Estructuras Algebraicas

Pablo Pallàs

31 de mayo de 2023

Índice

1. Introducción

Imaginemos un conjunto cualquiera, con sus respectivos elementos y luego usemos una operación, normalmente suma o producto. Si juntamos estos dos objetos tan simples (un conjunto y una operación) habremos creado sin darnos cuenta algo que ya conocemos como *estructura algebraica*. Esto que se acaba de explicar en unas pocas líneas llevó mucho más tiempo a los matemáticos del que pueda parecer, y cuando hablamos de mucho tiempo estamos hablando de siglos. Se sabe que incluso pueblos y civilizaciones anteriores a la griega ya conocían y hacían uso de las matemáticas, y la aparición y posterior definición y axiomatización de las estructuras algebraicas no tuvo lugar hasta el siglo XIX, así que estamos hablando de casi 5000 años.

Concretamente la primera piedra la pone un joven matemático noruego, hijo de un pastor luterano, llamado Niels Henrik Abel. Seguramente el nombre sea de sobra conocido por cualquier estudiante de matemáticas, y no es algo extraño teniendo en cuenta el enorme calibre de sus aportaciones. Como se ha dicho puso la primera piedra, con el permiso de Cauchy y Ruffini, para que puediera aparecer lo que hoy día se conoce como *álgebra abstracta*, también conocida como *álgebra moderna*. Como ya sabemos, cuando hablamos de *álgebra* en líneas generales nos referimos al estudio de las ecuaciones y sus soluciones, pero ¿a qué nos referimos cuando hablamos de álgebra moderna?

Ya desde los tiempos de los griegos se conocían los principales métodos de sustitución y resolución de ecuaciones de primer grado, incluso sabían resolver lo que hoy conocemos como ecuaciones de segundo grado, aunque las expresiones

$$ax^2 + bx + c = 0, \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

son modernas. Para la formalización del estudio de las ecuaciones cuadráticas y la aparición de estas expresiones hubo que esperar unos cuantos siglos, hasta el siglo IX d.C. cuando el matemático persa Abu Abdallah Muḥammad Ibn Mūsā Al-Jwarizmī publica el primer tratado considerado genuinamente algrebaico, el *Compendio de cálculo por reintegración y comparación*. De hecho el álgebra como la conocemos hoy no aparece hasta su llegada, para hacernos una idea de la importancia de la irrupción del gran matemático nacido en lo que hoy conocemos como Irán. De su nombre se deriva la palabra *algoritmo*, y de hecho la palabra *álgebra* proviene de *al-ŷabr*, que aparece en el título original del tratado mencionado anteriormente. Para la aparición y formalización del estudio de las ecuaciones de tercer y cuarto grado con sus respectivas fórmulas (bastante más complejas que en el caso de las cuadráticas) tuvimos que esperar al Renacimiento italiano con los *Niccolò Tartaglia, Gerolamo Cardano y Lodovico Ferrari* (una historia muy interesante de retos, traiciones y desprestigio entre ellos), aunque ya hicieron aportes y hay antecedentes de otros matemáticos que contribuyeron a su estudio anteriormente, como los italianos *Scipione del Ferro ó Fibonacci*, el indio *Bhaskara II* o el chino *Liu Hui*, quién en el siglo III ya publicó un tratado que contenía el estudio de algunos métodos para resolver ecuaciones cúbicas. El problema llegó al intentar dar una fórmula para las

ecuaciones de quinto grado.

Durante muchos años se intentó llegar a una fórmula que diera las soluciones de una ecuación quíntica, sin éxito. Este arduo trabajo frustró a muchos matemáticos durante toda la época moderna y pre-decimonónica, entre ellos Lagrange. Éste empleó como herramienta las permutaciones de ráices de polinomios para intentar abordar el problema, lo cúal fue muy interesante y supuso el comienzo de la utilización directa del concepto de permutación, que veremos en las siguientes páginas lo importante que es y los avances que supuso en la formación del álgebra moderna. Álgebra que poco tardaría en aparecer, en estos momentos, ante la frustración de Lagrange y toda la comunidad matemática de la época llegaría un Paolo Ruffini que, en contra de lo que por entonces se intentaba demostrar, estaba convencido de la imposibilidad de llegar a una fórmula que diera las soluciones de la ecuación de quinto grado como sí se hizo con las de tercer y cuarto grado. Fue de hecho él quién acuñó el término *permutazioni*, que hasta entonces simplemente se definían como ordenaciones, así como la forma en la que una permutación se transformaba en otra. Comenzó a partir de un conjunto de permutaciones, y estudió sus propiedades y cómo dos de éstas podían combinarse para dar una tercera. Observó algo intersante: que el orden en el que éstas se combinaban era importante, no producían la misma tercera permutación, es decir, si pensamos esa combinación de permutaciones como una operación entonces diríamos que esa operación no es conmutativa. Esto era bastante novedoso en ese momento, pues contrasta con lo que ocurre con las operaciones clásicas de la suma y la multiplicación ó producto. Ruffini utilizó estas *estructuras* para demostrar que no existía ninguna fórmula para las ecuaciones quínticas, sin embargo no encontró respuesta ni visibilidad a sus estudios por parte de Lagrange ni tampoco parecía que nadie en esa época tuviese interés alguno en esa nueva álgebra de permutaciones que había construido Ruffini. Nadie hasta que apareció Cauchy. Fue él quien visibilizó, a su manera, el trabajo de Ruffini y estableció la notación moderna de ciclos, de producto de permutaciones y también enunció resultados acerca de la conjugación de las mismas, algo que también veremos en las siguientes páginas. ES aquí cuando retomamos lo primero que hemos dicho, puesto que el siguiente paso lo da Abel, el que puso la primera piedra como dijimos. Y el siguiente paso, aunque realmente fue el mismo, lo daría otro famoso matemático conocido por sus grandísimos aportes y su épica historia de romance, traición y muerte a una edad temprana, hablamos de *Evariste Galois*. No se conocieron nunca, y sin embargo compartieron mucho más que descubrimientos, ambos mandaron sus aportes al también matemático y secretario por aquel entonces de la Academia de las Ciencias Joseph Fourier, y en ambos casos se reportaron dichos aportes a Cauchy, y también en ambos casos el resultado fue vano puesto que no les dió, al menos al principio, la importancia que merecían.

Pero, ¿qué fue lo que estos dos jóvenes matemáticos aportaron? ¿qué hicieron para que acabaran siendo reconocidos como fundadores del álgebra moderna?, de hecho ¿qué es el álgebra moderna?. Pues bien, lo que supuso realmente un salto cualitativo con respecto a todo lo que se hizo antes fue considerar estas *estructuras* formadas por las permutaciones y sus combinaciones, y centrar la atención en el estudio de las propiedades de éstas estructuras. Lo que hicieron Galois y Abel fue introducir todo un vocabulario matemático entero completamente nuevo que podía describir

bastante bien estas estructuras de permutaciones. Fue así como nació el concepto de *grupo*, y fueron las permutaciones sobre las que primero se definió esta estructura, que ya acuñarle un apellido y hablar así de *estructuras algebraicas*, conectando así con lo que se ha dicho al principio. Así, la diferencia fundamental entre el álgebra que nosotros conocemos del instituto, y que se desarrollo durante siglos, y el álgebra moderna es que en ésta última el objeto de estudio ya no son las ecuaciones (lineales, cuadráticas, etc.) sino estructuras algebraicas. La estructura de grupo fue la primera en aparecer, y supuso el que es con toda seguridad el avance más importante en la historia de las matemáticas.

Por lo tanto, el paso del álgebra convencional al álgebra absrtracta supuso pasar de estudiar ecuaciones a estudiar operaciones abstractas que definimos entre los elementos de un conjunto. Curiosamente la teoría de conjuntos no se formalizó hasta finales del s.XIX, casi cien años después.

A parte del grupo, existen otras estructuras algebraicas como anillos, dominios de integridad, cuerpos, módulos, o los espacios vectoriales. Todas ellas combinan distintas operaciones que definimos sobre unos conjuntos específicos y que cumplen una serie de propiedades.

2. Grupos

2.1. Generalidades

Supongamos que G es un conjunto no vacío. Entonces definimos una **operación binaria** en G como una aplicación $G \times G \longrightarrow G$. Usaremos esta operación:

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

y notar que no todas las operaciones binarias van a ser de interés para nuestros propósitos. Para que lo sean definiremos el concepto de ***grupo***.

Definición 2.1. *Diremos que G es un **grupo** con una operación $\cdot$ y lo denotaremos $(G, \cdot)$ si se satisfacen las siguientes condiciones:*

I. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\forall x, y, z \in G$.

II. *Existe un elemento $1 \in G$, que denotaremos e, tal que $e \cdot x = x \cdot e = x$. Este elemento lo denominaremos **elemento neutro**.*

III. $\forall x \in G$ *existe* $y \in G$ *tal que* $x \cdot y = y \cdot x = e$. *A este elemento lo denominaremos **elemento inverso** de x.*

*A esta operación se le suele llamar **producto**.*

Si G es un grupo, el elemento neutro es único, ya que si tenemos $e, e' \in G$ dos elementos neutros de G entonces

$$e = e \cdot e' = e'.$$

También el elemento inverso de un $x \in G$ cualquiera es único, ya que si $y, z \in G$ son inversos de x entonces

$$y = y \cdot e = y \cdot (x \cdot z) = (y \cdot x) \cdot z = e \cdot z = z.$$

Al inverso de un $x \in G$ lo denotaremos por x^{-1} y al producto lo podremos denotar por xy en vez de $x \cdot y$, con $x, y \in G$.

Definición 2.2. *Diremos que un grupo G es **finito** si G es un conjunto finito. En ese caso, llamaremos **orden** de G a su número de elementos, y lo denotaremos por $|G|$.*

Ejemplo 2.2.1. *Algunos ejemplos de grupos:*

1. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos con la suma usual. También lo son $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con la multiplicación usual.*

2. *Dado un conjunto no vacío Ω, consideramos S_Ω el conjunto de las aplicaciones biyectivas $\alpha \colon \Omega \longrightarrow \Omega$. Si $\alpha, \beta \in S_\Omega$ podemos componerlas y $\alpha \circ \beta \in S_\Omega$, así S_Ω es un grupo con la operación*

$$\alpha\beta = \alpha \circ \beta.$$

A este grupo lo denominaremos ***grupo simétrico*** *sobre Ω. Si Ω tiene n elementos, entonces hay $n!$ aplicaciones biyectivas $\Omega \longrightarrow \Omega$, por lo que $|S_\Omega| = n!$. Cuando $\Omega = \{1, 2, \ldots, n\}$ entonces escribiremos S_n.*

Este tipo de grupos los estudiaremos en detalle más adelante.

3. *Dado $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o en general cualquier cuerpo, entonces el conjunto $GL_n(K)$ de matrices $n \times n$ con coeficientes en K y cuyo determinante es no nulo es un grupo conocido como* ***grupo general lineal****.*

4. *Consideremos el siguiente subconjunto de los números complejos*

$$C = \{a + bi \in \mathbb{C} : a^2 + b^2 = 1\},$$

formado por los elementos de la circunferencia de radio 1. Entonces C es un grupo con la multiplicación de números complejos. Es lo que conocemos como ***grupo circular****. Si tenemos un n 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 $\xi = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ es también un grupo con la misma multiplicación, de un tipo que veremos más tarde conocido como ***grupo cíclico****.*

■

En general, dado un grupo G, no será cierto que $xy = yx$ para cualesquiera $x, y \in G$. Por ejemplo, en S_3, si $\alpha, \beta \in S_3$ con $\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1$, $\beta(1) = 2, \beta(2) = 1, \beta(3) = 3$, entonces $\alpha\beta \neq \beta\alpha$. Aquellos grupos G en los que sí se cumpla la igualdad, es decir $xy = yx \ \forall x, y \in G$, los denominaremos **grupos abelianos**.

Cuando trabajemos con grupos abelianos será habitual emplear la notación aditiva y escribiremos $x + y$ en lugar de xy, $-x$ en lugar de x^{-1} y el elemento neutro será 0.

Proposición 2.3. *Dado un grupo G tenemos:*

1. *Dados $x, y \in G$, si $xy = e$ entonces $x = y^{-1}$, $y = x^{-1}$. En particular, $(xy)^{-1} = y^{-1}x^{-1}$.*

2. *La aplicación*

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

es una biyección.

3. *Dado un $g \in G$, 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: Veamos:

1. Si $xy = 1$ entonces $x^{-1} = x^{-1}e = x^{-1}(xy) = y$, y análogo con y^{-1}. Ahora, como $(xy)(y^{-1}x^{-1}) = xex^{-1} = e$, de la primera parte ya se tiene.

2. Veamos que la aplicación 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, dado un $z \in G$ tenemos que z es el inverso de z^{-1} y también es suprayectiva.

3. Veamos que la aplicación
$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & xg \end{array}$$
es biyectiva. Si $xg = yg$, multiplicando por g^{-1} a la derecha tenemos que $x = y$ y así es inyectiva. Si $z \in G$ entonces existirá un elemento $zg^{-1} \in G$ por ser G grupo y la aplicación manda zg^{-1} a z y es suprayectiva también. Para ver la otra la demostración es completamente análoga.

□

Una vez definida una estructura algebtaica cualquiera siempre nos interesaremos por su subestructura. Esto es particularmente relevante en *Teoría de grupos.*

Definición 2.4. *Un* ***subgrupo*** *H de G, denotado $H \leq G$, es un subconjunto no vacío $H \subseteq G$ tal que $xy \in H$ para todos $x, y \in H$ y $x^{-1} \in H$ para todo $x \in H$. Es decir, que también es un grupo con la operación de G: la asociatividad se sigue de la de G, que $xy \in H$ para cualesquiera $x, y \in H$ quiere decir que la operación es binaria y como $x^{-1} \in H$ entonces $xx^{-1} = 1 \in H$.*

Ejemplo 2.4.1. *El subconjunto $SL_n(K)$ de matrices de determinante 1 con coeficientes en K es un subgrupo de $GL_n(K)$ conocido como* ***subgrupo especial lineal****.*

■

Observar que un grupo G siempre tiene al menos los subgrupos, $\{1\}$ y el propio G. Son los conocidos como **subgrupos triviales**. Los subgrupos $H \leq G$ tales que $H \neq G$, son los llamados subgrupos **propios**.

Veamos ahora la caracterización de los subgrupos:

Proposición 2.5. *Sea G un grupo y sea H un subconjunto no vacío de G. Entonces $H \leq G$ si y sólo si $xy^{-1} \in H$ para cualesquiera $x, y \in H$.*

Demostración: Supongamos que $H \leq G$ y sean $x, y \in H$. Entonces $y^{-1} \in H$ y $xy^{-1} \in H$ por definición. Recíprocamente, supongamos que $xy^{-1} \in H$ $\forall x, y \in H$. Eligiendo cualquier $h \in H$ tenemos que $1 = hh^{-1} \in H$. Luego $y^{-1} = 1y^{-1} \in H$ $\forall y \in H$. Finalmente, si $x, y \in H$ entonces $xy = x(y^{-1})^{-1} \in H$. Así, H es grupo.

□

Ejemplo 2.5.1. *Otro ejemplo podría ser el caso de los números enteros $\mathbb{Z}$. Sabemos que $\mathbb{Z}$ es un grupo con la suma usual, nos preguntamos ahora cómo son sus subgrupos.*

Es fácil comprobar que, dado un $n \in \mathbb{Z}$ cualquiera, los subconjuntos de $\mathbb{Z}$ de la forma

$$n\mathbb{Z} = \{nx : x \in \mathbb{Z}\},$$

conforman todos los subgrupos posibles de $\mathbb{Z}$. Basta ver que si $a, b \in n\mathbb{Z}$ entonces $a - b \in n\mathbb{Z}$, ya que si $a, b \in n\mathbb{Z}$ entonces $a = nx$ y $b = nx'$, con $x, x' \in \mathbb{Z}$, y $a - b = nx - nx' = n(x - x') \in n\mathbb{Z}$.

Notar que si tenemos un $p \in n\mathbb{Z}$, éste será de la forma $p = nx$, para un $x \in \mathbb{Z}$ cualquiera, es decir, que n dividirá a p (en capítulos posteriores veremos con más detalle el concepto de divisibilidad).

■

Definición 2.6. *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**. Igualmente también podremos definir su **intersección** como*

$$H \cap K = \{x : x \in H \wedge x \in K\}.$$

Si tenemos dos subgrupos cualesquiera H y K de G está claro que $H \cap K$ es subgrupo también. Sin embargo, en general HK no lo será. Para que lo sea ha de cumplirse la siguiente condición:

Proposición 2.7. *Sean $H, K \leq G$. Entonces $HK \leq G$ si y sólo si $HK = KH$.*

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 $h = h_1h_3 \in H$.

□

Ejemplo 2.7.1. *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 que utilizamos 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 $d = mcd(m, n)$ (más adelante veremos que este resultado se conoce como la identidad de Bézout):

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:

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

tendremos $d = (cu)a + (cv)b = c(ua + vb)$ 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 $mcd(m, n) = 1$, tenemos $m\mathbb{Z} + n\mathbb{Z} = 1\mathbb{Z}$ 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 $mcd(m, n) = 1$.

■

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 2.8. *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 2.8.1. *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 muy importantes e interesante, los *grupos cíclicos*, y que estudiaremos detalladamente más adelante.

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 2.9. *Dado H un subgrupo de un grupo G, llamaremos* ***centralizador*** *de H en G a*

$$C_G(H) = \{x \in G : xg = gx \ \forall g \in H\}.$$

Al caso particular de $H = G$, es decir, al centralizador de G en G lo denotaremos por $Z(G)$ y lo llamaremos ***centro*** *de G. Así,*

$$Z(G) = \{x \in G : xg = gx \ \forall g \in G\}.$$

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 es no vacío. Sean $x, y \in C_G(H)$, $g \in H$. Como $x \in C_G(H)$, $xg = gx$. Como $y \in C_G(H)$, $g^{-1} \in H$, $yg^{-1} = g^{-1}y$. Por lo tanto,

$$(xy^{-1})g = x(y^{-1}g) = x(g^{-1}y)^{-1} = x(yg^{-1})^{-1} = x(gy^{-1}) = (xg)y^{-1} = (gx)y^{-1} = g(xy^{-1})$$

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

□

Tanto el centralizador como el centro de un grupo necesitan de un subgrupo para poder definirse, y forman sendos subgrupos para un grupo G cualquiera, sin embargo lo que vamos a ver a continuación no necesita definirse sobre un subgrupo, con un simple conjunto basta.

Antes de eso necesitaremos definir el concepto de *conjugado*, que también se aplica sobre conjuntos en general:

Definición 2.10. *Si S es un subconjunto no vacío de un grupo G y $g \in G$, se llama* ***conjugado de*** *S* ***por*** *g al conjunto*

$$S^g = \{gxg^{-1} : x \in S\}$$

Diremos que $y \in S^g \Leftrightarrow g^{-1}yg \in S$. Ya que si $y \in S^g \Rightarrow y = gxg^{-1} \Rightarrow g^{-1}yg = x$, $x \in S$.

Definición 2.11. *Dado X un subconjunto no vacío de un grupo G, llamaremos* ***normalizador*** *de X en G a*

$$N_G(X) = \{g \in G : X^g = X\},$$

que además es un subgrupo de G.

Demostración: Ya sabemos que $X^1 = X$, por lo que $1 \in N_G(X)$ y así $N_G(X)$ es no vacío. Por otro lado, si $g, f \in N_G(X)$, $X^{gf^{-1}} = (X^g)^{f^{-1}} = X^{f^{-1}}$ pues $g \in N_G(X)$. Además, $X = X^1 = X^{ff^{-1}} = (X^f)^{f^{-1}} = X^{f^{-1}}$, ya que $f \in N_G(X)$. Tenemos entonces que $X^{gf^{-1}} = X$, luego $gf^{-1} \in N_G(X)$.

□

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

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

$$C_G(g) = \{x \in G : xg = gx\}$$

y, es obvio que

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

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

Definición 2.12. *Si $H \leq G$ y $x \in G$, llamamos a*

$$Hx = \{hx : h \in H\}$$

***clase a derecha** (o **coclase a derecha**) de x módulo H. Análogamente, a*

$$xH = \{xh : h \in H\}$$

*lo llamamos **clase a izquierda** (o **coclase a izquierda**) de x módulo H.*

En general, aunque ambos conjuntos contienen al elemento x, se tiene que $xH \neq Hx$. Más adelante veremos qué ocurre cuando estos conjuntos coinciden.

Proposición 2.13. *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 2.3 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 $xH = yH$. El recíproco es evidente.

□

El resultado anterior es completamente análogo para las clases a derecha.

Con esto, vamos a comprobar que la relación en G definida por: dados $x, y \in G$, entonces $x \sim_H y \iff xH = yH$ es una relación de equivalencia, de hecho la clase de equivalencia de $x \in G$ es xH, es decir, una clase (o coclase) a izquierda. Luego las coclases, tanto a izquierda como a derecha, forman una partición de G. Así, G es unión disjunta de estas clases:

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

con R un conjunto de representantes de las clases de equivalencia.

Con esto, podemos definir las siguientes relaciones de equivalencia:

Definición 2.14. *Sea G un grupo y H un subgrupo de G. Llamaremos $\sim_H$ y $\sim^H$ a las siguientes relaciones en G:*

$$x \sim^H y \text{ si y sólo si } xy^{-1} \in H$$
$$x \sim_H y \text{ si y sólo si } x^{-1}y \in H$$

Tanto $\sim_H$ como $\sim^H$ son relaciones de equivalencia.

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

1. Si $x \in G$, $x^{-1}x = 1 \in H$ luego $x \sim_H x$.
2. Si $x \sim_H y$ entonces $x^{-1}y \in H$, luego $(x^{-1}y)^{-1} \in H$, y esto es $y^{-1}x \in H$ así que $y \sim_H x$.
3. Si $x \sim_H y$, y $y \sim_H z$, entonces se tiene $x^{-1}y \in H$, $y^{-1}z \in H$ y así $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ por lo que $x \sim_H z$.

□

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

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

Análogo con $\sim^H$,

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

Notar que en este último caso tomamos los h de la forma ax^{-1} cuando la relación $\sim^H$ 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 e igual da hacer $x \sim^H a$ que $a \sim^H x$.

Definición 2.15. *A los conjuntos de estas clases los llamaremos* ***conjuntos cocientes*** *definidos por las respectivas relaciones de equivalencia (a izquierda o derecha). Los denotaremos:*

$$G/\sim_H = \{xH : x \in G\},$$
$$G/\sim^H = \{Hx : x \in G\}.$$

Proposición 2.16. *Sea $H \leq G$. Entonces:*

$$card(G/\sim_H) = card(G/\sim^H).$$

Demostración: Veamos que la aplicación

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

es biyectiva.

1. Veamos primero que Ψ está *bien definida*, es decir, si $xH = yH$ entonces $Hx^{-1} = Hy^{-1}$. En efecto, si $xH = yH$, entonces tenemos que $x \sim_H y$, es decir, $x^{-1}y \in H$. 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 $y^{-1} \sim^H x^{-1}$ y por tanto $Hy^{-1} = Hx^{-1}$.
2. Veamos ahora que es *inyectiva*. Sean xH, $yH \in G/\sim_H$. Si $\Psi(xH) = \Psi(yH)$, entonces $Hx^{-1} = Hy^{-1}$, luego $y^{-1} \sim^H x^{-1}$ 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 $x \sim_H y$ o lo que es lo mismo: que $xH = yH$. Así Ψ es inyectiva.
3. Veamos que es *suprayectiva*. Si $Hx \in G/\sim^H$, como $x^{-1}H \in G/\sim_H$ 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

$$card(G/\sim_H) = card(G/\sim^H).$$

□

Si tenemos que estos conjuntos de coclases son finitos (y por tanto de igual cardinal por el resultado que acabamos de ver) entonces:

Definición 2.17. *Dado $H \leq G$, llamamos* ***índice*** *de H en G, y lo denotamos por $[G : H]$, al número de elementos de $G/\sim_H$ (el mismo que $G/\sim^H$). Es decir, el número de coclases a izquierda (ó a derecha).*

$$[G : H] = card(G/\sim_H) = card(G/\sim^H).$$

Ejemplo 2.17.1. *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 $\sim_H$, que son las mismas que respecto $\sim_{m\mathbb{Z}}$, serán de la forma

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

Veamos que

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

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 $x \sim_{m\mathbb{Z}} r$, es decir, $x + m\mathbb{Z} = r + m\mathbb{Z}$, lo que prueba la igualdad. Además las clases son todas distintas, es decir, los elementos del segundo miembro son distintos, pues si $k + m\mathbb{Z} = l + m\mathbb{Z}$, con $0 \leq k, l \leq m - 1$, entonces $l \sim_{m\mathbb{Z}} k$, 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.

■

Teorema 2.18 (***Teorema de Lagrange***)**.** *Sea $H \leq G$. Si G es finito, entonces $|H|$ divide a $|G|$ y*

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

Demostración: Ya sabemos que

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

y que G es la unión disjunta de estas coclases a izquierda , cuyo número es $[G : H]$. Basta ver que todas estas clases a izquierda tienen cardinal $|H|$, pero esto ya lo vimos en 2.3 cuando vimos que la aplicación que manda $g \longmapsto xg$ es biyectiva.

□

Notar que, al ser grupos finitos podemos poner la anterior expresión como

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

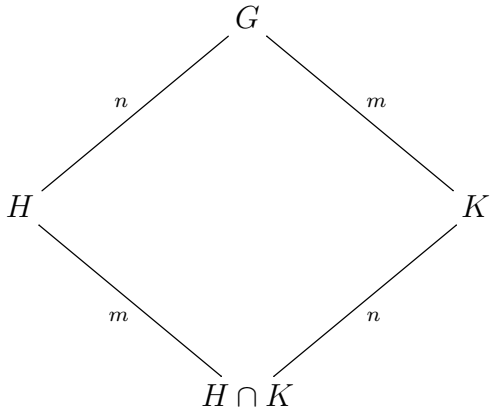
Notar también que, si tenemos $H \leq K \leq G$ entonces, aplicando dos veces el *Teorema de Lagrange* tenemos

$$[G : H] = [G : K][K : H],$$

es lo que se conoce como ***transitividad del índice***.

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, se tiene 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, después de ver el siguiente resultado será interesante volver a revisarlo.

Proposición 2.19. *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 de la forma $h_i k$, 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 $hk_1 \in HK$, tendremos que $h = h_i x$, con un i cualquiera, y $x \in H \cap K$. Así, $hk = h_i x k_1 = h_i(xk_1)$, con $xk_1 \in K$, haremos $xk_1 = k$. Ahora, supongamos que $h_i k = h_j k'$, con $1 \leq i, j \leq m$, $k, k' \in K$. Entonces, $h_j^{-1} h_i = k' k^{-1} \in H \cap K$. Por 2.13 tenemos que $h_i(H \cap K) = h_j(H \cap K)$. Pero 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 de la forma $h_i k$ 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.

