\mathbb{Z}_n$ puede estar generado por otros elementos además de $[1]$. Veamos para $\mathbb{Z}_8$.

Ya sabemos que $\mathbb{Z}_8 = \{[0]\,, [1]\,, [2]\,, [3]\,, [4]\,, [5]\,, [6]\,, [7]\}$, y además

$0\,[3] = 0(3+8\mathbb{Z}) = 0+8\mathbb{Z} = [0]\,, 1\,[3] = 1(3+8\mathbb{Z}) = 3+8\mathbb{Z} = [3]\,, 2\,[3] = 2(3+8\mathbb{Z}) = 6+8\mathbb{Z} = [6]\,,$

$3\,[3] = 3(3+8\mathbb{Z}) = 1+8\mathbb{Z} = [1]\,, 4\,[3] = 4(3+8\mathbb{Z}) = 4+8\mathbb{Z} = [4]\,, 5\,[3] = 5(3+8\mathbb{Z}) = 7+8\mathbb{Z} = [7]\,,$

$6\,[3] = 6(3+8\mathbb{Z}) = 2+8\mathbb{Z} = [2]\,, 7\,[3] = 7(3+8\mathbb{Z}) = 5+8\mathbb{Z} = [5]\,,$

con lo que $\mathbb{Z}_8 = \langle [3] \rangle$.

Por el resultado anterior sabemos que esto ocurre porque $mcd(3,8) = 1$*, igualmente con* $[5]$ *y con* $[7]$ *pero sin embargo con* $[2]$*:*

$0\,[2] = 0(2+8\mathbb{Z}) = 0+8\mathbb{Z} = [0]\,, 1\,[2] = 1(2+8\mathbb{Z}) = 2+8\mathbb{Z} = [2]\,, 2\,[2] = 2(2+8\mathbb{Z}) = 4+8\mathbb{Z} = [4]\,,$

$3\,[2] = 3(2+8\mathbb{Z}) = 6+8\mathbb{Z} = [2]\,, 4\,[2] = 4(2+8\mathbb{Z}) = 0+8\mathbb{Z} = [0]\,, 5\,[2] = 5(2+8\mathbb{Z}) = 2+8\mathbb{Z} = [2]\,,$

$6\,[2] = 6(2+8\mathbb{Z}) = 4+8\mathbb{Z} = [4]\,, 7\,[2] = 7(2+8\mathbb{Z}) = 6+8\mathbb{Z} = [6]\,,$

con lo que $\langle [2] \rangle = \{[0]\,, [2]\,, [4]\,, [6]\} \neq \mathbb{Z}_8$.

■

Notar que, dado un $\mathbb{Z}_n$, con $n > 1$, cuando hallamos todos los generadores lo que estamos haciendo es buscar todos los x tales que $mcd(x,n) = 1$, pero ésto no es más que la imagen de n por la conocida *función de Euler*. De esto se desprende la siguiente consecuencia:

Corolario 2.8.1. *Sea* $n \in \mathbb{Z}$ *con* $n > 1$ *y* $k \in \mathbb{N}$*. Entonces* $\mathbb{Z}_n = \langle [k] \rangle$ *si y sólo si* $[k] \in \mathbb{Z}_n^*$*. Recordando que*

$$\mathbb{Z}_n^* = \{a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} : mcd(a,n) = 1\}.$$

De todos estos resultados vistos, y empleando la *función de Euler* ϕ, podemos así afirmar el siguiente teorema, que además queda demostrado:

Teorema 2.9. *Sea* G *un grupo cíclico finito de orden* n*. Si* d *es un divisor de* n *(podemos suponerlo positivo), entonces el número de elementos de* G *de orden* d *es* $\phi(d)$*.*

Esto quiere decir básicamente que en un grupo cíclico G, el número de elementos que tengan orden d será el número de *coprimos* con d. En particular, si $d = n = |G|$, tendremos que el número de generadores de G será $\phi(d)$.

Proposición 2.10. *Si* G *es cíclico y* H *es un subgrupo normal de* G*, también el cociente* G/H *es cíclico.*

Demostración: Si $G = \langle a \rangle$, es obvio que $G/H = \langle aH \rangle$.

□

Como ya vimos en un ejemplo cuando vimos subgrupos normales, un subgrupo cualquiera $H = m\mathbb{Z}$ de $\mathbb{Z}$, con m entero positivo, es normal ya que $\mathbb{Z}$, y por tanto

$m\mathbb{Z}$, es abeliano. Luego, por lo que acabamos de ver, el grupo cociente $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ es cíclico y su orden en m. De hecho, como ya sabemos

$$\mathbb{Z}_m = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\},$$

y $\mathbb{Z}_m = \langle 1 + m\mathbb{Z} \rangle$. Por lo tanto, dependiendo de la m escogida, la *función de Euler* establece el número de generadores del grupo cociente $\mathbb{Z}_m$.

Ya hemos visto a lo largo de estos capítulos que el conjunto de los enteros y los enteros módulo n, $\mathbb{Z}$ y $\mathbb{Z}_n$, son grupos, y en concreto grupos cíclicos. Que se haya hecho un inciso especial en estos dos grupos no es casualidad, vamos a ver a continuación que son, por así decirlo, los «únicos» grupos cíclicos que existen. Es decir, que dado un grupo cíclico, o es equivalente a $\mathbb{Z}$ o a $\mathbb{Z}_n$, y ya vimos en el anterior capítulo que cuando hablamos de «igualdad» o «equivalencia» en *Teoría de Grupos* en realidad estamos hablando de isomorfismos. Básicamente todo grupo cíclico es isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_n$.

Teorema 2.11. *Sea G un grupo cíclico. Se verifica:*

1. *Si G es infinito, entonces es isomorfo a $(\mathbb{Z}, +)$.*
2. *Si G es finito de orden n, entonces es isomorfo a $(\mathbb{Z}_n, +)$.*

Demostración: (Notar que hemos especificado que la operación en ambos grupos $\mathbb{Z}$ y $\mathbb{Z}_n$ sea la adición, puesto que su elemento neutro será el 0 y no el 1) Sea $G = \langle x \rangle$ y consideremos el homomorfismo

$$\begin{array}{rccc} f\colon & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k, \end{array}$$

que es claramente sobreyectivo ($Imf = G$).

1. Basta comprobar que f es inyectiva. Para ello supongamos por reducción al absurdo que $Kerf \neq \{0\}$. Entonces, por ser $Kerf$ un subgrupo de $\mathbb{Z}$ no trivial, será de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{N}$ no nulo. Ahora, el *Primer Teorema de Isomorfía* nos asegura que $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \simeq G$, así G tendría n elementos, lo cual contradice la hipótesis de que sea infinito.

2. Si G es finito de orden n, no puede ser $Kerf = \{0\}$, puesto que en este caso f sería inyectiva y entonces G infinito. Así pues $Kerf = m\mathbb{Z}$ para algún $m \in \mathbb{N}$ no nulo, usando de nuevo el *Primer Teorema de Isomorfía* $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \simeq G$. Como $\mathbb{Z}_m$ y G han de tener el mismo orden, $m = n$.

□

Como consecuencia interesante tenemos:

Corolario 2.11.1. *Supongamos que $G = \langle a \rangle$ es un grupo cíclico. Entonces:*

1. *Si $o(a) = \infty$, entonces*

$$\begin{array}{rccc} f\colon & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & a^k, \end{array}$$

   es un isomorfismo.

2. *Si* $o(a) = n$, *entonces*

$$\begin{array}{rccc} f\colon & \mathbb{Z}_n & \longrightarrow & G \\ & [k] & \longmapsto & a^k, \end{array}$$

es un isomorfismo.

Además, el teorema anterior nos permite establecer una «igualdad» entre grupos cíclicos a través de isomorfismos:

Corolario 2.11.2. *Sean* G *y* H *grupos cíclicos. Entonces* $G \simeq H$ *si y sólo si* $o(H) = o(G)$.

Otra consecuencia, más bien lógica y evidente, del anterior teorema pero que podríamos haberla presentado perfectamente desde el principio es la que nos habla acerca de otro invariante bajo isomorfismos de grupos (ya vimos alguno en el anterior capítulo):

Corolario 2.11.3. *Sean dos grupos* G_1 *y* G_2 *isomorfos,* $G_1 \simeq G_2$, *y* G_1 *cíclico, entonces* G_2 *también será cíclico. En concreto, la propiedad de ser cíclico es un invariante bajo isomorfismo.*

Demostración: Sea $a \in G_1$ tal que $G_1 = \langle a \rangle$ y $f\colon G_1 \longrightarrow G_2$ un isomorfismo. Llamemos $b = f(a)$. Probemos que $G_2 = \langle b \rangle$.

Dado un $y \in G_2$, existe un $x \in G_1$ tal que $y = f(x)$. Como $x \in G_1 = \langle a \rangle$, existirá un entero k tal que $x = a^k$. Entonces

$$y = f(x) = f(a^k) = f(a)^k = b^k \in \langle b \rangle.$$

□

Por último aclarar que de ahora en adelante si hablamos de un grupo cíclico cualquiera de orden n lo denotaremos por C_n.

3. Grupos de automorfismos

3.1. Grupos de automorfismos y automorfismos internos

Del *Álgebra Lineal* conocemos ya los espacios vectoriales, y en concreto los isomorfismos de un espacio vectorial en sí mismo, que denotamos en su momento como *automorfismos*; también sabemos que ese conjunto de automorfismos no constituyen un espacio vectorial. Sin embargo cuando las estructuras sobre las que trabajemos sean los grupos sí se dará, el conjunto de los automorfismos de un grupo con la operación composición constituyen un grupo. En este capítulo nos dedicaremos a estudiarlos.

Definición 3.1. *Si* G *es un grupo, un* ***automorfismo*** *de* G *es un isomorfismo*

$$f\colon G \longrightarrow G.$$

Notaremos por $Aut(G)$ *el conjunto de los automorfismos de* G. $Aut(G)$ *es un subgrupo del grupo de las biyecciones de* G, $Biy(G)$. *En particular,* $Aut(G)$ *es un grupo*

con la operación composición. El contenido $Aut(G) \subseteq Biy(G)$ es evidente y como la aplicación identidad

$$\begin{array}{rccc} id_G\colon & G & \longrightarrow & G \\ & x & \longmapsto & x \end{array}$$

es un automorfismo de G, $Aut(G)$ no es vacío. Además, sabemos que dados $f, g \in Aut(G)$, $g^{-1} \in Aut(G)$, la composición $f \circ g^{-1}$ es biyectiva por serlo f y g^{-1}, y es homomorfismo por serlo la composición de homomorfismos. Así, $f \circ g^{-1} \in Aut(G)$. Como siempre, la asociatividad se desprende de la composición.

Ejemplo 3.1.1.

$$Aut(\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}.$$

Ya que si $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ es un automorfismo, sabemos de su estudio que existirá un $a \in \mathbb{Z}$ tal que

$$f(n) = an, \text{ para cada } n \in \mathbb{Z}.$$

Al ser f automorfismo, es sobreyectiva y así $1 \in Imf$. En consecuencia ha de existir un $n \in \mathbb{Z}$ tal que $an = 1$. Por lo tanto, sólo puede ser $a = +1$ ó $a = -1$. De hecho esos serán los elementos de $Aut(\mathbb{Z})$:

$$\begin{array}{rccc} f_1\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & n \end{array}$$

$$\begin{array}{rccc} f_{-1}\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & -n \end{array}$$

Recíprocamente, los homomorfismos

$$\begin{array}{rccc} f\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & n \end{array}$$

y

$$\begin{array}{rccc} g\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & -n \end{array}$$

son evidentemente automorfismos. Así $Aut(\mathbb{Z}) = \{f, g\}$ tiene dos elementos, y sabemos que todo grupo de orden primo es cíclico, por lo que $Aut(\mathbb{Z})$ es cíclico, y que todo cíclico finito de orden 2 es isomorfo a $\mathbb{Z}/2\mathbb{Z}$, por lo que ya está.

■

Proposición 3.2. *Sea C_n un grupo cíclico de orden n, entonces*

$$Aut(C_n) \simeq \mathcal{U}_n.$$

En particular, es un grupo abeliano de orden $\phi(n)$.

Demostración: Sea

$$\begin{array}{rccc} \psi\colon & \mathcal{U}_n & \longrightarrow & Aut(C_n) \\ & [u] & \longmapsto & f_u\colon C_n \longrightarrow C_n \\ & & & \qquad x \longmapsto x^u \end{array}$$

Veamos que ψ está bien definida:

$f_u(x^k) = f_u(x)^k = (x^u)^k = x^{uk}$, f_u es un homomorfismo y $f_u(\langle x\rangle) = \langle f_u(x)\rangle = \langle x^u\rangle = C_n$ ya que u es coprimo con n y por lo tanto x^u es generador de C_n. Esto quiere decir también que f_u es sobreyectiva, y como es una aplicación sobreyectiva entre dos conjuntos del mismo cardinal tenemos que es biyectiva y así $f_u \in Aut(C_n)$. Si tenemos que $[u] = [j]$ para algunos $[u], [j] \in \mathcal{U}_n$ entonces $\psi([u]) = \psi([j])$, pero $[u] = [j] \Rightarrow u = j + kn$ para algún $k \in \mathbb{Z}$. Así $f_u(x) = x^u = x^{j+kn} = x^j(x^n)^k = x^j = f_j(x)$ y así ψ está bien definida.

Veamos que ψ es homorfismo:

$\psi([u][j])(x) = f_{uj}(x) = x^{uj} = (x^j)^u = f_u(x^j) = f_u f_j(x) = [\psi([u]) \circ \psi([j])](x)$.

Es claramente sobreyectiva y para ver que es inyectiva:

$$Ker\ \psi = \{[u] \in \mathcal{U}_n : f_u = id \in Aut(C_n)\} = \{[u] \in \mathcal{U}_n : x^u = x\} = \{[u] \in \mathcal{U}_n x^{u-1} = 1\} = \{[u] \in \mathcal{U}_n : n \mid u - 1\},$$

luego $[u] \in Ker\ \psi$ si y sólo si $\exists k \in \mathbb{Z}$ tal que $u - 1 = kn$ si y sólo si $\exists k \in \mathbb{Z}$ tal que $u = 1 + kn$ si y sólo si $u \equiv 1 \bmod n$. Así, $Ker\ \psi = \{1\}$ y ψ es inyectiva.

□

Esto es lo mismo que decir que, dado n un número natural mayor que uno,

$$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}_n^*.$$

En particular, de todos estos resultados vistos tenemos:

Corolario 3.2.1. *Sea G un grupo, entonces:*

1. *$Aut(G) = \mathbb{Z}/2\mathbb{Z}$ si G es cíclico infinito*
2. *$Aut(G) = \mathbb{Z}_n^*$ si G es cíclico de orden n.*

Y ahora el siguiente teorema, que será útil más allá incluso de la presente obra:

Teorema 3.3. *Si dos grupos G_1 y G_2 son isomorfos, entonces también lo serán $Aut(G_1)$ y $Aut(G_2)$.*

Demostración: Sea $f\colon G_1 \longrightarrow G_2$ un isomorfismo. Construimos

$$\begin{array}{rccc} \phi\colon & Aut(G_2) & \longrightarrow & Aut(G_1) \\ & h & \longmapsto & f^{-1} \circ h \circ f. \end{array}$$

Y veamos que es el isomorfismo que buscamos. Evidentemente, cada automorfismo h de G_2 es un homomorfismo biyectivo, luego $f^{-1} \circ h \circ f \in Aut(G_1)$ y ϕ está bien definida. Veamos que es homomorfismo:

$$\phi(g \circ h) = f^{-1} \circ (g \circ h) \circ f = f^{-1} \circ g \circ f \circ f^{-1} \circ h \circ f = \phi(g) \circ \phi(h).$$

Si $h \in Ker\phi$, se tiene que $f^{-1} \circ h \circ f = I_{G_1}$, luego $h \circ f = f$ y de aquí $h = (h \circ f) \circ f^{-1} = f \circ f^{-1} = I_{G_1}$. Así, ϕ es inyectiva.

Finalmente, ϕ es sobreyectiva, pues dado $g \in Aut(G_1)$, existe

$$h = f \circ g \circ f^{-1} \in Aut(G_2)$$

tal que

$$\phi(h) = f^{-1} \circ h \circ f = f^{-1} \circ f \circ g \circ f^{-1} \circ f = g.$$

□

En cuanto a este resultado, importante decir que el recíproco no tiene por qué cumplirse, es decir, pueden existir grupos no isomorfos G_1 y G_2 tales que $Aut(G_1) \simeq Aut(G_2)$. Un ejemplo de ello es el siguiente:

Ejemplo 3.3.1. *Consideremos dos grupos, $G_1 = \mathbb{Z}/3\mathbb{Z}$ y $G_2 = \mathbb{Z}/4\mathbb{Z}$, que claramente no son isomorfos al no tener el mismo orden.*

De la proposición vista antes tenemos que

$$Aut(G_1) \simeq \mathbb{Z}_3^*,\ Aut(G_2) \simeq \mathbb{Z}_4^*.$$

Ahora, usando la función de Euler:

$$|\mathbb{Z}_3^*| = \phi(3) = 2,\ |\mathbb{Z}_4^*| = \phi(4) = 2.$$

Así, al tener ambos órdenes primos podemos decir que son cíclicos, y por tanto

$$\mathbb{Z}_3^* \simeq \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}_4^* \simeq \mathbb{Z}/2\mathbb{Z},$$

luego $Aut(G_1) \simeq Aut(G_2)$.

■

Antes de pasar al estudio de los llamados *automorfismos internos* veamos un ejemplo general de automorfismos que todos conocemos del *Álgebra Lineal*:

Ejemplo 3.3.2. *Sea $P \in GL_n(\mathbb{R})$ una matriz con determinante no nulo y coeficientes reales. Si $A \in GL_n(\mathbb{R})$, entonces $PAP^{-1} \in GL_n(\mathbb{R})$. Por tanto, podemos definir una aplicación*

$$\begin{array}{rccc} f\colon & GL_n(\mathbb{R}) & \longrightarrow & GL_n(\mathbb{R}) \\ & A & \longmapsto & PAP^{-1} \end{array}$$

para cualquier $A \in GL_n(\mathbb{R})$. Además, si $A, B \in GL_n(\mathbb{R})$, entonces

$$f(AB) = PABP^{-1} = PAP^{-1}PBP^{-1} = f(A)f(B),$$

con lo que f es homomorfismo.

Veamos cuál es el núcleo de esta aplicación, dada una $A \in GL_n(\mathbb{R})$ entonces que $f(A) = I_n$ (matriz identidad) quiere decir que $PAP^{-1} = I_n$ y esto implica que $A = I_n$. En consecuencia, $Kerf = \{I_n\}$, así que f es inyectiva.

Ahora, si $B \in GL_n(\mathbb{R})$, entonces $A = P^{-1}BP \in GL_n(\mathbb{R})$ y

$$f(A) = PAP^{-1} = PP^{-1}BPP^{-1} = B,$$

y así f es sobreyectiva. Luego f es un automorfismo de $GL_n(\mathbb{R})$.

■

Proposición 3.4. *Sea G un grupo y $g \in G$. Sea $x \in G$. Definimos $x^g = gxg^{-1}$. A x^g lo denominaremos* ***conjugado de*** *x* ***por*** *g ó simplemente* ***conjugado****. Entonces:*

1. *La aplicación*
$$\begin{array}{rccc} \alpha_g\colon & G & \longrightarrow & G \\ & x & \longmapsto & x^g \end{array}$$
es un automorfismo de G llamado ***automorfismo interno****.*
2. *$\alpha_g \circ \alpha_h = \alpha_{gh}$, $\forall g, h \in G$.*

Demostración: Para demostrar el resultado iremos por partes:

1. $\alpha_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \alpha_g(x)\alpha_g(y)$. Así, α_g es homomorfismo. Es evidente comprobar que es biyectivo teniendo en cuenta que su inversa es α_{g^1}, que es claro que va a existir.
2. $(\alpha_g \circ \alpha_h)(x) = \alpha_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \alpha_{gh}(x)$.

□

Ahora, dado que tenemos $\alpha_g \circ \alpha_h = \alpha_{gh}$ y que $(\alpha_g)^{-1} = \alpha_{g^{-1}}$ es claro que el conjunto de los automorfismos internos tendrá también estructura de grupo.

Definición 3.5. *Dado un grupo G, definimos el* ***grupo de los automorfismos internos de*** *G como*
$$Int(G) = \{\alpha_g : g \in G\}.$$

Es claro que $Int(G) \leq Aut(G)$.

Es más, se tiene que:

Proposición 3.6. *$Int(G)$ es un subgrupo normal de $Aut(G)$.*

Demostración: Vamos a comprobar que $(Int(G))^g \subseteq Int(G)$, $\forall g \in Aut(G)$. Sea así $f \in (Int(G))^g$. Por tanto, $g \circ f \circ g^{-1} \in Int(G)$, luego $\exists y \in G$ tal que $g \circ f \circ g^{-1} = \alpha_y$ y así $f = g^{-1} \circ \alpha_y \circ g$.

Entonces, dado $x \in G$ y llamando $b = g^{-1}(y)$, tenemos

$$f(x) = (g^{-1} \circ \alpha_y)(g(x)) = g^{-1}(yg(x)y^{-1}) = bxb^{-1} = \alpha_b(x).$$

Por lo que $f = \alpha_b \in Int(G)$.

□

Si consideramos ahora la aplicación

$$\begin{array}{rccc} \psi\colon & G & \longrightarrow & Aut(G) \\ & g & \longmapsto & \alpha_g, \end{array}$$

entonces es claro que la imagen es $Int(G)$, y si calculamos su núcleo:

$$Ker\ \psi = \{g \in G : \psi(g) = \alpha_g = id\} = \{g \in G : gxg^{-1} = x\ \ \forall x \in G\} = \{g \in G : gx = xg\ \ \forall x \in G\} = Z(G).$$

Y ahora, por el *Primer Teorema de Isomorfía* tenemos que

$$G/Z(G) \simeq Int(G).$$

De esto se deduce además dos propiedades elementales que condensaremos en la siguiente proposición:

Proposición 3.7. *Sea G un grupo. Son equivalentes:*

1. *G es abeliano.*
2. *$Int(G) = \{id_G\}$.*
3. *$Int(G)$ es un grupo cíclico.*

Demostración:
(1) $\Longrightarrow$ (2). Si G es abeliano coincide con su centro. Así que $G/Z(G)$ consta de un solo elemento y como $G/Z(G) \simeq Int(G)$, $Int(G) = \{id_G\}$.

(2) $\Longrightarrow$(3). Evidente, puesto que sólo tiene un elemento.

(3) $\Longrightarrow$(1). Sean $x, y \in G$. Vamos a probar que $xy = yx$. Sabemos que $Int(G)$ es cíclico, y como la propiedad de ser cíclico también es un invariante bajo isomorfismos, entonces $G/Z(G)$ también es cíclico; en consecuencia existirá $g \in G$ tal que $G/Z(G) = \langle Z(G)g\rangle$. Así, para los x, y anteriores,

$$Z(G)x = Z(G)g^k,\ Z(G)y = Z(G)g^l,$$

con k y l enteros.

Por lo tanto, $xg^{-k} \in Z(G)$, y también $yg^{-l} \in Z(G)$. Entonces

$$xy = xg^{-k}g^k y = g^k yxg^{-k} = g^k yg^{-l}g^l xg^{-k} = yg^{-l}g^k g^l xg^{-k} = yg^k xg^{-k} = yxg^{-k}g^k = yx,$$

donde es importante tener en cuenta que $g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$ en la quinta igualdad.

□

Y de estas propiedades deducimos las siguientes consecuencias:

Corolario 3.7.1. *Sean G un grupo y H subgrupo de G contenido en $Z(G)$. Entonces*

1. *H es subgrupo normal.*
2. *Si G/H es cíclico, G es abeliano.*

Demostración:
(1). Ya se vió.

(2). Por el *Segundo Teorema de Isomorfía*

$$G/Z(G) \simeq (G/H)/(Z(G)/H).$$

Como G/H es cíclico y $(Z(G)/H)$ es subgrupo normal, también lo será

$$(G/H)/(Z(G)/H)$$

y así $G/Z(G)$ también. Que G sea abeliano se deduce de los resultados anteriores.

□

En particular, si $H = Z(G)$ cumple entonces que es un subgrupo de G y evidentemente está contenido en $Z(G)$. Por lo que se tiene el corolario y llegaríamos al resultado que suele conocerse:

Si $G/Z(G)$ ***es cíclico entonces*** G ***es abeliano.***

3.2. Producto directo y semidirecto

Proposición 3.8. *Sean G_1 y G_2 grupos. Dado el producto cartesiano $G_1 \times G_2$ podemos convertirlo en un grupo con la siguiente operación:*

$$\cdot : (g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2, g_2').$$

Además, dado un grupo G y $N_1, N_2 \trianglelefteq G$ subgrupos normales tales que $G = N_1 N_2$ y $N_1 \cap N_2 = \{1_G\}$. Entonces

$$N_1 \times N_2 \simeq G.$$

Demostración: Para ver que es grupo con $\cdot$ basta con una simple comprobación. Para la segunda parte definimos la siguiente aplicación:

$$\begin{array}{rccc} f: & N_1 \times N_2 & \longrightarrow & G \\ & (n_1, n_2) & \longmapsto & n_1 n_2 \end{array}$$

Para ver que f es homomorfismo:

$$f((n_1, n_2)(n_1', n_2')) = f((n_1 n_1', n_2 n_2')) = n_1 n_1' n_2 n_2'.$$

$$f((n_1, n_2))f((n_1', n_2')) = n_1 n_2 n_1' n_2'.$$

Para comprobar que son iguales bastará probar que $xy = yx$ para todo $x \in N_1$, $y \in N_2$. Sea $x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in N_1$, como también $x^{-1}y^{-1}xy = (x^{-1}y^{-1}x)y \in N_2$ y por hipótesis tenemos que $N_1 \cap N_2 = \{1_G\}$, entonces será que $x^{-1}y^{-1}xy = 1$, luego $xy = yx$.

Ahora, como $G = N_1 N_2$, f es suprayectiva. $Kerf = \{(n_1, n_2) \in N_1 \times N_2 : n_1 n_2 = 1\}$. Si $n_1 n_2 = 1$, entonces $n_2 = n_1^{-1} \in N_1 \cap N_2 = \{1_G\}$. Así, $n_1 = n_2 = 1_G$ y $Kerf = \{1_G\}$ y f es inyectiva.

□

Definición 3.9. *Decimos que el producto cartesiano en el que hemos descompuesto G antes, $N_1 \times N_2$ con $N_1, N_2 \trianglelefteq G$ tales que con $G = N_1 N_2$ y $N_1 \cap N_2 = \{1_G\}$, es un* ***producto directo****.*

Proposición 3.10. *Sean N y H grupos. Sea $\varphi\colon H \longrightarrow Aut(N)$ un homomorfismo entre H y el grupo de los automorfismos de N. En el producto cartesiano $N \times H$ podemos definir una estructura de grupo conocida como* ***producto semidirecto de H por N vía φ*** *y denotada por $N \times_\varphi H$ de la siguiente manera:*

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2),$$

donde $\varphi(h_1)(n_2) = n_2^{h_1}$ normalmente, es decir, que el automorfismo en cuestión será la composición por un $h \in H$.

Ahora, sea G un grupo, $N \trianglelefteq G$ y $H \leq G$. Supongamos que $G = NH$ y $N \cap H = \{1_G\}$. Dado un

$$\begin{array}{rccc} \varphi\colon & H & \longrightarrow & Aut(N) \\ & h & \longmapsto & n \longmapsto n^h = hnh^{-1}. \end{array}$$

Entonces

$$N \times_\varphi H \simeq G.$$

Demostración: Comprobemos primero que es grupo. Cumple con la propiedad asociativa:

$$(n_1, h_1)((n_2, h_2)(n_3, h_3)) = (n_1, h_1)(n_2\varphi(h_2)(n_3), h_2h_3) = (n_1\varphi(h_1)(n_2\varphi(h_2)(n_3)), h_1h_2h_3) = (n_1\varphi(h_1)(n_2)\varphi(h_1h_2)(n_3), h_1h_2h_3).$$

$$((n_1, h_1)(n_2, h_2))(n_3, h_3) = (n_1\varphi(h_1)(n_2), h_1h_2)(n_3, h_3) = (n_1\varphi(h_1)(n_2)\varphi(h_1h_2)(n_3), h_1h_2h_3).$$

Tiene elemento neutro:

$$(n, h)(1, 1) = (n\varphi(h)(1), h) = (1\varphi(h)(n), h) = (1, 1)(n, h).$$

Cada elemento (n, h) tiene un inverso $(n, h)^{-1} = (\varphi(h^{-1})(n^{-1}), h^{-1})$.

$$(n, h)(\varphi(h^{-1})(n^{-1}), h^{-1}) = (n\varphi(h)(\varphi(h^{-1})(n^{-1})), 1) = (n\varphi(hh^{-1})(n^{-1}), 1) = (nn^{-1}, 1) = (1, 1).$$

$$(\varphi(h^{-1})(n^{-1}), h^{-1})(n, h) = (\varphi(h^{-1})(n^{-1})\varphi(h^{-1})(n), 1) = (\varphi(h^{-1})(n^{-1}n), 1) = (\varphi(h^{-1})(1), 1) = (1, 1).$$

Ahora, veamos la segunda parte. Sea $G = NH$, con $N \trianglelefteq G$, $H \leq G$ y $N \cap H = \{1_G\}$, y sea

$$\begin{array}{rccc} \varphi\colon & H & \longrightarrow & Aut(N) \\ & h & \longmapsto & n \longmapsto n^h = hnh^{-1}. \end{array}$$

Veamos que φ está bien definida: como $N \trianglelefteq G$, si $n \in N$ y $h \in H$, $hnh^{-1} \in N$. Ya sabemos que la conjugación es un automorfismo. Además φ es homorfismo:

$$\varphi(h_1, h_2)(n) = h_1h_2nh_2^{-1}h_1^{-1} = (\varphi(h_1) \circ \varphi(h_2))(n).$$

Definimos ahora

$$\begin{array}{rccc} f\colon & N \times_\varphi H & \longrightarrow & G \\ & (n, h) & \longmapsto & nh. \end{array}$$

y veamos que f es homomorfismo:

$$f((n_1,h_1)(n_2,h_2)) = f((n_1\varphi(h_1)(n_2),h_1h_2) = n_1\varphi(h_1)(n_2)h_1h_2 = n_1(h_1n2h_1^{-1})h_1h_2 = n_1h_1n_2h_2 = f((n_1,h_1))f((n_2,h_2)).$$

Como $G = NH$ f es claramente suprayectiva. Ahora, $Kerf = \{(n,h) \in N \times_\varphi H : nh = 1\}$. Y si $nh = 1$ entonces $n = h^{-1} \in N \cap H$, pero como $N \cap H = \{1_G\}$ tenemos que $n = h = 1_G$ y así f es inyectiva y por tanto isomorfismo.

□

Ejercicio *C_4 y $C_2 \times C_2$ son los únicos grupos de orden 4 salvo isomorfismo.*

Demostración: Usaremos el hecho de que, dado un grupo G en el que se cumple que $x^2 = 1\ \forall x \in G$ entonces G es abeliano. También se usará que, dado un grupo G y $N_1, N_2 \trianglelefteq G$ con $G = N_1N_2$ y $N_1 \cap N_2 = \{1_G\}$ entonces $G \simeq N_1 \times N_2$.

Sea así G un grupo tal que $|G| = 4$. Si existe un $x \in G$ tal que $o(x) = 4$ entonces $G \simeq C_4$ y ya está. Si no, entonces todos los elementos de G tienen necesariamente orden 2 salvo el neutro. Es decir, $x^2 = 1\ \forall x \in G$, entonces G es abeliano y así todos sus subgrupos son normales. Entonces, dados $x, y \in G$ elegimos $H = \langle x\rangle$ y $K = \langle y\rangle$ subgrupos propios distintos, y se verifica que $H, K \trianglelefteq G$, $H \cap K = \{1_G\}$ y

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{|\langle x\rangle||\langle y\rangle|}{1} = 2 \cdot 2 = 4,$$

y así $HK = G$. Luego $G \simeq H \times K = C_2 \times C_2$.

□

4. Acciones de grupos. Teoremas de Sylow

4.1. Acciones de grupos sobre conjuntos

Primero de todo, aclarar que se va a dar una definición de acción por así decirlo más desarrollada que la que normalmente se da. Realmente en el fondo es lo mismo, pero aquí comenzaremos con la definición desarrollada hasta llegar a lo que más tarde llamaremos representación de la acción.

Definición 4.1. *Sea G un grupo y X un conjunto no vacío. Entonces, una **acción de un grupo G sobre un conjunto** X es una aplicación*

$$\begin{array}{rccc} \varphi\colon & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & g(x) \end{array}$$

que cumple:

1. *$(gh)(x) = g(h(x))$ para todo $g, h \in G$ y $x \in X$.*
2. *$1_G(x) = x$ para todo $x \in X$.*

*Diremos así que G **actúa sobre el conjunto** X. En concreto, ésta es la definición de **acción a izquierda** del grupo G sobre el conjunto X, aunque simplemente la llamaremos acción. Análogamente, podemos definir una acción a derecha.*

Proposición 4.2. *Sea G un grupo actuando sobre un conjunto X con una aplicación $\varphi\colon G \times X \longrightarrow X$ tal que $\varphi(g,x) = g(x)$. Entonces:*

1. *Para cada $g \in G$, la aplicación*

$$\begin{array}{rccc} \varphi_g\colon & X & \longrightarrow & X \\ & x & \longmapsto & g(x) \end{array}$$

   es biyectiva.

2. *Existe un homomorfismo de grupos*

$$\begin{array}{rccc} \bar{\varphi}\colon & G & \longrightarrow & Biy(X) \\ & g & \longmapsto & \varphi_g \end{array}$$

Demostración: Demostremos cada parte:

1. Sea $g \in G$. Veamos primero que φ_g es inyectiva:

   Sean $x, y \in X$ tales que $\varphi_g(x) = \varphi_g(y)$. Entonces $g(x) = g(y)$, por lo que $g^{-1}(g(x)) = g^{-1}(g(y))$. Aplicando la primera condición de acción tenemos que $(g^{-1}g)(x) = (g^{-1}g)(y)$, y así $1_G(x) = 1_G(y)$ y por la segunda, $x = y$.

   Ahora, para demostrar la sobreyectividad, consideremos un elemento cualquiera $y \in X$. Entonces $g^{-1}(y) \in X$ y $\varphi_g(g^{-1}(y)) = y$. Así, φ_g es biyectiva.

2. Veamos que $\bar{\varphi}(gh) = \bar{\varphi}(g)\bar{\varphi}(h)$, para todo $g, h \in G$, es decir que $\varphi_{gh} = \varphi_g\varphi_h$. Sea $x \in X$. Entonces, aplicando las condiciones de acción sobre un conjunto:

$$\varphi_{gh}(x) = (gh)(x) = g(h(x)) = g\varphi_h(x) = \varphi_g(\varphi_h(x)) = \varphi_g\varphi_h(x).$$

□

Así que, finalmente podríamos simplemente definir la acción de un grupo G sobre un conjunto X como una aplicación ρ de un grupo G al grupo de permutaciones de X:

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & S_X \\ & g & \longmapsto & \varphi_g \end{array}$$

Con esto, podríamos decir que X es un ***G-conjunto***, y que φ_g es la permutación asociada al elemento $g \in G$. Así que, dado un un $x \in X$, $\varphi_g(x) = g(x)$ es su imagen, también en X y φ_g es la permutación. Y es a partir de aquí de dónde podríamos llegar a la aplicación que inicialmente hemos definido:

$$\begin{array}{rccc} \varphi\colon & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & g(x) \end{array}$$

asignando a cada par (g,x) un elemento de $g(x) \in X$ dado como antes.

Proposición 4.3. *Sea G un grupo y X un conjunto. Supongamos que existe un homomorfismo de grupos $\rho\colon G \longrightarrow S_X$. Entonces, el grupo G actúa sobre X, ya que podemos definir la acción*

$$\begin{array}{rccc} \varphi\colon & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & g(x) = (\rho(g))(x), \end{array}$$

donde $(\rho(g))(x)$ *es la imagen de* x *por la biyección* $\rho(g)$.

Por lo tanto, cuando hablemos de acción podremos referirnos indistintamente a ρ ó a φ. Aunque normalmente por convenio se utilizará ρ.

Ahora, consideremos ρ una acción (el homomorfismo representación $\bar{\varphi}$ de antes), entonces de acuerdo al *Primer Teorema de Isomorfía* tendremos que $G/Ker\rho$ es isomorfo a un subgrupo de S_X. Esto nos sugiere una pregunta interesante, ¿qué ocurriría si $Ker\,\rho = \{1_G\}$?, en ese caso tendríamos que G sería isomorfo a un subgrupo de S_X. Pasemos entonces a definir el ***núcleo de la acción***, $Ker\,\rho$:

$$Ker\,\rho = \{g \in G : g(x) = x\ \forall x \in X\}.$$

Es decir, todos los $g \in G$ cuya imagen sea la biyección identidad. Entonces la acción ρ (el homomorfismo representación) será inyectiva cuando $Ker\rho = \{1_G\}$, y se tendrá:

Definición 4.4. *Se dirá que la acción* ρ *de* G *sobre* X *es* ***fiel*** *si* $Ker\rho = \{1_G\}$. *En ese caso,* G *será isomorfo a un subgrupo de las biyecciones de* X, S_X.

Teorema 4.5 (***Teorema de Cayley***)**.** *Todo grupo* G *es isomorfo a un subgrupo de* S_G.

Demostración: Sea $X = G$ y consideremos la acción

$$\begin{array}{rccc} \varphi\colon & G \times G & \longrightarrow & G \\ & (g, x) & \longmapsto & g(x) = gx \end{array}$$

donde ahora gx es el producto de elementos g y x del grupo G. Desde luego es una acción, porque

$$(gh)(x) = ghx = g(h(x)),$$

$$1_G(x) = 1_G x = x.$$

También se podría representar como

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & S_G \\ & g & \longmapsto & \varphi_g(x) = gx \end{array}$$

Además, esta acción es fiel, pues para cada $g \neq 1_G$ tenemos que $g(1_G) = g1_G = g \neq 1_G$, y así $g \notin Ker\rho$ (= núcleo de la acción). Por lo tanto, G es isomorfo a un subgrupo de $S_X = S_G$.

□

A continuación definiremos una batería de conceptos importantes que serán esenciales para llegar a los principales resultados de la sección:

Definición 4.6. *Sea* $G \longrightarrow S_X$ *una acción de un grupo* G *sobre un conjunto* X, *y* $x \in X$. *Entonces, llamaremos* ***estabilizador*** *de* x *en* G *al conjunto*

$$G_x = \{g \in G : g(x) = x\}.$$

Además diremos que x *es un* ***punto fijo*** *de esta acción si* $G_x = G$.

Qué es el *estabilizador* con respecto a G y una propiedad fundamental del mismo nos lo dice el siguiente resultado:

Proposición 4.7. *Sea $G \longrightarrow S_X$ una acción de un grupo G sobre un conjunto X, y $x \in X$. Entonces:*

1. *G_x es un subgrupo de G.*
2. *Si $a \in G$, entonces $(G_x)^a = aG_xa^{-1} = G_{a(x)}$. Es decir, **el conjugado de un estabilizador es un estabilizador**.*

Demostración: Veamos:

1. Primero de todo, $1_G \in G_x$ por la segunda condición a cumplir de las acciones de grupos, así que G_x es no vacío. Ahora, sean $g, h \in G_x$. Está claro que $g(x) = x$, además

$$h^{-1}(x) = h^{-1}(h(x)) = (h^{-1}h)(x) = 1_G(x) = x.$$

   Por lo que

$$(gh^{-1})(x) = g(h^{-1}(x)) = g(x) = x,$$

   luego $gh^{-1} \in G_x$.

2. Sea $g \in G_x$. Como

$$(aga^{-1})(a(x)) = a(g1_G(x)) = a(g(x)) = a(x),$$

   tenemos que $aga^{-1} \in G_{a(x)}$, así que $(G_x)^a \subseteq G_{a(x)}$.

   Recíprocamente, si $g \in G_{a(x)}$, entonces $g(a(x)) = a(x)$, y así $(a^{-1}ga)(x) \in G_x$, luego $g \in (G_x)^a$.

□

Proposición 4.8. *Sea G un grupo actuando sobre un conjunto X con una acción ρ. Entonces*

$$Ker\rho = \bigcap_{x \in X} G_x.$$

Ejemplo 4.8.1. *Sean G un grupo y H un subgrupo de G. Llamamos $X = G/R^H$ y consideramos la acción de G sobre X definida por*

$$\begin{array}{ccc} G \times G/R^H & \longrightarrow & G/R^H \\ (g, xH) & \longmapsto & gxH. \end{array}$$

Es claro que se trata de una acción, puesto que dados $f, g \in G$:

$$(fg)(xH) = fgxH = f(gxH) = f(g(xH)).$$

y también

$$1_G(xH) = 1_GxH = xH.$$

Ahora calculemos los estabilizadores: dado un $xH \in G/R^H = X$, $g \in G_{xH}$ si y sólo si $g(xH) = xH$, esto es $gxH = xH$, es decir que $x^{-1}gx \in H$, luego $g \in H^{x^{-1}}$. Por lo que $G_{xH} = H^{x^{-1}}$. Por lo tanto, sabiendo esto, el núcleo de la acción será

$$Ker\rho = \bigcap_{xH \in G/R^H} H^{x^{-1}} = \bigcap_{x \in G} H^x = K(H),$$

con $K(H)$ el corazón de H que se introdujo en la definición 1.30. Notar que $K(H) \subseteq H$ es un subgrupo normal de G.

■

Ahora vamos a pasar con otro de los conceptos más importantes de la sección, fundamental para entender las acciones y los dos teoremas más importantes que veremos.

Cuando G actúa sobre un conjunto X define de forma natural una relación de equivalencia en X. Para cada $x, y \in X$ consideremos la siguiente relación binaria $\sim$:

$$x \sim y \iff \exists g \in G \text{ tal que } y = g(x).$$

Es simétrica: $g^{-1}(y) = g^{-1}(g(x)) = (g^{-1}g)(x) = x$, y como $g^{-1} \in G$ tenemos que si $x \sim y$ entonces $y \sim x$.

Es reflexiva: está claro que $x \sim x$ ya que $1 \cdot x = x$ y $1 \in G$.

Es transitiva: si $y = g(x)$ y $z = h(y)$ para algunos $g, h \in G$, entonces $z = h(y) = h(g(x)) = (hg)(x)$ y como $hg \in G$ entonces $x \sim z$.

Definición 4.9. *Cada clase de equivalencia de un elemento $x \in X$ de la relación de equivalencia anterior se llama **órbita** de x bajo la acción de G ó simplemente G-**órbita** de x, y se denota por O_x.*

$$O_x = \{g(x) : g \in G\} \subseteq X.$$

Como se tratan de clases de equivalencia, las órbitas forman una *partición* de X. Es decir, que su unión disjunta forma la totalidad de X. Así, si R es un conjunto de representantes de estas clases de equivalencia, se tiene que,

$$X = \bigsqcup_{x \in R} O_x.$$

Además, como la unión es disjunta, si X es finito, se tiene que

$$card\, X = \sum_{x \in R} card\, O_x.$$

Estas dos fórmulas equivalentes se conocen como ***fórmula de las órbitas***. Aunque O_x sea un conjunto y no un grupo, cuando hablemos del número de elementos ó **longitud** de la órbita escribiremos por convenio $|O_x|$.

Un tipo interesante de acciones serán las conocidas como *transitivas*.

Definición 4.10. *Sea $G \longrightarrow S_X$ una acción de un grupo G sobre un conjunto X. Diremos que la acción es* ***transitiva*** *si X es una G-órbita. Dicho de otra forma: si, dados $x, y \in X$, entonces existe un $g \in G$ tal que $g(x) = y$.*

Con todo esto nos preguntamos, sabiendo que el estabilizador de un elemento cualquiera de un conjunto sobre el que está actuando un grupo G es subgrupo de G, entonces ¿qué relación de equivalencia definirá el estabilizador como subgrupo de G?

Teorema 4.11 (***Teorema de la órbita estabilizadora***)**.** *Sea G un grupo actuando sobre un conjunto X, y $x \in X$. Entonces los conjuntos O_x y G/R^{G_x} son biyectivos. En particular, si G_x es un subgrupo de índice finito en G, la órbita O_x es un conjunto finito y tenemos*

$$|O_x| = [G : G_x].$$

En consecuencia, $|O_x|$ es un divisor de $|G|$.

Demostración: Consideremos la aplicación

$$\begin{array}{rccc} \psi\colon & G/R_{G_x} & \longrightarrow & O_x \\ & gG_x & \longmapsto & g(x). \end{array}$$

Veamos que está bien definida. Si $gG_x = hG_x$, se tiene que $g^{-1}h \in G_x$ luego $(g^{-1}h)(x) = x$, por lo que

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

Para la inyectividad, si $g(x) = h(x)$ se verifica que

$$(g^{-1}h)(x) = g^{-1}(h(x)) = g^{-1}(g(x)) = x,$$

por lo que $g^{-1}h \in G_x$ y así $gG_x = hG_x$. Además, la sobreyectivad es evidente y así se tiene la biyección.

□

Así, tenemos que

$$|O_x| = \frac{|G|}{|G_x|}.$$

Cuando un grupo G actúe sobre un conjunto X nos interesarán especialmente aquellos elementos de X que sean fijados por todos los elementos de G (el conjunto de los puntos fijos), es decir, aquellos $x \in X$ tales que $g(x) = x\ \forall g \in G$ ó, dicho de otra forma, aquellos $x \in X$ tales que $O_x = \{x\}$. Denotaremos por X_0 a:

$$X_0 = \{x \in X : |O_x| = 1\}.$$

Definición 4.12. *Sea un p primo. Diremos que un grupo G es un p-****grupo finito*** *si G es finito y su orden es una potencia de p, es decir,*

$$|G| = p^n,\ \ n \in \mathbb{N}.$$

Teorema 4.13. *Sea un grupo G actuando sobre un conjunto finito X. Escogemos $x_1, \ldots, x_s$ representantes de las órbitas de longitud mayor que 1. Entonces*

$$|X| = |X_0| + \sum_{j=1}^{s} |O_{x_j}|.$$

En particular, si G es un p-grupo finito, entonces

$$|X| \equiv |X_0| \ mod \ p.$$

Demostración: La primera parte es evidente a partir de la fórmula de las órbitas. Para el caso particular supongamos que $|G| = p^n$, con $n \in \mathbb{N}$. Por el teorema de la órbita estabilizadora se tiene que $|O_{x_j}| = [G : G_{x_j}] > 1$ para $j = 1, \ldots, s$. Como cada índice $[G : G_{x_j}]$ divide al orden de G, que es p^n, ya está.

□

Definición 4.14. *Consideremos la acción*

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & S_G \\ & g & \longmapsto & \alpha_g \end{array}$$

donde ya sabemos que $\alpha_g(x) = x^g = gxg^{-1}$ con $x \in G$. Notar que en este caso el conjunto sobre el que consideramos la acción es G, y que también la hemos presentado antes, al comienzo del capítulo concretamente, como la ***acción conjugación****.*

Como $\alpha_g \in Aut(G)$ tenemos que en particular es biyectiva. Además es claro que $\alpha_{gh} = \alpha_g \alpha_h$, luego φ es homomorfismo.

El núcleo de este homomorfismo, $Ker\, \varphi = \{g \in G : \alpha_g = id\} = \{g \in G : gxg^{-1} = x \ \forall x \in G\} = \{g \in G : gx = xg \ \forall x \in G\}$ ya lo conocemos, se presentó en el primer capítulo como ***centro de*** *G y se escribe $Z(G)$.*

El estabilizador, dado un $x \in G$, $G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$ también se presentó en el primer capítulo y lo denominamos ***centralizador de*** *x* ***en*** *G y se escribe como $C_G(x)$. Además, ya que $G_x \leq G$ entonces también $C_G(x) \leq G$ (algo que también sabíamos).*

Por último, si $x \in G$, su órbita O_x será entonces $O_x = \{gxg^{-1} : g \in G\}$. La denominaremos ***clase de conjugación de*** *x* ***en*** *G. Y, siguiendo el teorema de la órbita estabilizadora vemos que tiene $[G : C_G(x)] = \dfrac{|G|}{|C_G(x)|}$ elementos. En particular, la denotaremos por $Cl_G(x)$, es decir, tendremos:*

$$Cl_G(x) = \{gxg^{-1} : g \in G\}$$

Notar que cuando consideremos la acción de G sobre sí mismo por conjugación vamos a tener que, dado un $x \in G$ cualquiera, $|Cl_G(x)| = 1$ cuando, recordando lo visto anteriormente, ese elemento x sea fijado por todos los elementos de G al conjugarlo,

es decir, que va a cumplirse que $g(x) = x^g = gxg^{-1} = x$ para todo $g \in G$. Es decir, que $gx = xg \ \forall g \in G$. Pero el conjunto de estos elementos lo acabamos de ver, es el ***centro*** del grupo G, es decir, que $|Cl_G(x)| = 1 \Leftrightarrow x \in Z(G)$. Dicho de otra forma, en este caso se tiene que $X_0 = Z(G)$. Llegamos así a la conocida como *ecuación de clases*.

Teorema 4.15 (***Ecuación de las clases de conjugación de un grupo***)**.** *Sean G un grupo finito. Sean $K_1, \ldots, K_s$ las clases de conjugación de G de longitud mayor que 1. Entonces*

$$|G| = |Z(G)| + \sum_{j=1}^{s} |K_j|.$$

Esta fórmula recibe el nombre de ***ecuación de clases de conjugación de un grupo finito****.*

Demostración: Se sigue inmediatamente a partir de lo discutido anteriormente y del teorema 4.13. Notar que, por el teorema de la órbita estabilizadora, $|K_j| = |O_{x_j}| = [G : G_j] = [G : C_G(x_j)]$ para $j = 1, \ldots, s$, con los x_j representantes de las clases de conjugación (órbitas) de longitud mayor que 1. ($G = C_G(x) \Longleftrightarrow x \in Z(G)$, entonces $[G : C_G(x)] > 1$ si $x \notin Z(G)$.)