Volvamos ahora al diagrama en diamante antes dibujado. Si lo observamos, teniendo en cuenta lo que acabamos de ver y que habíamos definido $G = HK$, 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 $[G : K]$.

Ejemplo 2.19.1 (***El grupo cuaternión.***). *Consideremos los ocho símbolos siguientes:*

$$Q = \{1, -1, i, j, k, -i, -j, -k\}$$

y una operación $Q \times Q \longrightarrow Q$ que tiene a 1 por elemento neutro, cumple la propiedad asociativa, la regla de los signos que todos conocemos (por ejemplo $i(-k) = -(ik)$) y

$$\begin{aligned} &ij = k, \;\; ji = -k \\ &jk = i, \;\; kj = -i \\ &ki = j, \;\; ik = -j \\ &i^2 = j^2 = k^2 = -1 \end{aligned}$$

Con esto, está claro que Q es un grupo de orden 8. Sólo queda demostrar que tiene elemento inverso.

Como se cumple la regla de los signos tenemos que $(-1)^2 = 1$, luego $o(-1) = 2$ y -1 es su propio inverso. Como $i^2 = -1$, resulta que $(-i)^4 = (-1)^4 i^4 = i^4 = (-1)^2 = 1$, luego el orden de i $o(i) = o(-i) = 4$, y así $i^{-1} = i^3$ ya que $ii^3 = i^4 = 1$, además $(-i)^{-1} = -i^3$ ya que $-i(-i)^3 = (-i)^4 = 1$.

Análogamente, $o(j) = o(-j) = 4$ y $o(k) = o(-k) = 4$ y $j^{-1} = j^3$, $k^{-1} = k^3$, $(-j)^{-1} = -j^3$, $(-k)^{-1} = -k^3$. Luego todos los elementos tienen inverso y así Q es un grupo.

Veamos ahora cuáles son los subgrupos de Q. Evidentemente, $\{1\}$ y Q lo son y por el Teorema de Lagrange los demás han de tener orden 2 ó 4. Como -1 es el único elemento de orden 2 de Q $\{1, -1\}$ es el único subgrupo de orden 2. Si H es un subgrupo de orden 4, deberá contener algún elemento x que no sea el 1 ó el -1. Entonces necesariamente $o(x) = 4$ y como H es de orden 4 tendremos que $H = \langle x \rangle$. Además, como $-x = (-1)x = x^2 x = x^3 \in \langle x \rangle$ y $x = (-1)(-x) = (-x)^2(-x) = (-x)^3 \in \langle -x \rangle$, los subgrupos de orden 4 de Q serán $\langle i \rangle$, $\langle j \rangle$ y, $\langle k \rangle$.

*A este grupo Q lo llamaremos **grupo cuaternión**. Además estará generado por i y j, es decir, $Q = \langle i, j \rangle$ ya que*

$$\begin{aligned} &i = i, \;\; ij = k \\ &j = j, \;\; i^3 j = i^2 ij = (-1)k = -k \\ &i^0 = 1, \;\; i^3 = i^2 i = (-1)i = -i \\ &i^2 = -1, \;\; i^2 j = (-1)j = -j. \end{aligned}$$

Y así, se tiene que

$$Q = \{1, i, i^2, i^3, j, ij, i^2 j, i^3 j\}.$$

Este grupo además se suele presentar como el generado por las siguientes matrices:

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

■

Dentro de la ***Teoría de grupos***, un concepto fundamental es el de subgrupo *normal*. Antes habíamos mencionado que, dado un subgrupo H de un grupo G cualquiera y un elemento $x \in G$, en general no se cumplía $xH = Hx$. Veamos ahora qué ocurre en caso de que sí.

Definición 2.20. *Un subgrupo N de G se dice **normal** si*

$$xN = Nx,$$

para todo $x \in G$. En ese caso, escribiremos $N \trianglelefteq G$. También denotaremos por

$$G/N = \{gN : g \in G\}$$

al conjunto de las clases a izquierda de G módulo N. Si el conjunto G/N es finito, tenemos que

$$|G/N| = [G : N].$$

Notar que todo grupo posee al menos dos subgrupos normales, $1 \trianglelefteq G$, $G \trianglelefteq G$. NOtar también que el conjunto G/N puede estar formado igualmente por las clases a derecha, Ng, al ser el subgrupo N normal.

Definición 2.21. *Un grupo G cuyos únicos subgrupos normales sean $\{1\}$ y él mismo se dice que es **simple**.*

Teorema 2.22 (***Criterio de normalidad***)**.** *Sea N un subgrupo de G. Entonces son equivalentes:*

1. $N \trianglelefteq G$.
2. $xNx^{-1} = N \ \forall x \in G$.
3. $xNx^{-1} \subseteq N \ \forall x \in G$.

Demostración: Veamos primero que 1. $\Rightarrow$ 2., para ello notemos que si $y \in xNx^{-1}$ entonces $x^{-1}yx = n \in N$. Como $yx = xn \in xN = Nx$ existirá algún $n' \in N$ tal que $yx = n'x$, y simplificando tendremos que $y = n' \in N$, luego $xNx^{-1} \subseteq N$. Como esto es válido para todo $x \in G$, en particular si aplicamos este contenido para x^{-1} tenemos que $x^{-1}N(x^{-1})^{-1} = x^{-1}Nx \subseteq N$. Así, $N = xx^{-1}Nxx^{-1} = x(x^{-1}Nx)x^{-1} \subseteq xNx^{-1}$ y tenemos la igualdad.

Es evidente que 2. $\Rightarrow$ 3., así que veamos que 3. $\Rightarrow$ 1. Sabiendo que $xNx^{-1} \subseteq N$ $\forall x \in G$, lo aplicamos a x^{-1} y tenemos nuevamente que $N \subseteq xNx^{-1}$ $\forall x \in G$, así, tenemos la igualdad (2.) y de aquí sacamos que $xN = Nx$ y N es normal.

□

Ejemplo 2.22.1. *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 $GL_2(\mathbb{R})$:

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

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 2.23. *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 $G/\sim_H$ como $G/\sim^H$ tienen 2 elementos. Entonces, dado un $g \in G$, puede ocurrir que:

1. Si $g \in H$. En tal caso, $g^{-1}1 = g^{-1} \in H$ (por ser H subgrupo) y así $g \sim_H 1$, luego $gH = 1H = H$. Y como $g1^{-1} = g \in H$, entonces $g \sim^H 1$ y así, $Hg = H1 = H$. Por lo tanto,
$$gH = Hg.$$

2. Si $g \notin H$, $gH \neq H$. Como $G/\sim_H$ tiene dos elementos, tendremos que $G = H \sqcup gH$ (unión disjunta). Pero si $g \notin H$, también se cumplirá $H \neq Hg$. Y como $G/\sim^H$ también tiene dos elementos, tenemos $G = H \sqcup Hg$ (unión disjunta).

   Por lo tanto, $gH = G \setminus H = Hg$, 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 $g \notin H$.

□

Proposición 2.24. *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

$$Z(G) = \{x \in G : xg = gx\ \ \forall g \in G\}$$

y es subgrupo de G tal y como vimos en 2.9.

Basta probar que $H^g \subseteq H$ para cada $g \in G$. Sea $x \in H^g$. Así $g^{-1}xg = h \in H$, luego $x = ghg^{-1}$. Como $h \in H \subseteq Z(G)$, $gh = hg$ y así $x = hgg^{-1} = h \in H$.

□

Definición 2.25. *Si H y K son subgrupos de un grupo G decimos que K es un* ***subgrupo conjugado*** *de H si existe $g \in G$ tal que $K = H^g$.*

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

Proposición 2.26. *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*

$$\begin{array}{rccc} \varphi\colon & G/\sim_N & \longrightarrow & \Sigma \\ & gN & \longmapsto & H^g \end{array}$$

   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 $K = H^g$, $K^{g^{-1}} = (H^g)^{g^{-1}} = H$.
2. Comencemos por demostrar que φ está bien definida:

   Si $gN = fN$, entonces $g^{-1}f \in N$, luego $H^{g^{-1}f} = H$ y así $H^g = (H^{g^{-1}f})^g = H^f$. Veamos ahora que es inyectiva:

   Si $H^g = H^f$ se tiene $H^{g^{-1}f} = (H^f)^{g^{-1}} = (H^g)^{g^{-1}} = H$, luego $g^{-1}f \in N$ y $gN = fN$. Como la sobreyectividad es evidente, queda demostrado.
3. Es claro ya que
$$card\,\Sigma = card(G/\sim_N) = [G : N]\,.$$

□

Definición 2.27. *Si H es un subgrupo de un grupo G, se llama* ***corazón*** *de H a*

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

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

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

Sea $x \in K(H)^f$, tenemos que ver que $x \in H^g$ para cada $g \in G$. Pero $f^{-1}xf \in K(H) \subseteq H^{g^{-1}f}$ (ya que $g^{-1}f$ es un elemento de G), luego $g^{-1}f(f^{-1}xf)(g^{-1}f)^{-1} \in H$, y por lo tanto $g^{-1}xg \in H$ y $x \in H^g$.

□

Los subgrupos normales son importantes porque nos permiten construir un nuevo tipo de grupo.

Proposición 2.28. *Supongamos que $N \trianglelefteq G$. El conjunto G/N de las clases a izquierda módulo N es un grupo con la operación de G*

$$(xN)(yN) = xyN,$$

con $x, y \in G$. El elemento neutro del grupo G/N es N y $(xN)^{-1} = x^{-1}N$ para todo $x \in G$.

Demostración: Tenemos que

$$(xN)(yN) = x(Ny)N = x(yN)N = xyN.$$

Luego es una operación binaria.

Veamos que la operación está bien definida: sean $xN = x'N$, $yN = y'N$, veamos que $xyN = x'y'N$. Por 2.13, $x^{-1}x' \in N$, $y^{-1}y' \in N$. Ahora $(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}x^{-1}x'yy^{-1}y' = y^{-1}(x^{-1}x')y(y^{-1}y') \in N$. Nuevamente por 2.13 se tiene.

Como $N = 1N$, por lo primero tenemos que

$$(xN)N = xN = N(xN)$$

y así es el elemento neutro de G/N. También tenemos que

$$(xN)(x^{-1}N) = N = (x^{-1}N)(xN), \quad \forall x \in G.$$

□

Definición 2.29. *Dado $N \trianglelefteq G$, llamaremos **grupo cociente** de G por N al grupo G/N.*

Notar que en un grupo abeliano G, todo subgrupo H va a cumplir que $xH = Hx$, por lo que en un grupo abeliano todos sus subgrupos son normales.

Proposición 2.30. *Sea $N \trianglelefteq G$ y $H \leq G$. Entonces $HN \leq G$.*

Demostración: Como N es subgrupo normal:

$$NH = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = HN.$$

Aplicamos 2.7 y ya está.

□

Proposición 2.31. *Sea $N \trianglelefteq G$, sean $H, K \leq G$ tales que $H \trianglelefteq K$. Entonces HN es subgrupo normal de KN.*

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

En particular NH es subgrupo de NK, pues $NH \subseteq NK$. Si $x \in NH$ escribiremos $x = nh$, $n \in N$, $h \in H$. 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:

Veamos ahora 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.

□

Ejemplo 2.31.1. *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*

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

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

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

■

Veamos ahora una clase especial de grupos, los conocidos como *grupos cíclicos*. Ya hemos hablado antes de los generadores de un grupo, bien pues los grupos cíclicos son aquellos que están generados por un sólo elemento, repasemos las potencias y el concepto de grupo generado por un elemento:

Dado un n entero positivo y $x \in G$, tenemos que

$$x^n = x \underbrace{\ldots}_{n} x, \quad x^{-n} = x^{-1} \underbrace{\ldots}_{n} x^{-1}.$$

También convenimos que $x^0 = 1$. Si G es un grupo abeliano escribiremos

$$nx = x\underbrace{+\ldots+}_{n}x, \quad (-n)x = (-x)\underbrace{+\ldots+}_{n}(-x), \quad 0x = 0.$$

También es claro que

$$x^{n+m} = x^n x^m, \quad (x^n)^m = x^{nm}.$$

Definición 2.32. *Si consideramos un grupo G y un $x \in G$, entonces*

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

es un subgrupo de G que lo denominaremos ***subgrupo generado por*** *x. Es claro que si H es un subgrupo de G que contiene a x, entonces $\langle x \rangle \subseteq H$.*

Notar que, dado un grupo G y un $x \in G$, si estamos utilizando la notación aditiva entonces:

$$\langle x \rangle = \{kx : k \in \mathbb{Z}\}.$$

Definición 2.33. *Diremos que un grupo G es* ***cíclico*** *si existe un $x \in G$ tal que*

$$\langle x \rangle = G.$$

A este elemento x lo llamamos ***generador*** *de G. En general, un grupo cíclico puede tener varios elementos generadores. Además, a un grupo cíclico de orden n se le suele denotar C_n.*

Notar que, por ejemplo

$$\mathbb{Z} = \{1n \wedge 1(-n) : n \in \mathbb{N}\} = \langle 1 \rangle,$$

es un grupo cíclico infinito. O también el grupo visto al principio

$$C_n = \langle \xi \rangle, \quad \xi = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right),$$

es un grupo cíclico finito de orden n. Notar también que *los grupos cíclicos son abelianos*, ya que dados dos elementos $y, z \in G$ cíclico entonces $yz = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = zy$.

Estudiemos ahora los subgrupos de un grupo cíclico finito $\langle x \rangle$ de orden n.

Proposición 2.34. *Dado un grupo G cíclico y $H \leq G$. Entonces H es cíclico.*

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 $x^p = (x^k)^q \in \langle x^k \rangle$.

□

Por ejemplo, los subgrupos de $\mathbb{Z}$ son cíclicos y son de la forma

$$m\mathbb{Z} = \{mz : z \in \mathbb{Z}\} = \langle m \rangle.$$

El siguiente resultado ya lo habíamos tenido en cuenta cuando hablamos de los subgrupos, pero ahora lo formalizamos:

Corolario 2.34.1. *Sea H un subconjunto no vacío de $\mathbb{Z}$. Entonces $H \leq \mathbb{Z}$ si y sólo si existe un único entero no negativo d tal que $H = d\mathbb{Z}$. Además, si $e \in \mathbb{Z}$, entonces $d\mathbb{Z} \subseteq e\mathbb{Z}$ si y sólo si e divide a d.*

Demostración: Si $H = d\mathbb{Z}$, ya sabemos que H es subgrupo de $\mathbb{Z}$. Recíprocamente, si $H \leq \mathbb{Z}$, por el resultado anterior existirá un $d \in \mathbb{Z}$ tal que $H = d\mathbb{Z}$. Como $d\mathbb{Z} = (-d)\mathbb{Z}$ podemos elegir $d \geq 0$. Finalmente, $d\mathbb{Z} \subseteq e\mathbb{Z}$ si y sólo si $d \in e\mathbb{Z}$ si y sólo si e divide a d.

□

Corolario 2.34.2. *Sean $0 \neq a, b \in \mathbb{Z}$. Entonces:*

1. *Existe un único entero positivo $d \in \mathbb{Z}$ tal que*

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

   Además, $d = mcd(a, b)$.

2. *Si $d = mcd(a, b)$, entonces $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Demostración: Lo primero ya está probado en el ejemplo 2.7.1.

Si un entero positivo n divide a a/d y a b/d, entonces nd divide a a y a b. Entonces es claro que nd divide a d (por ser éste el mcd) y de aquí $n = 1$. Esto prueba 2.

□

Al principio definimos el orden de un grupo como el número de elementos que contiene, análogo al cardinal en los conjuntos. Ahora veremos que los elementos también tienen orden:

Definición 2.35. *Sea G un grupo y $x \in G$. Si no existe ningún entero positivo n tal que $x^n = 1$ decimos entonces que el **orden** de x es **infinito**. En caso contrario, diremos que el **orden** de x es **finito** y denominaremos **orden** de x al menor entero positivo n tal que $x^n = 1$. Lo escribiremos como $o(x) = n$ ó también $|x| = n$.*

Teorema 2.36. *Sea G un grupo y $x \in G$ de orden n. Entonces:*

1. *Si m es un entero, $x^m = 1$ si y sólo si n divide a m.*

2. *$\langle x\rangle = \{1, x, x^2, \ldots, x^{n-1}\}$ y $|\langle x\rangle| = n$. En particular, el orden de x coincide con el del subgrupo que genera.*

3. *Si $0 \neq m$ es un entero, entonces*

$$o(x^m) = \frac{n}{mcd(n,m)}.$$

En particular, x^m genera $\langle x\rangle$ si y sólo si n y m son coprimos.

4. *Para cada divisor d de n, $\langle x\rangle$ tiene un único subgrupo de orden d. Este es $\langle x^{n/d}\rangle$.*

Demostración: Veamos:

1. Si $m = np$ es múltiplo de n, $x^m = x^{np} = (x^n)^p = 1$. Recíprocamente, si m no es múltiplo de n, $m = np + r$, $1 \leq r \leq n-1$ por el algoritmo de la división, luego $x^m = x^{np+r} = (x^n)^p x^r = 1^p x^r = x^r \neq 1$.

2. Sea n el menor natural que cumple $x^n = 1$. Si probamos que

$$\langle x\rangle = \{1, x, x^2, \ldots, x^{n-1}\}$$

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

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

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

3. Llamaremos $d = mcd(n,m)$ y veamos que n/d es el menor entero positivo tal que $(x^m)^{n/d} = 1$.

Para comenzar,

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

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

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

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

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

4. Si d divide a n, tenemos que $\langle x^{n/d} \rangle$ es un subgrupo de orden d por los apartados anteriores. Supongamos ahora que $H \leq \langle x \rangle$ tiene orden d. Entonces H es cíclico por 2.34 y deducimos que existe un entero s tal que $H = \langle x^s \rangle$. Ahora, por el apartado 2. tenemos que

$$1 = (x^s)^{o(x^s)} = (x^s)^{|H|} = (x^s)^d = x^{sd},$$

y por tanto n divide a sd por el apartado 1. Se sigue que n/d divide a s. Por tanto, $x^s \in \langle x^{n/d} \rangle$ y así, $H = \langle x^s \rangle \subseteq \langle x^{n/d} \rangle$. Como ambos conjuntos tienen el mismo número de elementos, deben coincidir.

□

Corolario 2.36.1. *Sea $G \neq \{1\}$ un grupo finito. Entonces 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 primo, entonces G no tiene subgrupos propios por el *Teorema de Lagrange*. Supongamos ahora que G no tiene subgrupos propios. Sea $1 \neq x \in G$, entonces $\langle x \rangle = G$. Si p es un número primo que divide a $|G|$ entonces G tiene un subgrupo H de orden p por 2.36. Luego $G = H$ tiene orden p. Por último, como en un grupo abeliano todos sus subgrupos son normales ya está.

□

Este resultado que acabamos de ver tiene sentido porque el orden de un grupo siempre es un entero positivo, y éstos se pueden descomponer en un producto de factores primos tal y como veremos en la parte de anillos, por lo que siempre habrá un primo que lo divida.

Ya hemos analizado $\mathbb{Z}$ pero no sus cocientes. Si n es un entero, el grupo cociente $\mathbb{Z}/n\mathbb{Z}$ es un objeto matemático de interés. Ya sabemos que si $x, y \in \mathbb{Z}$ entonces $x + n\mathbb{Z} = y + n\mathbb{Z}$ si y sólo si $x - y \in n\mathbb{Z}$ si y sólo si n divide a $x - y$. Esto lo escribiremos como $x \equiv y \mod n$ y es la base de la conocida como *aritmética modular*.

Proposición 2.37. *Si $n \geq 1$, entonces*

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

es un grupo cíclico de orden n.

Demostración: Como $\mathbb{Z}$ es abeliano, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ y el grupo cociente $\mathbb{Z}/n\mathbb{Z}$ está bien definido. Si $x, y \in \mathbb{Z}$, entonces $x + n\mathbb{Z} = y + n\mathbb{Z}$ si y sólo si n divide a $x - y$. Así, tenemos que las clases $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$ son necesariamente distintas. Como $k(1 + n\mathbb{Z}) = k + n\mathbb{Z}$, con $k \in \mathbb{Z}$ deducimos que $o(1 + n\mathbb{Z}) = n$. Por lo que $|\mathbb{Z}/n\mathbb{Z}| = n$.

□

Definición 2.38. *Si n es un entero positivo, llamamos **función de Euler**, y la denotamos por φ, a*

$$\varphi(n) = |\{m \in \mathbb{Z} : 1 \leq m \leq n,\ mcd(n, m) = 1\}|.$$

Notar que, por 2.36, $\varphi(n)$ es el número de generadores en un grupo cíclico de orden n.

Acabemos este capítulo con un ejemplo:

Ejemplo 2.38.1. *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 $\langle [2] \rangle = \{[0]\,,[2]\,,[4]\,,[6]\} \neq \mathbb{Z}_8$.

■

2.2. Homomorfismos

Estudiaremos ahora aquellas aplicaciones *buenas* entre grupos, es decir, aquellas que preservan la estructura de grupo. Esto ocurre en todas las estructuras algebraicas, aplicaciones que envían elementos de una estructura a otro conjunto dotado de esa misma estructura, es decir, conserva todas las propiedades de la propia estructura.

Definición 2.39. *Dados G y H grupos, una aplicación $f\colon G \longrightarrow H$ es un **homomorfismo de grupos** si cumple*

$$f(xy) = f(x)f(y) \quad \forall x, y \in G.$$

Los homomorfismos son una potente herramienta para analizar los grupos que relaciona. Si estudiamos los homomorfismos de dos de los grupos más importantes: S_Ω y

$GL_n(K)$ llegaremos a dos subramas de la teoría de grupos: la teoría de permutaciones para el primero y la de representaciones de grupos para el segundo.

Ejemplo 2.39.1. *Algunos ejemplos importantes de homomorfismos:*

1. *La aplicación determinante*

$$\begin{array}{ccc} GL_n(K) & \longrightarrow & K^* \\ A & \longmapsto & det(A) \end{array}$$

2. *Dado un grupo G y $N \trianglelefteq G$, la aplicación*

$$\begin{array}{ccc} G & \longrightarrow & G/N \\ g & \longmapsto & gN \end{array}$$

   que se conoce como ***proyección canónica****.*

3. *Dado $G = \langle x \rangle$ un grupo cíclico, la aplicación*

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ m & \longmapsto & x^m \end{array}$$

■

Más adelante veremos más desarrollados estos homomorfismos. Ahora veamos algunas de las propiedades fundamentales de los homomorfismos:

Propiedades 2.39.1. *Consideremos un homomorfismo $f\colon G \longrightarrow H$. Entonces algunas propiedades sobre los homomorfismos de grupos que serán importantes tenerlas en cuenta son las siguientes:*

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. *$f(x^n) = f(x)^n$. Esto es así ya que $f(x^n) = f(\overbrace{x \cdots x}^{n}) = \overbrace{f(x) \cdots f(x)}^{n} = f(x)^n$.*
4. *$o(f(x))$ 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.*
5. *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 $xy^{-1} \in f^{-1}(Y)$ y $f^{-1}(Y)$ es subgrupo. Para probar la normalidad de $f^{-1}(Y)$ tenemos que ver que $[f^{-1}(Y)]^a \subseteq f^{-1}(Y)$, con $a \in G$. Sea $x \in [f^{-1}(Y)]^a$, luego $a^{-1}xa \in f^{-1}(Y)$ y así $f(a^{-1}xa) = f(a)^{-1}f(x)f(a) \in Y$, por lo que $f(x) \in Y^{f(a)}$ y como $f(a)$ es un elemento de H e Y es normal entonces $f(x) \in Y$ y así $x \in f^{-1}(Y)$.

6. *Si ahora además consideramos otro homomorfismo $g\colon H \longrightarrow Z$, con Z otro grupo, entonces, $g \circ f\colon G \longrightarrow Z$ también es homomorfismo, pues*

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

■

Notar que de lo último se puede ver que la composición de homomorfismos la hemos definido tal que

$$(g \circ f)(x) = g(f(x)),$$

con g, f sendos homomorfismos. Es importante aclararlo porque en otros textos es frecuente encontrar que actúan al revés, primero g y luego f.

Definición 2.40. *Si $f\colon G \longrightarrow H$ es un homomorfismo de grupos, llamaremos* ***núcleo de*** *f a*

$$Kerf = \{g \in G : f(g) = 1_H\}.$$

De igual manera, llamaremos ***imagen de*** *f al conjunto*

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

De hecho, en el ejemplo 2.39.1(1.) tenemos que $Ker(det) = SL_n(K)$ es el grupo especial lineal. Y en el ejemplo 2.39.1(2.) es el propio N.

Proposición 2.41. *Si consideramos $f\colon G \longrightarrow H$ un homomorfismo de grupos cualquiera, entonces $Kerf \trianglelefteq G$. Además, f es inyectiva si y sólo si $Kerf = \{1\}$.*

Demostración: Como $Kerf = f^{-1}(1_H)$, por 2.39.1(4.) tenemos que $Kerf$ es subgrupo de G. Probaremos ahora que, dados $x \in G$ y $z \in Kerf$, $xzx^{-1} \in Kerf$. Esto es claro, ya que

$$f(xzx^{-1}) = f(x)f(z)f(x)^{-1} = f(x)f(x)^{-1} = 1.$$

Ahora, si f es inyectiva y $x \in Kerf$ entonces $f(x) = 1 = f(1)$, por lo que $x = 1$ y así $Kerf = \{1\}$. Recíprocamente, si $Kerf = \{1\}$ y $x, y \in G$ son tales que $f(x) = f(y)$, entonces $f(xy^{-1}) = f(x)f(y)^{-1} = 1$, luego $xy^{-1} \in Kerf = \{1\}$ y así $x = y$.

□

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*** y ya lo habíamos visto antes en los ejemplos.

Definición 2.42. *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. Es decir, veamos una forma alternativa de caracterizarlos, que todo subgrupo normal es el núcleo de algún homomorfismo de grupos:

Proposición 2.43. *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

$$\forall g \in G, n \in N,\ gng^{-1} \in N \Longleftrightarrow \forall g \in G,\ gN = Ng.$$

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

$$H = G/N = \{gN : g \in G\} = \{Ng : g \in G\},$$

con la operación

$$\begin{array}{rccc} G/N \times G/N & \longrightarrow & G/N \\ (gN, hN) & \longmapsto & ghN \end{array}$$

que en 2.28 ya definimos y comprobamos que estaba bien definida, que era cerrada, que cumplía la asociatividad y la existencia del elemento neutro e inverso. Así que si consideramos la aplicación

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

entonces es claro que es homomorfismo puesto que es una proyección:

$$\varphi(gh) = ghN = (gN)(hN) = \varphi(g)\varphi(h).$$

Entonces

$$Ker\ \varphi = \{g \in G : gN = N\} = \{g \in G : g \in N\} = N.$$

□

Definición 2.44. *Diremos que un homomorfismo de grupos $f\colon G \longrightarrow H$ es un* ***isomorfismo*** *si la aplicación f es biyectiva. En tal caso diremos que G es* ***isomorfo*** *a H y lo denotaremos por $G \cong H$.*

Observación 2.44.1. *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 $G_1 \cong G_2$ entonces $G_2 \cong G_1$.*

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

Hablaremos así de una serie de resultados conocidos como *Teoremas de Isomorfía*, que los debemos a unos cuantos matemáticos y matemáticas, entra les que destaca la matemática alemana Emmy Noether, de la que también veremos más resultados más adelante.

Teorema 2.45 (***Primer Teorema de Isomorfía***). *Sea $f\colon G \longrightarrow H$ un homomorfismo de grupos. Entonces, la aplicación*

$$\begin{array}{rccc} \bar{f} & G/Kerf & \longrightarrow & f(G) \\ & xKerf & \longmapsto & f(x) \end{array}$$

es un isomorfismo de grupos.

Demostración: Sea $N = Kerf$. Sabemos por 2.13 que $xN = yN$ si y sólo si $x^{-1}y \in N$ si y sólo si $f(x^{-1}y) = 1$ si y sólo si $f(x)^{-1}f(y) = 1$ si y sólo si $f(x) = f(y)$. Si leemos esto de izquierda a derecha estamos probando que la aplicación $\bar{f}$ está bien definida, es decir, que la imagen por $\bar{f}$ de un elemento $xN \in G/N$ no depende del representante que escojamos. Si lo leemos de derecha a izquierda estaremos probando que $\bar{f}$ es inyectiva. Si $y \in f(G)$ (imagen de G por f) entonces $y = f(x) = \bar{f}(xKerf)$ con $x \in G$ y esto prueba la sobreyectividad. Además, es homomorfismo:

$$\bar{f}(xNyN) = \bar{f}(xyN) = f(xy) = f(x)f(y) = \bar{f}(xN)\bar{f}(yN).$$

□

Luego, dados dos grupos G, H, podemos expresar el *Primer Teorema de Isomorfía* tal que así:

$$G/Kerf \cong f(G).$$

Y notar que si f es suprayectiva, entonces:

$$G/Kerf \cong H.$$

Es decir, el *Primer Teorema de Isomorfía* hace conmutativo el siguiente diagrama,

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

donde π e i son los homomorfismos proyección e inclusión presentados antes respectivamente. Es decir,

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

Y a esta expresión la llamaremos ***descomposición canónica de un homomorfismo*** f.

Proposición 2.46. *Sea $N \trianglelefteq G$ y sea $f\colon G \longrightarrow G/N$ el homomorfismo $f(g) = gN$. Si $H \leq G$, entonces $f(H) = f(NH) = NH/N \leq G/N$.*

Demostración: Si $H \leq G$ sabemos que NH es subgrupo de G. Como $N \trianglelefteq G$ y $N \subseteq NH$, tenemos que $N \trianglelefteq NH$. Ahora,

$$f(H) = \{hN : h \in H\} = \{nhN : n, \in N, h \in H\} = NH/N.$$

Por 2.39.1, NH/N es un subgrupo de G/N.

□

Ejemplo 2.46.1. *Veamos algunos ejemplos:*

1. *Vamos a ver cómo son los homomorfismos de la forma* $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$.

   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,*

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

   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

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

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

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

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

   como $e^{2\pi xi} = \cos 2\pi x + i \sin 2\pi x = 1$ *si* $x \in \mathbb{Z}$, *deducimos que* $Kerf = \mathbb{Z}$. *Y como, para cualquier* $x \in \mathbb{R}$, *el valor absoluto o módulo del número complejo*

$e^{2\pi xi} = \cos 2\pi x + i \sin 2\pi x$ *es* $\sqrt{\cos^2 2\pi x + \sin^2 2\pi x} = 1$, *tenemos que* $Imf = S^1 = \{z \in \mathbb{C} : |z| = 1\}$ *(indicaremos el módulo con* $|\cdot|$*). Así, por el Primer Teorema de Isomorfía:*

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

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

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

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* $Kerf = \{+1, -1\}$*. 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: *Supongamos que* $|G| = 2k+1$ *impar, sea* $x \in Kerf$*. Así* $x^2 = 1$ *y también* $x^{2k+1} = 1$*, por ser el orden de* G *y* 2 *coprimo con* $2k+1$*. 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* $A_x = \{x, x^{-1}\}$*. 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, tuviesen dos elementos, entonces*

$$2k = |G| = cardA_1 + 2p = 2p + 1.$$

Y como éste último es impar sería absurdo. Luego ha de existir $1 \neq a \in G$ *tal que* $cardA_a = 1$*. 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 2.47 (***Segundo Teorema de Isomorfía***). *Sea $N \trianglelefteq G$ y sea $H \leq G$. Entonces $H \cap N \trianglelefteq H$ y*

$$H/H \cap N \cong NH/N.$$

Demostración: Consideremos el siguiente homomorfismo de grupos:

$$\begin{array}{rccc} f\colon & G & \longrightarrow & G/N \\ & x & \longmapsto & xN \end{array}$$

y sea $g = f|_H : H \longrightarrow G/N$ la restricción a H. Por el resultado anterior tenemos que $g(H) = f(H) = NH/N$. Notar que, como $N \trianglelefteq G$ y $H \leq G$, NH es grupo. El núcleo de g es:

$$Kerg = \{x \in H : xN = N\} = N \cap H.$$

El resultado se sigue de aplicar el *Primer Teorema de Isomorfía*.

□

Teorema 2.48 (***Tercer Teorema de Isomorfía***). *Sea G un grupo. Sean $N, M \trianglelefteq G$ y $N \subseteq M$. Entonces*

$$G/M \cong (G/N)/(M/N).$$

Demostración: Consideremos la aplicación suprayectiva

$$\begin{array}{rccc} f\colon & G/N & \longrightarrow & G/M \\ & gN & \longmapsto & gM \end{array}$$

Entonces f está bien definida ya que si $gN = hN$ entonces $g^{-1}h \in N \subseteq M$ y así $gM = hM$. Es claro que es homomorfismo y el núcleo es

$$Kerf = \{gN \in G/N : gM = M\} = \{gN \in G/N : g \in M\} = M/N.$$

El resultado se sigue de aplicar el *Primer Teorema de Isomorfía*.

□

También podemos estudiar los subgrupos de un grupo cociente G/N:

Teorema 2.49 (***Teorema de la correspondencia***). *Sea $N \trianglelefteq G$. La aplicación $K \longrightarrow G/N$ es una biyección entre el conjunto $\{K : N \subseteq K \leq G\}$ y los subgrupos de G/N.*

Demostración: Sea $f\colon G \longrightarrow G/N$ el homomorfismo dado por $f(g) = gN$. Supongamos que K es un subgrupo de G que contiene a N. Por 2.46, $K/N = f(K)$ es un subgrupo de G/N. Supongamos que J es otro subgrupo de G que contiene a N con $K/N = J/N$. Si $k \in K$, entonces $kN \in K/N = J/N$, por lo que existirá $j \in J$ tal que $kN = jN$. Así, $k \in jN \subseteq J$. Esto prueba que $K \subseteq J$. Análogamente, $J \subseteq K$ y tenemos que $K = J$. Esto prueba que la aplicación $K \longrightarrow K/N$ es inyectiva. Si $X \leq G/N$, entonces $f(f^{-1}(X)) = X$ pues f es suprayectiva. Sea $K = f^{-1}(X)$. Sabemos que $K \leq G$ por 2.39.1. Está claro que $N \subseteq K$ pues $f(n) = N \subseteq X$ para cada $n \in N$. Ahora, $X = f(K) = K/N$ y ya está.

□

Proposición 2.50. *K es subgrupo normal de G si y sólo si K/H es subgrupo normal de G/H.*

Demostración: Sea $K \trianglelefteq G$. Veamos que $(K/H)^x \subseteq K/H$ para todo $x \in G/H$ (x será de la forma $x = gH$). Sea $aH \in (K/H)^x$, entonces $aH = x(kH)x^{-1} = (gH)kH(g^{-1})H = gkg^{-1}H$, y como K es normal $gkg^{-1} \in K$ y así $aH \in K/H$.

Recíprocamente, sea $K/H \trianglelefteq G/H$, es decir, $xK/H = K/Hx$ para todo $x \in G/H$ (que será de la forma $x = gH$). Así, $(gH)(kH) = (k'H)(gH)$, para algunos $k, k' \in K$ y $g \in G$, luego $gk = k'g$ y así $gkg^{-1} = k' \in K$, es decir, $K^g \subseteq K$ y K es normal.

□

Definición 2.51. *Un **automorfismo** α de G es un isomorfismo $\alpha\colon G \longrightarrow G$. Denotaremos por $Aut(G)$ el conjunto de los automorfismos de G. Es claro que $Aut(G)$ es grupo con la operación composición de aplicaciones:*

$$\alpha \circ \beta = \alpha\beta.$$

Aunque en general no es sencillo calcular el grupo de automorfismos de un grupo G, nosotros estudiaremos un caso más simple, para ello tenemos que:

Definición 2.52. *Dado G un grupo y $x, g \in G$ tenemos que*

$$x^g = gxg^{-1}.$$

*A este x^g lo denominaremos **conjugado** de x por g. Igualmente para conjuntos, que ya lo habíamos definido al principio para presentar el normalizador, si $X \subseteq G$ y $g \in G$ escribiremos*

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

*También definimos la **aplicación conjugación por** g como*

$$\begin{array}{rccc} \alpha_g\colon & G & \longrightarrow & G \\ & x & \longmapsto & x^g = gxg^{-1} \end{array}$$

Notar que la conjugación la hemos definido para subconjuntos en general.

Proposición 2.53. *Sea G un grupo y $g \in G$. Entonces:*

1. *La aplicación α_g es un automorfismo de G. En particular, si $x, y \in G$ entonces $(xy)^g = x^g y^g$.*
2. *Si $h \in G$, entonces $\alpha_h\alpha_g = \alpha_{hg}$. En particular, si $x \in G$ entonces $(x^g)^h = x^{hg}$.*

Demostración: Veamos:

1. Tenemos que $\alpha_g\alpha_{g^{-1}} = \alpha_{g^{-1}}\alpha_g = 1$, luego $(\alpha_g)^{-1} = \alpha_{g^{-1}}$ y así α_g es biyectiva. Sean ahora $x, y \in G$, entonces:

   $$(xy)^g = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = x^g y^g.$$

   Luego α_g es un homomorfismo, y notar que α_1 es la identidad.

2. Sea $h \in G$, entonces:

$$(x^g)^h = h(gxg^{-1})h^{-1} = (hg)x(g^{-1}h^{-1}) = (hg)x(hg)^{-1} = x^{hg}.$$

Luego, $\alpha_h\alpha_g(x) = \alpha_h(\alpha_g(x)) = (x^g)^h = x^{hg} = \alpha_{hg}(x)$. Así, $\alpha_h\alpha_g = \alpha_{hg}$.

□

Notar que cuando hacemos $(x^g)^h$ primero actúa g y luego h, por eso $(x^g)^h = x^{hg}$.

Resulta que estos automorfismos especiales, las conjugaciones, forman un grupo y tienen características interesantes.

Definición 2.54. *Definimos*

$$Int(G) = \{\alpha_g : g \in G\}$$

como el conjunto de los ***automorfismos internos*** *de G.*

Para el siguiente resultado conviene repasar el concepto de centro de un grupo, que vimos en 2.9.

Proposición 2.55. *Si G es un grupo, entonces $Int(G) \trianglelefteq Aut(G)$. Además,*

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

Demostración: Sabemos que $\alpha_g\alpha_h = \alpha_{gh}$ y que $(\alpha_g)^{-1} = \alpha_{g^{-1}}$ por el resultado anterior. Así, tenemos que $Int(G) \leq Aut(G)$. Si $f \in Aut(G)$, veamos que $(\alpha_g)^f = \alpha_{f(g)}$: (recordar que f es un automorfismo y $g \in G$)

$$((\alpha_g)^f)(x) = (f\alpha_g f^{-1})(x) = f(\alpha_g(f^{-1}(x))) = f(g(f^{-1}(x))g^{-1}) = f(g)xf(g^{-1}) = f(g)x(f(g))^{-1} = \alpha_{f(g)}(x) = x^{f(g)}.$$

Esto demuestra que $Int(G) \trianglelefteq Aut(G)$.

Ahora, si consideramos la aplicación $G \longrightarrow Int(G)$ dada por $g \longmapsto \alpha_g$, es evidentemente suprayectiva y homomorfismo. El núcleo de esta aplicación será el conjunto $\{g \in G : \alpha_g = id\} = \{g \in G : gxg^{-1} = x\ \forall x \in G\} = \{g \in G : gx = xg\ \forall x \in G\}$, y este conjunto es el centro $Z(G)$. El resultado se sigue de aplicar el *Primer Teorema de Isomorfía*.

□

Finalmente, calculemos el grupo de automorfismos de un grupo cíclico. Será muy útil saber más adelante que este grupo es abeliano, veámoslo: si $G = \langle x \rangle$ y $\alpha, \beta \in Aut(G)$, entonces $\alpha(x) = x^d$ y $\beta(x) = x^e$ para algunos enteros d, e. Ahora, $\alpha\beta(x) = x^{de} = x^{ed} = \beta\alpha(x)$ y así $\alpha\beta = \beta\alpha$ (esto es así porque todos los elementos de G son potencias de x). Ahora examinaremos exactamente cómo es este grupo de automorfismos:

Si $n \in \mathbb{Z}$, consideramos el grupo abeliano $\mathbb{Z}/n\mathbb{Z}$. En $\mathbb{Z}/n\mathbb{Z}$ también se pueden multiplicar elementos: si $x + n\mathbb{Z} = x' + n\mathbb{Z}$, $y + n\mathbb{Z} = y' + n\mathbb{Z}$ tenemos que

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + y'(x - x') \in n\mathbb{Z},$$

luego es divisible por n. Luego $xy + n\mathbb{Z} = x'y' + n\mathbb{Z}$ y la multiplicación

$$(x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z},$$

está bien definida. Esta multiplicación es asociativa, por serlo la de $\mathbb{Z}$, y tiene elemento neutro $1 + n\mathbb{Z}$. Llamaremos $\mathcal{U}_n$ al conjunto de los elementos de $\mathbb{Z}/n\mathbb{Z}$ para los que existe un inverso respecto a la multiplicación.

Proposición 2.56. *Sea $n \geq 1$ y sea $0 \neq u \in \mathbb{Z}$, entonces $u + n\mathbb{Z}$ es invertible en $\mathbb{Z}/n\mathbb{Z}$ para la multiplicación si y sólo si $mcd(u, n) = 1$. En particular $|\mathcal{U}_n| = \varphi(n)$.*

Demostración: Se tiene que $u + n\mathbb{Z}$ es invertible en $\mathbb{Z}/n\mathbb{Z}$ si y sólo si existe $v \in \mathbb{Z}$ tal que $(u + n\mathbb{Z})(v + n\mathbb{Z}) = 1 + n\mathbb{Z}$. Por lo que $u + n\mathbb{Z}$ es invertible si y sólo si existe $v \in \mathbb{Z}$ tal que $uv - 1$ es divisible por n. Si esto ocurre, entonces $uv - 1 = kn$ para cierto k. Ahora, si d divide a u y a n, entonces d divide a $uv - kn = 1$, por lo que $mcd(u, n) = 1$. Recíprocamente, supongamos que $mcd(u, n) = 1$. Por la identidad de Bézout sabemos que existen $a, b \in \mathbb{Z}$ tales que $au + bn = 1$. Luego, $au - 1$ es divisible por n y así $u + n\mathbb{Z}$ tiene inverso.

□

Así, es claro que

$$\mathcal{U}_n = \{u \in \mathbb{Z}/n\mathbb{Z} : mcd(u, n) = 1\}.$$

Proposición 2.57. *Si C_n es un grupo cíclico de orden n, entonces $Aut(C_n) \cong \mathcal{U}_n$. En particular, $Aut(C_n)$ es abeliano.*

Demostración: Sea $C_n = \langle x \rangle$, con $o(x) = n$. Si $n = 1$ el resultado está claro. Sea $n \geq 2$. Sea d un entero cualquiera y definimos

$$\begin{array}{rccc} f_d\colon & C_n & \longrightarrow & C_n \\ & x^s & \longmapsto & x^{ds} \end{array}$$

con $s \in \mathbb{Z}$. Esta aplicación está bien definida, ya que si $x^s = x^t$, entonces $x^{ds} = (x^s)^d = (x^t)^d = x^{dt}$. Observamos que

$$f_d(x^s x^r) = f_d(x^{s+r}) = x^{d(s+r)} = x^{ds}x^{dr} = f_d(x^s)f_d(x^r),$$

con lo que f_d es homomomorfismo de grupos. Recíprocamente, si $f\colon C_n \longrightarrow C_n$ es un homomorfismo y escribimos $f(x) = x^d$, entonces para cada entero s tenemos que $f(x^s) = x^{ds}$ por 2.39.1 y deducimos que $f = f_d$. Notar también que claramente la aplicación es inyectiva y sobreyectiva, luego un isomorfismo y, en concreto, automorfismo.

Notamos también que $f_d \circ f_e = f_{ed} = f_e \circ f_d$ y que $f_e = f_d$ si y sólo si $x^d = x^e$ si y sólo si $x^{d-e} = 1$ si y sólo si n divide a $d - e$ si y sólo si $e + n\mathbb{Z} = d + n\mathbb{Z}$.

Ahora, $f_d(\langle x \rangle) = \langle x^d \rangle$ por 2.39.1. Si $d = 0$, entonces la aplicación f_d no es biyectiva (pues $n \geq 2$). Si $d \neq 0$, tenemos que f_d es biyectiva si y sólo si f_d es suprayectiva si y sólo si $\langle x^d \rangle = \langle x \rangle$ si y sólo si $mcd(d, n) = 1$, por 2.36.

Queda probado así que la aplicación

$$\begin{array}{rccc} \phi\colon & \mathcal{U}_n & \longrightarrow & Aut(C_n) \\ & d+n\mathbb{Z} & \longmapsto & f_d \end{array}$$

está bien definida y es un isomorfismo de grupos.

□

Gracias a estos dos últimos resultados concluimos que $|Aut(C_p)| = p-1$. De hecho, este grupo es cíclico.

Ahora volveremos brevemente a los grupos cíclicos para presentar un resultado que es ciertamente interesante e importante, y que necesitaba de los teoremas de isomorfía para verlo:

Ya hemos visto a lo largo de las páginas anteriores 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 hemos visto en este 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 2.58. *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 ($Imf = G$). Veamos los dos casos:

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 $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong G$, 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 ese 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* $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong G$. Como $\mathbb{Z}_m$ y G han de tener el mismo orden, $m = n$.

□

Como consecuencia interesante tenemos:

Corolario 2.58.1. *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.

Finalmente, veamos el producto directo y semidirecto:

Proposición 2.59. *Sean G_1 y G_2 grupos. Dado el producto cartesiano $G_1 \times G_2$, entonces podemos convertirlo en un grupo con la siguiente operación:*

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

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
$$N_1 \times N_2 \cong G.$$

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

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

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. $Ker f = \{(n_1, n_2) \in N_1 \times N_2 : n_1 n_2 = 1\}$. 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 $Ker f = \{1_G\}$ y f es inyectiva. El resultado se sigue del *Primer Teorema de Isomorfía.*

□

Definición 2.60. *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****.*

Ejemplo 2.60.1. *Un ejemplo de producto directo bastante conocido es el* ***grupo de Klein****, V_4. Formalmente, es el producto directo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, es decir, el producto directo de dos grupos cíclicos de orden 2. Se llama así en honor al matemático alemán Felix Klein y se denota por la letra V, del alemán Vierergruppe, que significa algo así como "grupo de cuatro".*

Evidentemente este grupo tiene 4 elementos, y veremos que cada uno de ellos es inverso de sí mismo, es decir, cada elemento tiene orden 2. Como ya sabemos

$$\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z}, 1 + \mathbb{Z}\}.$$

Y esto se podría interpretar como, por un lado $0 + 2\mathbb{Z}$ la clase de todos aquellos enteros que divididos entre 2 dan 0, es decir, los enteros pares, y $1 + 2\mathbb{Z}$ como la clase formada por todos aquellos cuyo resto de dividirlos entre 2 sea 1, es decir, los enteros impares. Como también sabemos, éste es un grupo cíclico de orden 2, por lo que el orden de sus dos elementos es 2 y así otra forma de interpretar a este grupo es verlo como aquel formado por 1 y -1, y así

$$\mathbb{Z}/2\mathbb{Z} = \{1, -1\}.$$

Así,

$$V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

es un grupo de 4 elementos que podríamos representarlos como $(1,1), (1,-1), (-1,1)$ y $(-1,-1)$. Su tabla:

	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,-1)$	$(1,-1)$	$(1,1)$	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	$(1,1)$	$(1,-1)$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$	$(1,1)$

Donde vemos que todos sus elementos tienen orden 2.

■

Proposición 2.61. *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 conjugación por un elemento de 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

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

Entonces

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

Demostración: Lo primero de todo, 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:

$$\varphi(h_1h_2)(n) = h_1h_2nh_2^{-1}h_1^{-1} = (\varphi(h_1) \circ \varphi(h_2))(n).$$

Ahora veamos 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:

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

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

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

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

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

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

Ya sabemos que φ está bien definida y que es un homomorfismo.

Definimos ahora

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

y veamos que f es homomorfismo:

$$f((n_1, h_1)(n_2, h_2)) = f((n_1\varphi(h_1)(n_2), h_1h_2) = n_1\varphi(h_1)(n_2)h_1h_2 = \\ n_1(h_1n_2h_1^{-1})h_1h_2 = n_1h_1n_2h_2 = f((n_1, h_1))f((n_2, h_2)).$$

Como $G = NH$ entonces f es claramente suprayectiva. Ahora, $Ker f = \{(n, h) \in N \times_\varphi H : nh = 1\}$. 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.

□

Y con esto finalizamos el capítulo de homomorfismos de grupos habiendo presentado las bases y los principales resultados. A continuación veremos una de las herramientas más poderosas que nos ofrecen los grupos y con la que podremos demostrar importantes resultados.

2.3. Acciones de grupos

Los grupos se manifiestan a través de sus acciones sobre espacios vectoriales, sobre otros grupos o, en general, sobre conjuntos. En esta sección veremos las acciones sobre conjuntos, o equivalentemente, los homomorfismos de G sobre grupos simétricos.

Definición 2.62. *Sea Ω un conjunto no vacío y sea G un grupo. Diremos que G **actúa** sobre Ω si $\forall \alpha \in \Omega$, $\forall g \in G$ tenemos definido un único elemento $g \cdot \alpha$ de tal forma que:*

1. $h \cdot (g \cdot \alpha) = (hg) \cdot \alpha \ \forall \alpha \in \Omega,\ g, h \in G.$
2. $1 \cdot \alpha = \alpha \ \forall \alpha \in \Omega.$

*En este caso, diremos que $\cdot$ define una **acción** de G sobre Ω.*

Ejemplo 2.62.1. *Los siguientes ejemplos son acciones de grupos sobre conjuntos:*

1. *Sea G un grupo y $H \leq G$. Sea $\Omega = \{xH : x \in G\}$. Si $g \in G$ y $\alpha \in \Omega$, definimos $g \cdot \alpha = g\alpha$, es decir:*

$$g \cdot (xH) = gxH, \quad \forall x, g \in G.$$

   Esta es la acción de G sobre el conjunto de las coclases a izquierda de H en G.

2. *Sea G un grupo y $\Omega = G$. Dado un $\alpha \in \Omega, g \in G$ definimos*

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

   *Esta es la **acción de G sobre G por conjugación** y ya la conocemos de haberla estudiado en los capítulos anteriores.*

3. *Sea $\Omega = \{H : H \leq G\}$ el conjunto de los subgrupos de G. Si $H \in \Omega$, $g \in G$ definimos*

$$g \cdot H = H^g.$$

   Esta es la acción de G sobre los subgrupos de G por conjugación.

4. *Sea Ω un conjunto no vacío y sea $G \leq S_\Omega$. Si $g \in G$, $\alpha \in \Omega$ definimos*

$$g \cdot \alpha = g(\alpha).$$

   *Esta es la **acción natural de G sobre Ω**. La llamamos así porque, como veremos más adelante, siempre va a existir una para cada grupo G sobre un conjunto cualquiera Ω al ser todo grupo finito G isomorfo a un subgrupo del grupo de permutaciones.*

■

Como se verá ahora, una acción de un grupo G sobre un conjunto Ω no es más que un homomorfismo de grupos $G \longrightarrow S_\Omega$.

Teorema 2.63. *Sea G un grupo y Ω un conjunto no vacío. Entonces:*

1. *Supongamos que G actúa sobre Ω. Para cada $g \in G$ consideremos la aplicación*

$$\begin{array}{rccc} \rho_g\colon & \Omega & \longrightarrow & \Omega \\ & \alpha & \longmapsto & g \cdot \alpha \end{array}$$

Tenemos que ρ_g es biyectiva y además la aplicación

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & S_\Omega \\ & g & \longmapsto & \rho_g \end{array}$$

es un homomorfismo de grupos.

2. *Sea $\rho\colon G \longrightarrow S_\Omega$ homomorfismo de grupos. Para cada $g \in G$ y $\alpha \in \Omega$ definimos $g \cdot \alpha = \rho(g)(\alpha)$. Entonces $\cdot$ define una acción de G sobre Ω.*

Demostración:

1. Sea $g \in G$, veamos que ρ_g es inyectiva. Si $\rho_g(\alpha) = \rho_g(\beta)$, con $\alpha, \beta \in \Omega$ entonces $g \cdot \alpha = g \cdot \beta$, por lo que $g^{-1} \cdot (g \cdot \alpha) = g^{-1} \cdot (g \cdot \beta)$ y aplicando las condiciones de las acciones tenemos que $(g^{-1}g) \cdot \alpha = (g^{-1}g) \cdot \beta \Rightarrow 1 \cdot \alpha = 1 \cdot \beta \Rightarrow \alpha = \beta$. Para la sobreyectividad consideremos $\beta \in \Omega$, entonces $g^{-1} \cdot \beta \in \Omega$ y $\rho_g(g^{-1} \cdot \beta) = g \cdot (g^{-1} \cdot \beta) = \beta$. Luego ρ_g es biyectiva.
2. Como $\rho(1)$ es la identidad tenemos que $1 \cdot \alpha = \alpha$, $\forall \alpha \in \Omega$. Ahora, si $g, h \in G$ y $\alpha \in \Omega$ tenemos que

$$(\rho(g)\rho(h))(\alpha) = \rho(g)(\rho(h)(\alpha)) = g \cdot (h \cdot \alpha) = (gh) \cdot \alpha = \rho_{gh}(\alpha) = \rho(gh)(\alpha).$$

□

Definición 2.64. *Si un grupo G actúa sobre un conjunto Ω, entonces podemos definir el siguiente conjunto.*

$$K = \{g \in G : g \cdot \alpha = \alpha \, \forall \alpha \in \Omega\},$$

*como el **núcleo** de la acción. Notar que $K = Ker(\rho) \trianglelefteq G$. Diremos que la acción de G sobre Ω es **fiel** si $K = \{1\}$.*

De hecho, el núcleo de la acción (que veremos más adelante en profundidad) de G sobre G por conjugación es

$$K = \{g \in G : x^g = x \, \forall x \in G\} = \{g \in G : gx = xg \, \forall x \in G\} = Z(G).$$

Veamos ahora cuál es el núcleo de la acción del primer ejemplo:

Proposición 2.65. *Sea $H \leq G$ y sea $K = \cap_{x \in G} H^x$. Entonces K es el núcleo de la acción de G sobre $\Omega = \{xH : x \in G\}$ por multiplicación a izquierda.*

Demostración: Sea $g \in G$, entonces $g \in Ker(\rho)$ si y sólo si $gxH = xH \ \forall x \in G$ si y sólo si $x^{-1}gxH = H \ \forall x \in G$ si y sólo si $x^{-1}gx \in H \ \forall x \in G$ si y sólo si $g \in H^x$ $\forall x \in G$ si y sólo si $g \in K$.