□

De la demostración se puede ver que esta fórmula también se puede escribir como:

$$|G| = |Z(G)| + \sum_{j=1}^{s} [G : C_G(x_j)].$$

Por último, dado un grupo G y el conjunto de sus subgrupos X, si tenemos en cuenta la siguiente acción:

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & S_X \\ & g & \longmapsto & \varphi_g(H) = H^g. \end{array}$$

podemos ver claramente que el estabilizador de un $H \leq G$ cualquiera, es decir, el conjunto

$$G_H = \{g \in G : \varphi_g(H) = H\} = \{g \in G : H^g = H\}$$

es un conjunto que ya conocemos, lo definimos en 1.9, es el ***normalizador*** de H en G, denotado por $N_G(H)$. Sabemos que $H \trianglelefteq N_G(H)$ y que $H \trianglelefteq G$ si y sólo si $N_G(H)$. Además, una consecuencia muy interesante sobre el normalizador es que, debido al teorema de la órbita estabilizadora, tenemos que **el número de subgrupos distintos de la forma H^g para cada $g \in G$ es** $[G : N_G(H)]$. Es decir, que el número de conjugados distintos de un subgrupo H de G viene dado por $[G : N_G(H)]$, algo que ya vimos en 1.27.

Proposición 4.16. *Sea G un grupo finito y $H \leq G$ un subgrupo de G tal que $|H| = p^m$, con p primo. Entonces,*

$$[G : H] \equiv [N_G(H) : H] \ mod \ p.$$

Demostración: Sea $X = \{xH : x \in G\}$. Tenemos que H actúa sobre X:

$$\begin{array}{rccc} \rho\colon & H & \longrightarrow & S_X \\ & h & \longmapsto & \varphi_h(xH) = hxH. \end{array}$$

Calculemos el conjunto de los puntos fijos. Tenemos que $hxH = xH$ para todo $h \in H$ si y sólo si $x^{-1}hx \in H$ para todo $h \in H$ si y sólo si $H^{x^{-1}} \subseteq H$ si y sólo si $H \subseteq H^x$ si y sólo si $H = H^x$ (ya que $|H| = |H^x|$) si y sólo si $x \in N_G(H)$. Es decir, que xH es punto fijo si y sólo si $x \in N_G(H)$. Luego $X_0 = [N_G(H) : H]$ y el resultado se tiene por la segunda parte de 4.13.

□

4.2. Teoremas de Sylow

Empezaremos con un resultado que es consecuencia de lo visto ahora y que básicamente nos dice que si tenemos un grupo de orden primo o múltiplo entonces contendrá un elemento de orden ese primo. Es el conocido como *Teorema de Cauchy*, que lo probaremos primero para grupos abelianos y más tarde generalizaremos a todos.

Teorema 4.17 (***Teorema de Cauchy para grupos abelianos.***)**.** *Sea G un grupo abeliano finito, y p un número primo que divide al orden de G. Entonces existirá $x \in G$ tal que $o(x) = p$.*

Demostración: Lo haremos por inducción sobre $|G|$. Sea H un subgrupo propio de G de orden lo mayor posible. Si $p \mid |H|$, por hipótesis de inducción existirá un $x \in H \subset G$ tal que $o(x) = p$. Por lo tanto podemos suponer que $p \nmid |H|$. Como $p \mid |G| = |G/H||H|$ por el *Teorema de Lagrange* (además podemos hacer el cociente porque al ser G abeliano todo subgrupo es normal), y esto quiere decir que $p \mid |G/H|$. Además, como H es de orden lo mayor posible entre los subgrupos de G, por el *Teorema de la correspondencia* G/H no tiene subgrupos propios no triviales y por tanto es simple.

Así, ahora partimos de que G/H es simple y abeliano y que $p \mid |G/H|$. Como los grupos simples abelianos son cíclicos de orden primo tenemos que

$$G/H \simeq C_p.$$

Sea $H \neq xH \in G/H$. Entonces es claro que $o(xH) = p$. Tenemos un elemento de orden p dentro del cociente y queremos encontrar un elemento de orden p dentro del grupo. Para ello construiremos el homomorfismo sobreyectivo que ya conocemos

$$\begin{array}{rccc} \pi\colon & G & \longrightarrow & G/H \\ & x & \longmapsto & xH \end{array}$$

y de las propiedades de los homomorfismos sabemos que $p = o(xH) = o(\pi(x)) \mid o(x)$. Esto quiere decir que $p \mid o(x)$ y así $x^{o(x)/p} \in G$ de orden p, ese es el elemento que buscábamos.

□

Ahora, el resultado general:

Teorema 4.18 (***Teorema de Cauchy.***). *Sea G un grupo finito y p un número primo que divide al orden de G. Entonces existirá un $x \in G$ tal que $o(x) = p$.*

Demostración: Por inducción nuevamente sobre $|G|$. Si existe un subgrupo propio H de G tal que $p \mid |H|$ ya hemos terminado, puesto que existirá un $x \in H \subset G$ tal que $o(x) = p$. Así, podemos suponer que $p \nmid |H|$ para todo H subgrupo propio de G. Ahora, de la ecuación de clases:

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)]$$

sabemos que como $1 < [G : C_G(x_i)]$ entonces $p \nmid |C_G(x_i)|$ $\forall i$, pero a la vez también $p \mid |G|$, esto quiere decir que $p \mid [G : C_G(x_i)]$ $\forall i$.

Como $p \mid |G|$ y $p \mid [G : C_G(x_i)]$ entonces necesariamente $p \mid |Z(G)|$, pero como p no divide al cardinal de ningún subgrupo propio tenemos que $Z(G) = G$ y así G es abeliano. Por el resultado para grupos abelianos tenemos éste.

□

Pasemos ya con las definiciones que emplearemos y con las que trabajaremos a partir de ahora:

Definición 4.19. *Sea G un grupo finito, y p un número primo que divide al orden de G. Por tanto $|G| = p^n m$, con m y n enteros positivos tales que p no divide a m, es decir, $mcd(p, m) = 1$. Notar que $n = 0$. Sea H subgrupo de G. Entonces:*

1. *Diremos que H es un p-**subgrupo** de G si el orden de H es potencia de p, es decir, $|H| = p^r$ con $r \geq 0$.*
2. *Diremos que H es un p-**subgrupo de Sylow** de G si H es un p-subgrupo de G y $[G : H]$ no es múltiplo de p, es decir, $|H| = p^n$ (la máxima potencia de p que divide al orden de G). Al conjunto de todos los p-subgrupos de Sylow de G los denotaremos por*

$$Syl_p(G) = \{H \leq G : |H| = p^n\}.$$

El objetivo fundamental de esta sección es demostrar que los subgrupos de Sylow siempre existen ($Syl_p(G) \neq \{\emptyset\}$, $\forall p$) y que son conjugados entre sí.

Teorema 4.20 (***Primer Teorema de Sylow***). *Sea G es un grupo finito y p un número primo, entonces G tiene un p-subgrupo de Sylow.*

Demostración: Lo haremos por inducción sobre el orden de G. Si $|G| = 1$, entonces es evidente. Supongamos ahora que todos los grupos de orden menor que $|G|$ tienen p-subgrupos de Sylow y veamos que G también los tiene. Si $p \nmid |G|$ entonces el subgrupo trivial es un p-subgrupo de Sylow de G. Por lo que supongamos que $p \mid |G|$, así $|G| = p^n m$ con p no dividiendo a m ($mcd(p, m) = 1$). Entonces, podemos distinguir dos casos:

Primero, que exista un subgrupo $H \leq G$ tal que $p \nmid [G : H]$. Entonces es claro que $p^n \mid |H|$ y por hipótesis de inducción se tiene que H tiene un p-subgrupo de Sylow de orden p^n, que llamaremos P y que también será p-subgrupo de Sylow de G .

Segundo, que para todo subgrupo H de G, $p \mid [G : H]$. Entonces, por la ecuación de clases tenemos que $p \mid |Z(G)|$, y como éste es un grupo abeliano entonces tiene un elemento de orden p, ó equivalentemente tiene un subgrupo $H \leq Z(G)$ de orden p. Como todos los elementos de H conmutan con todos los elementos de G entonces es claro que $H^g = H$ para todo $g \in G$, es decir, $H \trianglelefteq G$. Se cumple que $[G : H] = p^{n-1}m$ y tiene un subgrupo de Sylow P/H que cumplirá $[P : H] = p^{n-1}$, por lo que $|P| = p^n$ y así P es un p-subgrupo de Sylow de G.

□

Teorema 4.21 (***Segundo Teorema de Sylow***)**.** *Si G es un grupo finito, entonces todo p-subgrupo de G está contenido en un p-subgrupo de Sylow y dos p-subgrupos de Sylow cualesquiera son conjugados.*

Demostración: Sea P un p-subgrupo de Sylow de G y sea H un p-subgrupo arbitrario. Entonces H actúa sobre $X = G/R^P$ por multiplicación a izquierda como vimos en 4.8.1. Por el teorema de la órbita estabilizadora tenemos que las órbitas de Ω tienen cardinal potencia de p (incluyendo $p^0 = 1$). De hecho, alguna órbita ha de tener cardinal 1, pues de lo contrario el cardinal de Ω, que es $[G : P]$, sería suma de potencias (no triviales) de p, así sería múltiplo de p.

Por lo tanto, existirá un $g \in G$ tal que la clase de conjugación $x = gP$ formará una órbita trivial, con x como único elemento. Concretamente $hgP = gP$ para todo $h \in H$. En particular $hg \in gP$ y así $h \in P^g$ para todo $h \in H$. De aquí $H \leq P^g$ y así P^g es también p-subgrupo de Sylow.

En caso de que H sea un p-subgrupo de Sylow de G, entonces ha de darse la igualdad $H = P^g$, puesto que tenemos una inclusión y ambos tienen el mismo orden.

□

Por lo tanto, queda claro que los p-subgrupos de Sylow forman una órbita en la acción de G sobre el conjunto de todos sus subgrupos por conjugación. Luego, si P es un p-subgrupo de Sylow entonces el número total es $[G : N_G(P)]$. Éste número es un divisor del orden de G y también de $[G : P]$.

Corolario 4.21.1. *Sean p un número primo y G un grupo finito cuyo orden es $|G| = p^n m$ donde m y n son enteros positivos y p no divide a m. Sea H un p-subgrupo de Sylow de G. Entonces H es subgrupo normal si y sólo si es el único p-subgrupo de Sylow de G.*

Demostración: Los p-subgrupos de Sylow de G son, por el *Segundo Teorema de Sylow*, los subgrupos de G conjugados de H, y coinciden todos con H si y sólo si éste es normal. Es, por tanto, consecuencia inmediata de la definición de subgrupo normal y del *Segundo Teorema de Sylow*.

□

Finalmente veremos el último de los teoremas de Sylow:

Teorema 4.22 (***Tercer Teorema de Sylow***)**.** *El número v_p de p-subgrupos de Sylow de un grupo finito cumple que $v_p \equiv 1$ mod p.*

Demostración: Sea G un grupo finito y Ω el conjunto de sus p-subgrupos de Sylow. Sea un $P \in \Omega$ y consideremos la acción de P en Ω por conjugación. Es claro que $P^g = P$ para todo $g \in P$, luego la órbita de P es trivial. Veamos que es única. Dado otro $Q \in \Omega$, entonces se tiene que $Q^g = Q$ para todo $g \in P$, entonces $P \leq N_G(Q)$ y así P y Q son p-subgrupos de Sylow de $N_G(Q)$, luego son conjugados en $N_G(Q)$. Así, existe un $g \in N_G(Q)$ tal que $P = Q^g = Q$.

Las órbitas que P forma en Ω tienen cardinal potencia de p, y se ha visto que la única que tiene cardinal 1 es la de P, luego $v_p = |\Omega| \equiv 1 \bmod p$.

□

La última de las consecuencias es equivalente a decir que $[G : N_G(P)] \equiv 1$ *mod* p, con P un p-subgrupo de Sylow de G.

5. Grupos de permutaciones

A lo largo de este capítulo estudiaremos los conocidos como grupos simétricos o *permutaciones*. El objetivo principal será el de ver nuevamente el *Teorema de Cayley*, que ya vimos en la sección anterior de acciones de grupos, así como conceptos básicos como el de ciclo, transposición o soporte. También se verá otro importante resultado como es el *Teorema de Abel*, además de especificar qué es exactamente el *n-ésimo grupo alternado*.

5.1. Introducción y Teorema de Cayley

Definición 5.1. *Denotaremos, para cada entero $n > 0$, $E_n = \{1, \ldots, n\}$ y S_n como el conjunto de aplicaciones biyectivas del conjunto E_n en sí mismo, cuyo cardinal es $n!$. Ésto ya lo vimos en* **??**.

Además, la composición de biyecciones es de nuevo una biyección, así que podemos hablar de S_n como grupo. Dadas $\sigma, \tau \in S_n$ definiremos

$$\begin{array}{rccc} \sigma\tau\colon & E_n & \longrightarrow & E_n \\ & j & \longmapsto & \tau(\sigma(j)). \end{array}$$

Es evidente que el elemento neutro de este grupo es la aplicación identidad, que denotaremos por id, y el inverso de una biyección σ es la biyección σ^{-1} definida como $\sigma^{-1}(i) = j$ si y sólo si $\sigma(j) = i$. Así, llamaremos a S_n ***grupo de permutaciones de n elementos*** *ó* ***n-ésimo grupo simétrico****.*

Denotaremos a cada $\sigma \in S_n$ de la siguiente forma:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Notar que ya hemos empleado esta notación al escribir las acciones de un grupo G sobre un conjunto X cualquiera como una aplicación de G sobre S_X, hablábamos de permutaciones de X como las aplicaciones biyectivas de X en sí mismo. Es de hecho esta notación la que utilizaremos. Para ello, en vez de hablar de E_n como conjunto finito simplemente generalizaremos y denotaremos por Ω a un conjunto finito cualquiera (utilizado más frecuentemente que X cuando estamos hablando de permutaciones) de n elementos, o dicho de otra forma: que pueda ponerse en una biyección con E_n. Y denotaremos por S_n ó S_Ω a su grupo de permmutaciones.

Es decir, partiremos de un conjunto finito Ω cualquiera de orden n, y definiremos su grupo de permutaciones S_n. $Card\,\Omega = |\Omega| = n$ y $|S_n| = n!$.

Observación 5.1.1. *Veamos algunas observaciones interesantes:*

1. *Dados enteros $2 \leq n \leq m$, podemos ver a S_n como subgrupo de S_m. En efecto, para todo $\sigma \in S_n$ denotamos por $\sigma' \in S_m$ la biyección de E_m en sí mismo que actúa como σ sobre los primeros n enteros positivos y fija los comprendidos entre $n+1$ y m. Es decir, la aplicación*

$$\begin{array}{ccc} S_n & \longrightarrow & S_m \\ \sigma & \longmapsto & \sigma' \end{array}$$

   es un homomorfismo inyectivo de grupos y, por el Primer Teorema de Isomorfía, S_n es isomorfo a su imagen, que es un subgrupo de S_m.

2. *De todo lo visto hasta ahora, lo realmente importante no es la naturaleza del conjunto Ω como tal, sino el hecho de que tenga n elementos. Así, si I_n es otro conjunto con n elementos, el grupo $Biy(I_n)$ de biyecciones de I_n en sí mismo es isomorfo a S_n, y no distinguiremos entre ambos. Para verlo, fijada una biyección cualquiera $\alpha\colon \Omega \longrightarrow I_n$ se comprueba inmediatamente que la aplicación*

$$\begin{array}{ccc} Biy(I_n) & \longrightarrow & S_n \\ \beta & \longmapsto & \alpha \circ \beta \circ \alpha^{-1} \end{array}$$

   es un isomorfismo de grupos. Es por esta razón por la que hemos introducido la notación de Ω simplemente para hablar de un conjunto finito de n elementos cualquiera.

De lo primero se desprende que, dado $H = \{\sigma \in S_n : \sigma(n) = n\} \leq S_n$ el estabilizador de n en S_n en su acción sobre Ω, si $\sigma \in H$ y definimos $\bar{\sigma} \in S_{n-1}$ como $\bar{\sigma}(i) = \sigma(i)$ para $i = 1, \ldots, n-1$, entonces la aplicación

$$\begin{array}{ccc} H & \longrightarrow & S_{n-1} \\ \sigma & \longmapsto & \bar{\sigma} \end{array}$$

es un isomorfismo de grupos.

Teorema 5.2 (***Teorema de Cayley***)**.** *Todo grupo G es isomorfo a un subgrupo del grupo $Biy(G)$ (S_G). En particular todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.*

Demostración: La segunda parte es consecuencia inmediata de la primera. Para ésta, denotemos

$$\begin{array}{rccc} \bar{g}\colon & G & \longrightarrow & G \\ & h & \longmapsto & hg \end{array}$$

para cada $g \in G$. Esta aplicación es inyectiva pues si $\bar{g}(x) = \bar{g}(y)$ entonces $xg = yg$ y, simplificando, $x = y$. De hecho $\bar{g}$ es biyectiva pues para cada $y \in G$ se cumple la igualdad $\bar{g}(yg^{-1}) = y$.

Ahora, la aplicación

$$\begin{array}{rccc} \phi\colon & G & \longrightarrow & S_G \\ & g & \longmapsto & \bar{g} \end{array}$$

es un homomorfismo inyectivo, por lo que G es isomorfo a su imagen, que es un subgrupo de S_G, quien a su vez es isomorfo al grupo simétrico S_n. Para comprobar que ϕ es homomorfismo, hemos de comprobar la igualdad $\overline{g_1g_2} = \bar{g_1}\bar{g_2}$. Ahora bien, para todo $x \in G$,

$$(\bar{g_1} \cdot \bar{g_2})(x) = \bar{g_2}(\bar{g_1}(x)) = \bar{g_2}(xg_1) = (xg_1)g_2 = x(g_1g_2) = \overline{g_1g_2}(x),$$

por lo que $\overline{g_1g_2} = \bar{g_1}\bar{g_2}$. En cuanto a la inyectividad, basta ver que si $g \in Ker\,\phi$, entonces $\bar{g} = id_G$, o sea, $xg = x$ para cada $x \in G$, luego $g = 1_G$.

□

Lo que acabamos de ver nos establece un isomorfismo entre todo grupo finito de orden n y un subgrupo de S_n. Es decir, este resultado nos dice que todo grupo de orden n es subgrupo de un grupo de permutaciones de orden $n!$.

Definición 5.3. *Sean n y k enteros positivos, $k \leq n$. Un elemento $\sigma \in S_n$ se llama* ***ciclo de longitud*** *k o k-**ciclo** si existe un subconjunto con k elementos $\{a_1, \ldots, a_k\}$ de Ω tal que*

$$\sigma(a_i) = a_{i+1}, \;\; 1 \leq i \leq k-1;$$
$$\sigma(a_k) = a_1;$$
$$\sigma(j) = j, \;\; j \in \Omega \setminus \{a_1, \ldots, a_k\}.$$

Lo denotaremos $\sigma = (a_1, a_2, \ldots, a_k)$ en vez de

$$\begin{pmatrix} a_1 \ldots & a_{k-1} & a_k \ldots & j \\ a_2 \ldots & a_k & a_1 \ldots & j \end{pmatrix}.$$

Además, al conjunto $\{a_1, \ldots, a_k\}$ lo llamaremos ***soporte*** *del ciclo $\sigma = (a_1, \ldots, a_k)$ y lo denotaremos $sop(\sigma)$.*

Observación 5.3.1. *Es importante aclarar los siguientes puntos:*

1. *La forma de escribir un ciclo de longitud k no es única; por ejemplo*

$$(a_1, \ldots, a_k) = (a_k, a_1, \ldots, a_{k-1}).$$

Es evidente que existen k formas de escribir el mismo ciclo de longitud k (tantas como maneras de elegir el primer elemento). Así, el ciclo $\sigma = (1,3,4) \in S_4$ se escribe

$$\sigma = (1,3,4) = (4,1,3) = (3,4,1).$$

Sin embargo, $\sigma = (1,3,4) \neq (1,4,3) = \tau$ aunque ambos tengan el mismo soporte $\{1,3,4\}$, puesto que

$$\sigma(1) = 3 \neq 4 = \tau(1).$$

2. *Dados enteros positivos $a_1, \ldots, a_k$ puede resultar confuso hablar del ciclo $\sigma = (a_1, \ldots, a_k)$ si no se indica el grupo simétrico S_n al que pertenece σ. Por ejemplo*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \in S_4, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$$

son distintas, aunque ambas se escriben

$$\sigma = (1,3,4), \ \ \tau = (1,3,4).$$

3. *Si $\sigma \in S_n$ es un ciclo de longitud uno, existirá $a_1 \in \Omega$ tal que $\sigma(j) = j$ para cada $j \in \Omega \setminus \{a_1\}$. Entonces, como σ es biyectiva ha de ser $\sigma(a_1) = a_1$ y σ es la identidad. Así que de ahora en adelante sólo consideraremos ciclos de longitud mayor o igual que dos.*
4. *A los ciclos de longitud dos los llamaremos **transposiciones**.*
5. *Diremos que los ciclos $\sigma, \tau \in S_n$ son disjuntos si uno de ellos es la identidad, ó que se dé la condición $sop(\sigma) \cap sop(\tau) = \emptyset$.*

Una cuestión de notación y denominación será la que sigue: si por ejemplo consideramos el σ anterior entonces tendremos que $\sigma(3) = 4$ y diremos que *sigma* ***mueve*** 3, y en general diremos que una permutación $\sigma \in S_n$ mueve $a_i \in \Omega$ si $\sigma(a_i) = a_j$ con $i \neq j \in sop(\sigma)$. En cambio, $\sigma(2) = 2$ y diremos que σ ***fija*** 2, y en general diremos que una permutación $\sigma \in S_n$ fija $a_i \in \Omega$ si $\sigma(a_i) = a_i$.

A lo largo del capítulo utilizaremos las acciones de grupos sobre conjuntos para estudiar y probar siguientes resultados. Es de hecho una de las razones por las que se dan ahora las permutaciones. Así, el grupo S_n va a actuar sobre el conjunto Ω mediante una acción $\varphi_g(\alpha) = g(\alpha)$, dado un $g \in S_n$ y $\alpha \in \Omega$. En concreto, será muy útil usar la acción por conjugación vista en 4.14.

El siguiente resultado fija algunas propiedades elementales de los ciclos.

Proposición 5.4. *Sea $\sigma = (a_1, \ldots, a_k) \in S_n$ un ciclo de longitud $k \geq 2$.*

1. *$\sigma^{-1} = (a_k, a_{k-1}, \ldots, a_1)$. En particular σ^{-1} es un ciclo de longitud k.*
2. *El orden de σ como elemento de S_n es k.*
3. *Si $\tau = (b_1, \ldots, b_l) \in S_n$ es un ciclo de longitud l, y σ y τ son disjuntos, entonces $\sigma \circ \tau = \tau \circ \sigma$.*

Demostración: Veamos:

1. Es evidente haciendo la composición.

2. Para cada $1 \leq i < k$, $\sigma^i(a_1) = a_{1+i} \neq a_1$, luego σ^i no es la identidad y así $o(\sigma) \geq k$. Entonces tenemos que ver que $\sigma^k(j) = j$ para cada $j \in \Omega$. Pero esto es obvio si $j \notin sop(\sigma)$, pues en tal caso $\sigma(j) = j$. Ahora, dado $1 \leq i \leq k$, $\sigma^{k-i+1}(a_i) = a_1$, y por lo tanto, $\sigma^k(a_i) = \sigma^{i-1}(a_1) = a_{1+i-1} = a_i$.

3. Si τ es la identidad es obvio que $\sigma \circ \tau = \tau \circ \sigma$. Supongamos que $l \geq 2$, $sop(\sigma) \cap sop(\tau) = \emptyset$. Escribimos $M = sop(\sigma) \cup sop(\tau)$. Si $j \in \Omega \setminus M$ se cumple $\sigma(j) = j = \tau(j)$, luego
$$\sigma \circ \tau(j) = j = \tau \circ \sigma(j).$$
Por otra parte, si $j \in M$, entonces $j \in sop(\sigma)$, $j \notin sop(\tau)$, ó $j \in sop(\tau)$, $j \notin sop(\sigma)$. En el primer caso, como $j \in sop(\sigma)$, también $\sigma(j) \in sop(\sigma)$ y así $\sigma(j) \notin sop(\tau)$, con lo que
$$\tau(j) = j, \;\; \tau(\sigma(j)) = \sigma(j).$$
Así, $\sigma \circ \tau(j) = \sigma(j) = \tau \circ \sigma(j)$. Para el segundo caso, el razonamiento es análogo.

□

Lema 5.4.1. *Sea un producto de ciclos disjuntos dos a dos*
$$\sigma = (a_1, \ldots, a_m) \cdots (b_1, \ldots, b_n),$$
y sea $G = \langle \sigma \rangle \leq S_n$. *Entonces* $\sigma^i(a_1) = a_{i+1}$ *para* $1 \leq i \leq m-1$, $\sigma^m(a_1) = a_1, \ldots, \sigma^j(b_1) = b_{j+1}$ *para* $1 \leq j \leq n-1$ *y* $\sigma^n(b_1) = b_1$. *Como consecuencia, los conjuntos* $\{a_1, \ldots, a_m\}, \ldots, \{b_1, \ldots, b_n\}$ *son órbitas de la acción de* G *sobre* Ω *y las demás órbitas tienen longitud uno. Es decir, los soportes son las órbitas.*

Demostración: La primera parte es consecuencia directa de lo visto en la proposición anterior claramente. Tenemos que $\{a_1, \ldots, a_m\} = \{\sigma^r(a_1) : r \geq 0\}, \ldots, \{b_1, \ldots, b_n\} = \{\sigma^r(b_1) : r \geq 0\}$.

□

Los ciclos de S_n tienen interés, entre otras razones, porque constituyen un sistema generador de S_n tal y como veremos a continuación.

Proposición 5.5. *Sea* n *un entero positivo. Entonces cada elemento de* S_n *se puede escribir como composición de ciclos disjuntos dos a dos. Dicha descomposición es además única salvo en el orden de los factores. En particular, los ciclos de* S_n *constituyen un sistema generador de* S_n.

Demostración: Sea $\sigma \in S_n$ y $G = \langle \sigma \rangle$. Supongamos O una G-órbita. Si $|O| = m$ y $a \in O$ vamos a probar que $O = \{a, \sigma(a), \ldots, \sigma^{m-1}(a)\}$. Por el 4.11 *Teorema de la órbita estabilizadora* tenemos que $[G : G_a] = m$. Así, G/G_a es un grupo cíclico de orden m generado por σG_a. Luego, para cualquier entero n tenemos que $\sigma^n(a) = a$ si y sólo si $\sigma^n \in G_a$ si y sólo si $(\sigma G_a)^n = G_a$ si y sólo si $m \mid n$. Esto quiere decir que

los elementos $a, \sigma(a), \ldots, \sigma^{m-1}(a)$ de la G-órbita de a son distintos y que no puede haber más.

Supongamos ahora que $\{a, \sigma(a), \ldots, \sigma^{m-1}(a)\}, \ldots, \{b, \sigma(b), \ldots, \sigma^{n-1}(b)\}$ son todas las distintas G-órbitas. Entonces tenemos que

$$\sigma = (a, \sigma(a), \ldots, \sigma^{m-1}(a)) \cdots (b, \sigma(b), \ldots, \sigma^{n-1}(b)),$$

puesto que la aplicación de la derecha actúa sobre cada elemento de Ω de la misma forma que σ.

Por último, si $\sigma = (a_1, \ldots, a_m) \cdots (b_1, \ldots, b_n)$ se escribe como producto de ciclos disjuntos, entonces por el lema inmediatamente anterior tenemos que σ determina unívocamente los ciclos $(a_1, \ldots, a_m), \ldots, (b_1, \ldots, b_n)$, quedando así probada la unicidad.

□

Ahora, veamos un ejemplo donde se pueda apreciar lo que acabamos de probar:

Ejemplo 5.5.1. *Consideremos $\sigma \in S_9$ dado por*

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 5 & 9 & 1 & 2 & 8 & 7 & 4 \end{pmatrix}$$

Entonces es claro que la órbita de 1 bajo la acción anterior es

$$O_1 = \{1, \sigma(1) = 3, \sigma^2(1) = 5\}$$

y análogamente

$$O_2 = \{2, 6\}, \;\; O_4 = \{4, 9\}, \;\; O_7 = \{7, 8\}.$$

Así, los ciclos disjuntos

$$\tau_1 = (1, 3, 5), \;\; \tau_2 = (2, 6), \;\; \tau_3 = (4, 9), \;\; \tau_4 = (7, 8)$$

cumplen $\sigma = \tau_1 \circ \tau_2 \circ \tau_3 \circ \tau_4$.

■

Como una consecuencia de esta descomposición en ciclos disjuntos vamos a ver que cualquier k-ciclo se puede expresar como producto de los ciclos más simples que existen: las transposiciones.

Corolario 5.5.1. *Todo k-ciclo es producto de $k-1$ transposiciones. Luego, toda permutación $g \in S_n$ es producto de transposiciones (aunque no de forma única).*

Demostración: Hacemos $g = (a_1, \ldots, a_m) = (a_1, a_2)(a_2, a_3) \cdots (a_{k-1}, a_k)$.

□

Corolario 5.5.2. *Sean $\sigma \in S_n$ y $\tau_1, \ldots, \tau_k \in S_n$ ciclos disjuntos tales que $\sigma = \tau_1 \circ \ldots \circ \tau_k$. Entonces el orden de σ como elemento de S_n es el mínimo común múltiplo de las longitudes de los ciclos $\tau_1, \ldots, \tau_k$.*

Demostración: Llamemos l_j, $1 \leq j \leq k$ a la longitud del ciclo τ_j. Por 5.4, $l_j = o(\tau_j)$. Hacemos la demostración por inducción sobre k. El resultado es trivial si $k = 1$. Si $k > 1$, escribimos $\tau = \tau_1 \circ \ldots \tau_{k-1}$. Por hipótesis de inducción $o(\tau) = l = mcm(l_1, \ldots, l_{k-1})$. Sea $m = mcm(l, l_k)$. Así $\tau_k^m = \tau^m = 1$ y por 3. de 5.4, $\sigma^m = (\tau \circ \tau_k)^m = \tau^m \circ \tau_k^m = 1$.

Recíprocamente, sea s un entero positivo tal que $\sigma^s = 1$. Entonces $\tau^s \circ \tau_k^s = 1$ y por ello $j = (\tau^s \circ \tau_k^s)(j) = \tau^s(j)$ si $j \in sop(\tau)$ pues $sop(\tau) \cap sop(\tau_k^s) = \emptyset$, $j = \tau^s(j)$ si $j \notin sop(\tau)$. Esto demuestra que $\tau^s = 1$ y análogamente $\tau_k^s = 1$. En consecuencia s es múltiplo de $l_k = o(\tau_k)$ y de $l = o(\tau)$, es decir, s es múltiplo de m.

Queda probado así que $o(\sigma) = m = mcm(l, l_k) = mcm(l_1, \ldots, l_k)$.

□

Lema 5.5.1. *Supongamos que $\sigma = (a_1, \ldots, a_m)$ es un m-ciclo de S_n y sea $\tau \in S_n$. Entonces $\sigma^\tau = (\tau(a_1), \ldots, \tau(a_m))$.*

Demostración: Tenemos que $\sigma(a_i) = a_{i+1}$ para $i = 1, \ldots, m-1$ y $\sigma(a_m) = a_1$. Luego, $(\tau\sigma\tau^{-1}) \cdot (\tau(a_i)) = \tau(a_{i+1})$ para $i = 1, \ldots, m-1$ y $(\tau\sigma\tau^{-1}) \cdot (\tau(a_m)) = \tau(a_1)$.

Finalmente, si $w \in \Omega \setminus \{\tau(a_1), \ldots, \tau(a_m)\}$, entonces $\tau^{-1}(w) \in \Omega \setminus \{a_1, \ldots, a_m\}$. Por lo que $\sigma(\tau^{-1}(w)) = \tau^{-1}(w)$ y así σ^τ fija w. Así que tenemos que tanto σ^τ como $(\tau(a_1), \ldots, \tau(a_m))$ actúan igual sobre cada elemento de Ω, y por tanto han de ser iguales.

□

Una consecuencia muy útil de 5.5 es que vamos a poder clasificar cada permutación según la longitud de los ciclos disjuntos en los que se descomponga, lo cual nos permitirá estudiarlos con mayor profundidad a través de dichas longitudes. Llamaremos así al ***tipo de una permutación*** a la sucesión en orden descendente de las longitudes de los ciclos disjuntos en los que se descompone.

Por ejemplo, en el ejemplo 5.5.1 teníamos una permutación $\sigma \in S_9$ cuyo tipo es $[3, 2, 2, 2]$ porque se descompone en 4 ciclos disjuntos, de longitud 3, 2, 2 y 2 respectivamente. Se suele usar la notación () para denotar tipos, pero para no confundir con la permutación como tal emplearemos los corchetes. Notar que hay tantos tipos distintos como particiones tenga $n = |\Omega|$.

Una de las razones por las que se introduce este concepto es porque vamos a poder elegir una permutación cualquiera de cada tipo y usarla como representante de una clase de conjugación en el S_n que nos encontremos, es decir:

Proposición 5.6. *Dos permutaciones $\sigma, \tau \in S_n$ son conjugadas en S_n si y sólo si tienen el mismo tipo.*

Demostración: Si $\tau = (a_1, \ldots, a_m) \cdots (b_1, \ldots, b_n)$ es una descomposición de τ en ciclos disjuntos y $\gamma \in S_n$, por el lema anterior tenemos que

$$\tau^\gamma = (\gamma(a_1), \ldots, \gamma(a_m)) \cdots (\gamma(b_1), \ldots, \gamma(b_n))$$

es una descomposición en ciclos disjuntos de τ^γ. Por lo que dos permutaciones conjugadas tienen el mismo tipo.

Recíprocamente, supongamos que $\tau = (a_1, \ldots, a_m) \cdots (b_1, \ldots, b_n)$ y también $\gamma = (a'_1, \ldots, a'_m) \cdots (b'_1, \ldots, b'_n)$ tienen el mismo tipo, veamos que son conjugadas. Tenemos que

$$\Omega = \{a_1, \ldots, a_m\} \cup \cdots \cup \{b_1, \ldots, b_n\} = \{a'_1, \ldots, a'_m\} \cup \cdots \cup \{b'_1, \ldots, b'_n\}$$

son dos particiones de Ω. Por lo que existe una única $\sigma \in S_n$ tal que $\sigma(a_i) = \sigma(a'_i), \ldots, \sigma(b_j) = \sigma(b'_j)$ para $1 \leq i \leq m, \ldots, 1 \leq j \leq n$. Luego, por el lema anterior tenemos que $\tau^\sigma = \gamma$.

□

De este resultado tenemos una importante consecuencia, y es que dado un $\sigma \in S_n$, entonces ***la clase de conjugación de*** σ (ver 4.14) ***está formada por todas las permutaciones del mismo tipo que*** σ.

Observación 5.6.1. *Sea $k > 1$, entonces el número de k-ciclos que muevenn k elementos distintos $a_1, \ldots, a_k \in \Omega$ es $(k-1)!$. Si $|\Omega| = n$, el número de k-ciclos de S_n es $\binom{n}{k}(k-1)!$.*

Esto se puede generalizar a permutaciones de determinados tipos: es decir, si queremos saber el número de permutaciones de S_n con b_j ciclos de longitud j tendremos

$$\frac{n!}{1^{b_1} 2^{b_2} \cdots n^{b_n} b_1! b_2! \cdots b_n!}.$$

(odio la combinatoria)

Ejemplo 5.6.1. *Veamos las distintas clases de conjugación en S_5. Sabemos que hay 10 2-ciclos, 20 3-ciclos, 30 4-ciclos y 24 5-ciclos. Ciclos de tipo $[2,2]$ tenemos 15 ciclos. Ciclos de tipo $[3,2]$ tenemos 20 ciclos, y añadiendo la identidad tenemos:* $10 + 20 + 30 + 24 + 15 + 20 + 1 = 120$.

■

Ejemplo 5.6.2. *Sea $G = S_5$.*

1. *Sea $\tau = (1,2,3)$. Sabemos que $|Cl_G(\tau)| = 20$. Entonces $C_G(\tau) = \langle\tau\rangle\langle(4,5)\rangle$.*

   Por un lado, como $|Cl_G(\tau)| = 20$, entonces $|C_G(\tau)| = \dfrac{|G|}{20} = \dfrac{120}{20} = 6$.

   Por otro lado,

   $$\langle(1,2,3)\rangle = \{id, (1,2,3), (1,3,2)\},$$

   y

   $$\langle(4,5)\rangle = \{id, (4,5)\}$$

   (simple comprobación). Notar que $\langle(1,2,3)\rangle \cap \langle(4,5)\rangle = id$ y así $|\langle(1,2,3)\rangle\langle(4,5)\rangle| = \dfrac{|\langle(1,2,3)\rangle||\langle(4,5)\rangle|}{1} = 3 \cdot 2 = 6$. Como $(4,5)$ es disjunta con $(1,2,3)$, entonces conmutan y así $\langle(4,5)\rangle \leq C_G(\tau)$, y también $\langle(1,2,3)\rangle\langle(4,5)\rangle \leq C_G(\tau)$ y como tienen el mismo orden se da la igualdad.

2. *Sea γ un 5-ciclo de G. Entonces $C_G(\gamma) = \langle\gamma\rangle$.*

   Como $\langle\gamma\rangle$ es un grupo cíclico, luego abeliano, entonces todos sus elementos formarán parte de $C_G(\gamma)$, luego $\langle\gamma\rangle \leq C_G(\gamma)$. Y, como $|Cl_G(\gamma)| = 24$, entonces $|C_G(\gamma)| = \dfrac{|G|}{|Cl_G(\gamma)|} = \dfrac{120}{24} = 5 = |\langle\gamma\rangle|$, luego se tiene la igualdad.

3. *Sea $\sigma = (1,2)(3,4)$. Entonces $C_G(\sigma) = \langle(1,3,2,4),(1,3)(2,4)\rangle$. Además, este grupo es isomorfo a $\mathcal{D}_8$.*

   Por un lado, sabemos que hay 15 ciclos de tipo $[2,2]$, luego $|Cl_G(\sigma)| = 15 = \dfrac{|G|}{|C_G(\sigma)|} = \dfrac{120}{|C_G(\sigma)|}$, por lo que $|C_G(\sigma)| = \dfrac{120}{15} = 8$.

   Por otro lado, llamemos $a = (1,3,2,4)$ y $b = (1,3)(2,4)$. Es claro que $o(a) = 4$ y $o(b) = 2$ (simple comprobación). Entonces

$$\langle a\rangle = \{id, (1,3,2,4), (1,2)(3,4), (1,4,2,3)\},$$

   y

$$\langle b\rangle = \{id, (1,3)(2,4)\}.$$

   Luego $\langle a\rangle \cap \langle b\rangle = id$, y así $|\langle a\rangle\langle b\rangle| = |\langle a\rangle||\langle b\rangle| = 4 \cdot 2 = 8$. Sólo quedaría ver que $\langle(1,3,2,4),(1,3)(2,4)\rangle \leq C_G(\sigma)$, pero esto se desprende del hecho de que $\sigma \in \langle a\rangle$ (que es un grupo cíclico, luego abeliano) y de que $\sigma \cdot b = b \cdot \sigma = (1,4)(2,3)$ (simple comprobación). Así, tenemos un subgrupo del mismo orden que el centralizador, luego son lo mismo.

■

Proposición 5.7. *Sea $n \geq 3$. Entonces $Z(S_n) = 1$.*

Demostración: Sea $1 \neq \sigma \in Z(S_n)$. Entonces va a existir un $a \in \Omega$ tal que $\sigma(a) = b \neq a$, con $b \in \Omega$. Sea ahora $c \in \Omega \setminus \{a, b\}$ y sea $\tau = (b, c)$. Entonces $\tau\sigma\tau^{-1}(a) = \tau\sigma(a) = \tau(b) = c \neq b\ (= \sigma(a))$. Luego, $\sigma^\tau \neq \sigma$, lo cual es absurdo puesto que $\sigma \in Z(S_n)$.

□

5.2. El homomorfismo índice y el grupo alternado

Definición 5.8. *Para cada $\sigma \in S_n$ consideramos el endomorfismo*

$$\begin{array}{rccc} f_\sigma\colon & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ & e_j & \longmapsto & e_{\sigma(j)} \end{array}$$

con e_j un vector de la base $B = \{e_1, \ldots, e_n\}$ de $\mathbb{R}^n$. La aplicación

$$\begin{array}{rccc} \psi\colon & S_n & \longrightarrow & Aut(\mathbb{R}^n) \\ & \sigma & \longmapsto & f_\sigma \end{array}$$

es un homomorfismo de grupos, puesto que dados $\sigma, \tau \in S_n$ *y* $j = 1, \ldots, n$, *se tiene que*

$$f_{\sigma\cdot\tau} = e_{(\sigma\cdot\tau)(j)} = e_{\sigma(\tau(j))} = f_\sigma(e_{\tau(j)}) = f_\sigma(f_\tau(e_j)) = (f_\sigma \circ f_\tau)(e_j),$$

es decir, $\psi(\sigma \cdot \tau) = f_{\sigma\cdot\tau} = f_\sigma \circ f_\tau = \psi(\sigma) \circ \psi(\tau)$.

Ahora, observar que la matriz $M_{f_\sigma}(B)$ *de* f_σ *respecto de la base estándar se obtiene a partir de la matriz identidad desordenando las columnas de ésta. Del Álgebra Lineal sabemos que si intercambiamos dos columnas de una matriz obtenemos otra con el determinante opuesto a la de la matriz de partida, deducimos así que* $det(f_\sigma) \in \mathcal{U}_2 = \{+1, -1\}$. *Se define entonces el* ***homomorfismo índice ó signatura de una permutación*** *como*

$$\varepsilon = det \circ \psi \colon S_n \longrightarrow \mathcal{U}_2 = \{+1, -1\}$$

donde $det \colon Aut(\mathbb{R}^n) \longrightarrow \mathbb{R}$ *es el homomorfismo determinante. Además el homomorfismo índice es sobreyectivo pues*

$$\varepsilon(id) = det(f_{id}) = det(id_{\mathbb{R}^n}) = +1$$

y si σ *es una transposición cualquiera, la matriz* $M_{f_\sigma}(B)$ *es aquella en la que se han intercambiado dos columnas de la matriz identidad, y así*

$$\varepsilon(\sigma) = det(f_\sigma) = det(M_{f_\sigma}(B)) = -det(id_{\mathbb{R}^n}) = -1.$$

Así, a partir de la construcción de este *homomorfismo índice* como composición del homomorfismo determinante y ψ antes definido, podemos dar una definición formal de lo que es el *grupo alternado*:

Definición 5.9. *El núcleo de* ε *lo denotaremos* $\mathcal{A}_n$ *y lo llamaremos* n***-ésimo grupo alternado****. Las permutaciones* $\sigma \in \mathcal{A}_n$ *se denominan* ***pares****, y las que pertenecen a* $S_n \setminus \mathcal{A}_n$ *se denominan* ***impares****. Al ser el homomorfismo índice* ε *sobreyectivo, tenemos que* $|\mathcal{A}_n| = n!/2$. *Las permutaciones pares son aquellas que pueden escribirse como producto de un número par de transposiciones y tienen signatura* 1, *y las impares aquellas que pueden escribirse como producto de un número impar de transposiciones y tiene signatura* -1. *Esto se puede comprobar con el siguiente resultado:*

Proposición 5.10. *Sea* $\sigma = (a_1, \ldots, a_k) \in S_n$. *Las transposiciones* $\tau_j = (a_{j-1}, a_j)$, *donde* $2 \leq j \leq k$, *cumplen* $\sigma = \tau_k \cdot \tau_{k-1} \ldots \tau_2$. *En particular* $\sigma \in \mathcal{A}_n$ *si y sólo si* k *es impar.*

Demostración: La igualdad $\sigma = \tau_k \cdot \tau_{k-1} \ldots \tau_2$ se comprueba directamente. Además, como cada $\varepsilon(\tau_i) = -1$ resulta que

$$\varepsilon(\sigma) = \prod_{i=2}^{k} \varepsilon(\tau_i) = (-1)^{k-1},$$

luego $\sigma \in \mathcal{A}_n$ si y sólo si $1 = (-1)^{k-1}$, esto es, si k es impar.

□

Del resultado que acabamos de ver se tiene que, dado un k-ciclo $(a_1, \ldots, a_k) \in S_n$, entonces su signatura es $(-1)^{k-1}$.

Con todo esto podemos resumir el grupo alternado mediante el siguiente homomorfismo:

Proposición 5.11. *La aplicación signatura*

$$\begin{array}{rccc} sig\colon & S_n & \longrightarrow & \{-1,1\} \\ & \sigma & \longmapsto & sig(\sigma) \end{array}$$

es un homomorfismo de grupos. Su núcleo, que está formado por las permutaciones pares, es un subgrupo de índice 2*, el* ***grupo alternado*** $\mathcal{A}_n$*. Además,*

$$S_n/\mathcal{A}_n \simeq C_2.$$

Observación 5.11.1. *Para $n \geq 4$ el grupo alternado $\mathcal{A}_n$ no es abeliano puesto que las permutaciones $\sigma = (1,2,3) \in \mathcal{A}_n$ y $\tau = (1,2)(3,4) \in \mathcal{A}_n$, por la proposición anterior y que $\sigma\tau(1) = 1$ y $\tau\sigma(1) = 3$, cumplen $\sigma\tau \neq \tau\sigma$.*

Además, a partir de la proposición anterior y de 5.5, podemos afirmar que las transposiciones generan el grupo S_n, o sea que cada permutación es producto de transposiciones.

Ejemplo 5.11.1. *El grupo $\mathcal{A}_4$ tiene* 12 *elementos, que son los elementos de*

$$K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

y los 8 3*-ciclos de S_4. Además $K \trianglelefteq \mathcal{A}_4$ y así $\mathcal{A}_4$ no es simple, de hecho es el único subgrupo normal propio de $\mathcal{A}_4$.*

5.3. El teorema de Abel

Una vez visto las primeras definiciones y propiedades de lo que son el grupo simétrico y alternado demostraremos uno de los resultados más importantes en *Teoría de Grupos*: que $\mathcal{A}_n$ es simple si $n \geq 5$, también conocido como el *Teorema de Abel*, en honor de Niels Henrik Abel.

Proposición 5.12. *Si $n \geq 3$, entonces $\mathcal{A}_n$ es transitivo sobre $\Omega = \{1, \ldots, n\}$*

Demostración: Si $1 \leq i < j \leq n$, elegimos k distinto de i y de j y tenemos que $(i,j,k)(i) = j$. Claramente $(i,j,k) \in \mathcal{A}_n$.

□

Teorema 5.13 (***Teorema de Abel***)**.** *Si $n \geq 5$, entonces $\mathcal{A}_n$ es simple.*

Demostración: ***Primero demostraremos que $\mathcal{A}_5$ es simple***. En $\mathcal{A}_5$ tenemos 20 3-ciclos, 24 5-ciclos y 15 elementos del tipo $(a,b)(c,d)$. Veamos que los 3-ciclos son conjugados en $\mathcal{A}_5$. Sea $g = (1,2,3)$. Sabemos de 5.6.2 que $C_{S_5}(g) = \langle g \rangle \langle (4,5) \rangle$. Ahora,

$$\langle g \rangle \subseteq C_{\mathcal{A}_5}(g) \leq C_{S_5}(g)$$

puesto que $(4,5) \in C_{S_5}(g) \setminus \mathcal{A}_5$. Como $|C_{S_5}(g)| = 6$, concluimos que $C_{\mathcal{A}_5}(g) = \langle g \rangle$. Por lo tanto, $|Cl_{\mathcal{A}_5}(g)| = 60/3 = 20$.

Veamos ahora que los 15 elementos del tipo $(a,b)(c,d)$ son conjugados en $\mathcal{A}_5$. Nuevamente por 5.6.2 tenemos que

$$\langle (1,2)(3,4), (1,3)(2,4) \rangle \subseteq C_{\mathcal{A}_5}((1,2)(3,4)) \leq C_{S_5}((1,2)(3,4))$$

puesto que $(1,3,2,4) \in C_{S_5}((1,2)(3,4)) \setminus \mathcal{A}_5$. Como $|C_{S_5}((1,2)(3,4))| = 8$, concluimos que $|C_{\mathcal{A}_5}((1,2)(3,4))| = 4$ y así la clase de conjugación de $(1,2)(3,4)$ en $\mathcal{A}_5$ tiene 15 elementos. (Esto también se puede ver teniendo en cuenta que todas las permutaciones de tipo $[2,2]$ son pares, es decir, que todas forman parte del grupo alternado).

Finalmente, notamos que hay dos clases de conjugación en $\mathcal{A}_5$ de 5-ciclos. En efecto, sabemos que si g es un 5-ciclo, entonces $C_{S_5}(g) = \langle g \rangle = C_{\mathcal{A}_5}(g)$. Así, $|Cl_{\mathcal{A}_5}(g)| = 12$. Por tanto, las longitudes de las clases de conjugación de $\mathcal{A}_5$ son $1, 12, 12, 15$ y 20.

Sea ahora N un subgrupo normal propio de $\mathcal{A}_5$. Tenemos que N es una unión disjunta de clases de conjugación de $\mathcal{A}_5$ (siendo una de ellas el 1) y que $1 < |N| < 60$ es un divisor de 60. Por lo tanto,

$$|N| = 1 + 12a + 12b + 15c + 20d,$$

con $a, b, c, d \in \{0, 1\}$. Pero no hay ningún divisor de 60 de esta forma quitando el 1 y el propio 60. Luego no existe N subgrupo normal propio y así $\mathcal{A}_5$ es simple.

Probaremos ahora que $\mathcal{A}_n$ es simple para $n \geq 6$ por inducción sobre n. Supongamos que $n \geq 6$ y que $\mathcal{A}_{n-1}$ es simple. Sabemos que $\mathcal{A}_n$ actúa sobre $\{1, 2, \ldots, n\}$. Sea K el estabilizador de n en $\mathcal{A}_n$. Sea K el estabilizador de n en $\mathcal{A}_n$. Como hicimos en 5.1.1 para cada $\sigma \in K$, tenemos definido un $\bar{\sigma} \in S_{n-1}$. Como la descomposición de σ y $\bar{\sigma}$ como producto de ciclos disjuntos es la misma entonces σ es par si y sólo si $\bar{\sigma}$ lo es. Por lo tanto $K \simeq \mathcal{A}_{n-1}$ es simple.