□

Notar que el núcleo de la acción que acabamos de describir, la de G sobre el conjunto de las clases izquierda módulo H (un subgrupo suyo), es lo que habíamos definido en el primer capítulo como el corazón de H, $K(H)$.

Tal y como habíamos dicho cuando presentamos el ejemplo de la acción natural veamos que todo grupo finito es subgrupo de un grupo simétrico.

Teorema 2.66 (***Teorema de Cayley***)**.** *Sea $H \leq G$, con $[G : H] = n$. Entonces, existe $K \trianglelefteq G$ contenido en H tal que G/K es isomorfo a un subgrupo de S_n. En particular, si G tiene orden n, entonces G es isomorfo a un subgrupo de S_n.*

Demostración: Sea Ω el conjunto de las clases a izquierda de H en G. Luego, $|\Omega| = n$. Sea $K \trianglelefteq G$ el núcleo de la acción de G sobre Ω Por el resultado anterior tenemos que $K \subseteq H$. Por la primera parte de 2.63 existe un homomorfismo de grupos $G \longrightarrow S_\Omega$ de núcleo K. Por el *Primer Teorema de Isomorfía*, tenemos que G/K es isomorfo a un subgrupo de $S_\Omega = S_n$. Para lo segundo tomar simplemente $H = \{1\}$.

□

De este resultado podemos sacar algo de información para los grupos finitos simples:

Corolario 2.66.1. *Sea G un grupo finito simple y supongamos que $H \leq G$ es un subgrupo de índice $n > 1$. Entonces G es isomorfo a un subgrupo de S_n. En particular, $|G|$ divide a $n!$.*

Demostración: Teniendo en cuenta lo que hemos visto en el resultado anterior tenemos que K es un subgrupo normal de G contenido en $H \leq G$, por lo que $K = 1$. Así, G es isomorfo a un subgrupo de S_n por el resultado anterior. Para lo segundo basta aplicar el *Teorema de Lagrange*.

□

Ahora veremos que una acción de G puede definir una relación de equivalencia en Ω. En efecto, si $\alpha, \beta \in \Omega$ escribiremos $\alpha \sim \beta$ si existe $g \in G$ tal que $g \cdot \alpha = \beta$. Es decir, α y β van a estar relacionados si existe un elemento de G que actuando sobre α dé como resultado β. Esta relación va a dar mucho de que hablar, veamos que es de equivalencia:

$$g^{-1} \cdot \beta = g^{-1} \cdot (g \cdot \alpha) = (g^{-1}g) \cdot \alpha = \alpha,$$

luego si $\alpha \sim \beta$ entonces $\beta \sim \alpha$ y tenemos que esta relación es simétrica. Además es claro que $1 \cdot \alpha = \alpha$, luego $\alpha \sim \alpha$ y esta relación es reflexiva. Finalmente, si $g \cdot \alpha = \beta$ ($\alpha \sim \beta$) y $h \cdot \beta = \gamma$ ($\beta \sim \gamma$), con $g, h \in G$, entonces

$$\gamma = h \cdot (g \cdot \alpha) = (hg) \cdot \alpha,$$

y como $hg \in G$ por ser G grupo entonces $\alpha \sim \gamma$ y esta relación es transitiva.

Definición 2.67. *Dado un grupo G actuando sobre un conjunto Ω, $\alpha \in \Omega$ y considerando la relación de equivalencia $\sim$ que acabamos de ver, entonces la clase de*

equivalencia de α es

$$O_\alpha = \{g \cdot \alpha : g \in G\}.$$

A este conjunto lo llamamos ***órbita*** *de α por G ó G-**órbita** de α. Notar que su* ***longitud*** *es $|O_\alpha|$.*

Notar que al tratarse las órbitas de clases de equivalencia para la relación de equivalencia $\sim$ entre elementos de Ω antes vista, entonces van a formar una partición de Ω. Es decir, que su unión disjunta forman la totalidad de Ω. Así, si R es un conjunto de representantes de estas clases de equivalencia (órbitas de la acción), tenemos que

$$\Omega = \bigsqcup_{x \in R} O_x.$$

Como la unión es disjunta y Ω finito tenemos que

$$|\Omega| = \sum_{x \in R} |O_x|.$$

A estas dos fórmulas equivalentes se las conoce como ***fórmula de las órbitas***. (Se ha empleado $|\cdot|$ para hablar de cardinal de un conjunto, lo cuál podría considerarse abuso de notación).

Definición 2.68. *Dado un grupo G actuando sobre un conjunto Ω, si $\alpha \in \Omega$ entonces definimos el* ***estabilizador*** *de α en G como*

$$G_\alpha = \{g \in G : g \cdot \alpha = \alpha\}.$$

Qué es el *estabilizador* con respecto a G y una propiedad fundamental del mismo nos lo dice el siguiente resultado:

Proposición 2.69. *Sea $G \longrightarrow S_\Omega$ una acción de un grupo G sobre un conjunto Ω, y $\alpha \in \Omega$. Entonces:*

1. *G_α es un subgrupo de G.*
2. *Si $g \in G$, entonces $(G_\alpha)^g = gG_\alpha g^{-1} = G_{g\cdot\alpha}$. Es decir,* ***el conjugado de un estabilizador es un estabilizador****.*

Demostración: Veamos:

1. Primero de todo, $1_G \in G_\alpha$ por la segunda condición a cumplir de las acciones de grupos, así que G_α es no vacío. Ahora, sean $g, h \in G_\alpha$. Está claro que $g \cdot \alpha = h \cdot \alpha = \alpha$, además

   $$h^{-1} \cdot \alpha = h^{-1} \cdot (h \cdot \alpha) = (h^{-1}h) \cdot \alpha = 1_G\alpha = \alpha.$$

   Por lo que $(gh^{-1}) \cdot \alpha = g \cdot (h^{-1} \cdot \alpha) = g \cdot \alpha = \alpha$, luego $gh^{-1} \in G_\alpha$.

2. Sea $h \in G_\alpha$. Como

   $$(ghg^{-1}) \cdot (g \cdot \alpha) = g \cdot (h1_G \cdot \alpha) = g \cdot (h \cdot \alpha) = g \cdot \alpha,$$

   tenemos que $ghg^{-1} \in G_{g\cdot\alpha}$, así que $(G_\alpha)^g \subseteq G_{g\cdot\alpha}$.

   Recíprocamente, si $h \in G_{g\cdot\alpha}$, entonces $h \cdot (g \cdot \alpha) = g \cdot \alpha$, y así $(g^{-1}hg) \cdot \alpha = \alpha$, y $(g^{-1}hg) \in G_\alpha$, luego $h \in (G_\alpha)^g$.

□

De aquí es importante quedarse con que ***si dos elementos de un conjunto cuaquiera Ω están en la misma órbita entonces sus estabilizadores son conjugados.***

Teorema 2.70 (***Teorema de la órbita-estabilizadora***)**.** *Sea G un grupo que actúa sobre un conjunto Ω y sea $\alpha \in \Omega$. Entonces $G_\alpha \leq G$ y*

$$|O_\alpha| = [G : G_\alpha].$$

Demostración: Lo primero ya lo sabemos del resultado anterior.

Para lo segundo, busquemos una aplicación biyectiva $f\colon \{gG_\alpha : g \in G\} \longrightarrow O_\alpha$. Definimos $f(gG_\alpha) = g \cdot \alpha$. Ahora, $gG_\alpha = hG_\alpha$ si y sólo si $g^{-1}h \in G_\alpha$ si y sólo si $(g^{-1}h) \cdot \alpha = \alpha$ si y sólo si $g \cdot ((g^{-1}h) \cdot \alpha) = g \cdot \alpha$ si y sólo si $h \cdot \alpha = g \cdot \alpha$, luego f está bien definida y si lo leemos al revés podremos comprobar que también es inyectiva. Al ser f claramente suprayectiva, ya está.

□

Cuando un grupo G actúa sobre un conjunto Ω, de entre todos los elementos de Ω destacamos aquellos que son fijados por todos los elementos de G:

Definición 2.71. *Dado un grupo G actuando sobre un conjunto Ω, y dado un $\alpha \in \Omega$ decimos que α es un **punto fijo** de Ω si $g \cdot \alpha = \alpha \ \forall g \in G$, es decir aquellos $\alpha \in \Omega$ tales que $O_\alpha = \{\alpha\}$. Igualmente escribimos*

$$\Omega_0 = \{\alpha \in \Omega : |O_\alpha| = 1.\}$$

para referirnos al conjunto de los puntos fijos de Ω.

Proposición 2.72. *Sea un grupo G actuando sobre un conjunto Ω. Si $g \in G$, definimos $Fi(g) = \{i \in \Omega : g \cdot i = i\}$. Entonces, el número de órbitas de Ω bajo la acción de G es*

$$\frac{1}{|G|} \sum_{g \in G} |Fi(g)|.$$

Demostración: Hallaremos $|\{(g, i) \in G \times \Omega : g \cdot i = i\}|$. Contamos sus elementos de dos formas y tenemos que

$$\sum_{g \in G} |Fi(g)| = \sum_{i \in \Omega} |G_i|.$$

Además, por 2.69 si dos elementos de Ω pertenecen a la misma órbita entonces sus estabilizadores son conjugados, luego tienen el mismo orden. Sean $O_{i_1}, \ldots, O_{i_r}$ las r órbitas, entonces, teniendo en cuenta el *Teorema de la órbita estabilizadora*,

$$\sum_{i \in \Omega} |G_i| = \sum_{k=1}^{r} [G : G_{i_k}]|G_{i_k}| = \sum_{k=1}^{r} |G| = r|G| \Rightarrow r|G| = \sum_{g \in G} |Fi(g)|,$$

donde $[G : G_{i_k}]$ es el número de elementos de la órbita de i_k y $|G_{i_k}|$ es el número de elementos $g \in G$ tales que $g \cdot i_k = i_k$ (además está claro que el cardinal del conjunto

que hemos escrito al principio es la suma de los $[G : G_{i_k}]|G_{i_k}|$ para cada $k = 1, \ldots, r$, aquí cada i_k es un elemento de Ω). Y de aquí,

$$r = \frac{1}{|G|} \sum_{g \in G} |Fi(g)|.$$

□

Definición 2.73. *Sea p un número primo. Un grupo G es un p-**grupo finito** si G es finito y $|G|$ es una potencia de p.*

Teorema 2.74. *Sea G un grupo actuando sobre un conjunto finito Ω. Escogemos $\alpha_1, \ldots, \alpha_s$ representantes de las órbitas de longitud mayor que 1. Entonces*

$$|\Omega| = |\Omega_0| + \sum_{j=1}^{s} |O_{\alpha_j}|.$$

En particular, si G es un p-grupo finito, entonces

$$|\Omega| \equiv |\Omega_0| \; mod\, p.$$

Demostración: La primera parte se deduce de la fórmula de las órbitas y del teorema de la órbita estabilizadora. Sea ahora G un grupo tal que $|G| = p^n$. Por 2.70, tendremos que $|O_{\alpha_j}| = [G : G_{\alpha_j}] > 1$, con $j = 1, \ldots, s$. Como cada $[G : G_{\alpha_j}]$ divide a $|G| = p^n$, ya está.

□

La descomposición del conjunto Ω en unión de las diferentes órbitas tiene especial interés cuando la acción es la conjugación de un grupo G sobre sí mismo. En este caso consideraremos:

Definición 2.75. *Consideremos la acción de un grupo G sobre sí mismo, $\Omega = G$,*

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & S_G \\ & g & \longmapsto & \alpha_g \end{array}$$

*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 ρ es homomorfismo.

*El núcleo de ρ es $Ker\, \rho = \{g \in G : \alpha_g = id\} = \{g \in G : gxg^{-1} = x \; \forall x \in G\} = \{g \in G : gx = xg \; \forall x \in G\}$ y es el **centro de** G, que se escribe $Z(G)$.*

*El estabilizador de 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, como $G_x \leq G$ entonces también $C_G(x) \leq G$.*

Por último, si $x \in G$, su órbita O_x será $O_x = \{gxg^{-1} : g \in G\}$. La denominaremos ***clase de conjugación de*** x ***en*** G*. Y, siguiendo el teorema de la órbita estabilizadora vemos que tiene*

$$[G : C_G(x)] = \frac{|G|}{|C_G(x)|}$$

elementos. La denotaremos por $Cl_G(x)$, es decir, tendremos:

$$Cl_G(x) = \{gxg^{-1} : g \in G\}$$

$$|Cl_G(x)| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

Notar que $|Cl_G(x)| = 1$ si y sólo si $gx = xg \ \forall g \in G$, es decir, si y sólo si $x \in Z(G)$. Luego, en este caso $\Omega_0 = Z(G)$.

Todos estos conceptos ya los habíamos visto en el primer capítulo.

Teorema 2.76 (***Ecuación de las clases de conjugación de un grupo***)**.** *Sea 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 (en este caso $\Omega_0 = Z(G)$) y del teorema 2.74. Notar que, por el teorema de la órbita estabilizadora, $|K_j| = |O_{\alpha_j}| = [G : G_{\alpha_j}] = [G : C_G(\alpha_j)]$ para $j = 1, \ldots, s$, con los α_j representantes de las clases de conjugación (órbitas) de longitud mayor que 1. ($G = C_G(x) \iff x \in Z(G)$, entonces $[G : C_G(x)] > 1$ si y sólo si $x \notin Z(G)$.)

□

Se desprende de aquí claramente que

$$|G| \equiv |Z(G)| \mod p.$$

Proposición 2.77. *Sea $G \neq \{1\}$ un p-grupo finito. Entonces tenemos que $Z(G) \neq \{1\}$.*

Demostración: Por 2.74 y 2.76 tenemos que $|G| \equiv |Z(G)| \bmod p$. Como $|G| = p^n$ y $p^n \not\equiv 1 \bmod p$ ya está.

□

Corolario 2.77.1. *Sea G un p-grupo finito simple. Entonces $|G| = p$.*

Demostración: Si G es simple entonces $Z(G) = G$, ya que sabemos por el resultado anterior que $Z(G) \neq \{1\}$, y como el centro es un subgrupo normal y G es simple entonces necesariamente $Z(G) = G$. Luego G es abeliano y el resultado se sigue de 2.36.1.

□

Es decir, ***todo p-grupo finito simple es abeliano***.

Recordemos que si $H \leq G$ definíamos el **normalizador** de H en G como

$$N_G(H) = \{g \in G : H^g = H\}.$$

Notar que $N_G(H)$ es el estabilizador de H en la acción de G sobre sus subgrupos por conjugación:

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & S_\Omega \\ & g & \longmapsto & \rho_g(H) = H^g. \end{array}$$

donde Ω es el conjunto de subgrupos de G.

Es claro que $H \trianglelefteq N_G(H)$ y que $H \trianglelefteq G$ si y sólo si $N_G(H) = G$. Por el *Teorema de la órbita estabilizadora* tenemos que el número de subgrupos distintos de la forma H^g, con $g \in G$, es $[G : N_G(H)]$. Es decir, que el número de conjugados distintos de un subgrupo H de G viene dado por $[G : N_G(H)]$. Esto ya lo vimos en 2.26

Proposición 2.78. *Sea G un grupo finito y $H \leq G$ con $|H| = p^a$ para cierto primo p y $a \in \mathbb{N}$. Entonces*

$$[G : H] \equiv [N_G(H) : H] \bmod p.$$

Demostración: Consideremos el conjunto $\Omega = \{xH : x \in G\}$. Tenemos que H actúa sobre Ω por multiplicación a izquierda. Calculamos el número de puntos fijos, es decir Ω_0. Se tiene que $hxH = xH\ \forall h \in H$ si y sólo si $x^{-1}hx \in H\ \forall h \in H$ 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 $x \in N_G(H)$. El resultado se sigue de la segunda parte de 2.74.

□

Corolario 2.78.1. *Sea G un p-grupo finito. Si $H \leq G$ entonces $H \leq N_G(H)$.*

Demostración: Como $p^a \not\equiv 1 \bmod p$ si $a \geq 1$, aplicando el resultado anterior ya está.

□

Es decir, en los p-grupos los normalizadores crecen. El siguiente resultado es un caso particular del conocido *Teorema de Cauchy*.

Corolario 2.78.2. *Sea G un p-grupo finito. Si p^a divide a $|G|$, entonces G tiene un subgrupo de orden p^a.*

Demostración: Lo haremos por inducción sobre el orden de G. Podemos suponer que $G \neq \{1\}$ y que $p^a < |G|$. Entre los subgrupos propios de G elegimos el de mayor orden posible, H. Por el corolario anterior sabemos que $H \trianglelefteq G$. Por el *Teorema de*

correspondencia tenemos que G/H no tiene subgrupos propios. Por 2.36.1, se tiene que $[G : H] = p$. Ahora, p^a divide a $|H|$ y el resultado se sigue por inducción.

□

Finalmente, hablaremos de las acciones transitivas.

Definición 2.79. *Diremos que una acción de un grupo G sobre un conjunto Ω es* ***transitiva*** *si sólo hay una órbita, es decir, si Ω es una G-órbita. Dicho de otra manera: la acción de G sobre Ω es transitiva si para cualesquiera $\alpha, \beta \in \Omega$ existe un $g \in G$ tal que $g \cdot \alpha = \beta$.*

Proposición 2.80. *Sea G un grupo actuando sobre un conjunto Ω. Dados $\alpha \in \Omega$ y $g \in G$, entonces*

$$(G_\alpha)^g = G_{g\cdot\alpha}.$$

En particular, si la acción de G sobre Ω es transitiva, entonces todos los estabilizadores son conjugados.

Demostración: Lo primero ya se ha visto en el segundo apartado de 2.69.

Supongamos ahora que la acción de G sobre Ω es transitiva y sean $\alpha, \beta \in \Omega$. Entonces existe $g \in G$ tal que $g \cdot \alpha = \beta$ y

$$(G_\alpha)^g = G_\beta.$$

□

2.4. Grupos de permutaciones

Partimos de un conjunto finito Ω. Una ***permutación*** de Ω es una aplicación biyectiva $f : \Omega \longrightarrow \Omega$. A lo largo de esta sección estudiaremos el grupo S_Ω de permutaciones de Ω con la operación composición (producto) $g \circ f = gf$, con $g, f \in S_\Omega$. Recordemos que

$$|S_\Omega| = |\Omega|!.$$

Definición 2.81. *Dados $\alpha_1, \ldots, \alpha_n$ n elementos distintos de Ω, entonces designaremos por $(\alpha_1, \ldots, \alpha_n)$ a la única permutación $\sigma \in S_\Omega$ tal que $\sigma(\alpha) = \alpha$ si $\alpha \in \Omega \setminus \{\alpha_1, \ldots, \alpha_n\}$, $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$, …, $\sigma(\alpha_{n-1}) = \alpha_n$ y $\sigma(\alpha_n) = \alpha_1$. A la permutación $\sigma = (\alpha_1, \ldots, \alpha_n) \in S_\Omega$ la denominamos n-**ciclo** o* ***ciclo de longitud*** *n.*

Notar que los 1-ciclos son la aplicación identidad. A los 2-ciclos, dada la importancia especial que tienen y que iremos viendo, los llamaremos ***trasposiciones****. Notar que si t es una transposición entonces $o(t) = 2$ y $t = t^{-1}$.*

Definición 2.82. *Dada una permutación $\sigma \in S_n$, diremos que σ* ***mueve*** *un $\alpha_i \in \Omega$ si $\sigma(\alpha_i) = \alpha_j$, con $i \neq j$. Por el contrario, diremos que σ* ***fija*** *un $\alpha_i \in \Omega$ si $\sigma(\alpha_i) = \alpha_i$.*

Del conjunto Ω realmente lo que nos interesa desde el punto de vista de las permutaciones no es la naturaleza propia del conjunto o los elementos que la forman, sino que contiene un número n de elementos cualesquiera, por lo que podríamos simplemente escribir S_n para referirnos al grupo de permutaciones de un conjunto finito cualquiera Ω de n elementos en lugar de S_Ω. Veámoslo también así:

Observación 2.82.1. *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 $\sigma' \in S_m$ a la biyección de $\{1, \ldots, m\}$ 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. *Como hemos dicho antes, lo realmente importante del conjunto Ω es 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.

Se denotará indistintamente tanto S_n como S_Ω.

Cada elemento de S_n lo escribiremos en ocasiones de una forma un tanto especial, como sigue:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Esta notación nos ahorrará confusiones, ya que muestra el número n de elementos del que partimos, cosa que no aparece en la notación de ciclos. Es decir, si hablamos de la permutación $(1,2,3)$ no sabemos si estamos en S_3 o en S_5 o en cualquier S_n con $n > 3$, porque los elementos fijados no aparecen. En cambio, en la segunda notación sí apreciamos de que n partimos, por lo que sí sabemos en qué S_n nos encontramos.

Observar también que

$$(\alpha_1, \ldots, \alpha_n) = (\alpha_n, \alpha_1, \ldots, \alpha_{n-1}) = \ldots = (\alpha_2, \alpha_3, \ldots, \alpha_n, \alpha_1),$$

luego cada n-ciclo se puede escribir de n maneras distintas.

Para estudiar los grupos de permutaciones podemos usar las acciones de grupos sobre conjuntos, en concreto vemos que S_Ω actúa sobre Ω mediante $\sigma \cdot \alpha = \sigma(\alpha)$ (la acción natural), con $\sigma \in S_\Omega$, $\alpha \in \Omega$.

Definición 2.83. *Decimos que dos ciclos* $(\alpha_1, \ldots, \alpha_m)$, $(\beta_1, \ldots, \beta_n)$ *son* ***disjuntos*** *si los conjuntos* $\{\alpha_1, \ldots, \alpha_m\}$ *y* $\{\beta_1, \ldots, \beta_n\}$ *son disjuntos.*

Proposición 2.84. *Dado* Ω *un conjunto. Entonces:*

1. *Sea* $\sigma = (\alpha_1, \ldots, \alpha_m) \in S_\Omega$. *Entonces* $\sigma^i(\alpha_1) = \alpha_{i+1}$, *con* $1 \leq i \leq m-1$ *y* $\sigma^m(\alpha_1) = \alpha_1$. *En particular,* $o(\sigma) = m$.
2. *Si* $\gamma = (\beta_1, \ldots, \beta_n) \in S_\Omega$ *es disjunto con* $\sigma = (\alpha_1, \ldots, \alpha_m) \in S_\Omega$, *entonces* $\gamma\sigma = \sigma\gamma$.
3. *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.*

Demostración:

1. Es inmediato a partir de la definición de ciclo.
2. Comprobemos que $(\gamma\sigma) \cdot w = (\sigma\gamma) \cdot w$, $\forall w \in \Omega$. Si $w \neq \alpha_i$ y $w \neq \beta_j$, entonces es claro que $(\gamma\sigma) \cdot w = (\sigma\gamma) \cdot w$. Ahora, si $w \in \{\alpha_1, \ldots, \alpha_m\}$ entonces $\sigma \cdot w \in \{\alpha_1, \ldots, \alpha_m\}$, luego $\gamma \cdot w = w$, y también $\gamma \cdot (\sigma \cdot w) = \sigma \cdot w$, y así

   $$(\gamma\sigma) \cdot w = \gamma \cdot (\sigma \cdot w) = \sigma \cdot w = \sigma \cdot (\gamma \cdot w) = (\sigma\gamma) \cdot w.$$

   Y se razonaría de forma análoga si $w \in \{\beta_1, \ldots, \beta_n\}$.
3. La primera parte es consecuencia directa de lo visto en los apartados anteriores. Así, $\{a_1, \ldots, a_m\} = \{\sigma^r(a_1) : r \geq 0\}, \ldots, \{b_1, \ldots, b_n\} = \{\sigma^r(b_1) : r \geq 0\}$.

□

Proposición 2.85. *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 *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 resultado 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.

□

Ejemplo 2.85.1. *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 2.85.1. *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 2.85.2. *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: Sea h el mínimo común múltiplo de los números $o(\tau_i)$ para $1 \leq i \leq m$. Es decir, tenemos que $o(\tau_i)$ divide a h $\forall i$ y que si $o(\tau_i)$ divide a un entero m $\forall i$, entonces h divide a m.

Como $\tau_i \tau_j = \tau_j \tau_i$ $\forall i, j$ por el punto 2 de 2.84 tenemos que $(\tau_1 \ldots \tau_k)^n = (\tau_1)^n \ldots (\tau_k)^n$ para todo entero n. Así, observamos que $\sigma^h = 1$ y se deduce que $o(\sigma)$ divide a h.

Si $o(\sigma) = r$, entonces $(\tau_1)^r \ldots (\tau_k)^r = 1$. Probaremos que $(\tau_i)^r = 1$ para todo $1 \leq i \leq k$. Para ello, basta probar que $(\tau_i)^r$ fija todos los elementos de Ω. Dado un $\alpha \in \Omega$, si α

es fijado por τ_i, entonces α es fijado por $(\tau_i)^r$. Si τ_i mueve α, entonces α es fijado por τ_j para todo $j \neq i$, en particular por $(\tau_j)^r$. Por tanto $\alpha = (\tau_k)^r \dots (\tau_1)^r \cdot \alpha = (\tau_i)^r \cdot \alpha$ y deducimos que $(\tau_i)^r$ fija α. Concluimos que $(\tau_i)^r = 1$. Por lo tanto, $o(\tau_i)$ divide a r para todo i y tenemos que h divide a $r = o(\sigma)$. Luego $o(\sigma) = h$.