Por 5.12, $\mathcal{A}_n$ actúa transitivamente sobre $\{1, 2, \ldots, n\}$ y por sabemos que todos los estabilizadores son conjugados en $\mathcal{A}_n$. Por lo tanto, si $\sigma \in \mathcal{A}_n$ fija algún elemento, entonces $\sigma \in K^\tau$ para cierto $\tau \in \mathcal{A}_n$.

Sea ahora $N \trianglelefteq \mathcal{A}_n$. Entonces $K \cap N \trianglelefteq K$ y por la simplicidad de K concluimos que $K \subseteq N$ ó $K \cap N = 1$. En el primer caso tenemos que $K^\tau \subseteq N$ para todo $\tau \in \mathcal{A}_n$. Por lo tanto, si una permutación $\sigma \in \mathcal{A}_n$ fija un elemento, entonces $\sigma \in N$. En particular, N contiene todos los productos $(a,b)(c,d)$. Como toda permutación par es producto de un número par de transposiciones tenemos entonces que $N = \mathcal{A}_n$ en este caso.

En el segundo caso, $K \cap N = 1$. Por lo tanto, $K^\tau \cap N = (K \cap N)^\tau = 1$ para todo $\tau \in \mathcal{A}_n$. Es decir, si $1 \neq \sigma \in \mathcal{A}_n$ fija algún elemento, entonces σ no está en N.

Supongamos que $N > 1$ y sea $1 \neq \sigma \in N$. Supongamos primero que en la descomposición de σ como producto de ciclos disjuntos solo aparecen transposiciones. Tenemos que $\sigma = (a,b)(c,d)\cdots$. Sea e una cifra distinta de a, b, c, d. Entonces

$$\gamma = \sigma^{(a,b)(d,e)} = (b,a)(c,e)\cdots \in N.$$

Ahora $\sigma\gamma \in N$, $\sigma\gamma$ fija a y $1 \neq \sigma\gamma$ (ya que manda d a e). Esto es una contradicción. Finalmente, supongamos que en la descomposición de σ como producto de ciclos disjuntos tenemos un m-ciclo con $m \geq 3$. Podemos escribir $\sigma(a, b, c, \ldots) \cdots$. Elegimos ahora dos cifras d, e distintas de a, b, c y escribimos

$$\gamma = \sigma^{(c,d,e)} = (a, b, d, \ldots) \cdots \in N.$$

Tenemos que $\gamma \neq \sigma$ y $1 \neq \sigma\gamma^{-1} \in N$ fija a. Esta contradicción final prueba el teorema.

□

Por lo tanto, sabemos que para $n \geq 5$, $\mathcal{A}_n$ es simple. Si recordamos, definimos el grupo alternado como el núcleo de un homomorfismo, el *homomorfismo índice*, y sabemos de 1.35 que el núcleo de un homomorfismo es siempre un subgrupo normal del grupo de partida, es decir que en este caso

$$\mathcal{A}_n \trianglelefteq S_n.$$

Además, por el *Primer Teorema de Isomorfía*

$$S_n/\mathcal{A}_n \simeq \mathcal{U}_2 = \{+1, -1\}.$$

Aunque esto ya lo habíamos visto antes.

6. Generalidades sobre anillos

6.1. Introducción

Definición 6.1. *Decimos que un conjunto A dotado de dos operaciones, que usualmente denominaremos suma y producto,*

$$\begin{array}{rccc} +: & A \times A & \longrightarrow & A \\ & (a, b) & \longmapsto & a + b \end{array}$$

$$\begin{array}{rccc} \cdot: & A \times A & \longrightarrow & A \\ & (a, b) & \longmapsto & ab \end{array}$$

*es un **anillo** si cumple que*

1. *A dotado de la suma es un **grupo conmutativo**, es decir,*
   - *La suma cumple las propiedades asociativa y conmutativa.*
   - *Existe un único elemento $0 \in A$ tal que $a + 0 = 0 + a = a$ $\forall a \in A$, que denominaremos **elemento neutro ó cero**.*
   - *Para todo $a \in A$ existe un único elemento b tal que $a + b = b + a = 0$, que denominaremos **elemento opuesto** y denotaremos por $-a$.*
2. *A dotado del producto es un **semigrupo**, es decir, que el producto cumple la propiedad **asociativa**. Dados $a, b, c \in A$, entonces se tiene que*

$$a(bc) = (ab)c.$$

*3. La propiedad **distributiva**, es decir que dados $a, b, c \in A$, tenemos que*

$$(a+b)c = ac + bc, \quad a(b+c) = ab + ac.$$

Además es importante matizar que el elemento neutro para la suma, el cero, podrá escribirse como 0_A ó simplemente 0. Denotaremos por $A^* = A \setminus \{0\}$. Y, como al ver grupos, la operación conocida como producto podrá denotarse con un $\cdot$ en ocasiones ó con simple yuxtaposición.

Finalmente, una notación usual para los anillos será $(A, +, \cdot)$, que incluye el conjunto y las dos operaciones dotadas.

Definición 6.2. *Llamaremos **anillo unitario** a un anillo A que posea **elemento unidad**, es decir,si existe $1_A = 1 \in A$ tal que $1 \cdot a = a \cdot 1 = a \quad \forall a \in A$. También se puede denominar uno.*

Aclaremos algo desde el principio: si tenemos un anillo A, utilizaremos la notación aditiva en el grupo abeliano, es decir hablaremos de $(A, +)$, 0 será el neutro y $-r$ el opuesto de un $r \in A$ cualquiera. Dado un $n \in \mathbb{Z}$ también tendremos definido nr.

Observación 6.2.1. *Notar que podría ocurrir que $1 = 0$, y entonces $A = \{0\}$ ya que si $x \in A$ entonces $0 = 0 \cdot x = 1 \cdot x = x$. Así que para evitar este tipo de confusiones supondremos que $0 \neq 1$.*

A lo largo de las siguiente páginas siempre trabajaremos con anillos unitarios, y en este tipo de anillos podremos distinguir un tipo especial de elementos:

Definición 6.3. *Sea A un anillo unitario. Una **unidad** de A es un elemento $a \in A$ para el que existe un $b \in A$ tal que*

$$ab = ba = 1.$$

*Es decir, b será el **inverso** de a con respecto al producto. Lo denotaremos por a^{-1}, y observar que si ciertos $a, b, c \in A$ verifican $ab = ca = 1$, entonces*

$$c = c(ab) = (ca)b = b.$$

Por lo que, de existir el inverso, será único. El conjunto de todas las unidades de A lo denotaremos por $\mathcal{U}(A)$, que es un grupo con la operación producto. En efecto, dados $a, b \in \mathcal{U}(A)$, entonces

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1 = b^{-1}b = b^{-1}(a^{-1}a)b = (b^{-1}a^{-1})(ab).$$

*De aquí deducimos que $(ab)^{-1} = b^{-1}a^{-1}$. Finalmente, diremos que un anillo es **conmutativo** si se cumple, para cualesquiera $a, b \in A$ que*

$$ab = ba.$$

Observación 6.3.1. *Es importante tener en cuenta que a lo largo de las siguientes páginas en ocasiones podremos escribir x/y en vez de xy^{-1}, siempre que $x \in A$ e $y \in \mathcal{U}(A)$.*

Definición 6.4. *Llamaremos* ***cuerpo*** *a un anillo K tal que $K^* = K \setminus \{0\}$ forma un grupo con la multiplicación. Dicho de otra forma, en todo anillo unitario vamos a tener que $\mathcal{U}(A) \subset A^*$, y los cuerpos son aquellos anillos unitarios tales que $\mathcal{U}(A) = K^*$. De igual manera que para anillos, también podremos definir los* ***cuerpos conmutativos*** *como aquellos que, para cualesquiera $a, b \in K$ se tiene que*

$$ab = ba.$$

Además, un elemento $a \in A$ diremos que es ***idempotente*** *si $a^2 = a$. Y diremos que es* ***nilpotente*** *si existe un entero positivo n tal que $a^n = 0$. Un anillo cuyo único elemento nilpotente sea el 0 se dirá* ***reducido****.*

Propiedades 6.4.1. *Algunas propiedades básicas:*

1. *Para cada $a \in A$ y n, m enteros, podremos definir*

$$na = \overbrace{a + \ldots + a}^{n}$$

$$a^n = \overbrace{a \cdots a}^{n}$$

   y se cumplirán las siguientes propiedades:

$$a^{n+m} = a^n a^m$$

$$a^{nm} = (a^n)^m.$$

2. *Si $a, b \in A$ y tenemos que $ab = ba$, entonces se cumplirá la conocida como* ***Fórmula de Newton****:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

   Y esto es así ya que, como $ab = ba$, el producto $(a+b)\cdots(a+b)$ es, por la propiedad distributiva, una suma de productos de la forma $a^k b^{n-k}$, con $0 \leq k \leq n$, cada uno de ellos obtenido al seleccionar un a en k de los factores $(a+b)$ y un b en los restantes. Y el número de sumandos de esta forma es igual al número de maneras de elegir los k factores, de entre los n dados, en los que el elemento seleccionado es a, es decir $\binom{n}{k}$.

Una vez vistas las primeras definiciones, veamos algunos ejemplos clásicos de anillos:

Ejemplo 6.4.1. *Algunos de estos ejemplos ya los conocemos, de hecho algunos son bastante familiares:*

1. *El conjunto $\mathbb{Z}$ de los números enteros, dotado con la suma y producto habituales, es un anillo conmutativo y unitario. Sus únicas unidades son 1 y -1, por lo que no es un cuerpo.*

2. *Los números pares, $2\mathbb{Z}$, constituyen un anillo conmutativo pero no unitario, puesto que no existe ningún elemento $u \in 2\mathbb{Z}$, es decir, de la forma $2z$ con z algún entero, tal que $2z \cdot 2a = 2a$ con $a \in \mathbb{Z}$.*

3. *Los conjuntos $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ de los números racionales, reales y complejos respectivamente, son cuerpos conmutativos.*

4. *Sea A el conjunto de los números complejos $a+bi$, con $a, b \in \mathbb{Z}$. Como $i^2 = -1$, este conjunto A es un anillo con las operaciones heredadas de $\mathbb{C}$. Tenemos que*

$$(a+bi)(c+di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \in A.$$

A este anillo se le denota $\mathbb{Z}[i]$ y a estos números se les conocen como ***enteros de Gauss****.*

5. *Sean A un anillo y $M_2 = M_2(A)$ el conjunto de las matrices cuadradas de orden 2 de elementos de A. Este conjunto es un anillo con la suma y producto como siguen:*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Además este anillo será unitario si y sólo si A lo es. En cuyo caso, el elemento unidad ó uno será

$$1_{M_2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A partir de aquí, calculemos las unidades. Para esto, vamos a considerar el ***determinante*** *de una matriz $a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2$ cualquiera, que ya conocemos, y en este caso lo vamos a definir como sigue:*

$$\delta = det(a) = a_{11}a_{22} - a_{12}a_{21}$$

y consideremos

$$b = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

Entonces, por como hemos elegido las matrices, tenemos fácilmente que

$$a \cdot b = \begin{pmatrix} \delta & 0 \\ 0 & \delta \end{pmatrix}.$$

Así, si $\delta \in \mathcal{U}(A)$, entonces a será una unidad y tendremos que

$$a^{-1} = \begin{pmatrix} a_{22}/\delta & -a_{12}/\delta \\ -a_{21}\delta & a_{11}/\delta \end{pmatrix}.$$

Recíprocamente, si existe $c = a^{-1}$, también existirá $d = b^{-1}$, que se obtiene de igual forma. Entonces,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = d(ca)b = (dc)(ab) = \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix} \begin{pmatrix} \delta & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} e_{11}\delta & e_{12}\delta \\ e_{21}\delta & e_{22}\delta \end{pmatrix}$$

y, por tanto, $e_{11}\delta = e_{22}\delta = 1$*, y así* $\delta \in \mathcal{U}(A)$*.*

En resumen, $a \in \mathcal{U}(M_2)$ *si y sólo si* $det(a) \in \mathcal{U}(A)$*. Por ejemplo, si* $A = \mathbb{Z}$*, los enteros,* a *será unidad si y sólo si* $det(a) = \pm 1$*. Pero si* $A = \mathbb{Q}$ *(ó cualquier cuerpo),* a *será unidad si y sólo si* $det(a) \neq 0$*, ya que en un cuerpo todos los elementos menos el* 0 *son unidades.*

De todo esto podemos decir que el ***determinante*** *nos puede caracterizar las unidades y nos permite, como ya sabemos del álgebra lineal, el cálculo de inversos. Si lo vemos como un homomorfismo de grupos, es fácil demostrar que, dados* $a, b \in M_2$

$$det(ab) = det(a)det(b).$$

Finalmente apuntar que todo lo visto en este ejemplo es aplicable para matrices de un orden $n \geq 2$ *cualquiera.*

6. *Sea* $A = \mathcal{C}(\mathbb{R}, \mathbb{R})$ *el conjunto de las funciones continuas reales de variable real. En este caso, dicho conjunto es un anillo; en efecto dados* $t \in \mathbb{R}$ *y* $f, g \in A$*, podemos definir las operaciones*

$$(f + g)(t) = f(t) + g(t)$$

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

Además, es conmutativo y unitario, con el elemento neutro la función constante

$$c_1(t) = 1.$$

■

Una vez vistos estos ejemplos y definiciones vamos a definir unos elementos que son de gran importancia en un anillo, y que nos abrirán las puertas a otra estructura algebraica.

Definición 6.5. *Sea* A *un anillo. Llamaremos* ***divisor de cero*** *a un elemento* $a \in A$ *no nulo tal que* $ab = 0$ *para algún* $b \in A$ *no nulo.*

Observación 6.5.1. *Hay ejemplos de anillos que sí tienen divisores de cero, como es el último ejemplo anterior,* $\mathcal{C}(\mathbb{R}, \mathbb{R})$*, ya que si consideramos las funciones*

$$f\colon t \longrightarrow t - |t|$$

$$g\colon t \longrightarrow t + |t|$$

Entonces $(fg)(t) = (t - |t|)(t + |t|) = t^2 - |t|^2 = 0$*.*

Es claro además que los cuerpos no tienen divisores de cero, ya que si tenemos que $ab = 0$, con a y b no nulos, entonces

$$a = a(bb^{-1}) = (ab)b^{-1} = 0b^{-1} = 0.$$

Pero el no tener divisores de cero tampoco hace a un anillo un cuerpo, por ejemplo $\mathbb{Z}$ no los tiene, pero sin embargo tampoco es un cuerpo. Por lo tanto, se ha de introducir una clase de anillos más amplia que se encuentre entre ambas estructuras, es de aquí de dónde surge la siguiente definición:

Definición 6.6. *Llamaremos* ***dominio de integridad****, ó D.I, a un anillo unitario y conmutativo sin divisores de cero.*

Importante remarcar una propiedad fundamental de los dominios de integridad, y también de los cuerpos: se pueden simplificar factores comunes en las igualdades ya que si tenemos $ab = ac$*, con* $a \neq 0$*, entonces* $a(b-c) = 0$*, y al no ser* a *un divisor de cero, tenemos que* $b - c = 0$ *y de aquí* $b = c$*. Esto se conoce como* ***ley cancelativa*** *y también puede darse en estructuras de anillos, siempre y cuando los elementos implicados no sean divisores de cero.*

Y aunque no sean cuerpos, podremos asociarles de forma natural uno con la construcción del llamado ***cuerpo de fracciones de un dominio de integridad***. Veámoslo.

Definición 6.7 (***Cuerpo de fracciones de un dominio de integridad.***)**.** *Sean* A *un dominio de integridad y* $T = A \times A^*$*. En* T *podremos definir una relación de equivalencia como sigue:*

$$(a, b) \sim (a', b') \Leftrightarrow ab' = ba'.$$

A la clase de (x, y) *la denotaremos por* $[a, b]$*. Así, el conjunto cociente* $T/\sim$ *para esta relación, que denotaremos* K*, es un anillo con las operaciones suma y producto como sigue:*

$$[a, b] + [a', b'] = [ab' + ba', bb']$$
$$[a, b] \cdot [a', b'] = [aa', bb'].$$

Y, efectivamente, K *también será un cuerpo ya que su elemento neutro para la suma (cero) es* $[0, 1]$ *y para todo* $[a, b] \in K$ *tal que* $[a, b] \neq [0, 1]$ *existirá un* $[b, a] \in K$ *que cumplirá*

$$[a, b] \cdot [b, a] = [ab, ab] = [1, 1],$$

siendo éste último el elemento neutro para el producto en K*.*

A este cuerpo $K = T/\sim$ *lo denominaremos* ***cuerpo de fracciones de*** A*, y representaremos a sus elementos por* a/b *en lugar de* $[a, b]$*. Al verlos de esta forma se puede entender mejor el por qué de operarlos así. Además, podremos identificar* a A *con el subconjunto de* K *de los elementos* $a/1$*, con* $a \in A$*.*

Así, si $A = \mathbb{Z}$, entonces la anterior construcción nos devolverá el cuerpo $\mathbb{Q}$ de los números racionales.

Ahora un concepto que es propio de los anillos en general, análogo al de los subgrupos en los grupos. Y es que, como ya se dijo entonces para los grupos, dada una estructura algebraica cualquiera siempre es natural preguntarse si van a poder definirse subconjuntos que mantengan esa estructura.

Definición 6.8. *Sea* B *un anillo conmutativo y unitario,* $A \subset B$ *un subconjunto que, con las operaciones inducidas por* B*, es a su vez un anillo unitario tal que* $1_B = 1_A$*. Diremos que* A *es un* ***subanillo*** *de* B*, y ya sabemos que la aplicación*

$$\begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & x \end{array}$$

*es un monomorfismo, la inclusión canónica. Si A y B son cuerpos diremos que A es un **subcuerpo** de B. Además, todo dominio de integridad es subanillo de su cuerpo de fracciones, vía el monomorfismo $x \longrightarrow x/1$.*

Es decir, diremos que un subconjunto A de un anillo R es **subanillo** de R si $s-t, st \in A \quad \forall st, \in A$. En particular, A es subgrupo de R.

Además, resulta que la interseccion es cerrada para los subanillos:

Observación 6.8.1. *Si $\{A_i : i \in I\}$, con I una colección finita de índices, es una familia de subanillos (subcuerpos respectivamente) de un anillo B, entonces su intersección*

$$A = \bigcap_{i \in I} A_i$$

es también un subanillo (subcuerpo) de B.

Ejemplo 6.8.1. *Veamos algunos ejemplos de dominios de integridad:*

1. *Sea A un anillo, el anillo de matrices M_2 con elementos de A nunca es dominio de integridad, ya que por ejemplo dado un $x \in A$ tenemos*

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

2. *Al hacer un **producto de anillos** siempre obtenemos otro anillo que sí contiene divisores de cero. Sean A y B dos anillos unitarios y conmutativos. Entonces $C = A \times B$ es un anillo unitario y conmutativo con las operaciones*

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Es claro que $0_{A\times B} = (0_A, 0_B)$ y que $1_{A\times B} = (1_A, 1_B)$. Y como divisores de cero tendremos a aquellos elementos que sean de la forma $(0, b)$ ó $(a, 0)$ ya que

$$(0, b)(a, 0) = (0 \cdot a, b \cdot 0) = (0_A, 0_B).$$

*Y esto ocurrirá aunque A y B sean dominios de integridad. Además, igualmente podremos construir de forma análoga un **producto de una colección finita de anillos**.*

■

Observación 6.8.2. *A propósito del producto de anillos, se puede comprobar fácilmente que*

$$\mathcal{U}(A \times B) = \mathcal{U}(A) \times \mathcal{U}(B).$$

Ahora introduciremos uno de los conceptos más importantes que veremos a lo largo de este capítulo y que será de todavía mayor importancia en lo sucesivo. Es algo así como la extensión del concepto de subgrupo normal para los anillos:

Definición 6.9. *Sea A un anillo conmutativo y unitario. Llamaremos* ***ideal*** *a un subconjunto $I \subset A$ que cumplirá las siguientes condiciones:*

1. *I es un subgrupo de A para la suma, así habrá de incluir el elemento neutro, es decir, $0 \in I$.*
2. *$\forall x \in I, a \in A$ tenemos que $ax \in I$.*

Aunque la primera condición es también equivalente a:

1. *$\forall x, y \in I$, se tiene que $x + y \in I$.*

Y esto es así ya que, al cumplirse b. y esta nueva condición, tendremos que dados $x, y \in I$

$$x - y = x + (-1)y \in I$$

(ya que $(-1)y \in I$ por b.). Así, I será subgrupo para la suma.

Es inmediato comprobar que, por ejemplo, los múltiplos de un número entero, es decir, conjuntos de la forma $n\mathbb{Z}$ con n un entero cualquiera, forman un ideal del anillo de los números enteros $\mathbb{Z}$.

Definición 6.10. *Algunas definiciones de especial interés:*

1. *El conjunto $\{0\}$ es un ideal de A, denominado* ***ideal nulo****. También A cumple con las condiciones, así que también es ideal de A, y tanto este como el ideal nulo son los llamados* ***ideales impropios*** *de A. Esto sirve para distinguirlos de aquellos ideales $I \neq A$, a los que llamaremos* ***ideales propios*** *de A. Notar que si $1 \in I$, entonces por la segunda condición tenemos que $x = x \cdot 1 \in I$ para cualquier $x \in A$. Por lo tanto será importante para tener en cuenta que I* ***es propio si y sólo si*** *$1 \notin I$.*
2. *Si $x \in A$, entonces el conjunto*

$$xA = \{xa : \ a \in A\}$$

es un ideal de A, denominado ***ideal principal generado por*** *x. Un ejemplo de esto podrían ser los ideales de $\mathbb{Z}$ mencionados anteriormente, los conjuntos $n\mathbb{Z}$. Más adelante veremos esta expresión generalizada para hablar de ideales generados por conjuntos.*

Con esto, podemos enunciar el primer resultado, que define los cuerpos a partir de los ideales:

Proposición 6.11. *Un anillo A es un cuerpo si y sólo si sus únicos ideales son los impropios, es decir, el mismo A y $\{0\}$.*

Demostración: Si A es un cuerpo e I un ideal no nulo de A entonces contendrá algún elemento $a \neq 0$ y así $aa^{-1} = 1 \in A$, por lo que $I = A$. Recíprocamente, supongamos que los únicos ideales de A son los impropios. Entonces, para cada $a \in A$ no nulo el ideal aA también es no nulo, y así $aA = A$; pero esto quiere decir que existirá un $b \in A$ tal que $ab = 1$. Por lo tanto, $a \in \mathcal{U}(A)$ y como esto es así para cualquier $a \in A$ no nulo, A es un cuerpo.

□

Con todo esto, sería normal preguntarse para qué hemos definido este concepto, el de ideal. Y es que la noción de ideal, como ya se ha dicho, es de gran importancia principalmente porque nos va a permitir definir relaciones de equivalencia en un anillo de tal forma que el conjunto cociente podrá heredar la estructura de anillo. Es algo similar a lo que pasa con los *subgrupos normales* en *Teoría de Grupos*.

Definición 6.12. ***Anillos cociente.*** *Sea A un anillo conmutativo y unitario e $I \subset A$ un ideal propio. Definiremos la siguiente relación de equivalencia:*

$$x \sim y \text{ si } x - y \in I, \text{ con } x, y \in A.$$

Es evidente que es una relación de equivalencia (cumple las propiedades reflexiva, simétrica y transitiva).

El conjunto cociente de A para esta relación la denotaremos A/I y la clase de equivalencia de un elemento $x \in A$ será:

$$x + I = \{x + a : \ a \in I\}.$$

Que un elemento y esté en la clase de equivalencia de x significa que existirá un elemento $a \in I$ de la forma $a = y - x$. Además,

$$x + I = y + I \Leftrightarrow x \equiv y \ mod \ I, \text{ es decir, que tanto } x - y \in I \text{ como } y - x \in I.$$

Ahora, dotaremos a A/I de dos operaciones que lo convertirán en un anillo, dados $x, y \in A$:

$$\begin{array}{rccl} +: & A/I \times A/I & \longrightarrow & A/I \\ & ((x+I),(y+I)) & \longmapsto & (x+I)+(y+I) = (x+y)+I, \end{array}$$

que le confiere a A/I estructura de grupo abeliano (conmutativo), y

$$\begin{array}{rccl} \cdot: & A/I \times A/I & \longrightarrow & A/I \\ & ((x+I),(y+I)) & \longmapsto & (x+I)\cdot(y+I) = xy+I. \end{array}$$

Esta última operación además no depende de los representantes elegidos. Supongamos que $x + I = x' + I$ (es decir, $x - x' \in I$) y que $y + I = y' + I$ ($y - y' \in I$). Entonces $xy + I = x'y' + I$, ya que

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y') \in I$$

esto último es así por la segunda condición que deben cumplir los ideales.

Una vez visto esto, las propiedades asociativa y conmutativa del producto, así como la distributiva, son inmediatas. El ***elemento neutro*** *de A/I será $1 + I$. Así, A/I dotado con las dos operaciones, suma y producto respectivamente, y las demás propiedades enunciadas tiene estructura de anillo conmutativo unitario, que denominaremos* ***anillo cociente ó anillo de clases de restos módulo*** *I.*

Finalmente, los ideales del cociente A/I serán aquellos ideales de A que contengan

a I, de hecho se puede establecer fácilmente una biyección entre ambos conjuntos. Sea L un ideal del anillo cociente y consideremos el conjunto

$$J = \{x \in A : x + I \in L\}.$$

Entonces es claro que J es un ideal de A y que contiene a I, puesto que si $x \in I$ entonces $x + I = 0 + I \in L$. Luego la biyección se establece entre los conjuntos de la forma L y de la forma J, es decir, entre los ideales de A/I y los ideales de A que contienen a I respectivamente.

Observación 6.12.1. *Notar que si $x \in I$, entonces $x + I$ será el conjunto de los $x + a$ con $a \in I$, pero como $x \in I$ entonces $x + a \in I$ y así $x + I = 0 + I = I$.*

En resumen, llamaremos anillo cociente al conjunto A/I de las clases de equivalencia de un anillo respecto a la relación de equivalencia $x \sim y$ si $x - y \in I$, con I un ideal propio de A, y dotado con las operaciones antes definidas y que le confieren una estructura de anillo conmutativo unitario.

A continuación desarrollaremos la idea de subconjuntos que generan ideales. Anteriormente vimos cuando un ideal es generado por un sólo elemento, denominado ideal principal generado por ese elemento, y ahora generalizaremos ese concepto. Definiremos ideal generado por un subconjunto a través de la siguiente proposición:

Proposición 6.13 (***Ideales generados por un subconjunto***)**.** *Sea A un anillo conmutativo y unitario, y L un subconjunto de A, que carece de estructura algebraica. Consideremos el conjunto $I \subset A$ de todas las sumas finitas de la forma*

$$a_1x_1 + \ldots + a_rx_r, \;\; a_1, \ldots, a_r \in A, \;\; x_1, \ldots, x_r \in L, \;\; r \geq 1.$$

Entonces tenemos que

1. *I es un ideal.*
2. *I es el mínimo ideal que contiene a L, es decir, si $\mathcal{L}$ es la colección de todos los ideales $J \subset A$ tales que $L \subset J$, se verifica que*

$$I = \bigcap_{J \in \mathcal{L}} J.$$

Demostración: Veamos 1.. Comprobemos , para ello sean

$$a = \sum_{k=1}^{r} a_k x_k, \;\; b = \sum_{l=1}^{s} b_l y_l \in I, \quad c \in A.$$

Entonces es evidente que

$$a + b = a_1x_1 + \ldots + a_rx_r + b_1y_1 + \ldots + b_sy_s \in I$$

$$c \cdot a = c(a_1x_1 + \ldots + a_rx_r) = (ca_1)x_1 + \ldots + (ca_r)x_r \in I.$$

Para probar 2. observar que $I \in \mathcal{L}$, puesto que I es un ideal que contiene a L, luego

$$\bigcap_{J \in \mathcal{L}} J \subset I.$$

Pero, por otra parte, si $J \in \mathcal{L}$, $a_1, \ldots, a_r \in A$, $x_1, \ldots, x_r \in L$, tenemos $a_1x_1, \ldots, a_rx_r \in J$ y $a_1x_1 + \ldots + a_rx_r \in J$ por ser J un ideal de A que contiene a L. Esto demuestra que todos los elementos de I están también en J, así $I \subset J$. Siendo esto igual para todo ideal J de $\mathcal{L}$, tenemos que

$$I \subset \bigcap_{J \in \mathcal{L}} J.$$

Por tanto, la igualdad.

Este ideal I que acabamos de construir es lo que conoceremos como ***ideal generado por*** L.

□

Definición 6.14. *Sea A un anillo conmutativo y unitario. Un ideal $I \subset A$ se llama **finitamente generado** si un el ideal generado por un subconjunto finito $L = \{x_1, \ldots, x_r\} \subset A$. En dicho caso,*

$$I = Ax_1 + \ldots + Ax_r = \left\{ \sum_{k=1}^{r} a_k x_k : \ a_1, \ldots, a_r \in A \right\}.$$

*Lo denotaremos $I = (x_1, \ldots, x_r)$. Y recordar que si $r = 1$, es decir, que el ideal está generado por un solo elemento entonces I se llama **ideal principal**.*

Definición 6.15. *Un anillo A se dirá **noetheriano**, en honor a la gran matemática alemana Emmy Noether, si todos sus ideales son finitamente generados.*

Es claro que todo cuerpo K es un anillo noetheriano.

Definición 6.16 (***Operaciones con ideales.***)**.** *Sean I, J ideales de un anillo unitario y conmutativo A. Veamos las operaciones que se pueden realizar con ellos:*

1. ***Suma**. La denotaremos $I+J$, y consiste en todos los elementos de la forma $x+y$, con $x \in I$, $y \in J$. Coincide con el ideal generado por $I \cup J$. En efecto, dados $a_1, \ldots, a_r, b_1, \ldots, b_s \in A$, $x_1, \ldots, x_r \in I$, $y_1, \ldots, y_s \in J$, podremos escribir $a_1x_1 + \ldots + a_rx_r + b_1y_1 + \ldots + b_sy_s = x + y$ si $x = a_1x_1 + \ldots + a_rx_r \in I$, e $y = b_1y_1 + \ldots + b_sy_s \in J$.*
2. ***Producto**. Se denota por $I \cdot J$ ó también IJ, y es el ideal generado por todos los productos xy, con $x \in I$, $y \in J$. Consiste en el siguiente conjunto:*

$$IJ = \{x_1y_1 + \ldots + x_ry_r : \ x_1, \ldots, x_r \in I, \ y_1, \ldots, y_r \in J, \ r \geq 1\}.$$

3. ***Intersección**. La denotaremos por $I \cap J$, y es, de forma inmediata, un ideal de A. De hecho, también es un ideal de A la intersección de una colección infinita de ideales.*

De estas definiciones deducimos el siguiente resultado:

Proposición 6.17. *Dado un anillo conmutativo y unitario A, y dos ideales I, J de A, entonces tendremos:*

1. *$IJ \subset I \cap J$.*

2. *En general IJ y $I \cap J$ no coincidirán.*

3. *Dada una colección finita de ideales $I_1, \ldots, I_r$ de A, con $r \geq 1$, entonces*

$$I_1 \cdots I_r \subset I_1 \cap \cdots \cap I_r.$$

Demostración: Para probar 1. simplemente hay que tener en cuenta que, como $IJ = \{x_1y_1 + \ldots + x_ry_r : x_1, \ldots, x_r \in I,\ y_1, \ldots, y_r \in J,\ r \geq 1\}$, entonces cada $x_iy_i \in I$ puesto que cada $x_i \in I$ y cada $y_i \in A$ al pertenecer a J, y análogamente $x_iy_i \in J$, así que $x_iy_i \in I \cap J$. Y como $I \cap J$ es ideal, entonces las sumas también pertenecerán. La comprobación de que IJ es ideal es también directa.

Para ver 2. daremos un contraejemlo. Consideremos $A = \mathbb{Z}$, $I = 4\mathbb{Z}$ y $J = 6\mathbb{Z}$, respectivamente los múltiplos de 4 y de 6. Entonces la $I \cap J$ estará formado por aquellos elementos que sean múltiplos de 4 y de 6, es decir múltiplos de 12, luego $I \cap J = 12\mathbb{Z}$. Sin embargo, $IJ = 24\mathbb{Z}$, luego el contenido de IJ en la intersección es estricto.

3. es evidente por recurrencia ya que

$$I_1 \cdots I_r \subset (I_1 \cdots I_{r-1})I_r \subset (I_1 \cdots I_{r-1}) \cap I_r \subset (I_1 \cap \cdots \cap I_{r-1}) \cap I_r \subset I_1 \cap \cdots \cap I_r.$$

□

Definición 6.18. *Sea un anillo conmutativo y unitario A y dos ideales I, J de A. Entonces diremos que I y J son **comaximales** si $I + J = A$. Además, en tal caso se tendrá que $IJ = I \cap J$.*

Observación 6.18.1. *Efectivamente, se tiene la igualdad $IJ = I \cap J$ ya que al ser comaximales existirán $x \in I$ e $y \in J$ tales que $x+y = 1$. Y ahora, dado un $a \in I \cap J$, $a, x \in I$ y también $a, y \in J$, así que*

$$a = a1 = a(x + y) = ax + ay \in IJ.$$

Ejemplo 6.18.1. *En el anillo $\mathbb{Z}$ de los números enteros todos los ideales son principales, tal y como veremos más adelante. Así, para cada número entero k se tiene el ideal*

$$(k) = I_k = k\mathbb{Z} = \{pk : p \in \mathbb{Z}\}.$$

Y es claro que tanto k como $-k$ generan el mismo ideal, así que tomaremos $k \geq 0$. Esto establece una biyección entre los ideales de $\mathbb{Z}$ y los enteros no negativos, con $0 = 0\mathbb{Z} = \{0\}$ y $1\mathbb{Z} = \mathbb{Z}$. Veamoslo:

Supongamos que $(k) = (l)$, con $k, l \geq 0$. Entonces $k \in (l)$ y $l \in (k)$. Si $l ==$, entonces $k \in (l) = (0) = \{0\}$, luego $k = l = 0$. Igualmente si $k = 0$. Ahora, sea $k, l > 0$. Entonces

$$k = ql,\ \ l = pk,\ \ 0 < q, p \in \mathbb{Z}.$$

Y, por lo tanto, $k \geq l$ y $l \geq k$, y de aquí la igualdad.

■

Ahora se introducirá dos clases muy importantes de ideales, que serán esenciales en lo que sigue.

Definición 6.19. *Sea A un anillo no necesariamente conmutativo ni unitario e I un ideal de A. Diremos que I es **maximal** si lo es, respecto de la inclusión, en la familia de todos los ideales propios de A, es decir, si no existe ningún ideal propio J de A que lo contenga estrictamente ($I \subsetneq J$).*

A continuación daremos una caracterización de estos ideales:

Proposición 6.20. *Sea A un anillo conmutativo y unitario e I un ideal de A. Entonces I será **maximal** si se cumple algunas de las siguientes condiciones equivalentes:*

1. *El anillo cociente A/I es un cuerpo.*
2. *I es un ideal propio y ningún otro ideal propio lo contiene estrictamente.*

Demostración: Sea A/I un cuerpo y supongamos que I no es maximal. Entonces existirá un ideal J de A tal que $I \subsetneq J \subsetneq A$. Sea $x \in J \setminus I$ un elemento de J que no pertenece a I. Entonces $x + I$ es un elemento no nulo del cuerpo A/I ya que $x \notin I$, por lo que tendrá inverso, es decir, existirá $y \in A$ tal que

$$1 + I = (x + I)(y + I) = xy + I,$$

y en consecuencia $1 - ab \in I \subset J$. Ahora como $ab \in J$, por ser J un ideal, tendremos que $1 = (1 - ab) + ab \in J$ y así $J = A$, lo cual es falso.

Recíprocamente, sea $x + I$ un elemento no nulo de A/I. Entonces $x \in A \setminus I$, es decir, será un elemento de A que no estará en I, por lo que el ideal $I + xA$ contiene estrictamente a I. Como este último es maximal tendremos que $I + xA = A$, es decir que existirá $b \in I$ e $y \in A$ tal que $b + xy = 1$. Así que $1 - xy \in I$, es decir,

$$xy + I = (x + I)(y + I) = 1 + I,$$

por lo que A/I es un cuerpo.

□

La siguiente proposición caracterizará a la otra clase de ideales que veremos, los ideales ***primos***:

Proposición 6.21. *Sea A un anillo conmutativo y unitario e I un ideal de A. Diremos que I es **primo** si se verifica alguna de las siguientes condiciones:*

1. *El anillo cociente A/I es un dominio de integridad.*
2. *I es un ideal propio y para cualesquiera $x, y \in A$, si $xy \in I$, entonces $x \in I$ ó $y \in I$.*

Demostración: Si $xy \in I$, entonces $0 + I = xy + I = (x + I)(y + I)$, y como A/I es dominio de integridad ó $x + I = 0 + I$ y $x \in I$ ó $y + I = 0 + I$ y así $y \in I$.

Recíprocamente, $0 + I = xy + I = (x + I)(y + I)$ ya que $xy \in I$, y como ó $x \in I$ ó $y \in I$, entonces ó $(x + I) = 0 + I$ ó $(y + I) = 0 + I$ respectivamente. Así A/I es dominio de integridad.

□

El por qué del término ideal primo se debe a que los ideales primos no nulos del anillo de los enteros $\mathbb{Z}$ son precisamente los generados por los números primos, aunque esto lo veremos más adelante.

Observación 6.21.1. *Todo ideal maximal es primo, ya que todo cuerpo es dominio de integridad.*

Proposición 6.22. *Sea I es un ideal primo de un anillo unitario y conmutativo A tal que el anillo cociente A/I es finito, entonces I es un ideal maximal.*

Demostración: Tenemos que ver que $B = A/I$ es un cuerpo. Sea $x \in B$ un elemento no nulo, entonces la aplicación

$$\begin{array}{rccc} h\colon & B^* & \longrightarrow & B^* \\ & y & \longmapsto & xy, \end{array}$$

es inyectiva, puesto que $xy = xy'$ implica que $x(y - y') = 0$ y como B no tiene divisores de cero, por ser A/I dominio de integridad, $y = y'$. Y como B es finito la aplicación h ha de ser necesariamente suprayectiva y así $1_B = xy$ para algún $y \in B^*$, luego x es unidad. Como esto se puede hacer para cualquier $x \in B$ no nulo, B es un cuerpo.

□

6.2. Homomorfismos de anillos

Ahora, al igual que con pasaba con grupos, introduciremos las aplicaciones que conservan la estructura de anillo, para a partir de ellas estudiar lo que resta.

Definición 6.23. *Sean A y B dos anillos conmutativos y unitarios. Definiremos un* ***homomorfismo de anillos*** *de A en B como una aplicación*

$$f\colon A \longrightarrow B$$

tal que:

1. $f(x + y) = f(x) + f(y)$, $\forall x, y \in A$.
2. $f(xy) = f(x)f(y)$, $\forall x, y \in A$.
3. $f(1_A) = 1_B$.

Observación 6.23.1. *La última condición es muy importante y de no darse no podrían excluirse algunas aplicaciones que, aunque conserven las operaciones, podrían ser contraproducentes. Ya que, si $x \in A$*

$$f(x) \cdot (f(1_A) - 1_B) = f(x)f(1_A) - f(x)1_B = f(x \cdot 1_A) - f(x) = 0.$$

Así, si $f(1_A) \neq 1_B$, todos los elementos de $f(A)$ serían divisores de cero.

Ejemplo 6.23.1. *Veamos dos ejemplos de homomorfismos:*

1. *La conjugación*

$$\begin{array}{rccc} f\colon & \mathbb{Z}[i] & \longrightarrow & \mathbb{Z}[i] \\ & x=a+bi & \longmapsto & \bar{x}=a-bi, \end{array}$$

es un homomorfismo. Evidentemente $f(1)=1$ ya que es real, sea $x=a+bi$ e $y=c+di$, entonces

$$f(x+y)=\overline{x+y}=\overline{(a+bi)+(c+di)}=\overline{(a+c)+(b+d)i}=$$
$$(a+c)-(b+d)i=(a-bi)+(c-di)=\overline{x}+\overline{y}=f(x)+f(y),$$

$$f(xy)=\overline{xy}=\overline{(a+bi)(c+di)}=\overline{(ac-bd)+(ad+bc)i}=$$
$$(ac-bd)-(ad+bc)i=(a-bi)(c-di)=\bar{x}\bar{y}=f(x)f(y).$$

2. *Sea $A=\mathcal{C}(\mathbb{R},\mathbb{R})$ el anillo de las funciones continuas reales de variable real definido en 6.4.1. Podemos ver la composición como el siguiente homomorfismo:*

$$\begin{array}{rccc} \phi\colon & A & \longrightarrow & A \\ & g & \longmapsto & g\circ f. \end{array}$$

Entonces

$$\phi(g+h)(t)=((g+h)\circ f)(t)=(g+h)(f(t))=g(f(t))+h(f(t))=$$
$$(g\circ f)(t)+(h\circ f)(t)=((g\circ f)+(h\circ f))(t)=(\phi(g)+\phi(h))(t),$$

y como esto es para todo $t\in\mathbb{R}$ tenemos que

$$\phi(g+h)=\phi(g)+\phi(h).$$

Igualmente para el resto de condiciones.

■

Veamos ahora las definiciones esenciales para homomorfismos, igual que en grupos pero en anillos:

Definición 6.24. *Sea $f\colon A\longrightarrow B$ un homomorfismo de anillos conmutativos y unitarios. Entonces:*

1. *Llamaremos **núcleo** de f y lo denotaremos $kerf$ al ideal*

$$Kerf=\{x\in A: f(x)=0\}.$$

Es un ideal ya que, si $x,y\in kerf$, $a\in A$, tenemos que

$$f(x+y)=f(x)+f(y)=0+0=0,$$

$$f(ax)=f(a)f(x)=f(a)\cdot 0=0.$$

2. *Llamaremos **imagen** de f y la denotaremos Imf al anillo*

$$Imf=\{y\in B:\ \exists x\in A,\ y=f(x)\}.$$

Es un anillo conmutativo y unitario con las operaciones heredadas de B, ya que si $y = f(x)$, $v = f(u)$, $x, u \in A$, tenemos que

$$y - v = f(x) - f(u) = f(x - u) \in imf,$$

$$y \cdot v = f(x)f(u) = f(xu) \in imf,$$

$$1_B = f(1_A) \in imf.$$

Proposición 6.25. *Sea $f\colon A \longrightarrow B$ un homomorfismo de anillos conmutativos y unitarios. Como $f(1_A) = 1_B \neq 0$, $kerf$ es un ideal propio de A. Además, f es inyectiva si y sólo si $kerf = \{0\}$.*

Demostración: Sea f inyectiva, como $f(0) = 0$, entonces el núcleo ha de reducirse al elemento neutro 0. Recíprocamente, supongamos que $kerf = \{0\}$. Si $x, y \in A$ y tenemos que $f(x) = f(y)$, entonces $f(x-y) = 0$. Esto quiere decir que $x-y \in Kerf$, pero $kerf = \{0\}$ luego $x - y = 0$ y finalmente $x = y$. Y así, f es inyectiva.

□

Observación 6.25.1. *Si $f\colon K \longrightarrow B$ es un homomorfismo de anillos conmutativos y unitarios, y K es un cuerpo, entonces f ha de ser inyectiva. Observar que esto es así ya que al ser $kerf$ un ideal de K distinto de K (ya que $f(1_K) = 1_B$), por* **??** *sólo puede ser $\{0\}$, y así f es inyectiva.*

Ahora, al igual que con grupos, veremos los *Teoremas de Isomorfía*, que funcionan de forma análoga a los de grupos y que también nos serán muy útiles . Antes de eso definamos brevemente los distintos homomorfismos de anillos, también de forma análoga a los de los grupos.

Definición 6.26. *Sea $f\colon A \longrightarrow B$ un homomorfismo de anillos conmutativos y unitarios. Entonces diremos que:*

1. *f es un* ***epimorfismo****, si es una aplicación suprayectiva.*
2. *f es un* ***monomorfismo****, si es una aplicación inyectiva.*
3. *f es un* ***isomorfismo****, si es una aplicación biyectiva.*

De hecho, vamos a desarrollar un poco el concepto de *anillos isomorfos* para entender mejor qué significa que dos anillos lo sean. Ya sabemos que, en álgebra, el hecho de que dos objetos sean isomorfos quiere decir que esencialmente son el mismo, sólo cambian los nombres de sus elementos. Así, dados dos anillos conmutativos y unitarios A y B, diremos que son *isomorfos* cuando existe un isomorfismo $f\colon A \longrightarrow B$. Esto así implica inmediatamente que existe la aplicación inversa $f^{-1}\colon B \longrightarrow A$ y que es también un homomorfismo. Por tanto, si tenemos dos elementos $u, v \in B$, entonces $u = f(x), v = f(y)$ para ciertos $x, y \in A$, éstos son únicos (por ser biyectiva) y así, tenemos que

$$f(x + y) = f(x) + f(y) = u + v.$$

$$f^{-1}(u + v) = f^{-1}(u) + f^{-1}(v) = x + y.$$

Además, cuando dos anillos cualesquiera A y B sean isomorfos, escribiremos $A \simeq B$. También es inmediato comprobar que un isomorfismo f entre dos anillos conmutativos y unitarios A y B induce un isomorfismo de grupos entre $\mathcal{U}(A)$ y $\mathcal{U}(B)$.

Teorema 6.27 (***Primer Teorema de Isomorfía***)**.** *Sea $f\colon A \longrightarrow B$ un homomorfismo de anillos conmutativos y unitarios. Consideremos el diagrama siguiente:*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle \pi}\downarrow & & \uparrow{\scriptstyle i} \\ A/Kerf & \xrightarrow{\quad \bar{f} \quad} & Imf \end{array}$$

con $A/Kerf$ el anillo de clases módulo $Kerf$ y

$$\begin{array}{rccc} \pi\colon & A & \longrightarrow & A/Kerf \\ & x & \longmapsto & x + Kerf, \end{array}$$

la proyección canónica, que es suprayectiva.

$$\begin{array}{rccc} \bar{f}\colon & A/Kerf & \longrightarrow & Imf \\ & x + Kerf & \longmapsto & f(x), \end{array}$$

la aplicación que nos induce, que será biyectiva, es decir, un isomorfismo.

$$\begin{array}{rccc} i\colon & Imf & \longrightarrow & B \\ & f(x) & \longmapsto & f(x) = y, \end{array}$$

la inclusión canónica, que será inyectiva.

Así, en estas condiciones, todas las aplicaciones son homomorfismos y el diagrama es conmutativo, es decir,

$$f = i \circ \bar{f} \circ \pi.$$

Demostración: Veamos que $\bar{f}$

1. está bien definida, y es que si $x + Kerf = y + Kerf$ entonces tenemos que $x - y \in Kerf$ y así $f(x - y) = 0$, pero $f(x - y) = f(x) - f(y)$ y de aquí deducimos que
$$f(x) = f(y),$$
y así $\bar{f}(x + Kerf)$ no depende del representante que escojamos de la clase.

2. es inyectiva. Sean $x, y \in A$ tales que $\bar{f}(x + Kerf) = \bar{f}(y + Kerf)$. Esto quiere decir que $f(x) = f(y)$, y así $f(x) - f(y) = f(x - y) = 0$, luego $x - y \in Kerf$. Así, $x + Kerf = y + Kerf$ y $\bar{f}$ es inyectiva.

3. es suprayectiva. Sea $y \in Imf$, entonces $y = f(x)$ para algún $x \in A$ y así,
$$y = \bar{f}(x + Kerf),$$
y $\bar{f}$ es suprayectiva, es decir, $\forall y \in Imf$ existe un $x + Kef \in A/Kerf$ tal que $\bar{f}(x + Kerf) = y$.

Lo último es claro ya que, dado un $x \in A$, tenemos que

$$f(x) = (i \circ \bar{f} \circ \pi)(x) = i(\bar{f}(\pi(x))) = i(\bar{f}(x + Kerf)) = i(f(x)) = f(x).$$

□

Teorema 6.28 (***Segundo Teorema de Isomorfía***)**.** *Sean $A \subset B$ dos anillos conmutativos y unitarios, e I un ideal de B. Entonces $A + I$ es un subanillo de B que contiene a I. Además, los anillos $(A + I)/I$ y $A/(A \cap I)$ son isomorfos.*

Demostración: Que $A + I$ es subanillo de B es inmediato. Para ver lo segundo consideremos el siguiente homomorfismo:

$$\begin{array}{rccc} f\colon & A & \longrightarrow & (A+I)/I \\ & x & \longmapsto & x + I. \end{array}$$

Su núcleo estará formado por todos los elementos $x \in A$ que también estén en I, es decir, $Kerf = A \cap I$. Además f es suprayectiva, ya que para todo $y \in (A + I)/I$ existen $x \in A$ y $b \in I$ tales que $y = (x + b) + I = x + I = f(x)$. Entonces, por el *Primer Teorema de Isomorfía* 6.27, los anillos $A/(A \cap I)$ y $(A + I)/I$ son isomorfos.

□

Teorema 6.29 (***Tercer Teorema de Isomorfía***)**.** *Sean A un anillo conmutativo y unitario, y J, I ideales de A tales que $J \subset I$. Entonces los anillos $(A/J)/(I/J)$ y A/I son isomorfos.*

Demostración: En este caso consideraremos el siguiente homomorfismo de anillos conmutativos y unitarios:

$$\begin{array}{rccc} f\colon & A/J & \longrightarrow & A/I \\ & x + J & \longmapsto & x + I. \end{array}$$

Evidentemente es suprayectivo y está bien definido, pues $J \subset I$. Ahora, $Kerf = \{a + J : a \in I\} = I/J$. De nuevo, por el *Primer Teorema de Isomorfía* 6.27 tenemos que $(A/J)/(I/J) \simeq A/I$.

□

Ejemplo 6.29.1. *Dos ejemplos conocidos:*

1. *Sea A un anillo conmutativo y unitario, e I un ideal propio de A. Entonces podemos definir una aplicación*

$$\begin{array}{rccc} p\colon & A & \longrightarrow & A/I \\ & x & \longmapsto & x + I, \end{array}$$

   que será siempre un epimorfismo, es decir, suprayectiva.