□

Proposición 2.86. *Sea $\sigma = (\alpha_1, \dots, \alpha_k)$ es un k-ciclo de S_n y sea $\gamma \in S_n$. Entonces $\sigma^\gamma = (\gamma(\alpha_1), \dots, \gamma(\alpha_k))$.*

Demostración: Sabemos que $\sigma(\alpha_i) = \alpha_{i+1}$, con $i = 1, \dots, k-1$ y $\sigma(\alpha_k) = \alpha_1$ (recordemos que la acción es $\sigma \cdot \alpha = \sigma(\alpha)$). Así, $(\gamma\sigma\gamma^{-1})(\gamma(\alpha_i)) = \gamma(\alpha_{i+1})$, con $i = 1, \dots, k-1$ y $(\gamma\sigma\gamma^{-1})(\gamma(\alpha_k)) = \gamma(\alpha_1)$. Finalmente, si $\beta \in \Omega \setminus \{\sigma(\alpha_1), \dots, \sigma(\alpha_k)\}$ entonces $\gamma^{-1}(\beta) \in \Omega \setminus \{\alpha_1, \dots, \alpha_k\}$. Por lo que $\sigma \cdot (\gamma^{-1}(\beta)) = \gamma^{-1}(\beta)$ y así σ^γ fija β. Luego σ^γ y $(\gamma(\alpha_1), \dots, \gamma(\alpha_k))$ actúan igual sobre cada elemento de Ω y así son iguales.

□

Una consecuencia muy útil de 2.85 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. En ocasiones también será conocido como **estructura de ciclos**, y habrá tantas distintas como particiones del número $|\Omega|$.

Proposición 2.87. *Dos permutaciones $\gamma, \tau \in S_n$ son conjugadas en S_n si y sólo si tienen el mismo tipo.*

Demostración: Si $\tau = (a_1, \dots, a_m) \cdots (b_1, \dots, b_n)$ es una descomposición de τ en ciclos disjuntos y $\gamma \in S_n$ es tal que $\sigma = \tau^\gamma$, entonces por el resultado anterior tenemos que

$$\sigma = \tau^\gamma = (\gamma(a_1), \dots, \gamma(a_m)) \cdots (\gamma(b_1), \dots, \gamma(b_n))$$

es una descomposición en ciclos disjuntos de $\sigma (= \tau^\gamma)$. Por lo que dos permutaciones conjugadas tienen el mismo tipo.

Recíprocamente, supongamos que $\tau = (a_1, \dots, a_m) \cdots (b_1, \dots, b_n)$ y también $\gamma = (a'_1, \dots, a'_m) \cdots (b'_1, \dots, b'_n)$ tienen el mismo tipo, veamos que son conjugadas (en estas expresiones se han incluido los 1-ciclos también). Tenemos que

$$\Omega = \{a_1, \dots, a_m\} \cup \cdots \cup \{b_1, \dots, b_n\} = \{a'_1, \dots, a'_m\} \cup \cdots \cup \{b'_1, \dots, b'_n\}$$

son dos particiones de Ω. Por lo que existe una única $\sigma \in S_n$ tal que $\sigma(a_i) = a'_i, \dots, \sigma(b_j) = b'_j$ para $1 \leq i \leq m, \dots, 1 \leq j \leq n$. Luego, por el resultado 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 2.75) ***está formada por todas las permutaciones del mismo tipo que*** σ.

Observación 2.87.1. *Sea $k > 1$, entonces el número de k-ciclos que mueven 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 2.87.1. *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 2.87.2. *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).

   $\langle(1,2,3)\rangle \cap \langle(4,5)\rangle = id$ 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 2.88. *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 $\sigma \in Z(S_n)$.

□

Ahora, estudiaremos el conocido como *grupo alternado*, pero antes veamos qué son las permutaciones pares e impares.

Sea $\Omega = \{1, 2, \ldots, n\}$, ya sabemos que en este caso hablaremos de S_n en lugar de S_Ω. Ahora, consideremos el conjunto $\mathcal{C}$ de los subconjuntos de Ω que tienen dos elementos, es decir,

$$\mathcal{C} = \{X \subseteq \Omega : |X| = 2\}.$$

Sea ahora un $\sigma \in S_n$, y sea $X = \{i, j\} \in \mathcal{C}$. Puede pasar que el signo del entero $i - j$ sea el mismo que el signo del entero $\sigma(i) - \sigma(j)$. En este caso, el signo de $j - i$ también es el signo de $\sigma(j) - \sigma(i)$, por lo que no importa si $i < j$ ó $j < i$. En este caso, escribiremos

$$inv_\sigma(X) = 0$$

y diremos que σ ***no invierte*** X. También puede ocurrir que los enteros $i - j$ y $\sigma(i) - \sigma(j)$ tengan signos opuestos. En este caso también lo tendrán $j - i$ y $\sigma(j) - \sigma(i)$ y escribiremos

$$inv_\sigma(X) = 1$$

y diremos que σ ***invierte*** X.

Así, definimos:

Definición 2.89. *Dado un* $\sigma \in S_n$*, su* ***signatura*** *es*

$$sig(\sigma) = (-1)^{\sum_{X \in \mathcal{C}} inv_\sigma(X)}.$$

Diremos que σ *es* ***par*** *si* $sig(\sigma) = 1$ *y que* σ *es* ***impar*** *si* $sig(\sigma) = -1$*.*

Otra forma de definirla es:

Definición 2.90. *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 con el homomorfismo ψ antes definido, podemos dar una definición formal de lo que es el *grupo alternado*:

Definición 2.91. *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 2.92. *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 2.93. *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,*

$$S_n/\mathcal{A}_n \cong C_2.$$

Observación 2.93.1. *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 $\sigma\tau(1) = 1 \neq 3 = \tau\sigma(1)$.*

Además, a partir de la proposición anterior y de 2.85, podemos afirmar que las transposiciones generan el grupo S_n, o sea que cada permutación es producto de transposiciones.

Ejemplo 2.93.1. *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 $\mathcal{A}_4$.*

■

Una vez visto las primeras definiciones y propiedades de los grupos de permutaciones 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 al matemático noruego Niels Henrik Abel. Así, tal y como hemos visto en el ejemplo anterior, $\mathcal{A}_4$ es el último grupo alternado que no es simple, a partir de ahí $\mathcal{A}_n$ es simple para $n > 4$.

Proposición 2.94. *Si $n \geq 3$, entonces $\mathcal{A}_n$ es transitivo sobre $\Omega = \{1, \ldots, n\}$*

Demostración: Si $1 \leq i < j \leq n$, elegimos un $k \neq i, j$ y tenemos que $(i,j,k)(i) = j$ (la permutación (i,j,k) sobre i). Claramente $(i,j,k) \in \mathcal{A}_n$.

□

Teorema 2.95 (***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 2.87.2 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 2.87.2 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 2.82.1 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 $K \cong \mathcal{A}_{n-1}$ es simple.

Por el resultado anterior $\mathcal{A}_n$ 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.

□

2.5. 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 2.96 (***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 un $x \in G$ 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

$$G/H \cong C_p.$$

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 2.97 (***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: Lo haremos nuevamente por inducción 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 $[G : C_G(x_i)] > 1$ 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.

□

De aquí podemos sacar la siguiente conclusión interesante: ***dado un grupo finito G y p un número primo, si p no divide al orden de ningún subgrupo propio de G entonces éste será abeliano.***

Pasemos ya con las definiciones que emplearemos y con las que trabajaremos a partir de ahora:

Definición 2.98. *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 $n \neq 0$. 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 2.99 (***Primer Teorema de Sylow***). *Sea G 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 2.76 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 2.100 (***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 $\Omega = G/\sim_P$ por multiplicación a izquierda como vimos en el primer ejemplo de 2.62.1. 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 de p-subgrupos de Sylow es $[G : N_G(P)]$. Éste número es un divisor del orden de G y también de $[G : P]$.***

Corolario 2.100.1. *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*.

□

Definición 2.101. *Los grupos finitos con un único p-Sylow para cada divisor primo p de |G| se llaman* ***grupos nilpotentes finitos****.*

Finalmente veremos el último de los teoremas de Sylow:

Teorema 2.102 (***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 sobre Ω por conjugación. Ya sabemos que $v_p = [G : N_G(P)]$. Es claro que $P^g = P$ para todo $g \in P$, luego la órbita de P es trivial. Veamos que es la única. Si $Q \in \Omega$ cumple 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 la acción de 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.

2.6. Resolubilidad

Definición 2.103. *Un grupo G se dice* ***resoluble*** *si existen subgrupos*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{k-1} \trianglelefteq G_k = G$$

tales que G_{i+1}/G_i es abeliano para todo $i = 0, \ldots, k-1$. Como G_{i+1}/G_i es abeliano si y sólo si

$$xG_iyG_i = yG_ixG_i$$

para todo $x, y \in G_{i+1}$, concluimos que G_{i+1}/G_i es abeliano si y sólo $xyx^{-1}y^{-1} \in G_i$ para todo $x, y \in G_{i+1}$.

La importancia de este concepto es fundamental en álgebra abstracta, ya que a cada *ecuación polinómica* de la forma

$$a_nx^n + \ldots + a_1x + a_0 = 0, \;\; a_0, \ldots, a_n \in \mathbb{Q}$$

se le puede asociar un grupo, y que dicho grupo sea resoluble es condición necesaria y suficiente para que las soluciones de la ecuación polinómica anterior se puedan expresar mediante sumas, restas, multiplicaciones, divisiones y extracción de raíces de números racionales. A esto se le conoce como *ser resoluble por radicales*, y es ésta la razón de llamar así a estos grupos, porque podríamos resumirlo en: *ecuación resoluble por radicales* $\iff$ *grupo asociado resoluble*. Esto es lo que se desarolla y

estudia en el seno de la *Teoría de Galois*. Podríamos considerar los grupos y su teoría como un ¿ingrediente? más, bastante potente y uno de los pilares, pero no el único. Como acabamos de ver los polinomios también juegan un papel central, y para poder relacionarlo con todo lo visto necesitaremos entender qué son y sobre qué estructuras se definen, pero eso lo veremos en la sección de anillos.

Proposición 2.104. *Sea G un grupo.*

1. *Si $H \leq G$ y G es resoluble, entonces H es resoluble.*
2. *Supongamos que $N \trianglelefteq G$. Entonces G es resoluble si y sólo si N y G/N son resolubles.*

Demostración: Supongamos que

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{k-1} \trianglelefteq G_k = G$$

son tales que G_{i+1}/G_i es abeliano para todo $i = 0, \ldots, k-1$. Por tanto, $xyx^{-1}y^{-1} \in G_i$ para todos $x, y \in G_{i+1}$ y para todo $i = 0, \ldots, k-1$.

Supongamos ahora que $H \leq G$. Sea $H_i = H \cap G_i$ para $i = 0, \ldots, k$. Tenemos que $H \cap G_{i+1} \leq G_{i+1}$ y $G_i \trianglelefteq G_{i+1}$. Por el *Segundo Teorema de Isomorfía*, tenemos que $H_i = H \cap G_i \trianglelefteq H \cap G_{i+1} = H_{i+1}$ y

$$H_{i+1}G_i/G_i \cong H_{i+1}/H_i.$$

Este grupo es abeliano ya que es isomorfo a un subgrupo de G_{i+1}/G_i. Tenemos que la serie $1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{k-1} \trianglelefteq H_k = H$, es tal que H_{i+1}/H_i es abeliano.

Supongamos ahora que $N \trianglelefteq G$. Como $G_i \trianglelefteq G_{i+1}$, se tiene que $NG_i \trianglelefteq NG_{i+1}$ por 2.31. Por tanto, $NG_i/N \trianglelefteq NG_{i+1}/N$ por 2.50. Así, tenemos una serie

$$N = NG_0/N \trianglelefteq NG_1/N \trianglelefteq \ldots \trianglelefteq NG_{k-1}/N \trianglelefteq NG_k/N = G/N.$$

Notar que $NG_{i+1}/N = \{Nx : x \in G_{i+1}\}$. Ahora,

$$(Nx)(Ny)(Nx)^{-1}(Ny)^{-1} = Nxyx^{-1}y^{-1} \in NG_i/N, \quad \forall x, y \in G_{i+1}.$$

Esto prueba que G/N es resoluble.

Supongamos finalmente que N y G/N son resolubles. Entonces existen series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_k = N$$

$$N = G_0 \trianglelefteq G_1/N \trianglelefteq \ldots \trianglelefteq G_n/N = G/N$$

tales que N_{i+1}/N_i y $(G_{j+1}/N)/(G_j/N)$ son abelianos para $i = 0, \ldots, k-1$ y $j = 0, \ldots, n-1$. Como $G_{j+1}/G_j \cong (G_{j+1}/N)/(G_j/N)$ por el *Tercer Teorema de Isomorfía* la serie

$$1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = N = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$$

prueba que G es resoluble.

□

Proposición 2.105. *Si G es un grupo nilpotente finito, entonces G es resoluble.*

Demostración: Por inducción sobre $|G|$. Sea p un divisor primo de $|G|$. Si G es un p-grupo, por 2.78.2 podemos hallar subgrupos

$$1 = G_0 \leq G_1 \leq \ldots \leq G_k = G$$

tales que $[G_{i+1} : G_i] = p$, con $i = 0, \ldots, k-1$. Por 2.78.1, tenemos que $G_i \trianglelefteq G_{i+1}$. Por tanto, G_{i+1}/G_i es cíclico de orden p y G es resoluble.

Por tanto, podemos suponer que G no es un p-grupo. Sea $P \in Syl_p(G)$. Tenemos que G/P es nilpotente. Por inducción, G/P es resoluble. Como ya sabemos que P es resoluble, el resultado queda demostrado aplicando el segundo apartado del resultado anterior.

□

Ahora podemos redefinir la caracterización de los grupos resolubles:

Teorema 2.106. *Un grupo finito G es resoluble si y sólo si G tiene una serie*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G,$$

donde G_{i+1}/G_i es cíclico de orden primo, con $i = 0, \ldots, k-1$.

Demostración: Si G tiene tal serie está claro que es resoluble. Para ver el recíproco, lo probaremos por inducción sobre $|G|$. Por ser G resoluble, existe $N \trianglelefteq G$ de orden más pequeño que el orden de G tal que G/N es abeliano. Sea M/N un subgrupo propio de G/N de orden el más mayor posible. Por el *Teorema de la correspondencia* y de 2.36.1 tenemos que G/M es cíclico de orden primo. Ahora, por la primera parte de 2.104, M es resoluble y aplicamos la hipótesis de inducción.

□

Proposición 2.107. *Si $n \geq 5$, entonces S_n no es resoluble.*

Demostración: Si S_n es resoluble, entonces A_n es resoluble aplicando la primera parte de 2.104. Por tanto, existe $N \trianglelefteq A_n$, tal que A_n/N es abeliano. Como A_n es simple, tenemos que $N = 1$. Pero A_n no es abeliano, contradicción

□

3. Anillos

3.1. Generalidades

Definición 3.1. *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*

I. *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 $-a$.*

II. *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*

$$a(bc)=(ab)c.$$

III. *La propiedad* ***distributiva*** *del producto con respecto a la suma, 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 o simplemente 0. Denotaremos por $A^*=A\setminus\{0\}$. Y, como en grupos, la operación conocida como producto podrá denotarse con un $\cdot$ en ocasiones o con simple yuxtaposición.

Finalmente, una notación usual para los anillos será $(A,+,\cdot)$, que incluye el conjunto y las dos operaciones dotadas.

Definición 3.2. *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 3.2.1. *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 3.3. *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 3.3.1. *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 3.4. *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* $\mathcal{U}(A) \subseteq A^*$*, y los cuerpos son aquellos anillos unitarios* K *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****.*

Más adelante veremos un ejemplo bastante interesante de anillo en el que todos sus elementos son idempotentes.

Propiedades 3.4.1. *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 3.4.1. *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 $u \in 2\mathbb{Z}$ de la forma $2z$ con z algún entero, tal que $2z \cdot 2a = 2a$ con $a \in \mathbb{Z}$.*

3. *Los cocientes de $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, con $n \in \mathbb{N}$, también forman un anillo cuyas unidades serán todos los elementos $a+n\mathbb{Z}$ tales que $mcd(a, n) = 1$. Más adelante veremos detalladamente este anillo, que es bastante interesante. De hecho si n es primo también será un cuerpo.*

4. *Los conjuntos $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ de los números racionales, reales y complejos respectivamente son cuerpos conmutativos.*

5. *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****.*

$$\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}.$$

6. *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 a excepción del 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.

7. *Denotaremos por $M_n(K)$ al conjunto de las matrices cuadradas de orden n con coeficientes en un cuerpo $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Entonces el conjunto de sus unidades (que de hecho será un grupo) es $GL_n(K)$.*

8. *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

$$c_1(t) = 1.$$

9. *Si A es un anillo, podemos construir el **anillo de polinomios** $A[x]$ sobre A. Más adelante detallaremos en una sección propia este particular anillo, pero ahora podemos presentarlo en líneas generales para poder ver algunos resultados referentes a él en las siguientes páginas.*

   Un polinomio $p \in A[x]$ es una suma de la forma

$$p = \sum_n a_n x^n,$$

   *con $a_n \in A$ para todo n y donde existe un m tal que $a_n = 0$ si $n > m$. En ocasiones también podremos escribir estos elementos como $p(x)$. Si tenemos que $p = a_m x^m + \ldots + a_1 x + a_0$, y $a_m \neq 0$ entonces podremos decir que el **grado** de p, $\delta(p)$, es m. También diremos que los términos $a_m, \ldots, a_1, a_0$ son los **coeficientes** de p y concretamente que a_m es el **coeficiente director** de p. Si este coeficiente director a_m cumple que $a_m = 1$ diremos que p es **mónico**. El polinomio 0 se suele convenir que tiene grado $-\infty$.*

   Diremos que dos polinomios $p = \sum_n a_n x^n$, $q = \sum_n b_n x^n$ son iguales si y sólo si $a_n = b_n$ para todo n. También los podremos sumar y multiplicar:

$$p + q = \sum_n (a_n + b_n) x^n,$$

$$pq = \sum_n \left(\sum_{\substack{i+j=n \\ i,j \geq 0}} a_i b_j \right) x^n.$$

■

Un anillo clásico muy interesante es el siguiente:

Ejemplo 3.4.2. *Sea X un conjunto, si consideramos el conjunto de las partes de X*

$$\mathcal{P}(X) = \{A : A \subseteq X\},$$

junto con las dos operaciones

$$A + B = (A \setminus B) \cup (B \setminus A), \quad \forall A, B \in \mathcal{P}(X),$$

$$A \cdot B = A \cap B, \quad \forall A, B \in \mathcal{P}(X).$$

*Entonces $(\mathcal{P}(X), +, \cdot)$ es un anillo conmutativo pero no unitario. A la operación $+$ la denominaremos **diferencia simétrica**, y se suele representar por Δ.*

*Veámoslo, para ello definamos la **función característica de un conjunto**: dado dos conjuntos cualesquiera A, X tales que $A \subseteq X$,*

$$\begin{array}{rccl} \mathcal{X}_A\colon & X & \longrightarrow & \{1,0\} \\ & x & \longmapsto & \mathcal{X}_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases} \end{array}$$

Esta función cumple:

1. $\mathcal{X}_A = \mathcal{X}_B \Leftrightarrow A = B$.

   En efecto, si $x \in A$, entonces $\mathcal{X}_A(x) = 1$. Por hiótesis $\mathcal{X}_A = \mathcal{X}_B$, luego $\mathcal{X}_B(x) = 1$, y $x \in B$ y así $A \subseteq B$. Para el otro contenido es análogo. Reciprocamente, por hipótesis $A = B$ y si $x \in A = B$ entonces $\mathcal{X}_A(x) = \mathcal{X}_B(x) = 1$. Si $x \notin A = B$ entonces $\mathcal{X}_A(x) = \mathcal{X}_B(x) = 0$. Como $\mathcal{X}_A(x) = \mathcal{X}_B(x)$ para todo $x \in X$ concluimos que $\mathcal{X}_A = \mathcal{X}_B$.

2. $\mathcal{X}_{A^c} = 1 - \mathcal{X}_A$.

   Si $x \in A$, entonces $x \notin A^c$, luego $\mathcal{X}_A(x) = 1$ y $\mathcal{X}_{A^c}(x) = 0$, así que $\mathcal{X}_{A^c}(x) = 1 - \mathcal{X}_A(x)$. Si $x \notin A$, entonces $x \in A^c$, luego $\mathcal{X}_A(x) = 0$ y $\mathcal{X}_{A^c}(x) = 1$, así que $\mathcal{X}_{A^c}(x) = 1 - \mathcal{X}_A(x)$. Como esto se tiene para todo $x \in X$, concluimos que $\mathcal{X}_{A^c} = 1 - \mathcal{X}_A$.

3. $\mathcal{X}_{A\cap B} = \mathcal{X}_A \cdot \mathcal{X}_B$.

   Si $x \in A \cap B$ entonces $x \in A$ y $x \in B$, luego $\mathcal{X}_{A\cap B} = 1$, y $\mathcal{X}_A = 1$, $\mathcal{X}_B = 1$. Es decir, si $x \in A \cap B$ entonces $\mathcal{X}_{A\cap B}(x) = \mathcal{X}_A(x) \cdot \mathcal{X}_B(x)$. Por otra parte, si $x \notin \mathcal{X}_{A\cap B}$ entonces $x \notin A$ ó $x \notin B$, luego $\mathcal{X}_{A\cap B}(x) = 0$ y ó $\mathcal{X}_A(x) = 0$ ó $\mathcal{X}_B(x) = 0$. Por lo tanto, si $x \notin A \cap B$ entonces también se tiene que $\mathcal{X}_{A\cap B}(x) = \mathcal{X}_A(x) \cdot \mathcal{X}_B(x)$. Concluimos que $\mathcal{X}_{A\cap B} = \mathcal{X}_A \cdot \mathcal{X}_B$.

4. $\mathcal{X}_{A\cup B} = \mathcal{X}_A + \mathcal{X}_B - \mathcal{X}_A \cdot \mathcal{X}_B$.

   Si $x \in A \cup B$ entonces $\mathcal{X}_{A\cup B}(x) = 1$. Según los distintos casos tenemos: si $x \in A \cap B$ entonces $\mathcal{X}_A(x) + \mathcal{X}_B(x) - \mathcal{X}_A(x) \cdot \mathcal{X}_B(x) = 1 + 1 - 1 \cdot 1 = 1$. Si $x \in A$ y $x \notin B$ entonces $\mathcal{X}_A(x) + \mathcal{X}_B(x) - \mathcal{X}_A(x) \cdot \mathcal{X}_B(x) = 1 + 0 - 1 \cdot 0 = 1$. Si $x \notin A$ y $x \in B$ entonces $\mathcal{X}_A(x) + \mathcal{X}_B(x) - \mathcal{X}_A(x) \cdot \mathcal{X}_B(x) = 0 + 1 - 0 \cdot 1 = 1$. Si $x \notin A \cup B$, entonces $\mathcal{X}_{A\cup B}(x) = 0$, y como $x \notin A$, $x \notin B$: $\mathcal{X}_A(x) +$

$\mathcal{X}_B(x) - \mathcal{X}_A(x) \cdot \mathcal{X}_B(x) = 0 + 0 - 0 \cdot 0 = 0$. *Por lo tanto, para todo* $x \in X$ *se tiene que* $\mathcal{X}_{A\cup B}(x) = \mathcal{X}_A(x) + \mathcal{X}_B(x) - \mathcal{X}_A(x) \cdot \mathcal{X}_B(x)$, *luego concluimos que* $\mathcal{X}_{A\cup B} = \mathcal{X}_A + \mathcal{X}_B - \mathcal{X}_A \cdot \mathcal{X}_B$.

5. $\mathcal{X}_{A\Delta B} = \mathcal{X}_A + \mathcal{X}_B - 2 \cdot \mathcal{X}_A \cdot \mathcal{X}_B$.

   Para todo $x \in X$ *se tiene que* $\mathcal{X}_\emptyset(x) = 0$ *ya que* $x \notin \emptyset$. *Es decir,* $\mathcal{X}_\emptyset = 0$. *Por los dos apartados anteriores tenemos que* $\mathcal{X}_{A\cup B} = \mathcal{X}_A + \mathcal{X}_B - \mathcal{X}_{A\cap B}$ *y si* $A \cap B = \emptyset$ *entonces* $\mathcal{X}_{A\cup B} = \mathcal{X}_A + \mathcal{X}_B$. *La diferencia simétrica sabemos que la podemos expresar como* $(A \setminus B) \cup (B \setminus A)$, *siendo esta unión disjunta, luego* $\mathcal{X}_{A\Delta B} = \mathbb{X}_{A\setminus B} + \mathcal{X}_{B\setminus A} = \mathcal{X}_{A\cap B^c} + \mathcal{X}_{B\cap A^c} = \mathcal{X}_A \cdot \mathcal{X}_{B^c} + \mathcal{X}_B \cdot \mathcal{X}_{A^c} = \mathcal{X}_A \cdot (1 - \mathcal{X}_B) + \mathcal{X}_B \cdot (1 - \mathcal{X}_A) = \mathcal{X}_A + \mathcal{X}_B - 2 \cdot \mathcal{X}_A \cdot \mathcal{X}_B$.

Comprobemos ahora que es un anillo:

1. *La propiedad más costosa de ver es la asociativa para* $+$, *que sabemos que es la diferencia simétrica* Δ, *así que todo se reduce a ver que, dados* $A, B, C \in \mathcal{P}(X)$, $(A + B) + C = A + (B + C)$ *ó dicho de otra forma:* $(A\Delta B)\Delta C = A\Delta(B\Delta C)$. *Usaremos las propiedades que hemos visto de la función característica, ya que sabemos que dos subconjuntos* $A = B$ *son iguales si y sólo si sus funciones características coinciden.*

   $\mathcal{X}_{(A\Delta B)\Delta C} = \mathcal{X}_{A\Delta B} + \mathcal{X}_C - 2\cdot\mathcal{X}_{A\Delta B}\cdot\mathcal{X}_C = \mathcal{X}_A + \mathcal{X}_B - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_B + \mathcal{X}_C - 2\cdot(\mathcal{X}_A + \mathcal{X}_B - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_B)\cdot\mathcal{X}_C = \mathcal{X}_A + \mathcal{X}_B - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_B + \mathcal{X}_C - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_C - 2\cdot\mathcal{X}_B\cdot\mathcal{X}_C + 4\cdot\mathcal{X}_A\cdot\mathcal{X}_B\cdot\mathcal{X}_C$.

   $\mathcal{X}_{A\Delta(B\Delta C)} = \mathcal{X}_A + \mathcal{X}_{B\Delta C} - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_{B\Delta C} = \mathcal{X}_A + \mathcal{X}_B + \mathcal{X}_C - 2\cdot\mathcal{X}_B\cdot\mathcal{X}_C - 2\cdot\mathcal{X}_A\cdot(\mathcal{X}_B + \mathcal{X}_C - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_C) = \mathcal{X}_A + \mathcal{X}_B + \mathcal{X}_C - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_B - 2\cdot\mathcal{X}_A\cdot\mathcal{X}_C - 2\cdot\mathcal{X}_B\cdot\mathcal{X}_C + 4\cdot\mathcal{X}_A\cdot\mathcal{X}_B\cdot\mathcal{X}_C$.

   Y se tiene la igualdad, luego se tiene que $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.

2. *Para el elemento neutro, notar que* $A\Delta\emptyset = \emptyset\Delta A = A$ *para todo* $A \in \mathcal{P}(X)$.

3. *Cada elemento es inverso de sí mismo, ya que* $A\Delta A = \emptyset$ *para todo* $A \in \mathcal{P}(X)$.

4. *La operación* Δ *es conmutativa, ya que* $A\Delta B = B\Delta A$ *para cualesquiera* $A, B \in \mathcal{P}(X)$.

5. *La operación* $\cdot$ *es asociativa, ya que* $(A\cap B)\cap C = A\cap(B\cap C)$ *para cualesquiera* $A, B, C \in \mathcal{P}(X)$. *Notar que también es conmutativa.*

6. *Veamos la propiedad distributiva de* $\cdot$ *respecto de* Δ. *Dados* $A, B, C \in \mathcal{P}(X)$, *entonces* $(A\Delta B) \cdot C = ((A \setminus B) \cup (B \setminus A)) \cdot C = ((A \setminus B) \cup (B \setminus A)) \cap C = ((A \setminus B) \cap C) \cup ((B \setminus A) \cap C) = ((A \cap C) \setminus B) \cup ((B \cap C) \setminus A) = ((A \cap C) \setminus (B \cap C)) \cup ((B \cap C) \setminus (A \cap C)) = (A \cap C)\Delta(B \cap C) = (A \cdot C)\Delta(B \cdot C)$.

7. *Notar que no existe elemento* 1 *ya que el único elemento* $B \in \mathcal{P}(X)$ *que cumple que para cualquier subconjunto* $A \in \mathcal{P}(X)$, $A \cdot B = A$ *es el propio* A.

Así, queda probad que $(\mathcal{P}(X), \Delta, \cdot)$ *es un anillo conmutativo, en el que además se tiene que* $A^2 = A$ *para cualquier* $A \in \mathcal{P}(X)$.

■

Los anillos A como el anterior que cumplan que para todo elemento $a \in A$ se tiene $a^2 = a$, que todo elemento sea idempotente, se denominan ***anillo de Boole***.

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 3.5. *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 3.5.1. *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 $(fg)(t) = (t - |t|)(t + |t|) = t^2 - |t|^2 = 0$.

Ejemplo 3.5.1. *Otros ejemplos de divisores de cero son:*

1. *En el anillo de las matrices cuadradas de orden 2 con coeficientes en $\mathbb{Z}$, $M_2(\mathbb{Z})$ tenemos:*
$$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

2. *En el anillo $\mathbb{Z}/n\mathbb{Z}$, si dos enteros a, b son tales que $ab = n$, entonces $a + n\mathbb{Z}$ y $b + n\mathbb{Z}$ son divisores de cero.*

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 fuerte que se encuentre entre ambas estructuras, es de aquí de dónde surge la siguiente definición:

Definición 3.6. *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. 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 3.7 (***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 (a, b) 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 $a \in A$.*

Notar que si A no es conmutativo, entonces su cuerpo de fracciones tampoco lo será.

Así, si $A = \mathbb{Z}$, entonces la anterior construcción nos devolverá el cuerpo $\mathbb{Q}$ de los números racionales.

Presentamos ahora la noción de característica de un anillo, que más adelante la detallaremos y analizaremos con más profundidad:

Definición 3.8 (***Característica de un anillo***)**.** *Llamaremos* ***característica*** *de un anillo A al menor natural no nulo n tal que $n \cdot 1 = n1 = 0$. En caso de que no exista diremos que A tiene característica 0.*

Es decir, la característica de un anillo es el mínimo número de veces que hay que sumar 1 consigo mismo para obtener 0, y si no existe dicho número entonces diremos que será 0.

Claramente los anillos $\mathbb{Z}$ y $\mathbb{Q}$ tienen característica 0, mientras que los cocientes de $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ tienen característica n.

Aunque no hemos dado una definición formal de qué es un número primo (y resultará importante darla para los objetivos de esta parte del texto) en la siguiente proposición nos bastará con emplear la que nos viene dada directamente de la aritmética: aquel que no puede descomponerse en un producto de otros números que no sean él mismo y el 1.

Proposición 3.9. *La característica de un dominio de integridad A es 0 o p, con p primo.*

Demostración: Supongamos que A es un dominio de integridad cuya característica no es 0. Sea p la característica de A y supongamos que no es primo, luego $p = nm$, con $n, m > 1$ enteros, y $m1 \neq 0 \neq n1$ pero $(m1)(n1) = (nm)1 = 0$, contradiciendo que A sea dominio de integridad.

□

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 3.10. *Sea B un anillo conmutativo y unitario, $A \subseteq B$ 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 $s-t, st \in A \; \forall st, \in A$. En particular, A es subgrupo de R.

Definición 3.11. *Llamaremos **cuerpo primo**, o también **subcuerpo primo**, de un cuerpo K a la intersección de todos los subcuerpos de K. Es decir, el subcuerpo primo de un cuerpo es el menor subcuerpo que contiene.*

Los denominamos cuerpos primos porque, tal y como veremos más adelante, serán de la forma $\mathbb{Z}_p$ con p primo, o $\mathbb{Q}$, es decir, el cuerpo de los racionales.

Además, resulta que la interseccion es cerrada para los subanillos:

Observación 3.11.1. *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 3.11.1. *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 3.11.2. *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 3.12. *Sea A un anillo conmutativo y unitario. Llamaremos* ***ideal*** *a un subconjunto $I \subseteq A$ 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 2. 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 2.). Así, I será subgrupo para la suma. Estas dos últimas condiciones son las que dió en su momento el matemático Richard Dedekind cuando definió el concepto de ideal (la primera es de Kummer).

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 3.13. *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 $\{0\} \neq I \neq A$, 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 $x \in A$ y así $I = A$. Por lo tanto será importante 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 y lo denotaremos 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 siguiente resultado, que define los cuerpos a partir de los ideales:

Proposición 3.14. *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 I contendrá algún elemento $a \neq 0$ y así $aa^{-1} = 1 \in I$, por lo que $I = A$. Recíprocamente, supongamos que los únicos ideales de A son los impropios. Sea un $0 \neq a \in A$ y consideremos el ideal que genera, $I = (a)$. Como a es no nulo I no es trivial, y así $I = A$, luego $1 \in I$ y esto quiere decir que existe 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, se tiene que A es un cuerpo.

□

Es decir: en un cuerpo K no hay más ideales que $\{0\}$ y el propio K.

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 3.15. ***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) ya que I tiene estructura de subgrupo.

El conjunto cociente de A para esta relación lo 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,

$$x + I = y + I \Leftrightarrow x \equiv y \ mod\ I, \text{ es decir, que } x - y, y - x \in I.$$

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.

En el siguiente capítulo desarrollaremos adecuadamente este último resultado.

Observación 3.15.1. *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 3.16 (***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 $I \subseteq A$ 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 $J \subseteq A$ tales que $L \subseteq J$, 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

$$\bigcap_{J \in \mathcal{L}} J \subseteq I.$$

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 $I \subseteq J$. Siendo esto igual para todo ideal J de $\mathcal{L}$, tenemos que

$$I \subseteq \bigcap_{J \in \mathcal{L}} J.$$

Por tanto, la igualdad.

Este ideal I que acabamos de construir es lo que conoceremos como ***ideal generado por*** L.

□

Definición 3.17. *Sea A un anillo conmutativo y unitario. Un ideal $I \subseteq A$ se llama* ***finitamente generado*** *si es un ideal generado por un subconjunto finito $L = \{x_1, \ldots, x_r\} \subseteq A$. 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, si el ideal está generado por un solo elemento, entonces I se llama ***ideal principal****.*

Definición 3.18. *Un anillo A se dirá* ***noetheriano****, en honor a la gran matemática alemana Emmy Noether, si todos sus ideales son finitamente generados.*

Los anillos noetherianos cumplen la siguiente condición:

Teorema 3.19 (***Condición de cadena ascendente***)**.** *Sea A un dominio de integridad. Entonces son equivalentes:*

1. *A es un anillo noetheriano.*
2. *Para toda cadena ascendente de ideales de A*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

existe un número natural n tal que $I_n = I_m$ para todo $m \geq n$.

3. *Toda familia no vacía de ideales de A tiene un maximal*

Demostración: Si $I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ es una cadena ascendente de ideales de A, es fácil ver que la unión $I = \bigcup_{i=0} I_i$ es también un ideal de A. Si A es noetheriano entonces I ha de tener un generador finito X. Cada elemento de X está en uno de los ideales I_i, y como X es finito y los ideales forman una cadena, existirá un natural n tal que $X \subseteq I_n$, pero entonces $\bigcup_{i=0} I_i = (X) \subseteq I_n$, lo que implica que $I_i = I_n$ para todo $i \geq n$. Por tanto 1 implica 2.

Si una familia no vacía de ideales de A no tuviera maximal, se podría extraer una cadena ascendente de ideales que contradijera 2, luego 2 implica 3.

Si A tuviera un ideal I que no admitiera un generador finito, entonces, dado cualquier elemento a_0 de I, se cumple que $(a_0) \neq I$, luego existe un elemento $a_1 \in I \setminus (a_0)$, luego $(a_0) \subseteq (a_0, a_1) \neq I$ y de esta forma podemos conseguir una cadena de ideales $(a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \dots$ sin que ninguno de ellos sea maximal. Luego 3 implica 1.

□

Es claro que todo cuerpo K es un anillo noetheriano.

Definición 3.20 (***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 $a_1, \dots, a_r, b_1, \dots, b_s \in A$, $x_1, \dots, x_r \in I$, $y_1, \dots, y_s \in J$, podremos escribir $a_1x_1 + \dots + a_rx_r + b_1y_1 + \dots + b_sy_s = x + y$, con $x = a_1x_1 + \dots + a_rx_r \in I$, e $y = b_1y_1 + \dots + b_sy_s \in J$.*
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:*

$$IJ = \{x_1y_1 + \dots + x_ry_r : x_1, \dots, x_r \in I,\ y_1, \dots, y_r \in J,\ r \geq 1\}.$$

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 3.21. *Dado un anillo conmutativo y unitario A, y dos ideales I, J de A, entonces tendremos:*

1. *$IJ \subseteq I \cap J$.*
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*

$$I_1 \cdots I_r \subseteq I_1 \cap \cdots \cap I_r.$$

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

$$I_1 \cdots I_r \subseteq (I_1 \cdots I_{r-1})I_r \subseteq (I_1 \cdots I_{r-1}) \cap I_r \subseteq (I_1 \cap \cdots \cap I_{r-1}) \cap I_r \subseteq I_1 \cap \cdots \cap I_r.$$

□

Definición 3.22. *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 3.22.1. *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 $ax \in J$, $ay \in I$ y se tendrá:*

$$a = a1 = a(x + y) = ax + ay \in IJ.$$

Ahora se introducirá dos clases muy importantes de ideales, que serán esenciales en lo que sigue.

Definición 3.23. *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 3.24. *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 $1 - xy \in I \subseteq J$. Ahora como $xy \in J$, por ser J un ideal, tendremos que $1 = (1 - xy) + xy \in J$ y así $J = A$, lo cual es absurdo.

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 $I + (x)$ contiene estrictamente a I. Como este último es maximal tendremos que $I + (x) = A$, 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 3.25. *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 3.25.1. *Todo ideal maximal es primo, ya que todo cuerpo es dominio de integridad.*

Observación 3.25.2. *Notar que $A = A/(0)$, con A un anillo cualquiera. Luego A es un dominio de integridad si y sólo si (0) es primo y A es cuerpo si y sólo si (0) es maximal.*

Finalmente, estudiaremos dos clases concretas de ideales bastante interesantes:

Definición 3.26. *Sea A un anillo conmutativo y unitario, se dice que un ideal I de A es **radical** si para todo $x \in A$ tal que $x^n \in I$, con n un entero positivo, se cumple que $x \in I$.*

Proposición 3.27. *Todo ideal primo I de un anillo conmutativo y unitario A es radical.*

Demostración: Tenemos que ver que si $x \in A$ y $n > 0$ es un entero tal que $x^n \in I$ entonces $x \in I$. Lo haremos por inducción sobre n: es evidente para $n = 1$. Ahora, si $n > 1$ y $x^n \in I$ entonces $x \cdot x^{n-1} \in I$ y por ser I primo entonces ó $x \in I$ y ya hemos terminado, ó $x^{n-1} \in I$. En el segundo caso la hipótesis de inducción asegura que $x \in I$.

□

Proposición 3.28. *Sean A un anillo e I un ideal propio de A. Entonces:*

1. *Existe un ideal maximal M de A que contiene a I.*
2. *El anillo A posee algún ideal maximal.*
3. *Para cada $x \in A \setminus \mathcal{U}(A)$ existe un ideal maximal M de A tal que $x \in M$.*

Demostración:

1. La familia de ideales

$$\mathcal{F} = \{J \subseteq A \text{ ideal de } A \ : I \subset J\},$$

   es no vacía pues contiene al ideal I y está parcialmente ordenada con respecto a la inclusión. Toda cadena de ideales $\mathcal{C} = \{J_l\}_{l \in L}$ de $\mathcal{F}$ está acotada superiormente ya que $J = \cup_l J_l \in \mathcal{F}$ es una cota superior suya. Por el *Lema de Zorn* existe un elemento maximal $M \in \mathcal{F}$. Veamos que M es un ideal maximal de A que contiene a I:

   La inclusión $I \subseteq M$ se deduce de que $M \in \mathcal{F}$. Por otro lado, si M no es un ideal maximal de A, existe un ideal J tal que $M \subset J \subset A$. Pero entoncces $I \subseteq M \subset J \subset A$ y así $J \in \mathcal{F}$, y esto contradice la maximalidad de M.

2. Basta aplicar el apartado anterior al ideal $I = \{0\}$.

3. Como x no es unidad, se tiene que el ideal $(x) \neq A$, luego por 1. existe un ideal maximal M de A que contiene a (x), y así $x \in M$.

□

Definición 3.29. *Llamaremos **radical de Jacobson** I de A, con A un anillo conmutativo y unitario, a la intersección de todos los ideales maximales de A. Lo denotaremos por $\mathcal{R}$.*

Además, los podemos caracterizar de la siguiente forma:

Proposición 3.30. *Dado A un anillo conmutativo y unitario, $x \in \mathcal{R}$ si y sólo si $1 - xy$ es una unidad en A para todo $y \in A$.*

Demostración: Sea $x \in \mathcal{R}$ y supongamos que $1 - xy$ no es unidad. Entonces, por el resultado anterior, $1 - xy$ pertenece a un ideal maximal M, pero $x \in \mathcal{R} \subseteq M$, por lo que $xy \in M$ y así $1 \in M$, absurdo.

Recíprocamente, supongamos que $x \notin M$ para todo ideal maximal M. Entonces M y x generan el ideal (1), luego $u + xy = 1$ para algún $u \in M$ y algún $y \in A$. Por lo tanto, $1 - xy \in M$ y esto implicaría que $1 - xy$ no es una unidad, contradiciendo la hipótesis.

□

3.2. Homomorfismos

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 3.31. *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 3.31.1. *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 3.31.1. *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 3.4.1. 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 3.32. *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

$$y - v = f(x) - f(u) = f(x-u) \in imf,$$

$$y \cdot v = f(x)f(u) = f(xu) \in imf,$$

$$1_B = f(1_A) \in imf.$$

Un homomorfismo muy importante es el conocido como *homomorfismo evaluación*, que involucra anillos de polinomios. Si $p(x) = a_k x^k + \ldots + a_1 x + a_0 \in A[x]$ y $a \in A$, con A un anillo conmutativo y unitario, entonces definimos $p(b) = a_k b^k + \ldots + a_1 b + a_0$. Es decir, tratamos a x como una variable que puede ser evaluada en distintos *valores* b. Esto lo veremos más adelante.

Proposición 3.33 (***Homomorfismo evaluación***). *Sean A y B anillos conmutativos y unitarios tales que $A \subseteq B$ (A subanillo de B), y supongamos que $b \in A$. Entonces, la aplicación*

$$\begin{array}{rccc} ev_b\colon & A[x] & \longrightarrow & B \\ & p = \sum_i a_i x^i & \longmapsto & p(b) = \sum_i a_i b^i \end{array}$$

es un homomorfismo de anillos.

Demostración: Observar que $ev_b(1) = 1$. Si $p(x) = \sum_i a_i x^i$ y $q(x) = \sum_i c_i x^i$ hay que comprobar que $(p+q)(b) = p(b)+q(b)$ y que $pq(b) = p(b)q(b)$. Es un simple ejercicio.

□

Notar que el ***núcleo del homomorfismo evaluación*** en b estará formado por todos los polinomios que anulen b, ó dicho de otra manera: que tengan a b por raíz (más adelante definiremos raíz de un polinomio de manera formal). Además, la ***imagen del homomorfismo evaluación*** en b será el menor subanillo de B que contiene a A y a b, que denotaremos por $A[b]$.

Proposición 3.34. *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.

□

Proposición 3.35. *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.

□

Como si I es primo el cociente A/I es dominio de integridad, de este resultado deducimos que ***todo dominio de integridad finito es un cuerpo***.

Observación 3.35.1. *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 $ker f$ un ideal de K distinto de K (ya que $f(1_K) = 1_B$), por 3.14 sólo puede ser $\{0\}$, y así f es inyectiva.

Notar que, dado un homomorfismo de anillos $f\colon A \longrightarrow B$, si $I \subseteq A$ es un ideal de A, entonces $f(I)$ no tiene por qué ser necesariamente un ideal de B. Por ejemplo, si consideramos la inclusión $i\colon \mathbb{Z} \longrightarrow \mathbb{Q}$ y un ideal I de $\mathbb{Z}$, y $f(I)$ no es ideal de $\mathbb{Q}$ ya que $\mathbb{Q}$ es un cuerpo y sus únicos ideales son él mismo y el trivial. Sin embargo,

Proposición 3.36. *Dado un homomorfismo de anillos sobreyectivo $f\colon A \longrightarrow B$ e I un ideal de A, entonces $f(I)$ es un ideal de B.*

Demostración: Si $b_1, b_2 \in f(I)$ existen $a_1, a_2 \in I$ tales que $f(a_i) = b_i$, y como $a_1 + a_2 \in I$ entonces $b_1 + b_2 = f(a_1) + f(a_2) = f(a_1 + a_2) \in f(I)$. Además, dados $b \in B$ e $y \in f(I)$ existen, por ser f sobreyectiva, $a \in A, x \in I$ tal que $f(a) = b$ y $f(x) = y$. Como $ax \in I$, se tiene que $by = f(a)f(x) = f(ax) \in f(I)$.

□

Además,

Proposición 3.37. *Dado un homomorfismo de anillos $f\colon A \longrightarrow B$ y J un ideal de B. Entonces $I = f^{-1}(J)$ es un ideal de A. Además, si $J \neq B$ entonces $I \neq A$.*

Demostración: Dados $a_1, a_2 \in I$, sus imágenes $f(a_1), f(a_2) \in J$, luego $f(a_1 + a_2) = f(a_1) + f(a_2) \in J$, es decir, $a_1 + a_2 \in I$. Además, si $a \in A$ y $x \in I$ se tiene que $f(a) \in B$, $f(x) \in J$, por lo que $f(ax) = f(a)f(x) \in J$ y así $ax \in I$.

Para lo último, notar que si $I = A$ entonces $1 \in I$, por lo que $1 = f(1) \in J$ y así $J = B$.

□

Si tenemos un homomorfismo de anillos $f\colon A \longrightarrow B$ como en la proposición anterior diremos que I es el ***contraído*** de J mediante f. Notar que $ker f = f^{-1}(0)$, luego $ker f \subseteq f^{-1}(J)$, con J un ideal cualquiera de B.

Notar también que, dado un homomorfismo de anillos conmutativos y unitarios $f\colon A \longrightarrow B$ y M un ideal maximal de B, no siempre se va a tener que $f^{-1}(M)$ sea un ideal maximal de A. Por ejemplo, en la inclusión $i\colon \mathbb{Z} \longrightarrow \mathbb{Q}$, $M = (0)$ es un ideal maximal en $\mathbb{Q}$, ya que $\mathbb{Q}$ es un cuerpo, pero $(0) = i^{-1}(M)$ no es un ideal maximal de $\mathbb{Z}$.

Sin embargo, sí va a ocurrir con los ideales primos. Es decir, dado un homomorfismo de anillos $f\colon A \longrightarrow B$, si J es un ideal primo de B, entonces $I = f^{-1}(J)$ va a ser un ideal primo de A. Sean $a, x \in A$ tales que $ax \in I$. Así, $f(ax) = f(a)f(x) \in J$ y como J es primo entonces ó $f(a) \in J$ ó $f(x) \in J$. Si $f(a) \in J$ entonces $a \in I$ y si $f(x) \in J$ entonces $x \in I$, luego I es primo.

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 3.38. *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.*

Ejemplo 3.38.1. *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 el conjunto de los ideales de $\mathbb{Z}$, $\mathcal{I}$, y los enteros no negativos, $\mathbb{Z}^+$, con $(0) = 0\mathbb{Z} = \{0\}$ y $1\mathbb{Z} = \mathbb{Z}$:

$$\begin{array}{ccc} \mathbb{Z}^+ & \longrightarrow & \mathcal{I} \\ k & \longmapsto & (k), \end{array}$$

Veamoslo:

Supongamos que $(k) = (l)$, con $k, l \geq 0$. Entonces $k \in (l)$ y $l \in (k)$. Si $l = 0$, 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.

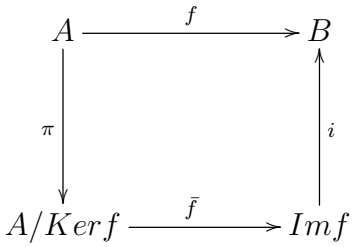
■

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. Luego, dados dos anillos conmutativos y unitarios A y B, diremos que son *isomorfos* cuando exista un isomorfismo $f\colon A \longrightarrow B$. Esto 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 $A \cong B$. 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 3.39 (***Primer Teorema de Isomorfía***). *Sea $f\colon A \longrightarrow B$ un homomorfismo de anillos conmutativos y unitarios. Consideremos el diagrama siguiente:*



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:

$$A/Kerf \cong Imf.$$

y

$$\begin{array}{rccc} i\colon & Imf & \longrightarrow & B \\ & f(x) & \longmapsto & f(x) = y, \end{array}$$

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 $\bar{f}(x + Kerf) = \bar{f}(y + Kerf)$, es decir, $\bar{f}$ 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

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

□

Observación 3.39.1. *Notar que si aplicamos el Primer Teorema de Isomorfía al homomorfismo evaluación ev un $b \in A$ cualquiera, tenemos que*

$$A[x]/ker\ ev_b \cong A[b].$$

Corolario 3.39.1. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Demostración: Consideremos el homomorfismo $f\colon \mathbb{R}[x] \longrightarrow \mathbb{C}$ definido por la inclusión $\mathbb{R} \subseteq \mathbb{C}$ y tal que $f(x) = i$. Este homomorfismo es sobreyectivo ya que, dado $a + bi \in \mathbb{C}$, $f(a + bx) = a + ib$, por tanto $Imf = \mathbb{C}$. Basta ahora ver que $Kerf = (x^2 + 1)$. Como $\mathbb{R}$ es un cuerpo, todo ideal no trivial de $\mathbb{R}[x]$ está generado por cualquiera de sus elementos no nulos de grado mínimo. Por tanto, es suficiente comprobar que $x^2 + 1 \in Kerf$ y que $Kerf$ no posee ningún polinomio no trivial de grado menor que 2. Claramente $f(x^2 + 1) = i^2 + 1 = 0$. Si $a + bx \in \mathbb{R}[x]$ es un polinomio no trivial entonces $f(a + bx) = a + ib$ es un número complejo no trivial, con lo que queda demostrado.

□

Definición 3.40 (***Anillos*** $\mathbb{Z}[\sqrt{n}]$)**.** *Sea $n \in \mathbb{Z}$ que no es cuadrado de ningún entero. Entonces $\sqrt{n} \in \mathbb{C} \setminus \mathbb{Q}$.*

Esto es así ya que por el Teorema fundamental de la aritmética $n = p_1^{m_1} \dots p_r^{m_r}$, con $p_1, \dots, p_r$ primos distinto y $m_1, \dots, _r$ enteros positivos tales que m_1 es impar. Si $\sqrt{n}$ fuese racional entonces existirían enteros positivos y primos entre sí a, b tales que $\sqrt{n} = a/b$, por lo que $a^2 = nb^2$. Pero esto es imposible porque la mayor potencia de p_1 que divide al antero a^2 es par, mientras que la mayor potencia de p_1 que divide a nb^2 es impar.