2. *La conjugación del* ***anillo de los enteros de Gauss****:*

$$\begin{array}{rccc} f\colon & \mathbb{Z}[i] & \longrightarrow & \mathbb{Z}[i] \\ & x & \longmapsto & \bar{x} \end{array}$$

es un isomorfismo. De hecho, su inversa es ella misma, ya que

$$f^2(a+bi) = (f \circ f)(a+bi) = f(a-bi) = a+bi.$$

También lo será cuando nos encontremos en el cuerpo de los complejos $\mathbb{C}$.

■

Finalmente, terminaremos estas generalidades de anillos enunciando y demostrando un resultado más que interesante que se conoce ya de aritmética. Es el *Teorema chino de los restos*. Necesitaremos recordar la noción de ideales comaximales, presentada en 6.18.

Teorema 6.30 (***Teorema chino de los restos.***). *Sea* A *un anillo,* $r \geq 2$ *un número entero e* $I_1, \cdots, I_r$ *ideales de* A *comaximales dos a dos, es decir,* $I_i + I_j = A$ *si* $i \neq j$. *Entonces, se tiene:*

1. $I_1 + (I_2 \cdots I_r) = A$.
2. $I = I_1 \cap \cdots \cap I_r = I_1 \ldots I_r$.
3. *El homomorfismo*

$$\begin{array}{rccc} f\colon & A & \longrightarrow & A/I_1 \times \cdots A/I_r \\ & x & \longmapsto & (x+I_1, \ldots, x+I_r), \end{array}$$

   es sobreyectivo.

4. *Los anillos* A/I *y* $A/I_1 \times \cdots A/I_r$ *son isomorfos.*

Demostración: Veámoslo punto por punto:

1. Lo demostraremos por inducción sobre r, siendo obvio para $r = 2$. Sea $r \geq 3$ y supondremos probado que $I_1 + (I_2 \cdots I_{r-1}) = A$, como $I_1 + I_r = A$ existirán $x_1, y_1 \in I_1$, $x \in I_2 \cdots I_{r-1}$, $y \in I_r$ tales que $1 = x_1 + x$ y $1 = y_1 + y$. Por lo que

$$1 = (x_1+x)(y_1+y) = (x_1y_1 + x_1y + xy_1) + xy \in I_1 + (I_2 \cdots I_{r-1}I_r),$$

   y así $I_1 + (I_2 \cdots I_r) = A$.

2. En el anterior apartado se ha visto que I_1 y $J = I_2 \cdots I_r$ son comaximales, y de 6.18 deducimos que

$$I_1 \cap \ldots \cap I_r = I_1 \cap J = I_1 J = I_1 \cdot (I_2 \cdots I_r) = I_1 \cdots I_r.$$

3. Deducimos de 1. que para cada índice $1 \leq i \leq r$, $I_i + I_1 \cdots I_{i-1} \cdot I_{i+1} \cdots I_r = A$. Por lo tanto, existen $u_i \in I_i$ y $v_i \in I_1 \cdots I_{i-1} \cdot I_{i+1} \cdots I_r$ tales que $u_i + v_i = 1$, para cada $i = 1, \ldots, r$. Así, dados $x_1, \ldots, x_r \in A$, elegimos $x = x_1v_1 + \ldots + x_rv_r \in A$ y tenemos que

$$x + I_i = x_1v_1 + \ldots + x_rv_r + I_i = x_iv_i + I_i = x_iv_i + x_iu_i + I_i = x_i(v_i+u_i) + I_i = x_i + I_i,$$

   donde al pasar a la tercera igualdad x_iu_i aparece porque $u_i \in I_i$. Así, $f(x) = f(x_1 + I_1, \ldots, x_r + I_r)$ y f es sobreyectiva.

4. Se deduce fácilmente que $Kerf = I_1 \cap \cdots \cap I_r = I$, y aplicando el *Primer Teorema de Isomorfía* 6.27 ya está.

□

7. Divisibilidad de anillos

Durante esta sección consideraremos a A como un dominio de integridad.

Definición 7.1. *Sean x, y elementos de A tales que $x \neq 0$. Se dice que x* ***divide a y, que x es un divisor de y, que y es divisible por x ó que y es un múltiplo de*** *x si existe $a \in A$ tal que $y = ax$. Se escribe $x \mid y$. Si x no divide a y se escribe $x \nmid y$.*

En otras palabras, $x \mid y \Leftrightarrow y \in (x)$, ó equivalentemente $(y) \subset (x)$.

Esto nos presenta la divisibilidad como una relación de orden parcial que será inmediata para ideales pero que para entenderla entre elementos habrá que describir la relación de igualdad asociada:

$$x \text{ está relacionado con } y \text{ si } x \mid y \text{ e } y \mid x, \text{ o sea si } (x) = (y).$$

Estas condiciones son equivalentes a:

1. Existe una unidad $a \in \mathcal{U}(A)$ tal que $y = ax$. Esto es así ya que si $(y) = (x)$ tendremos que $y \in (x), x \in (y)$, luego $y = ax$ y $x = by$. Luego $y = aby$ y como A es un dominio de integridad podremos simplificar y obtener $1 = ab$, y así a es unidad.

2. Si $y \in A^*$ no es unidad, denotaremos $div(y)$ el conjunto de todos los divisores de y. Es claro que los conjuntos $y \cdot \mathcal{U}(A)$ y $\mathcal{U}(A)$ están contenidos en $div(y)$. Así, si y no tiene más divisores que las unidades y los productos del propio y por unidades diremos que y es ***irreducible***.

3. Si $y \in A^*$ genera un ideal primo diremos que y es primo. ***Todo elemento primo es irreducible***. Veámoslo.

   Demostración: Sea $y = ax$. Si (y) es primo, $a \in (y)$ ó $x \in (y)$. Si $a \in (y)$ tendremos que $a = zy$, luego $y = zyx$ y $1 = zx$. Así, $x \in \mathcal{U}(A)$ y $a = yx^{-1} \in y \cdot \mathcal{U}(A)$. Análogo si $x \in (y)$.

   □

   El recíproco en general no se cumple, aunque esto lo desarrollaremos más adelante.

Una clase importante de dominios de integridad, en la que la relación de divisibilidad puede ser estudiada con ventaja, es:

7.1. Dominio euclídeo

Definición 7.2. *Diremos que A es un **dominio euclídeo**, escrito DE, si existe una aplicación*

$$\|\cdot\|\colon A \longrightarrow \mathbb{N}$$

con $\mathbb{N}$ el conjunto de los enteros no negativos, y que cumpla:

1. $\|x\| = 0$ *si y sólo si* $x = 0$.
2. $\|xy\| = \|x\| \cdot \|y\|$.
3. *Si $x, y \in A^*$, existe $r \in A$ tal que $y \mid (x - r)$ y $\|r\| < \|y\|$. Esto no viene a ser más que la división de los enteros, donde r es el resto y el elemento $q \in A$ tal que $x - r = qy$ el cociente.*

En un dominio euclídeo se cumple la siguiente propiedad:

Proposición 7.3. *Sea A un dominio euclídeo. Entonces:*

$$\mathcal{U}(A) = \{x \in A : \|x\| = 1\}.$$

Demostración: Lo primero notar que $\|1_A\| = 1$, puesto que $\|1_A\| = \|1_A \cdot 1_A\| = \|1_A\|^2$ y como $\|1_A\| \neq 0$, tenemos que $\|1_A\| = 1$.

Veamos que $\mathcal{U}(A) \subset \{x \in A : \|x\| = 1\}$. Si $x \in A$ tiene inverso x^{-1}, resulta que $\|x\| \cdot \|x^{-1}\| = \|x \cdot x^{-1}\| = \|1_A\| = 1$. Luego necesariamente $\|x\| = 1$ (recordar que son naturales).

Recíprocamente, sea $x \in A$ con $\|x\| = 1$. Entonces $x \neq 0$ y por definición se tiene que $x \mid (1_A - r)$ para un cierto $r \in A$, con $\|r\| < \|x\|$. Como $\|x\| = 1$, sólo puede ser $\|r\| = 0$, luego $r = 0$. Así $x \mid 1_A$ y por tanto se trata de una unidad.

□

Por ejemplo, en el caso de $\mathbb{Z}[i]$, si definimos el módulo de un elemento $z = a+bi \in \mathbb{Z}[i]$ como $\|z\| = a^2 + b^2$ y para calcular sus unidades veamos aquellos que cumplen que $a^2 + b^2 = 1$. Como $a, b \in \mathbb{Z}$, tenemos que uno de ellos es 0 y el otro es ± 1. Por lo que

$$\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}.$$

Proposición 7.4. *En un dominio euclídeo todos los ideales son principales.*

Demostración: Sea I un ideal no nulo de un dominio euclídeo A. Elijamos un $x \in I$ tal que

$$\|x\| = \min\{\|y\| : 0 \neq y \in I\}.$$

Este mínimo existe y es > 0, puesto que es el mínimo de un conjunto no vacío de números naturales positivos. Afirmamos que I está generado por x.

En efecto, sea $y \in I$, $y \neq 0$. Entonces como $x \in A^*$, existirá $r \in A$ tal que $x \mid (y - r)$ y con $\|r\| < \|x\|$. De esto deducimos que $y - r \in (x) \subset I$, y como $y \in I$ e I es ideal, $r \in I$. Pero la minimalidad de $\|x\|$ y la condición de que $\|r\| < \|x\|$ implican que $r = 0$. Así, $y = y - r$ está en (x), y por lo tanto $I = (x)$.

□

Este resultado que acabamos de ver nos dice que todos los dominios euclídeos tienen todos sus ideales generados por un sólo elemento, si definimos a éstos como una nueva clase de dominios habremos encontrado otra estructura que nos facilitará mucho el trabajo con ideales.

7.2. Dominio de ideales principales

Definición 7.5. *Llamaremos* ***dominio de ideales principales****, escrito como* DIP*, a un dominio de integridad en el que todos sus ideales son principales. Todo* DE *es un* DIP*.*

Por ejemplo, tanto $\mathbb{Z}$ como $\mathbb{Z}[i]$ son DIP.

Proposición 7.6. *Sea* A *un* DIP*. Entonces todo elemento irreducible* $a \in A^*$ *genera un ideal maximal.*

Demostración: Sea $I \subset A$ un ideal que contiene al ideal principal (a), generado por el elemento irreducible a. Veamos que ó bien $I = (a)$ ó $I = A$. Pero por ser A un DIP, existirá un $b \in A$ tal que $I = (b)$. En consecuencia, $(a) \subset I = (b)$ y $b \mid a$. Como a es irreducible, tendremos dos opciones:

1. O bien $b = u \cdot a$, con $u \in \mathcal{U}(A)$, y entonces $(a) = (b) = I$.
2. O bien $b \in \mathcal{U}(A)$, y entonces $A = (b) = I$.

□

A continuación pasaremos a dar una definición muy importante, tanto para anillos como para cuerpos, y que nos habla sobre el menor entero tal que multiplicado por el neutro de un anillo/cuerpo nos da el cero.

Definición 7.7 (***Característica de un dominio de integridad.***)**.** *Consideremos de nuevo un dominio* A*. Si* $k \in \mathbb{Z}$*, definimos un elemento* $k \cdot 1_A \in A$*:*

$$k \cdot 1_A = 1_A + \cdots + 1_A \text{ si } k¿0$$

$$k \cdot 1_A = 0 \text{ si } k = 0$$

$$k \cdot 1_A = -((-k) \cdot 1_A) \text{ si } k¡0.$$

Entonces,

$$\begin{array}{rccc} \phi\colon & \mathbb{Z} & \longrightarrow & A \\ & k & \longmapsto & k \cdot 1_A \end{array}$$

es un homomorfismo de anillos. Consideremos su núcleo $Ker\ \phi$*. Entonces pueden darse dos casos:*

1. $ker\ \phi = \{0\}$*. Entonces* $\mathbb{Z} \subset A$ *vía* ϕ*, y diremos que* A *tiene* ***característica*** 0*. Esto ocurre, por ejemplo para* $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}o\mathbb{Z}[i]$*. En este caso el menor entero* k *tal que* $k \cdot 1_A = 0$*, es el* 0*.*

2. *$\ker\phi \neq \{0\}$. Como $\mathbb{Z}/Ker\,\phi \simeq Im\,\phi \subset A$ y A es dominio de integridad, $\mathbb{Z}/\ker\phi$ también lo será, y en así $\ker\phi$ será un ideal primo. Como $\mathbb{Z}$ es un DIP, $\ker\phi = (p)$, con p primo. Diremos entonces que A tiene* ***característica*** *p. De hecho, por el resultado anterior, $\mathbb{Z}/(p)$ es un cuerpo. Además, todo anillo finito tiene característica positiva.*

Definición 7.8. *Sean $x, y \in A \setminus \{0\}$. Diremos que $z \in A$ es:*

1. *Un* ***máximo común divisor*** *(mcd) de x, y si z divide tanto a x como a y, y es múltiplo de cualquier otro divisor de ambos.*
2. *Un* ***mínimo común múltiplo*** *(mcm) dex, y si z es múltiplo de x y de y, y además divide a cualquier otro múltiplo de ambos.*

Observación 7.8.1. *Algunas observaciones respecto a estas definiciones:*

1. *Si z, z' son dos mcd de x, y entonces $z \mid z'$ y $z' \mid z$, luego los elementos difieren en una unidad, es decir, $(z) = (z')$. En este sentido se tiene la unicidad del mcd. Igualmente para el mcm.*
2. *Podemos expresar el mcd en términos de ideales así:*

$$(x) + (y) \subset (z) \subset \bigcap \{I : I \supset (x) + (y),\ I \text{ principal}\}.$$

3. *La descripción del mcm mediante ideales es: z es mcm de x, y si y sólo si*

$$(x) \cap (y) = (z).$$

   En efecto, si z es el mcm, $z \subset (x)$ y $z \subset (y)$, luego se tiene el contenido $(x) \cap (y) \supset (z)$. Pero si $t \in (x) \cap (y)$, entonces t e múltiplo de x y de y, luego $z \mid t$ y $t \in (z)$. Esto da la igualdad. Recíprocamente, si $(x) \cap (y) = (z)$, entonces $x \mid z$, $y \mid z$, y si t es otro múltiplo común, entonces $t \in (x) \cap (y) = (z)$ y $z \mid t$.

4. *En general, el mcd puede no existir, y esto estará relacionado con las propiedades de los elementos irreducibles de A.*

Proposición 7.9. *Sean $x, y \in A \setminus \{0\}$, y supongamos que tienen un mcm z. Entonces $t = xy/z \in A$ y es un mcd de x, y.*

Demostración: Por definición de *mcm*, z divide a xy, luego t es un elemento de A bien definido. Por otra parte, $x \mid z$ e $y \mid z$, luego $z = ax$, $z = by$, con $a, b \in A$.

Se tiene $zx = byx = btz$, y como A es dominio $x = bt$ y $t \mid x$. Análogamente, $t \mid y$. Por otra parte, si u es un divisor común de x e y, entonces $x = cu, y = du$, con $c, d \in A$. Observamos que

$$xy/u = (x/u)y = cy, \quad xy/u = (y/u)x = dx,$$

luego xy/u es múltiplo común de x e y, con lo que z divide a xy/u, y en consecuencia, u divide a $xy/z = t$. Esto prueba que t es múltiplo de cualquier divisor común u de x e y.

□

Proposición 7.10. *Sea A un dominio de integridad, entonces son equivalentes:*

1. *Todo par de elementos no nulos tienen mcm.*
2. *Todo par de elementos no nulos tienen mcd.*

Y se cumple que, si $x, y \in A^*$, entonces

$$mcm(x, y) \cdot mcd(x, y) = xy.$$

Demostración: Que el primero implica el segundo es claro por el lema anterior. Veamos el recíproco. Sean $x, y \in A$, $t = mcd(x, y)$. Entonces

$$z = xy/t = (x/t)y = x(y/t)$$

es múltiplo de x y de y. Consideremos otro múltiplo común u. Entonces

$$tu = mcd(xu, yu) \ (*).$$

En efecto, sea $d = mcd(xu, yu)$. Evidentemente $tu \mid d$ y así $d = tuv$. Entonces tuv divide a xu y a yu, de donde tv divide a x e y, luego tv divide a t y v es unidad. Así, tenemos $(*)$.

Claramente $xy \mid xu$ y $xy \mid tu$, esto es, xy/t divide a u. Así $z = xy/t = mcm(x, y)$, y multiplicando esta igualdad por t queda $zt = xy$.

□

Corolario 7.10.1. *Sea A un dominio de ideales principales. Entonces el mcd y el mcm de dos elementos no nulos cualesquiera de A siempre existe, y se tiene que:*

1. $(x) + (y) = (mcd)$.
2. $(x) \cap (y) = (mcm)$.
3. $xy = mcd \cdot mcm$.

Demostración: Por la hipótesis sobre A, $(x) \cap (y)$ es principal, luego por 7.8.1 (3) existe el mcm y se cumple 2.. Ahora, por 7.9 existe el mcd y se cumple 3. Finalmente, de nuevo por ser A un DIP, $(x) + (y)$ es principal, y de 7.8.1 (2) se sigue 1.

□

Anteriormente vimos que todo elemento primo es irreducible, ahora veremos que dadas unas condiciones también se cumple el recíproco.

Proposición 7.11. *Supongamos que en un dominio de integridad A se cumple cualquiera de las condiciones de 7.10. Entonces todo elemento irreducible de A es primo.*

Demostración: Sean $a \in A$ irreducible e $I = (a)$. Para comprobar que I es primo consideremos $x, y \in A$ con $xy \in I$. Entonces $xy = ab$ con $b \in A$. Por la hipótesis existen

$$\alpha = mcm(y, b)$$

$$\beta = mcd(y, b)$$

y se verifica $\alpha\beta = yb$. Observemos ahora que xy es múltiplo de b y de y, luego $\alpha \mid xy$. En consecuencia, podemos escribir

$$a = \frac{xy}{\alpha} \cdot \frac{\alpha}{b};\ \ \frac{xy}{\alpha}, \frac{\alpha}{b} \in A.$$

Por ser a irreducible existe una unidad $u \in A$ tal que se verifica una de las dos condiciones siguientes:

1. $xy/\alpha = ua$. Entonces $x = u(\alpha/y)a$, con lo que $x \in (a) = I$. (Notar que $y \mid \alpha$, luego $\alpha/y \in A$.)
2. $a/b = ua$. Entonces $y = \alpha\beta/b = u\beta a$ y así $y \in (a) = I$.

□

Proposición 7.12 (***Identidad de Bézout***)**.** *Sean $x, y \in A^*$, y supongamos que generan un ideal principal. Entonces existe $z = mcd(x, y)$ y*

$$z = ax + by$$

con $a, b \in A$.

Demostración: Sea $z \in A$ un generador de $(x) + (y)$. Entonces:

1. $x, y \in (z)$, luego z es un divisor común de x e y.
2. $z = ax + by$ para ciertos $a, b \in A$.

Por último, además, si $t \mid x$ y $t \mid y$, es claro que $t \mid z$. Por lo que tendremos que $z = mcd(x, y)$.

□

Definición 7.13. *Dos elementos $x, y \in A^*$ se denominan **primos entre sí** cuando no comparten más divisores comunes que las unidades, es decir, cuando $mcd(x, y) = 1$.*

Por ejemplo, si tenemos que $1 = ax + by$, con $a, b \in A$, entonces x e y son primos entre sí, pues la condición impuesta significa $1 \in (x) + (y)$ y por 7.8.1 (2) se tiene $1 = mcd(x, y)$.

Con todo esto, hemos visto las nociones básicas de divisibilidad y también se ha podido comprobar que en los dominios de ideales principales se cumple:

1. (P) Todo elemento irreducible es primo.
2. (MC) Siempre existen mcd y mcm.
3. (B) La identidad de Bézout.

A partir de aquí y con esto, vamos a poder definir una nueva estructura algebraica, que presentaremos más adelante, aunque necesitaremos añadir otra propiedad a estas 3 ya conocidas.

7.3. Dominio de factorización única

Proposición 7.14. *Sea A un dominio de ideales principales. Para cada elemento $x \in A^*$ que no es unidad se verifica:*

1. *Existen elementos irreducibles $a_1, \ldots, a_r$ dos a dos primos entre sí, enteros $\alpha_1, \ldots, \alpha_r > 0$ y $u \in \mathcal{U}(A)$ tales que*

$$x = u a_1^{\alpha_1} \ldots a_r^{\alpha_r}.$$

   *Estos a_i se llaman **factores irreducibles** de x.*

2. *Los elementos $a_1, \ldots, a_r$ son únicos, salvo producto por unidades de A, así como los enteros $\alpha_1, \ldots, \alpha_r$.*

Demostración: Veamos primero (2). Sea

$$x = a_1^{\alpha_1} \ldots a_r^{\alpha_r} = b_1^{\beta_1} \ldots a_s^{\beta_s}.$$

Para cada i tenemos $a_i \mid b_1^{\beta_1} \ldots b_s^{\beta_s}$. Como a_i es irreducible, de tenemos que

$$a_i \mid b_{\sigma(i)}$$

para algún $\sigma(i)$. Análogamente

$$b_{\sigma(i)} \mid a_j$$

para algún j. Por tanto, $a_i \mid a_j$, luego a_i y a_j no son primos entre sí, e $i = j$. Así, existe una unidad $u_i \in \mathcal{U}(A)$ con

$$b_{\sigma(i)} = u_i a_i.$$

Se observa que $\sigma(i) \neq \sigma(j)$ si $i \neq j$, pues en otro caso $u_i a_i = u_j a_j$, o sea, $a_j = (u_j^{-1} u_i) a_i$ y se tendría $a_i \mid a_j$ con $i \neq j$. Así, $\sigma \colon i \longrightarrow \sigma(i)$ es inyectiva, y $r \leq s$. Por simetría $r = s$, y σ es una permutación de $\{1, \ldots, r\}$ tal que:

$$b_{\sigma(1)} = u_1 a_1, \ldots, b_{\sigma(r)} = u_r a_r; \;\; u_1, \ldots, u_r \in \mathcal{U}(A).$$

En fin, $\beta_{\sigma(i)} = \alpha_i \quad \forall i$. En efecto,

$$a_i^{\alpha_i} \mid x = u a_1^{\beta_{\sigma(1)}} \ldots a_r^{\beta_{\sigma(r)}},$$

donde $u = u_1^{\beta_{\sigma(1)}} \ldots u_r^{\beta_{\sigma(r)}} \in \mathcal{U}(A)$. Si $\alpha_i > \beta_{\sigma(i)}$, simplificando $a_i^{\beta_{\sigma(i)}}$ obtendríamos

$$a_i \mid a_i^{y_i} \mid u a_1^{\beta_{\sigma(1)}} \ldots a_i^{\beta_{\sigma(i)}} \ldots a_r^{\beta_{\sigma(r)}},$$

pues $y_i = \alpha_i - \beta_{\sigma(i)} \geq 1$. Entonces $a_i \mid a_j$ para algún $i \neq j$, que es absurdo. Tiene que ser $\alpha_i \leq \beta_{\sigma(i)}$, y por simetría se tiene la igualdad.

Pasemos a probar ahora (1). Primeramente, afirmamos que x tiene algún divisor irreducible. Ciertamente, pues de no tenerlo entonces el propio x sería reducible (si no lo fuera sería un divisor irreducible de sí mismo), y tendría algún divisor x_1 con

$(x) \subset (x_1) \subset A$. A su vez x_1 sería reducible, y existiría $x_2 \in A$ con $(x_1) \subset (x_2) \subset A$. Recurrentemente obtendríamos una sucesión $x = x_0, x_1, x_2, \ldots, x_n, \ldots$ tal que

$$(x_0) \subset (x_1) \subset (x_2) \subset \ldots \subset (x_n) \subset \ldots.$$

Y esto no es posible. Para verlo, sea:

$$I = \bigcup_{i \geq 0} (x_i).$$

Entonces I es un ideal:

1. Si $a, b \in I$ es $a \in (x_i), b \in (x_j)$, escribimos $k = maxi, j$ y tenemos $a, b \in (x_k)$, luego $a + b \in (x_k) \subset I$.
2. Si $a \in I, b \in A$, entonces $a \in (x_i)$ para algún i, y $ba \in (x_i) \subset I$.

Como I tiene que ser principal, existe un $z \in A$ con

$$(z) = \bigcup_{i \geq 0} (x_i).$$

Luego $z \in (x_{i_0})$ para algún i_0, con lo que

$$(x_{i_0+1}) \subset I = (z) \subset (x_{i_0}),$$

y así $(x_{i_0+1}) = (x_{i_0})$, que es absurdo.

Sea ahora a_1 un divisor irreducible de x. Entonces

$$x = a_1 x_1, \;\; x_1 \in A.$$

Si x_1 es unidad ya hemos acabado. Si no, x_1 tendrá algún divisor irreducible a_2 y $x_1 = a_2 x_2$, donde o bien x_2 es unidad, y así habremos acabado, o bien x_2 tiene un divisor irreducible a_3. Si después de una cantidad finita de pasos encontramos una unidad $u = u_r \in \mathcal{U}(A)$, será

$$x = a_1 a_2 \ldots a_r u,$$

y agrupando los a_i iguales tendremos la descomposición que buscábamos. Sólo queda ver que este proceso es finito. Si no lo fuera obtendríamos una sucesión

$$(x) \subset (x_1) \subset (x_2) \subset \ldots \subset (x_n) \subset \ldots.$$

Y, como hicimos anteriormente, se tendría $(x_{i_0}) = (x_{i_0+1})$ para cierto i_0, es decir,

$$a_{i_0+1} = x_{i_0}/x_{i_0+1} \in \mathcal{U}(A),$$

lo que es absurdo.

□

Esta factorización que acabamos de describir nos permite establecer un nuevo tipo de anillos que definiremos a continuación:

Definición 7.15. *Un **dominio de factorización única**, escrito DFU es un dominio de integridad en el que se cumple:*

1. *Todo elemento irreducible es primo.*
2. *Todo elemento no nulo que no sea unidad es producto de elementos irreducibles.*

Observación 7.15.1. *Algunas observaciones:*

1. *Que todo elemento no nulo que no sea unidad sea producto de elementos irreducibles no garantiza la unicidad de dicha factorización. Es necesaria también la primera condición, ya que la unicidad se desprende de que ésta se cumple sobre un dominio de ideales principales.*
2. *En un DFU siempre existen mcd y mcm. Efectivamente, puesto que el mcd es el producto de los factores irreducibles comunes elevados al menor exponente y el mcm es el producto de todos los factores irreducibles (comunes y no comunes) elevados al mayor exponente.*
3. *Las relaciones entre las distintas estructuras algebraicas estudiadas se puede resumir en:*

$$Cuerpos \subseteq DE \subseteq DIP \subseteq DFU \subseteq DI \subseteq Anillo.$$

Por ejemplo, las matrices constituyen un anillo pero no un DI, $\mathbb{Z}[\sqrt{-3}]$ es un DI que no es DFU (puesto que $(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$), el anillo de los polinomios con coeficientes enteros $\mathbb{Z}[X]$ es un DFU que no es DIP o $\mathbb{Z}$ es un DE que no es un cuerpo.

*Los anillos $\mathbb{Z}$ y $\mathbb{Z}[i]$ son DE y por tanto DFU. Es precisamente en $\mathbb{Z}$ donde éste resultado se manifiesta como el **teorema fundamental de la Aritmética**: todo número entero positivo n se escribe de modo único como producto de números primos positivos $p_1, \ldots, p_r$ de la forma $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$.*

A continuación veremos todas las propiedades vistas hasta ahora a través de un ejemplo bastante completo:

Ejemplo 7.15.1. *Nos situaremos en el subanillo $A \subset \mathbb{C}$ de los números complejos de la forma $a + b\sqrt{-5}$, $a, b \in \mathbb{Z}$. Lo denotaremos $A = \mathbb{Z}[\sqrt{-5}]$ y efectivamente*

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

A lo largo del ejemplo se usará indistintamente tanto A como $\mathbb{Z}[\sqrt{-5}]$.

Estudiaremos primero las unidades. Sea un elemento $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, entonces $a + b\sqrt{-5} \in \mathcal{U}(\mathbb{Z}[\sqrt{-5}])$ si y sólo si existen $c, d \in \mathbb{Z}$ tales que

$$1 = (c + d\sqrt{-5})(a + b\sqrt{-5}) = (ca - 5db) + (cb + da)\sqrt{-5}.$$

Y esto quiere decir que $ca - 5db = 1$ y $cb + da = 0$. De lo que se obtiene las siguientes soluciones

$$c = \frac{a}{a^2 + 5b^2}, \quad d = \frac{-b}{a^2 + 5b^2}.$$

Esto quiere decir que $(a^2+5b^2) \mid a$ *y que* $(a^2+5b^2) \mid b$*; por lo que* $|b| \geq a^2+5b^2$ *y de esto* $|b| = 0$ *ya que de lo contrario tendríamos que* $a^2+5b^2 \geq 5b^2 > b^2 \geq |b|$*, que es una contradicción. Así* $|b| = 0$ *y* $b = 0$*, y como nuevamente* $|a| \geq a^2 + 5b^2 = a^2$ *entonces* $|a| \leq 1$*. Pero* a *no puede ser* 0 *porque sino también lo sería* $a+b\sqrt{-5}$*, luego* $a = \pm 1$*. Esto deja como posibles soluciones* $(a, b) = (\pm 1, 0)$*. Así,* $\mathcal{U}(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$*.*

Por lo tanto, las unidades de $\mathbb{Z}[\sqrt{-5}]$ *son los elementos* $a+b\sqrt{-5}$ *tales que* $a^2+5b^2 = 1$*. Ahora, definamos una aplicación*

$$\begin{array}{rccc} \phi\colon & A & \longrightarrow & \mathbb{N} \\ & a+b\sqrt{-5} & \longmapsto & a^2+5b^2. \end{array}$$

El haber definido una aplicación así nos puede sugerir que, entonces, A *sea un* DE*, sin embargo no va a ser el caso puesto que no va a cumplir la última de las condiciones vistas cuando definimos los* DE *en 7.2. Esto tiene todo el sentido del mundo ya que, de ser un* DE*, entonces todo elemento irreducible sería primo y veremos más adelante que esto no es así.*

Aunque esta última condición no se cumpla sí lo hace la otra de los DFU*, es decir, todo elemento no nulo que no sea unidad es producto de elementos irreducibles. Para ver esto es suficiente con ver que* A *no contiene sucesiones infinitas de la forma*

$$(x_0) \subset (x_1) \subset (x_2) \subset \ldots \subset (x_n) \subset \ldots.$$

Y efectivamente así es, de no serlo tendríamos $x_i = a_{i+1}x_{i+1}$*, con* $a_{i+1} \notin \mathcal{U}(A)$ *y por tanto* $\phi(a_{i+}) > 1$*, luego* $\phi(x_i) > \phi(x_{i+1})$*. Y como está claro que no puede existir la sucesión de números naturales*

$$\phi(x_0) > \phi(x_1) > \ldots > \phi(x_n) > \ldots,$$

entonces tampoco lo hará

$$(x_0) \subset (x_1) \subset (x_2) \subset \ldots \subset (x_n) \subset \ldots.$$

Además, en $\mathbb{Z}[\sqrt{-5}]$ *no hay unicidad de factorización:*

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

y los elementos $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ *son irreducibles. De lo contrario, si alguno de estos elementos, que denotaremos por* x*, fuera reducible tendríamos* $x = x_1x_2, x_i \notin \mathcal{U}(A)$*, luego* $\phi(x) = \phi(x_1)\phi(x_2)$ *con* $\phi(x_i) > 1$*, donde* $\phi(x) = 4, 9, 6, 6$ *respectivamente. Sea* $\phi(x_i) = a_i^2 + 5b_i^2$*. En* $\mathbb{Z}$ *sí hay unicidad de factorización, luego en cualquiera de los casos* $a_i^2 + 5b_i^2 = 2$ *ó* 3 *para* $i = 1, 2$*, lo cual es imposible.*

Por todo esto, A *no es un* DFU*, sin embargo hemos visto que sí cumple con la condición de que todo elemento no nulo que no sea unidad es producto de elementos irreducibles, así que entonces debe fallar la otra condición: hay elementos irreducibles que no son primos. Esto es así, por ejemplo* $1+\sqrt{-5}$*.*

Por lo que acabamos de ver es claro que habrá al menos dos elementos $x, y \in A$ que no tienen mcd, y tiene sentido porque no es DFU. Busquemos un par que lo cumpla: para eso sean

$$x = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$
$$y = 2 \cdot (1 + \sqrt{-5}).$$

Supongamos que existe $z = mcd(xy)$. Al ser 2 y $1 + \sqrt{-5}$ divisores tanto de x como de y existirán entonces $u, v \in A$ tales que $z = 2u = (1 + \sqrt{-5})v$. Como 2 y $1 + \sqrt{-5}$ son primos entre sí, u no puede ser unidad, así que

$$\phi(u) > 1.$$

También tenemos que $z \mid x$, $z \mid y$, luego $x = zx_1$, $y = zy_1$ con $x_1, y_1 \in A$. Conocemos los valores de $\phi(x)$ y $\phi(y)$ de antes, luego

$$4 \cdot 9 = \phi(x) = \phi(z)\phi(x_1) = 4\phi(u)\phi(x_1).$$
$$4 \cdot 6 = \phi(y) = \phi(z)\phi(y_1) = 4\phi(u)\phi(y_1).$$

De aquí sacamos que $9 = \phi(u)\phi(x_1)$, $6 = \phi(u)\phi(y_1)$ y como $\phi(u) > 1$, necesariamente

$$3 = \phi(u) = a^2 + 5b^2, \;\; u = a + b\sqrt{-5}.$$

Esto es absurdo.

Veamos ahora que la identidad de Bézout no se cumple en $\mathbb{Z}[\sqrt{-5}]$. Por ejemplo, si tomamos $x = 2$, $y = 1 - \sqrt{-5}$ entonces x e y son primos entre sí luego $1 = mcd(x, y)$. Sin embargo, vamos a comprobar que no existen $u, v \in A$ tales que $1 = ux + vy$. Supongamos lo contrario y lleguemos a una contradicción: sean $u = a + b\sqrt{-5}$, $v = c + d\sqrt{-5}$ entonces

$$1 = 2a + c + 5d,$$
$$0 = 2b - c + d$$

y de aquí sumándolas

$$1 = 2a + 2b + 6d = 2(a + b + 3d).$$

Esto último es imposible ya que $a, b, d \in \mathbb{Z}$.

Por último veamos que no todo par de elementos de A tienen mínimo común múltiplo. Por ejemplo, si escogemos nuevamente el mismo par de antes $x = 2$, $y = 1 - \sqrt{-5}$ ya sabemos entonces que su mcd es 1, luego por 7.10 su mcm ha de ser xy. Pero claro,

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

luego el mcm dividirá a 6. Luego existirá un $u \in A$ tal que $6 = uxy = (a + b\sqrt{-5}) \cdot 2 \cdot (1 - \sqrt{-5})$. Operando, obtenemos

$$6 = 2a + 10b,$$
$$0 = -2a + 2b.$$

De esto deducimos que $6 = 12b$, que es imposible teniendo en cuenta que $b \in \mathbb{Z}$, luego no tienen solución entera.

■

7.4. Anillos de restos

A lo largo de la presente sección se llevará a cabo el estudio de los cocientes del anillo de los números enteros $\mathbb{Z}$. Pero antes de eso veamos algunas propiedades del anillo en el que nos encontramos y que ya conocemos gracias a todo lo visto en las secciones anteriores:

1. Un número entero p es *irreducible* si y solo si es primo, si y sólo si genera un ideal maximal y si y sólo si $\mathbb{Z}/(p)$ es un cuerpo.
2. El anillo $\mathbb{Z}$ es un *dominio de factorización única* (en particular es un DE). Todo entero $n > 1$ se escribe de manera única como sigue:

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s},$$

   con p_i números primos conocidos como factores primos de n.
3. El conjunto de los números primos es infinito. Para verlo, dado un primo p, si definimos el número $n = p! + 1$ y consideramos un factor primo cualquiera p' de n, entonces p' es estrictamente mayor que p (y así sucesivamente). Si no lo fuera, entonces necesariamente $p' \mid p! = n - 1$ y así, como p' divide tanto a n (por ser un factor suyo) y a $n - 1$, $p' \mid (n - (n - 1)) = 1$, y esto es absurdo.

Con esto ya podemos pasar a describir los cocientes de $\mathbb{Z}$:

Definición 7.16. *Sea n un número entero. Llamaremos* ***anillo de restos módulo*** *n al cociente $\mathbb{Z}/(n)$. Como $(n) = (-n)$ al ser -1 unidad, podremos suponer que $n \geq 0$. Si $n = 0$ el cociente es el propio $\mathbb{Z}$ y si $n = 1$ entonces $(n) = \mathbb{Z}$ y no tendría sentido considerar el cociente. Luego $n > 1$.*

Sea $k \in \mathbb{Z}$. Denotaremos $[k]_n$, ó simplemente $[k]$ si no es necesario especificar, la clase de k

$$k + (n) = \{k + qn : q \in \mathbb{Z}\}.$$

Para obtener otro representante de la clase de k, $[k]$, dividiremos por n y tendremos $k = qn + r$. El resto ha de ser positivo o nulo y esto plantea un problema si $k < 0$ (porque recordemos que k es un entero), bastará dividir por exceso en vez de por defecto y ya está. Con esto $k - r = qn \in (n)$, por lo tanto $[k] = [r]$.

Por ejemplo, en $\mathbb{Z}/(3)$ si $k = -8$ tenemos que $-8 = -3 \cdot 3 + 1$, luego -8 pertenece a la clase de $[1]$ y así la clase de $[-8] = [1] = \{\dots, -11, -8, -5, -2, 1, 4, 7, 10, \dots\}$ (notar que en $\mathbb{Z}/(3)$ la clase de 8 no es la de -8).

Consideremos ahora dos restos $0 \leq r < s < n$. Si $[r] = [s]$, entonces $s - r \in (n)$, y así $n \mid (s - r)$, y en particular $n \leq s - r$. Esto es absurdo porque $s - r \leq s < n$. Por lo tanto, en $\mathbb{Z}/(n)$ cada clase de equivalencia está determinada por un ***único*** *representante r tal que $0 \leq r < n$, es decir,*

$$\mathbb{Z}/(n) = \{[0], [1], \dots, [n-1]\}.$$

En particular, $\mathbb{Z}/(n)$ tiene n elementos. $[0]$ y $[1]$ son el cero y el uno de $\mathbb{Z}/(n)$. Es evidente que si sumamos n veces la clase del uno tenemos: $[1] + \dots + [1] = [n] = [0]$,

y que $-[1] = [-1] = [n-1]$*. Con esto recordemos que las igualdades entre clases las podemos escribir como*

$$k \equiv l \bmod n$$

y viene a decir que $[k] = [l]$*, es decir, que* $k - l = qn$ *con un* $q \in \mathbb{Z}$*.*

Si nos situamos, por ejemplo, en $\mathbb{Z}/(5)$*, tenemos que* $[3]+[1] = [4]$*, que* $[2]+[0] = [2]$ *y que* $[4]+[3] = [2]$*, además* $[2]\cdot[2] = [4]$*,* $[4]\cdot[1] = [4]$ *y* $[2]\cdot[4] = [3]$*; esto por poner sólo unos ejemplos. En* $\mathbb{Z}/(6)$*, sin embargo,* $[2]\cdot[4] = [2]$ *y* $[4]+[3] = [1]$*.*

Pasemos a ver ahora cómo son los ideales de un anillo de restos:

Definición 7.17. *Sea* $n > 1$*. Ya vimos en 6.12 que los ideales de* $\mathbb{Z}/(n)$ *están en biyección con los ideales* $I \subset \mathbb{Z}$ *que contienen* (n)*. Sea entonces un ideal* $I = (m) \subset \mathbb{Z}$ *tal que* $(m) \supset (n)$*. Entonces* $m \mid n$*, y así los ideales de* $\mathbb{Z}/(n)$ *están en biyección con aquellos ideales generados por los divisores positivos de* n *(positivos porque* $I = (-m) = (m)$*).*

Y veamos también los homomorfismos entre anillos de restos:

Definición 7.18. *Vamos a centrarnos en 5 puntos:*

1. *No existe ningún homomorfismo de anillos unitarios de la forma* $f\colon \mathbb{Z}/(n) \longrightarrow \mathbb{Z}$ *con* $n > 0$*. De no ser así tendríamos que*

$$0 = f([0]) = f([1]\overbrace{+\ldots+}^{n}[1]) = f([1])\overbrace{+\ldots+}^{n}f([1]) = 1\overbrace{+\ldots+}^{n}1 = n,$$

   que es absurdo.

2. *La identidad es el único homomorfismo de anillos unitarios* $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$*. En efecto, sea* $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ *uno de ellos, como* $f(1) = 1$ *entonces, dado un entero* k*,*

$$f(k) = f(1\overbrace{+\ldots+}^{k}1) = f(1)\overbrace{+\ldots+}^{k}f(1) = 1\overbrace{+\ldots+}^{k}1 = k,$$
$$f(-k) = -f(k) = -k.$$

   Y este homomorfismo es la identidad: $f = id_{\mathbb{Z}}$*.*

3. *Nos situamos ahora en los homomorfismos de* $\mathbb{Z}$ *en* $\mathbb{Z}/(n)$ *con* $n > 1$*. Sea* k *un entero positivo. Entonces*

$$f(k) = f(k) = f(1\overbrace{+\ldots+}^{k}1) = f(1)\overbrace{+\ldots+}^{k}f(1) = [1]\overbrace{+\ldots+}^{k}[1] = [k],$$
$$f(-k) = -f(k) = -[k] = [-k].$$

   Este es el único homomorfismo de anillos unitarios $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}/(n)$*.*

4. *Veamos ahora qué ocurre en los homomorfismos del tipo* $f\colon \mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$*. Sea* f *uno de ellos, entonces:*

$$[0]_n = f([0]_m) = f([1]_m\overbrace{+\ldots+}^{m}[1]_m) = f([1]_m)\overbrace{+\ldots+}^{m}f([1]_m) =$$
$$[1]_n\overbrace{+\ldots+}^{m}[1]_n = [m]_n.$$

Y esto quiere decir que $m \equiv 0 \bmod n$, luego $n \mid m$. Por lo tanto, n ha de dividir a m.

5. *Si $n > 1$ y $n \mid m$ entonces existirá un único homomorfismo de anillos unitarios $f\colon \mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$, y además será un epimorfismo. Dicho homomorfismo lo podremos definir como:*

$$\begin{array}{rccc} f\colon & \mathbb{Z}/(m) & \longrightarrow & \mathbb{Z}/(n) \\ & [k]_m & \longmapsto & [k]_n \end{array}$$

El cuál ya sabemos que existe por el punto anterior, y está bien definido porque si $k \equiv l \bmod m$ entonces $m \mid (k-l)$, y como $n \mid m$ tendremos entonces que $n \mid (k-l)$, es decir, que $k \equiv l \bmod n$.

Podemos dar una versión alternativa del teorema chino de los restos:

Teorema 7.19 (***Teorema Chino del resto***)**.** *Si a, b son enteros primos entre sí, entonces se tendrá un isomorfismo de anillos unitarios*

$$\mathbb{Z}(ab) \simeq \mathbb{Z}/(a) \times \mathbb{Z}/(b).$$

Demostración: Definimos

$$\begin{array}{rccc} f\colon & \mathbb{Z}/(ab) & \longrightarrow & \mathbb{Z}/(a) \times \mathbb{Z}/(b) \\ & [k]_{ab} & \longmapsto & ([k]_a, [k]_b). \end{array}$$

Está bien definido, pues si $k \equiv l \bmod ab$ entonces $ab \mid (k-l)$ y así tanto a como b dividen a $k-l$ y tenemos que $k \equiv l \bmod a$ y $k \equiv l \bmod b$.

Que es homomorfismo es evidente. Es inyectiva, sea k un entero tal que $f([k]_{ab}) = 0$, entonces $([k]_a, [k]_b) = (0,0)$ y así

$$k \equiv 0 \bmod a$$

$$k \equiv 0 \bmod b.$$

Esto quiere decir que $a \mid k$ y $b \mid k$, luego $mcm(a,b) \mid k$; pero como a y b son primos entre sí tenemos que $mcm(a,b) = ab$. Por lo tanto, $ab \mid k$, es decir,

$$k \equiv 0 \bmod ab.$$

Luego $kerf = \{0\}$ y f es inyectiva.

Como es una aplicación inyectiva entre dos conjuntos finitos de igual cardinal ab entonces también será biyectiva, y así isomorfismo.

□

Veamos las unidades de los anillos de restos:

Proposición 7.20. *Sean $n > 1$ y $k \in \mathbb{Z}$. Entonces son equivalentes:*

1. $[k] \in \mathcal{U}(\mathbb{Z}/(n))$.

2. $mcd(k, n) = 1$.

3. $[k] \neq 0$ *y no es divisor de cero en* $\mathbb{Z}/(n)$.

Demostración: Si $[k]$ es unidad, existirá un $l \in \mathbb{Z}$ tal que

$$[1] = [l] \cdot [k] = [lk],$$

y así $1 - lk \in (n)$, es decir, $1 - lk = mn$ para algún $m \in \mathbb{Z}$. Con esto,

$$1 = lk + mn,$$

y por tanto, $mcd(k, n) = 1$. Tenemos así la primera implicación. Haciendo lo mismo al revés tenemos la implicación inversa y en cualquier anillo 1. $\Rightarrow$ 3.

Veamos ahora que 3. $\Rightarrow$ 2., es decir, dado $mcd(k, n) = d > 1$ entonces o bien $[k] = [0]$ o bien es un divisor de cero. Como

$$n \mid \left(\frac{k}{d}\right) n = k \left(\frac{n}{d}\right),$$

o bien $[k] = [0]$, ó $[k]$ es divisor de cero, ó $\left[\frac{n}{d}\right] = [0]$, pero en este último caso se tendría que $n \mid \frac{n}{d}$ luego $d = 1$, lo cuál contradice la hipótesis.

□

Con este último resultado del capítulo llegamos a un concepto que ya vimos antes:

Definición 7.21. *Dado un m entero positivo. Denotaremos por $\phi(m)$ el número de enteros k que cumplen:*

1. $0 < k \leq m$.

2. $mcd(k, m) = 1$.

Esta aplicación ϕ ya la conocemos, es la llamada ***función de Euler****.*

Sobre los anillos la *función de Euler* puede tomar una interpretación diferente: si $n > 1$, entonces $\phi(n)$ es el número de unidades de $\mathbb{Z}/(n)$. En efecto, por la proposición anterior

$$\mathcal{U}(\mathbb{Z}/(n)) = \{[k] : 0 < k < n,\ mcd(k, n) = 1\}.$$

Ya sabemos que, dado un primo $p > 1$, $\phi(p) = p - 1$. Esto está relacionado con el hecho de que si p es primo entonces el cociente $\mathbb{Z}/(p)$ es un cuerpo. Entonces:

$$\mathcal{U}(\mathbb{Z}/(p)) = \{[1], \ldots, [p-1]\}.$$

8. Anillos de polinomios

Definición 8.1. *Sea A un anillo conmutativo y unitario. Diremos que X es una* ***indeterminada*** *ó* ***variable*** *si sus potencias son algebraicamente independientes, es decir,*

$$\sum_{i=0}^{n} a_i X^i = 0,\ \ a_i \in A \Longleftrightarrow a_0 = \ldots = a_n = 0 \forall n.$$

*Un **polinomio en** X con coeficientes en A es una suma finita*

$$f(X) = a_0 + a_1X + \ldots + a_nXn,\ a_0, a_1, \ldots, a_n \in A$$

a la que se puede agregar un número finito y arbitrario de ceros.

Definición 8.2. *Dados polinomios $f(X) = \sum_{i=0}^{n} a_iX^i$ y $g(X) = \sum_{j=0}^{m} b_jX^j$ y $s = max\{n, m\}$ definimos su **suma** por*

$$f(X) + g(X) = \sum_{k\geq 0}^{s}(a_k + b_k)X^k = (a_0 + b_0) + \ldots + (a_k + b_k)X^k + \ldots + (a_s + b_s)X^s,$$

*y su **producto** como*

$$f(X) \cdot g(X) = \sum_{k=1}^{n+m} c_kX^k,\ \ c_k = \sum_{i+j=k} a_ib_j,$$

teniendo en cuenta que sii algún coeficiente a_i ó b_j no aparece es 0.

*Así, construimos un nuevo anillo $A[X]$ cuyo **cero** es $0 = 0X + \ldots + 0X^n$, y cuyo **uno** es $1 = 1 + 0X + \ldots + 0X^n$. Diremos que $A[X]$ es el **anillo de polinomios en la variable X con coeficientes en A**.*

Observación 8.2.1. *Este nuevo anillo, $A[X]$, contiene a A ya que los elementos de A son polinomios de la forma $a = a + 0X + \ldots + 0X^n$.*

Definición 8.3. *Dados dos anillos $A \leq B$, si $f(X) \in A[X]$ y $b \in B$, al elemento $f(b) \in B$ se le suele llamar **valor** de $f(X)$ en b. De igual forma, al conjunto*

$$A[b] = \{f(b) : f(X) \in A[x]\},$$

*de todos ellos lo llamaremos **anillo de valores de** b en $A[X]$. Si el valor $f(b) = 0$ se dice que b es una **raíz** de $f(X)$.*

Si $X_1, \ldots, X_n$ son variables independientes, el **anillo de polinomios** $A[X_1, \ldots, X_n]$ en las variables $X_1, \ldots, X_n$ con coeficientes en A entonces podemos definir de manera inductiva

$$A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n].$$

A partir de ahora supondremos que A es un dominio de integridad.

Definición 8.4. *Si $0 \neq f(X) = \sum_{i=0}^{n} a_nX^n \in A[X]$, el **grado** de $f(X)$ es el mayor entero $n \geq 0$ tal que $a_n \neq 0$ y se denota $\delta(f)$. Los polinomios de grados $0, 1, 2, 3, 4$ los llamaremos constantes, lineales, cuadráticos, cúbicos y cuárticos respectivamente.*

*Diremos que un a_iX^i es el término de grado i. El de grado 0 se denomina **término independiente**. El coeficiente del término de mayor grado lo llamaremos **coeficiente director de** $f(X)$. Diremos que un $f(X)$ es mónico si su coeficiente director es una unidad del anillo.*

Ahora, dado $0 \neq f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ el grado