Veamos que $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}$ es subanillo de $\mathbb{C}$ para cualquier $n \in \mathbb{Z}$ no cuadrado de ningún otro entero. Sean $a + b\sqrt{n}, a' + b'\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, entonces

$$(a + b\sqrt{n}) - (a' + b'\sqrt{n}) = (a - a') + (b - b')\sqrt{n} \in \mathbb{Z}[\sqrt{n}],$$

ya que $(a - a')$ y $(b - b')$ son enteros. Por otro lado,

$$(a + b\sqrt{n})(a' + b'\sqrt{n}) = (aa') + (bb')n + (ab' + a'b)\sqrt{n} \in \mathbb{Z}[\sqrt{n}],$$

ya que $(aa'), (bb')n, (ab' + a'b)$ *son enteros.*

Sin embargo, también podemos verlo de la siguiente forma: si $n \in \mathbb{Z}$ *no es un cuadrado en* $\mathbb{Z}$ *entonces el conjunto* $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}$ *es un subanillo de* $\mathbb{C}$ *por ser la imagen del homomorfismo evaluación*

$$\begin{array}{rccc} ev_{\sqrt{n}}\colon & \mathbb{Z}[x] & \longrightarrow & \mathbb{C} \\ & f & \longmapsto & f(\sqrt{n}) \end{array}$$

y de hecho es el menor subanillo de $\mathbb{C}$ *que contiene a* $\mathbb{Z}$ *y a* $\sqrt{n}$*. El núcleo de este homomorfismo es* $\ker ev_{\sqrt{n}} = (x^2 - n) \in \mathbb{Z}[x]$*, luego, por el Primer Teorema de Isomorfía,*

$$\mathbb{Z}[x]/(x^2 - n) \cong \mathbb{Z}[\sqrt{n}].$$

Esto es así ya que es evidente que $x^2 - n \in \ker ev_{\sqrt{n}}$*. Recíprocamente, sea* $f \in \ker ev_{\sqrt{n}}$*, y supongamos que es de grado menor que* 2*, es decir, de la forma* $a + bx$ *con* $a, b \in \mathbb{Z}$*, tal que* $ev_{\sqrt{n}}(f) = 0$*. Así,* $ev_{\sqrt{n}}(f) = a + b\sqrt{n} = 0$*, de lo que deducimos que* $\sqrt{n} = -a/b \in \mathbb{Q}$*, lo cuál es absurdo por lo primero que hemos visto. Así, el polinomio mónico de menor grado es* $x^2 - n$*, luego* $\ker ev_{\sqrt{n}} = (x^2 - n)$*.*

Para todo $\alpha = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ *definimos el* ***conjugado*** *de* α *como* $\overline{\alpha} = a - b\sqrt{n}$*. Veamos que para cualesquiera* $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$ *se verifica que* $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$*.*

Si $\alpha = a + b\sqrt{n}$*,* $\beta = a' + b'\sqrt{n}$*, entonces:*

$$\overline{\alpha}\,\overline{\beta} = (a - b\sqrt{n})(a' - b'\sqrt{n}) = aa' - ab'\sqrt{n} - a'b\sqrt{n} + bb'n = (aa' + bb'n) - (ab' + a'b)\sqrt{n},$$

$$\overline{\alpha\beta} = \overline{aa' + ab'\sqrt{n} + a'b\sqrt{n} + bb'n} = (aa' + bb'n) - (ab' + a'b)\sqrt{n}.$$

Además, notar que evidentemente $\alpha\overline{\alpha} = \overline{\alpha}\alpha$ *para cualquier* $\alpha \in \mathbb{Z}[\sqrt{n}]$*.*

De hecho, para todo $\alpha \in \mathbb{Z}[\sqrt{n}]$ *definimos la* ***norma*** *de* α *como* $N(\alpha) = \alpha\overline{\alpha}$*. Notar que, dado un* $\alpha = a + b\sqrt{n}$*, entonces* $N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - nb^2 \in \mathbb{Z}$*. Por otra parte, para todo* $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$ *tenemos que*

$$N(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\beta\overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta).$$

Veamos que, dado un $\alpha \in \mathbb{Z}[\sqrt{n}]$*,* $N(\alpha) = \pm 1 \Leftrightarrow \alpha$ *es unidad en* $\mathbb{Z}[\sqrt{n}]$*.*

Si $N(\alpha) = 1$*, entonces* $\alpha\overline{\alpha} = 1$ *y así* α *es unidad en* $\mathbb{Z}[\sqrt{n}]$*. Si* $N(\alpha) = -1$*, entonces* $\alpha(-\overline{\alpha}) = 1$ *y así* α *es nuevamente unidad en* $\mathbb{Z}[\sqrt{n}]$*. Recíprocamente, si* $\alpha \in \mathbb{Z}[\sqrt{n}]$ *es unidad, existirá un* $\beta \in \mathbb{Z}[\sqrt{n}]$ *tal que* $\alpha\beta = 1$*. Tomando normas:*

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta),$$

pero la norma es un número entero, luego $N(\alpha)$ *sólo puede ser* 1 *o* -1*.*

Teorema 3.41 (***Segundo Teorema de Isomorfía***)**.** *Sean* $A \subseteq B$ *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* 3.39, los anillos $A/(A \cap I)$ y $(A+I)/I$ son isomorfos.

□

Teorema 3.42 (***Tercer Teorema de Isomorfía***)**.** *Sean A un anillo conmutativo y unitario, y J, I ideales de A tales que $J \subseteq I$. 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 $J \subseteq I$. Ahora, $Kerf = \{a + J : a \in I\} = I/J$. De nuevo, por el *Primer Teorema de Isomorfía* 3.39 tenemos que $(A/J)/(I/J) \cong A/I$.

□

Ejemplo 3.42.1. *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 $\mathbb{C}$.

■

Teorema 3.43 (***Teorema de la Correspondencia***). *Sean A un anillo e I un ideal de A. Sea $\mathcal{I}$ el conjunto de los ideales de A que contienen al ideal I y $\mathcal{J}$ el conjunto de los ideales de A/I. Entonces la aplicación*

$$\begin{array}{rccl} f\colon & \mathcal{I} & \longrightarrow & \mathcal{J} \\ & T & \longmapsto & T/I = \{x+I : x \in T\} \end{array}$$

es biyectiva.

Demostración: Consideramos la proyección canónica $\pi\colon A \longrightarrow A/I$, que sabemos es un epimorfismo. Como la aplicación es sobreyectiva sabemos que para un ideal $T \in \mathcal{I}$ su imagen $T/I \in A/I$ es también un ideal de A/I, luego f está bien definida.

Veamos ahora que es biyectiva, para lo cuál construiremos su inversa. Por 3.37, si J es un ideal de A/I se tiene que $\pi^{-1}(J) = T$ es un ideal de A que contiene a $ker\ \pi = I$, es decir, $T \in \mathcal{I}$. Así, obtenemos una aplicación

$$\begin{array}{rccl} h\colon & \mathcal{J} & \longrightarrow & \mathcal{I} \\ & J & \longmapsto & \pi^{-1}(J) \end{array}$$

tal que $f \circ h = id_{\mathcal{J}}$ y $h \circ f = id_{\mathcal{I}}$.

□

Es decir, los ideales de A/I serán aquellos ideales de A que contengan al ideal I, tal y como vimos en el capítulo anterior.

Proposición 3.44. *Sea A un anillo e I un ideal de A. Consideremos el anillo cociente A/I e $\mathcal{I}$ el conjunto de los ideales de A que contienen a I. Entonces:*

1. *Un ideal $P \in \mathcal{I}$ es primo si y sólo si P/I es un ideal primo de A/I.*
2. *Un ideal $M \in \mathcal{I}$ es maximal si y sólo si M/I es un ideal maximal de A/I.*

Demostración: Veamos el primer resultado. Si consideramos la proyección canónica $\pi\colon A \longrightarrow A/I$, sabemos que si $\pi(P) = P/I$ es un ideal primo entonces $P = \pi^{-1}(P/I)$ es también primo. Recíprocamente, supongamos que P es un ideal primo de A que contiene a I y veamos que P/I es primo. Sean $a, b \in A/I$ tales que $ab \in P/I$. Entonces existen $c, d \in A$ tales que $a = c+I$ y $b = d+I$, por lo que $cd+I = ab \in P/I$, luego $cd \in P$. Como P es un ideal primo podemos suponer que $c \in P$, por lo que $a = c + I \in P/I$, luego P/I es primo.

Veamos ahora la segunda parte. Supongamos que M es un ideal maximal de A que contiene a I pero M/I no es un ideal maximal de A/I. Entonces existe un ideal $(b) \subset A$ que contiene a I tal que $M/I \subset (b)/I$, luego $M = \pi^{-1}(M/I) \subset \pi^{-1}((b)/I) = (b)$. Esto implica, por ser M maximal, que $M = (b)$, luego $M/I = (b)/I$, que es una contradicción. Recíprocamente, supongamos que (c) es un ideal no maximal de A tal que $J = (c)/I$ es un ideal maximal de A/I. Existe por tanto un ideal propio M de A tal que $(c) \subset M$. En particular, $J = (c)/I \subset M/I$ y como J es maximal tendremos la igualdad $J = M/I$. Esto implica que $(c) = \pi^{-1}(J) = \pi^{-1}(M/I) = M$, que de nuevo es una contradicción.

□

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 3.22.

Teorema 3.45 (***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*

$$\begin{array}{rccc} f\colon & A & \longrightarrow & A/I_1 \times \cdots \times A/I_r \\ & x & \longmapsto & (x + I_1, \ldots, x + I_r), \end{array}$$

   es sobreyectivo.
4. *Los anillos A/I y $A/I_1 \times \cdots \times A/I_r$ 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 3.22 deducimos que

$$I = I_1 \cap \ldots \cap I_r = I_1 \cap J = I_1J = I_1 \cdot (I_2 \cdots I_r) = I_1 \cdots I_r.$$

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, $f(x) = x_1 + I_1, \ldots, x_r + I_r$ y f es sobreyectiva.
4. Se deduce fácilmente que $Ker f = I_1 \cap \cdots \cap I_r = I$, con f el homomorfismo del apartado anterior, y aplicando el *Primer Teorema de Isomorfía* 3.39 ya está.

□

3.3. Divisibilidad

Durante esta sección consideraremos a A como un dominio de integridad. Empezaremos dando unas definiciones:

Definición 3.46. *Sean a, b elementos de A con $a \neq 0$. Se dice que a* ***divide a*** *b,* ***que*** *a* ***es un divisor de*** *b,* ***que*** *b* ***es divisible por*** *a* ***o que*** *b* ***es un múltiplo de*** *a si existe un $c \in A$ tal que $b = ac$. Se escribe $a \mid b$. Si a no divide a b se escribe $a \nmid b$.*

En otras palabras, $a \mid b \Leftrightarrow a \in (b)$, ó equivalentemente $(b) \subseteq (a)$.

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:

$$a \text{ está relacionado con } b \text{ si } a \mid b \text{ y } b \mid a, \text{ o sea si } (a) = (b).$$

Esto es equivalente a:

Existe una unidad $u \in \mathcal{U}(A)$ tal que $b = ua$. Esto es así ya que si $(b) = (a)$ tendremos que $b \in (a), a \in (b)$, luego $b = ac$ y $a = bd$, con $c, d \in A$. Luego $b = bdc$ y como A es un dominio de integridad podremos simplificar y obtener $1 = dc$, y así c es unidad.

Y de aquí llegamos a la definición de *elementos asociados.*

Definición 3.47. *Dos elemento $a, b \in A$ se dirán* ***asociados*** *en A si $a \mid b$ y $b \mid a$. Por ejemplo, en $\mathbb{Z}$ n y $-n$ lo son. Ser asociados es una relación de equivalencia en A, en la que la clase de un a cualquiera (sus asociados) estará formada por elementos de la forma ua, con $u \in \mathcal{U}(A)$.*

Lo podemos resumir diciendo que dos elementos $a, b \in A$ son asociados si y sólo si $(a) = (b)$. De igual forma diremos que b es un asociado de a si $a = ub$, con $u \in \mathcal{U}(A)$.

Estos elementos son distintos, pero se comportan de forma análoga desde el punto de vista de la divisibilidad, es decir, tienen los mismos múltiplos y los mismos divisores.

Definición 3.48. *Dado A un dominio de integridad, y $a \in A$ no nulo. Diremos que a es* ***primo*** *si el ideal que genera, $I = aA = (a)$, es primo. Diremos que a es* ***reducible*** *en A si existen $b, c \in A \setminus \mathcal{U}(A)$ tales que $a = bc$. Si a no es reducible ni unidad se dice que es* ***irreducible*** *en A.*

Alternativamente, podemos definir elementos irreducibles así:

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***.

Así, hablaremos de ***elementos irreducibles*** cuando sus únicos divisores sean unidades y asociados.

Proposición 3.49. *Sea A un anillo y $a \in A \setminus \mathcal{U}(A)$ un elemento no nulo.*

1. *El elemento a es primo si y sólo si para cada par de elementos $b, c \in A$ tales que $a \mid bc$ se cumple que $a \mid b$ ó $a \mid c$.*

2. *Si A es dominio de integridad y $a \neq 0$ es primo, entonces a es irreducible.*

3. *Sea A un dominio de integridad. Entonces, un elemento no nulo $a \in A$ es irreducible si y sólo si $I = (a)$ es un ideal maximal entre los ideales principales propios de A.*

Demostración:

1. Supongamos que a es primo, luego $I = (a)$ es primo, y sean $b, c \in A$ tales que $a \mid bc$. Entonces $bc \in I$, y como I es primo entonces $b \in I$ o $c \in I$. En el primer caso $a \mid b$ y en el segundo caso $a \mid c$.

   Recíprocamente, sean $a, b, c \in A$, $I = (a)$, tales que $a \mid bc$ y así $bc \in I$, si $a \mid b$ entonces $b \in I$ y si $a \mid c$ entonces $c \in I$. Así I es primo.

2. Sea a primo e $I = (a)$, supongamos que a es reducible. Entonces $a = bc$, con $b, c \in A \setminus \mathcal{U}(A)$. Como bc I y este ideal es primo, podemos suponer que $b \in I$, luego existe $u \in A$ tal que $b = au$. Así, $a = bc = auc$, luego, como $a \neq 0$ y A es dominio de integridad, $1 = uc$. Esto querría decir que $c \in \mathcal{U}(A)$, absurdo.

3. Supongamos que el ideal I no es maximal entre los ideales principales propios de A. Entonces, existe un $b \in A$ tal que $(a) = I \subset (b) = J \neq A$. En particular, ni a ni b son unidades de A y existe un $c \in A$ tal que $a = bc$. Tampoco c es unidad en A porque la inclusión $I \subset J$ es estricta. Por lo tanto a es reducible.

   Recíprocamente, si a es reducible existen $b, c \in A \setminus \mathcal{U}(A)$ tales que $a = bc$. Por lo tanto, $(a) = I \subset (b) = J \neq A$ ya que b no es unidad en A. Veamos que la inclusión es estricta, y es que si no lo fuera entonces a y b serían asociados. Así, existiría una unidad $u \in A$ tal que $a = bu$. Por lo tanto, $b(c - u) = bc - bu = a - a = 0$ y como A es dominio de integridad, $b = 0$ ó $c = u$. Lo primero implicaría que $a = 0$, lo cual es falso. Así, $c = u \in \mathcal{U}(A)$, que también es falso.

□

El recíproco de 2. en general no se cumple, para que lo haga se tendrá que cumplir que todos los ideales de A sean principales 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:

3.3.1. Dominios euclídeos

Definición 3.50. *Diremos que A es un **dominio euclídeo**, escrito DE, si existe una aplicación*

$$\|\cdot\| \colon A \longrightarrow \mathbb{N}$$

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.*

A esta aplicación la denominaremos ***norma euclídea****.*

La última condición puede ser reformulada tal que así: dados $x, y \in A$ no nulos (en realidad bastaría con que sólo lo fuera y) existen r y q tales que $x = qy + r$, con $r = 0$ ó bien $\|r\| < \|y\|$.

Notar que el anillo de los enteros $\mathbb{Z}$ es un dominio eculídeo tomando como aplicación el módulo $|\cdot|$.

En un dominio euclídeo se cumple la siguiente propiedad, que ya vimos por encima cuando hablamos de los anillos $\mathbb{Z}[\sqrt{n}]$ en 3.40.

Proposición 3.51. *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 $\mathcal{U}(A) \subseteq \{x \in A : \|x\| = 1\}$. 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

$$\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}.$$

Ejemplo 3.51.1. *Sea $A = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$. La aplicación*

$$\begin{array}{rccc} \varphi\colon & A \setminus \{0\} & \longrightarrow & \mathbb{N} \\ & x = a + b\sqrt{-2} & \longmapsto & x\bar{x} = a^2 + 2b^2 \end{array}$$

dota al anillo A de estructura de dominio euclídeo, cuyas unidades son 1 y -1. Tal y como vimos en 3.40, como -2 es un entero que es no cuadrado de ningún otro entero, sabemos que A es un subanillo de $\mathbb{C}$. De 3.40 también vemos fácilmente que A cumple con las dos primeras propiedades de los DE y también que sus unidades son 1 y -1.

Veamos ahora que existe división euclídea con respecto a φ. Sean $x = a + b\sqrt{-2}$, $y = c + d\sqrt{-2} \in A$ con $y \neq 0$. Dividiendo,

$$\frac{x}{y} = \frac{x\bar{y}}{y\bar{y}} = \frac{(u + v\sqrt{-2})}{\|y\|},$$

con $u, v \in \mathbb{Z}$, $\|y\| > 0$. Los números $q_1 = u/\|y\|$, $q_2 = v/\|y\|$ son reales, por lo que existirán enteros α, β tales que $|q_1 - \alpha| \leq 1/2$, $|q_2 - \beta| \leq 1/2$. Si denotamos por $r_1 = q_1 - \alpha$ y $r_2 = q_2 - \beta$ tenemos

$$x = (q_1 + q_2\sqrt{-2})y, \quad q_1 + q_2\sqrt{-2} = \alpha + r_1 + (\beta + r_2)\sqrt{-2} = \alpha + \beta\sqrt{-2} + (r_1 + r_2\sqrt{-2}),$$

con $|r_1|, |r_2| \leq 1/2$. Así, $x = (\alpha + \beta\sqrt{-2})y + (r_1 + r_2\sqrt{-2})y$, por lo que sólo tenemos que comprobar que $\|(r_1 + r_2\sqrt{-2})y\| < \|y\|$. $\|(r_1 + r_2\sqrt{-2})y\| = (r_1 + r_2\sqrt{-2})y\overline{(r_1 + r_2\sqrt{-2})y} = y\bar{y}(r_1 + r_2\sqrt{-2})\overline{(r_1 + r_2\sqrt{-2})} = \|y\|(r_1^2 + 2r_2^2) \leq (1/4 + 2/4)\|y\| < \|y\|$.

■

Proposición 3.52. *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

$$\|x\| = \text{mín}\{\|y\| : 0 \neq y \in I\}.$$

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 $y - r \in (x) \subseteq I$, 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 en los dominios euclídeos todos los ideales son generados por un sólo elemento, luego principales, y si definimos a éstos como una nueva clase de dominios habremos encontrado otra estructura que nos facilitará mucho el trabajo con ideales.

3.3.2. Dominios de ideales principales

Definición 3.53. *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.*

Aunque ya sabemos que $\mathbb{Z}$, como es dominio euclídeo, es un DIP, es interesante notar que no haría falta que pudiese definirse el módulo para que fuera un DIP:

Proposición 3.54. *$\mathbb{Z}$ es un DIP.*

Demostración: Si $I \subseteq \mathbb{Z}$ es un ideal, en particular es subgrupo, y como $\mathbb{Z}$ es cíclico todos sus subgrupos lo son, es decir, $I = \langle n \rangle = (n)$, para algún entero n.

□

De la demostración también vemos que $\mathbb{Z}$ es un anillo noetheriano. De hecho, como en un dominio de ideales principales todos los ideales son finitamente generados, ***todos los*** DIP ***son anillos noetherianos***.

En concreto ya sabemos que todos los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$.

Proposición 3.55. *Sea A un DIP. Entonces todo elemento irreducible $a \in A^*$ genera un ideal maximal.*

Demostración: Sabemos de 3.49 que un elemento irreducible genera un ideal maximal entre los ideales principales propios de A, pero como A es DIP todos sus ideales son principales, luego el ideal que genera a será maximal.

□

De este resultado se desprende de forma clara que en un dominio de ideales principales todos los ideales primos son maximales.

Anteriormente vimos que todo elemento primo es irreducible, ahora veremos que dadas unas condiciones también se cumple el recíproco.

Proposición 3.56. *Sea A un DIP. Entonces todo elemento irreducible de A es primo.*

Demostración: Por el resultado anterior sabemos que todo elemento irreducible genera un ideal maximal, y como todo ideal maximal es primo, llegamos a la conclusión de que ese elemento es primo.

□

A continuación desarrollaremos una definición que ya vimos anteriormente, 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 3.57 (***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 $\mathbb{Z} \subseteq A$ vía ϕ, y diremos que A tiene* ***característica*** *0. Esto ocurre, por ejemplo para $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ó $\mathbb{Z}[i]$. En este caso el menor entero k tal que $k \cdot 1_A = 0$, es el 0.*

2. *$Ker\,\phi \neq \{0\}$. Como $\mathbb{Z}/Ker\,\phi \cong Im\,\phi \subseteq A$ y A es dominio de integridad, $\mathbb{Z}/Ker\,\phi$ también lo será, y 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.*

Es decir, la característica de un anillo A es el núcleo del homomorfismo anterior.

Definición 3.58. *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 3.58.1. *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:*

$$(x) + (y) \subseteq (z) \subseteq \bigcap \{I : I \supseteq (x) + (y),\ I \text{ principal}\}.$$

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, $z \subseteq (x)$ y $z \subseteq (y)$, luego se tiene el contenido $(x) \cap (y) \supseteq (z)$. 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 3.59. *Sean $x, y \in A \setminus \{0\}$, y supongamos que tienen un mcm z. Entonces $t = xy/z \in A$ y t 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 3.60. *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 resultado 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 3.60.1. *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 3.58.1 (3) existe el mcm y se cumple 2.. Ahora, por 3.59 existe el mcd y se cumple 3. Finalmente, de nuevo por ser A un DIP, $(x) + (y)$ es principal, y de 3.58.1 (2) se sigue 1.

□

Proposición 3.61 (*Identidad de Bézout*). *Sean $x, y \in A^*$, y supongamos que generan un ideal principal. Entonces existen $z = mcd(x, y)$, $a, b \in A$ tales que*

$$z = ax + by.$$

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 3.62. *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 3.58.1 (2) se tiene $1 = mcd(x, y)$.

Finalmente daremos un criterio que nos asegurará cuándo los ideales de un dominio son principales:

Proposición 3.63 (***Criterio de Hasse***)**.** *Sea A un dominio de integridad y supongamos que existe una función $\varphi\colon A \longrightarrow \mathbb{N}$ tal que $\varphi^{-1}(0) = \{0\}$ y cumple: para cada par de elementos $a, b \in A$ tales que $b \neq 0$, $a \notin (b)$ y $\varphi(b) \leq \varphi(a)$ entonces existen $c, d \in A$ tales que $0 < \varphi(ac - bd) < \varphi(b)$. Entonces A es un dominio de ideales principales.*

Demostración: Sea I un ideal no nulo de A y sea $M = \{\varphi(x) : x \in I \setminus \{0\}\} \subseteq \mathbb{N}$. Como $\mathbb{N}$ está bien ordenado existirá un $b \in I \setminus \{0\}$ tal que $\varphi(b) \leq \varphi(x)$ para cada $x \in I \setminus \{0\}$, y veamos que $I = (b)$. Está claro que $(b) \subseteq I$, y supongamos, por reducción al absurdo, que existe un $a \in I \setminus (b)$. Como $b \neq 0$ y $\varphi(b) \leq \varphi(a)$ existen $c, d \in A$ tales que $0 < \varphi(ac - bd) < \varphi(b)$. Así, $e = ac - bd \in I \setminus \{0\}$ y $\varphi(e) < \varphi(b)$, en contra de la elección de b.

□

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.

3.3.3. Dominios de factorización única

Definición 3.64. *Un **dominio de factorización única** (o simplemente **dominio factorial**), 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.*

A ese producto de elementos irreducibles la denominaremos también ***factorización única***. Existen entonces 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

$$x = ua_1^{\alpha_1} \ldots a_r^{\alpha_r}.$$

Estos a_i se llaman **factores irreducibles** de x.

Que todo elemento irreducible sea primo se cumple siempre que nos encontremos en un dominio de ideales principales, tal y como vimos anteriormente. También se puede ver como una consecuencia de la *Identidad de Bézout*: supongamos que tenemos un elemento irreducible p tal que $p \mid ab$, para ciertos $a, b \in A$, con A un DIP. Entonces, si $p \nmid a$, $mcd(p, a) = 1$ y por la *Identidad de Bézout* existirán $x, y \in A$ tales que $1 = xp + ya$, luego $b = bxp + yab$, y como $p \mid ab$ (y evidentemente $p \mid p$) entonces $p \mid b$. Análogo en caso de que $p \nmid b$.

Proposición 3.65. *Sea A un dominio de ideales principales. Entonces A es un dominio de factorización única.*

Demostración: Veamos primero que todo elemento no nulo de A tiene una factorización en elementos irreducibles. Sea S el conjunto de los ideales principales no nulos cuyos generadores no tienen una factorización en elementos irreducibles, y supongamos que S es no vacío. Sea $(a_1) \in S$. Consideremos la siguiente cadena ascendente:

$$(a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots$$

de ideales en S. Podemos suponer que esta cadena no es infinita. De hecho, la unión de todos los ideales de esa cadena es un ideal de A, y por tanto principal, digamos (a). Este generador a tiene que pertenecer a algún elemento de la cadena, digamos (a_n), luego podemos observar que $(a_n) \subset (a) \subset (a_n)$, por lo que la cadena se estabiliza en (a_n). Así, S está ordenado y tiene un elemento maximal, (a). Por lo tanto, todo ideal de A que contenga a (a) y sea distinto de (a) tiene un generador que admite una factorizacón en elementos irreducibles.

Observar que a no puede ser irreducible, de lo contrario tendría una factorización, por lo que podemos escribirlo como $a = bc$, con $b, c \in A \setminus \mathcal{U}(A)$. Pero entonces $(b) \neq (a)$, $(c) \neq (a)$ y $(a) \subset (b)$, $(a) \subset (c)$. Así, b, c admiten factorizaciones en elementos irreducibles. El producto de esas factorizaciones es una factorización en elementos irreducibles de a, lo cuál es absurdo.

Para probar la unicidad, supongamos que a tiene dos factorizaciones en elementos irreducibles

$$a = p_1 \ldots p_r = q_1 \ldots q_s.$$

Como p_1 divide al producto de la derecha y es irreducible entonces necesariamente divide a uno de los factores, que podemos asumir que es q_1 tras una reordenación. Así,

existirá una unidad u_1 tal que $q_1 = up_1$ (ya que q_1 es irreducible). Ahora podemos cancelar p_1 en ambas factorizaciones, quedando

$$p_2 \dots p_r = u_1 q_2 \dots q_s.$$

El resultado se tiene por inducción.

□

Ejemplo 3.65.1. *Veamos que* $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$ *es dominio de integridad con las operaciones habituales de suma y producto de complejos:*

Como $\mathbb{Z}[\sqrt{5}i] \subseteq \mathbb{C}$ *bastará demostrar que* $\mathbb{Z}[\sqrt{5}i]$ *es subanillo de* $\mathbb{C}$*. Usamos el conocido teorema de caracterización de subanillos. Claramente,* $\mathbb{Z}[\sqrt{5}i] \neq 0$*. Para cada par de elementos* $a + b\sqrt{5}i, c + d\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ *tenemos*

$$(a + b\sqrt{5}i) - (c + d\sqrt{5}i) = (a - c) + (b - d)\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$$

$$(a + b\sqrt{5}i)(c + d\sqrt{5}i) = (ac - 5bd) + (ad + bc)\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i].$$

Así, $\mathbb{Z}[\sqrt{5}i]$ *es subanillo, y como* $\mathbb{C}$ *es conmutativo, también lo será* $\mathbb{Z}[\sqrt{5}i]$*. Además,* $1 = 1 + 0\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$*, luego es unitario. Como* $(\mathbb{C}, +, \cdot)$ *es dominio de integridad, también lo será* $\mathbb{Z}[\sqrt{5}i]$*.*

■

Notar que de la proposición anterior tenemos que los DFU satisfacen la condición de cadena ascendente para ideales principales.

Observación 3.65.1. *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* $p_1, \dots, p_r$ *de la forma* $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$*.*

A continuación veremos todas las propiedades vistas hasta ahora a través de un ejemplo bastante completo, se trata de $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[\sqrt{5}i]$, que ya habíamos probado que era subanillo:

Ejemplo 3.65.2. *Nos situaremos en el subanillo $A \subseteq \mathbb{C}$ 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

$$c = \frac{a}{a^2 + 5b^2}, \;\; d = \frac{-b}{a^2 + 5b^2}.$$

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 3.50. 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

$$(x_0) \subseteq (x_1) \subseteq (x_2) \subseteq \ldots \subseteq (x_n) \subseteq \ldots.$$

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

$$(x_0) \subseteq (x_1) \subseteq (x_2) \subseteq \ldots \subseteq (x_n) \subseteq \ldots.$$

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 3.60 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.*

■

3.3.4. 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:

Primero, el resultado central de la sección, y a partir del cual desarrollaremos el resto.

Proposición 3.66. *Sea* n *un entero positivo. El anillo* $\mathbb{Z}/n\mathbb{Z}$ *es un cuerpo si y sólo si* n *es primo.*

Demostración: Está claro que podemos suponer que $n \geq 2$. Supongamos que $n = ab$, con $1 < a, b < n$ y que $\mathbb{Z}/n\mathbb{Z}$ es cuerpo. Entonces $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 0$ pero esto sería absurdo si $a+n\mathbb{Z}, b+n\mathbb{Z} \neq 0$ puesto que un $\mathbb{Z}/n\mathbb{Z}$ es cuerpo y no tiene divisores de cero, así que necesariamente n es primo.

Recíprocamente, supongamos que n es primo, y sea $1 \leq m < n$, entonces se tiene que $mcd(n, m) = 1$. En este caso, sabemos que van a existir $a, b \in \mathbb{Z}$ tales que $an + bm = 1$ por la identidad de Bézout. Por lo tanto,

$$(m + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z},$$

y tenemos que $m + n\mathbb{Z}$ es invertible.

□

A este anillo lo podremos denotar indistintamente tanto $\mathbb{Z}/n\mathbb{Z}$ como $\mathbb{Z}/(n)$ tal y como iremos viendo.

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 3.67. *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 3.68. *Sea* $n > 1$*. Ya vimos en 3.15 que los ideales de* $\mathbb{Z}/(n)$ *están en biyección con los ideales* $I \subseteq \mathbb{Z}$ *que contienen* (n)*. Sea entonces un ideal* $I = (m) \subseteq \mathbb{Z}$ *tal que* $(m) \supseteq (n)$*. 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 3.69. *Vamos a centrarnos en 5 puntos:*

1. *No existe ningún homomorfismo de anillos unitarios de la siguiente 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 3.70. *Si a, b son enteros primos entre sí, entonces se tendrá un isomorfismo de anillos unitarios*

$$\mathbb{Z}(ab) \cong \mathbb{Z}/(a) \times \mathbb{Z}/(b).$$

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.

□

Lema 3.70.1. *Sean m y n enteros positivos tales que $mcd(m,n) = 1$. Entonces, dados $a, b \in \mathbb{Z}$, el sistema*

$$x \equiv a \bmod m$$

$$x \equiv b \bmod n$$

tiene solución. Si x_1, x_2 son dos soluciones del sistema, entonces $x_1 \equiv x_2 \bmod mn$.

Demostración: La ecuación $x \equiv a \bmod m$ tiene solución puesto que $a + km$ satisface la ecuación para cualquier $k \in \mathbb{Z}$. Debemos mostrar que existe un entero k_1 tal que

$$a + k_1 m \equiv b \bmod n.$$

Esto es equivalente a mostrar que

$$k_1 m \equiv (b - a) \bmod n$$

tiene solución para k_1. Como m y n son coprimos, existen enteros s y t tales que $ms + nt = 1$. Concluimos que $(b-a)ms = (b-a) - (b-a)nt$ y así

$$(b - a)ms \equiv (b - a) \bmod n.$$

Tomamos $k_1 = (b - a)s$ y ya está.

Para ver ahora que dos soluciones cualesquiera son congruentes módulo mn, sean c_1 y c_2 dos soluciones del sistema. Es decir,

$$c_i \equiv a \bmod m$$

$$c_i \equiv b \bmod n$$

para $i = 1, 2$. Entonces

$$c_2 \equiv c_1 \bmod m$$

$$c_2 \equiv c_1 \bmod n$$

por lo que tanto m como n dividen a $c_2 - c_1$. Así, $c_2 \equiv c_1 \bmod mn$.

□

Ejemplo 3.70.1. *Resolvamos el siguiente sistema:*

$$x \equiv 3 \ mod\, 4$$

$$x \equiv 4 \ mod\, 4$$

Usando el algoritmo de Euclides podemos encontrar enteros s, t tales que $4s+5t = 1$. Una posibilidad para tales enteros es $s = 4$ y $t = -3$. Tenemos que $a = 3$, $b = 4$, $m = 4$ y $n = 5$, luego $k_1 = (4 - 3)4$ y concluimos así que

$$x = a + k_1 m = 3 + 4k_1 = 3 + 4((4 - 3)4) = 19.$$

Por extensión a k ecuaciones llegamos a:

Teorema 3.71 (***Teorema Chino de los restos***)**.** *Sean $n_1, n_2, \ldots, n_k$ enteros positivos tales que $mcd(n_i, n_j) = 1$ con $i \neq j$, es decir, coprimos dos a dos. Entonces para enteros cualesquiera $a_1, \ldots, a_k$ el sistema*

$$x \equiv a_1 \ mod\, n_1$$

$$x \equiv a_2 \ mod\, n_2$$

$$\vdots$$

$$x \equiv a_k \ mod\, n_k$$

tiene solución. Más aún, dos soluciones cualesquiera de sistema son congruentes módulo $n_1, n_2, \ldots, n_k$.

Demostración: Lo haremos por inducción sobre el número de ecuaciones en el sistema. Si hay $k = 2$ ecuaciones entonces el resultado se da por el lema anterior. Ahora supongamos que el resultado es cierto para un sistema de k o menos ecuaciones y que queremos encontrar una solución de

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$\vdots$$

$$x \equiv a_{k+1} \bmod n_{k+1}.$$

Considerando las primeras k ecuaciones, existe una solución que es única módulo $n_1 \dots n_k$, digamos a. Como $n_1 \dots n_k$ y n_{k+1} son coprimos entre sí el sistema

$$x \equiv a \bmod n_1 \dots n_k$$

$$x \equiv a_{k+1} \bmod n_{k+1}$$

tiene una solución que es única módulo $n_1 \dots n_{k+1}$ por el lema anterior.

□

Veamos las unidades de los anillos de restos:

Proposición 3.72. *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 3.73. *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:

$$\mathcal{U}(\mathbb{Z}/(p)) = \{[1], \ldots, [p-1]\}.$$

3.4. Anillos de polinomios

Definición 3.74. *Sea A un anillo conmutativo y unitario. Diremos que X es una* ***indeterminada*** *ó* ***variable*** *si sus potencias son algebraicamente independientes, es decir,*

$$\sum_{i=0}^{n} a_i X^i = 0,\ \ a_i \in A \Longleftrightarrow a_0 = \ldots = a_n = 0 \quad \forall n.$$

Un ***polinomio en*** *X con coeficientes en A es una suma finita*

$$f(X) = a_0 + a_1 X + \ldots + a_n X n,\ a_0, a_1, \ldots, a_n \in A$$

a la que se puede agregar un número finito y arbitrario de ceros.

Definición 3.75. *Dados polinomios $f(X) = \sum_{i=0}^{n} a_i X^i$ y $g(X) = \sum_{j=0}^{m} b_j X^j$ 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*

$$f(X) \cdot g(X) = \sum_{k=1}^{n+m} c_k X^k,\ \ c_k = \sum_{i+j=k} a_i b_j,$$

teniendo en cuenta que si 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 3.75.1. *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 3.76. *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 se puede 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 3.77. *Si $0 \neq f(X) = \sum_{i=0}^{n} a_n X^n \in A[X]$, 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 $a_i X^i$ 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 $grado_{X_i}(f)$ ó $\delta_{X_i}(f)$ es el grado de f como polinomio en X_i. El **grado total** de $f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$ es el máximo $\{i_1 + \ldots + i_n : a_{i_1 \ldots i_n} \neq 0\}$.

Por convenio asumiremos que el polinomio cero no tiene grado o que tiene grado $-\infty$.

Proposición 3.78. *Un anillo de polinomios $A[X]$ es dominio de integridad (DI) si y sólo si lo es A.*

Demostración: Como A es subanillo de $A[X]$, el sólo si es claro. Supongamos ahora que A es DI. Consideremos la indeterminada X y dos polinomios de $A[X]$:

$$f = a_0 + a_1 X + \ldots + a_p X^p, \;\; g = b_0 + b_1 X + \ldots + b_q X^q,$$

vemos que $\delta(f) = p$ y que $\delta(g) = q$, lo que significa que $a_p \neq 0$, $b_q \neq 0$. Hagamos su producto:

$$fg = \sum_{r}^{p+q} c_r X^r = a_0 b_0 + \ldots + (a_{p-1} b_q + a_p b_{q-1}) X^{p+q-1} + a_p b_q X^{p+q}.$$

Por tanto, $c_{p+q} = a_p b_q \neq 0$ ya que A es DI. Pero esto quiere decir que $fg \neq 0$ pues al menos el coeficiente c_{p+q} es no nulo. Quedaría así probado que $A[X]$ es DI.

□

Notar que este resultado se puede extender de forma natural por inducción a varias variables, es decir: $A[X_1, \ldots, X_n]$ es dominio de integridad (DI) si y sólo si lo es A.

De esto se deduce que, como hemos considerado que de ahora en adelante A será un dominio de integridad, $A[X]$ va a ser un dominio de integridad.

De hecho, en general vamos a tener que $\delta(f \cdot g) \leq \delta(f) + \delta(g)$, pero como $A[X]$ es dominio de integridad entonces:

$$\delta(f \cdot g) = \delta(f) + \delta(g).$$

Es decir,

Proposición 3.79. *Dado $A[X]$ un dominio de integridad, $f, g \in A[X]$. Entonces:*

1. $\delta(f + g) \leq max\{\delta(f), \delta(g)\}$.
2. $\delta(fg) = \delta(f) + \delta(g)$.

Además,

Corolario 3.79.1. *Si A es un dominio de integridad, entonces*

$$\mathcal{U}(A) = \mathcal{U}(A[X]).$$

Demostración: Si $a \in \mathcal{U}(A)$ existirá $a^{-1} \in A$ y a^{-1} será también el inverso de a en $A[X]$, luego $a \in \mathcal{U}(A[X])$. Recíprocamente, sea $f \in \mathcal{U}(A[X])$. Entonces existe $g \in A[X]$ con $1 = fg$ $(*)$. Como A es dominio de integridad, tenemos que

$$0 = \delta(1) = \delta(fg) = \delta(f) + \delta(g).$$

Esto sólo puede significar que $\delta(f) = \delta(g) = 0$, es decir, $f \in A$ y $g \in A$. Así, por $(*)$ f es unidad en A.

□

Es además una propiedad que se puede extender por inducción a un anillo de polinomios en varias variables:

$$\mathcal{U}(A) = \mathcal{U}(A[X_1, \ldots, X_n]).$$

La división en $A[X]$ está regulada por la conocida como ***pseudodivisión***.

Proposición 3.80. *Dados $0 \neq f(X), g(X) \in A[X]$, si a es el coeficiente director de $f(X)$, existen un entero $t \geq 0$ y polinomios $q(X), r(X) \in A[X]$ tales que $a^t g(X) = f(X)q(X) + r(X)$ y ó $r(X) = 0$ ó $\delta(r) < \delta(f)$.*

Demostración: Si $\delta(g) < \delta(f)$, basta tomar $t = 0$, $q(X) = 0$ y $r(X) = g(X)$. Supongamos $m = \delta(g) \geq \delta(f) = n$ y procedamos por inducción sobre m. Sea b el coeficiente director de $g(X)$. Si $m = 0$, se tiene que $g(X) = b$ y $n = 0$. Como $ag(X) = f(X)b$, basta tomar $t = 1$, $q(X) = b$ y $r(X) = 0$. Si $m > 0$, sea $h(X) = ag(X) - bf(X)X^{m-n}$. Como $\delta(h) < \delta(g) = m$, por inducción existen $t' \geq 0$ y $q'(X), r'(X) \in A[X]$ verificando $a^{t'}h(X) = q'(X)f(X) + r'(X)$, donde ó $r'(X) = 0$

ó $\delta(r') < \delta(f)$. Así $a^{t'+1}g(X) = (q'(X) + a^{t'}bX^{m-n})f(X) + r'(X)$ y basta tomar $t = t' + 1$, $q(X) = q'(X) + a^{t'}bX^{m-n}$ y $r(X) = r'(X)$.

□

Proposición 3.81. *Si K es un cuerpo, entonces $K[X]$ es un DIP.*

Demostración: Sea I un ideal de $K[X]$ y supongamos que $I \neq 0$. Sea $g \in I$ del menor grado posible. Sea f un elemento de I cualquiera no nulo. Por el algoritmo de la división, existen $q, r \in K[X]$ tales que

$$f = qg + r$$

y se tiene que $\delta(r) < \delta(g)$. Pero $r = f - qg$ y así $r \in I$. Como g es el elemento de I de grado mínimo se sigue que $r = 0$ necesariamente. Así, I estará formado por todos los polinomios $f = qg$. Por último, sólo basta comprobar que f es mónico para que se tenga el resultado, pero esto es fácil, si f es mónico ya está, y si no lo es multiplicamos por el inverso del coeficiente director de f, que siempre existe por ser K un cuerpo, y ya está. Así I es principal.

□

De hecho,

Corolario 3.81.1. *SI K es un cuerpo, $K[X]$ es un dominio euclídeo.*

Demostración: En este caso, el grado es una función euclídea.

□

Corolario 3.81.2 (***Teorema del resto***)**.** *Si $a \in A$ y $f(X) \in A[X]$, el resto de dividir $f(X)$ por $(X - a)$ es $f(a)$. En particular, $f(a) = 0$ si y sólo si $X - a \mid f(X)$.*

Demostración: Aplicamos 3.80, quedando $f(X) = (X - a)g(X) + r(X)$, con $f(X)$ como dividendo, $X - a$ como divisor, $g(X)$ un polinomio cualquiera de $A[X]$ y $r(X)$ el resto. Entonces ó $r(X) = 0$, y así está claro que $f(a)$ es el resto (que es 0), ó $\delta(r) < \delta(X - a)$, y así $r(X)$ sería una constante y $f(a) = (a - a)g(a) + r = r$.

□

La aplicación reiterada del *Teorema del resto* permite deducir una cierta factorización de un polinomio quitándole sus raíces en A. Es decir, si $f(X) \in A[X]$ y $a_1, a_2, \ldots, a_r \in A$ son sus raíces en A, cada una de ellas apareciendo $m_1, \ldots, m_r$ veces respectivamente, entonces existe $g(X) \in A[X]$ tal que

$$f(X) = (X - a_1)^{m_1} \ldots (X - a_r)^{m_r} g(X),$$

donde $g(a) \neq 0$, para todo $a \in A$. Cada factor $X - a_i$ es irreducible, puesto que es mónico de grado 1, aunque $g(X)$ no tiene por qué serlo. Se tiene que $\delta(f) = m_1 + m_2 + \ldots + m_r + \delta(g)$, luego $\sum_i^r m_i \leq \delta(f)$.

- *Raíces* en A: la condición necesaria para su existencia es la *regla de Ruffini*: $f(X) = a_n X^n + \ldots + a_1 X + a_0 \in A[X]$, $a \in A$ y $f(a) = 0 \Rightarrow a \mid a_0$.

- *Multiplicidades de raíces*: que se caracterizará usando el criterio de la derivada, para ello recordamos que la derivación de polinomios es una aplicación lineal

$$\begin{array}{ccc} A[X] & \longrightarrow & A[X] \\ f(X) = \sum_{i=0}^{n} a_i X^i & \longmapsto & f'(X) = \sum_{i=1}^{n-1} i a_i X \end{array}$$

Notar que es una aplicación que se puede aplicar tantas veces como queramos, obteniendo las derivadas sucesivas del polinomio: $f''(X), \ldots, f^{(n}(X), \ldots$, esto lo hacemos de forma inductiva: $f^{(0}(X) = f(X)$ y $f^{(n}(X) = (f^{(n-1}(X))'$, con $n > 0$.

Recordamos también las siguientes propiedades de la derivación de polinomios:

1. Si $a \in A$, $a' = 0$.
2. Si $n \geq 1$, $(X^n)' = nX^{n-1}$.
3. $(f(X) + g(X))' = f' + g'$.
4. $(f(X)g(X))' = f'(X)g(X) + f(X)g'(X)$. (*Regla de Leibniz*)

Notar que podría ser $f(X)$ no constante y $f'(X)$ nulo. Esto pasaría si $f(X) \in A[X^n]$, con n la característica de A.

Proposición 3.82. *Si la característica de A no divide al grado de $f(X) \in A[X]$, entonces $a \in A$ es una raíz múltiple de $f(X)$ si y sólo si $f(a) = f'(a) = 0$.*

Demostración: En general, tenemos que $f(X) = (X-a)^n g(X)$ con $n \geq 0$ y $g(a) \neq 0$. Así, se tiene que $f'(X) = n(X-a)^{n-1}g(X) + (X-a)^n g'(X)$. El resultado se obtiene aplicando el *Teorema del resto*, teniendo en cuenta que a se repite si y sólo si $n > 1$.

□

Definición 3.83. *Una raíz $a \in A$ de un polinomio $f(X) \in A[X]$ se dice que es **simple** si $f'(a) \neq 0$ y **múltiple** en caso contrario. El menor $n \geq 1$ tal que $f^n(a) \neq 0$ se llama **multiplicidad de** a como raíz de $f(X)$. Así, a será simple si y sólo si $n = 1$ y múltiple si y sólo si $n > 1$.*

Diremos que las raíces de multiplicidad $2, 3, 4, \ldots$ se denominan dobles, triples, cuádruples, ..., respectivamente.

A partir de ahora consideraremos A como un dominio de factorización única y K como su cuerpo de fracciones.

Definición 3.84. *Dado $0 \neq f(X) = a_n X^n + \ldots + a_1 X^1 + a_0 \in A[X]$, definimos el **contenido** de f, y lo denotamos $c(f)$, como el máximo común divisor de los coeficientes nu nulos de $f(X)$. Igualmente, diremos que $f(X)$ es **primitivo** si $c(f) \in \mathcal{U}(A)$.*

Dado un $f(X) \in A[X]$ arbitrario, se tiene que $f(X) = c(f)f_1(X)$, con $f_1(X) \in A[X]$ primmitivo. En particular, un polinomio *irreducible* es *primitivo*.

Lema 3.84.1 (***Lema de Gauss***)**.** *El producto de polinomios primitivos es primitivo.*

Demostración: Sean $f(X) = a_nX^n + \ldots + a_1X + a_0$, $g(X) = b_mX^m + \ldots + b_1X + b_0 \in A[X]$ primitivos. Su producto es $f(X)g(X) = c_{n+m}X^{n+m} + \ldots + c_1X + c_0 \in A[X]$, con $c_k = a_0b_k + \ldots + a_ib_{k-i} + \ldots + a_kb_0$. Si $f(X)g(X)$ no es primitivo, entonces existe un primo $p \in A$ tal que $p \mid c_k$, $\forall k$. Como $f(X)$ y $g(X)$ son primitivos, existen $s, t \geq 0$ tales que $p \mid a_i$ si $i < s$, pero $p \nmid a_s$ y $p \mid b_j$ si $j < t$, pero $p \nmid b_t$. Como p $midc_{s+t}$, se deduce que $p \mid a_sb_t$, absurdo.

□

De hecho, tenemos que $c(f \cdot g) \sim c(f) \cdot c(g)$, con $f(X), g(X) \in A[X]$.

Proposición 3.85. *Sean $f(X), g(X) \in A[X]$ dos polinomios primitivos. Entonces $f(X)$ y $g(X)$ son asociados en $A[X]$ si y sólo si lo son en $K[X]$.*

Demostración: El directo es inmediato, veamos el recíproco. Supongamos que $f(X) = \alpha g(X)$, con $\alpha \in \mathcal{U}(K[X]) = K^*$. Si $\alpha = a/b$, con $a, b \in A$, deducimos que $bf(X) = ag(X)$. Como $f(X)$ y $g(X)$ son primitivos, tomando contenidos, $a \sim b$, luego $\alpha \in \mathcal{U}(A) = \mathcal{U}(A[X])$.

□

Proposición 3.86. *Un polinomio no constante primitivo $f(X) \in A[X]$ es irreducible en $A[X]$ si y sólo si lo es en $K[X]$.*

Demostración: Sea $f(X)$ irreducible en $A[X]$ y supongamos que $f(X) = g(X)h(X)$, con $g(X), h(X) \in K[X]$. Al quitar los denominadores de los coeficientes del segundo término, calcular el contenido del polinomio resultante y aplicar el *Lema de Gauss*, queda $f(X) = (a/b)g_1(X)h_1(X)$, con $a, b \in A$ y $g_1(X), h_1(X) \in A[X]$ son primitivos con $\delta(g_1) = \delta(g)$ y $\delta(h_1) = \delta(h)$. Como en el resultado anterior, operando y tomando contenidos, se tiene que $a/b \in \mathcal{U}(A)$. Por lo tanto, $g_1(X)$ ó $h_1(X)$ es constante no nulo, luego unidad de K. Así, $f(X)$ es irreducible en $K[X]$.

Recíprocamente, supongamos que $f(X)$ es irreducible en $K[X]$ y que $f(X) = g(X)h(X)$, con $g(X), h(X) \in A[X]$. Leyendo la expresión en $K[X]$ deducimos que uno de sus factores, por ejemplo $g(X)$, debe ser una unidad en $K[X]$, es decir, $g(X) \in K$. Como $g(X) \in A[X]$, esto indica que $g(X) = a \in A$ es constante. Como $f(X)$ es primitivo, el *Lema de Gauss* implica que $a \in \mathcal{U}(A)$. Por lo tanto, $f(X)$ es irreducible en $A[X]$.

□

Teorema 3.87 (***Teorema de Gauss***)**.** *Si A es un DFU, entonces también lo es $A[X]$.*

Demostración: Sea $f(X) \in A[X]$ un polinomio no nulo y no unidad. Escribamos $f(X) = c(f)f_1(X)$, con $f_1(X) \in A[X]$ primitivo, y factorizemos $f_1(X)$ en $K[X]$. Si $p(X) \in K[X]$ es uno de sus factores irreducibles, procediendo de modo habitual, podemos escribir $p(X) = (a/b)p'(X)$, con $a, b \in A$ y $p'(X) \in A[X]$ es primitivo. Más aún, como $p(X)$ es irreducible en $K[X]$, $p'(X)$ es irreducible en $K[X]$, luego, por primitividad, $p'(X)$ es irreducible en $A[X]$. Igualmente, otra vez por primitividad,

$a/b \in \mathcal{U}(A) = \mathcal{U}(A[X])$. Por lo tanto, factorizando $c(f)$ en A, podemos escribir

$$f(X) = ua_1 \cdots a_r p_1'(X) \cdots p_n'(X),$$

con $u \in \mathcal{U}(A[X])$, $a_1, \ldots, a_r \in A$ irreducibles en A y $p_1'(X), \ldots, p_n'(X) \in A[X]$ irreducibles en $A[X]$. Notemos que cada a_i es irreducible en $A[X]$ puesto que lo es en A. Por lo tanto la factorización existe.

Veamos ahora que es única. Sea $a_1 \cdots a_r p_1(X) \cdots p_n(X) = b_1 \cdots b_s q_1(X) \cdots q_m(X)$, donde $a_1, \ldots, a_r, b_1, \ldots, b_s \in A$ son irreducibles en $A[X]$, luego también en A, y $p_1(X), \ldots, p_n(X), q_1(X), \ldots, q_m(X) \in A[X]$ son polinomios no constantes irreducibles en $A[X]$. Por primitividad, $a_1 \cdots a_r \sim b_1 \cdots b_s$, luego $r = s$ y, salvo el orden, $a_i \sim b_i$. Así, $p_1(X) \cdots p_n(X)$ y $q_1(X) \cdots q_m(X)$ son asociados en $K[X]$, pues lo son en $A[X]$ y son primitivos. Por lo tanto $n = m$ y, salvo el orden nuevamente, $p_j(X) \sim q_j(X)$ en $A[X]$, pues son polinomios primitivos asociados en $K[X]$. Así, la factorización es única

□

Teorema 3.88. *Sea A un dominio de integridad. Entonces $A[x]$ es DIP si y sólo si A es un cuerpo.*

Demostración: Si A es un cuerpo sabemos que $A[x]$ es un dominio euclídeo, luego un DIP. Recíprocamente, si $A[x]$ es DIP, sea $a \in A$ un elemento no nulo y veamos que es una unidad en A. Para ello consideramos el ideal (x, a) de $A[x]$. Como ha de ser principal existirá un polinomio $p \in A[x]$ tal que $(x, a) = (p)$, luego $a = pq$ para cierto $q \in A[x]$, pero entonces $\delta(p) + \delta(q) = \delta(a) = 0$, luego $\delta(p) = 0$ y así $p \in A$. Por otra parte, $x = pr$ para cierto $r \in A[x]$, pero entonces el coeficiente director de x, que es 1, es el producto de p por el coeficiente director de r, luego p es una unidad y $(p) = A[x]$.

Entoncecs, $1 \in (p) = (x, a)$, luego $1 = ux + va$, para ciertos polinomios $u, v \in A[x]$. Sin embargo, el término independiente de ux es 0 y el de va es ba, donde b es el término independiente de v. Resulta así que $1 = ba$ y a es una unidad en A.

□

Finalmente, veamos uno de los criterios de irreducibilidad de polinomios más conocidos y útiles:

Proposición 3.89 (***Criterio de Eisenstein***)**.** *Si $f(X) = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ es primitivo y existe un primo p tal que:*

1. *$p \mid a_i$, con $i = 0, \ldots, n-1$.*
2. *$p \nmid a_n$.*
3. *$p^2 \nmid a_0$*

Entonces $f(X)$ es irreducible en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$.

Demostración: Basta ver que $f(X)$ es irreducible en $\mathbb{Z}[X]$. Si $f(X)$ es reducible, existen $g(X), h(X) \in \mathbb{Z}[X]$ no constantes tales que $f(X) = g(X)h(X)$. Sean $g(X) =$

$b_rX^r+\ldots+b_1X+b_0 \in \mathbb{Z}[X]$ y $h(X) = c_sX^s+\ldots+c_1X+c_0 \in \mathbb{Z}[X]$. Como $a_0 = b_0c_0$, se tiene que p divide sólo a uno de los dos, a b_0 ó a c_0. Supongamos que $p \mid b_0$ y que $p \nmid c_0$. Como p no puede dividir a todos los coeficientes de $g(X)$, ya que no divide a a_n, existe $r \geq m > 0$ tal que $p \mid b_i$, si $i = 0, \ldots, m-1$ y $p \nmid b_m$. Como $m \leq r < n$, se deduce que $p \mid a_m = \sum_{i=0}^{m} b_ic_{m-i}$, lo que fuerza a que $p \mid b_mc_0$, una contradicción.

□