# Introducción a la Teoría de Galois

Pablo Pallàs

20 de junio de 2023

# Índice

# 1. Introducción y contexto

# 2. Grupos y anillos

## 2.1. Generalidades de grupos

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:

**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 $e \cdot x = x \cdot e = x$.*

III. $\forall x \in G$ *existe* $y \in G$ *tal que* $x \cdot y = y \cdot x = e$.

*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 $\Omega$, consideramos $S_\Omega$ 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 $S_\Omega$ es un grupo con la operación*

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

*A este grupo lo denominaremos* ***grupo simétrico*** *sobre $\Omega$. Si $\Omega$ 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.** *Sea $G$ un grupo. Un subconjunto $H$ de $G$ se dice* ***subgrupo*** *si es grupo con la restricción a $H$ de la operación de $G$. Lo denotaremos por $H \leq G$.*

**Ejemplo 2.4.1.** *Por ejemplo 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**. El resto de subgrupos, aquellos $H \leq G$ tales que $H \neq G$, son los llamados subgrupos **propios**.

**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.

□

**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.

**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 $h = h_1h_3 \in H$.

□

**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****.*

**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 $G$.

□

**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 $gf^{-1} \in N_G(X)$.

□

**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, es fácilmente comprobable 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 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.

**Definición 2.14.** *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 2.15** (***Teorema de Lagrange y definición de índice***)**.** *Sea $G$ un grupo finito y $H \leq G$. Sea $a$ el número de coclases a izquierda módulo $H$ y $b$ el número de coclases a derecha módulo $H$. Entonces $|G| = a|H| = b|H|$. Así, $a = b$. Tanto $a$ $b$ como $a$ $a$ lo llamaremos* ***índice*** *de $H$ en $G$ y se escribe como $[G : H]$.*

*Así, tenemos*

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

*Demostración.* Sabemos que las coclases a izquierda (o derecha) forman una partición de $G$. Además, también sabemos por que cada coclase $xH$ (o $Hx$) es biyectiva con $H$, luego $|xH| = |H| = |Hx|$. Así, $|G| = a|H| = b|H|$. Luego $a = b$.

Así, $|G| = [G : H]|H|$.

□

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***.

Dentro de la **Teoría de grupos**, un concepto fundamental es el de subgrupo *normal*.

**Definición 2.16.** *Un subgrupo $N$ de $G$ se dice **normal** si*

$$xN = Nx,$$

*para todo $x \in G$. En ese caso, escribimos $N \trianglelefteq G$. 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, $1 \trianglelefteq G$, $G \trianglelefteq G$.

**Definición 2.17.** *Un grupo $G$ cuyos únicos subgrupos normales sean $\{1\}$ y él mismo se dice que es **simple**.*

**Teorema 2.18** (***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.

□

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

**Proposición 2.19.** *Supongamos que $N \trianglelefteq G$. El conjunto $G/N$ de las coclases 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 tod $x \in G$.*

*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 tenemmos que

$$(xN)(x^{-1}N) = N = (x^{-1}N)(xN),$$

para todo $x \in G$.

□

**Definición 2.20.** *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 2.21.** *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.

□

Los homomorfismos son las aplicaciones que conservan la estructura de grupo.

**Definición 2.22.** *Dados $G$ y $H$ grupos, una aplicación $f\colon G \longrightarrow H$ es un **homomorfismo de grupos** si cumple*

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

**Definición 2.23.** *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 $G \cong H$. Si $f$ es un isomorfismo y además es de la forma $f\colon G \longrightarrow G$ entonces diremos que $f$ es un **automorfismo**.*

**Ejemplo 2.23.1.** *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 2.23.1.** *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 2.24.** *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 2.23.1(1.) tenemos que $Ker(det) = SL_n(K)$ es el grupo especial lineal. Y en el ejemplo 2.23.1(2.) es el propio $N$.

**Proposición 2.25.** *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 2.23.1(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 $x = y$.

□

**Definición 2.26.** *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.*

**Teorema 2.27** (***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:

$$G/Kerf \cong H.$$

**Proposición 2.28.** *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 2.23.1, $NH/N$ es un subgrupo de $G/N$.

□

**Teorema 2.29** (***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 2.30** (***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

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

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

□

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

**Teorema 2.31** (***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 2.28, $K/N = f(K)$ 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 2.23.1. 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 2.32.** *$K$ es subgrupo normal de $G$ si y sólo si $K/H$ es subgrupo normal de $G/H$.*

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

□

**Definición 2.33.** *Un **automorfismo** $\alpha$ 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 2.34.** *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*

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

**Proposición 2.35.** *Sea $G$ un grupo y $g \in G$. Entonces:*

1. *La aplicación $\alpha_g$ 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 $\alpha_g$ es biyectiva. Sean ahora $x, y \in G$, entonces:

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

   Luego $\alpha_g$ es un homomorfismo, y notar que $\alpha_1$ 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 2.36.** *Definimos*

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

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

**Proposición 2.37.** *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.*

□

**Definición 2.38.** *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 2.39.** *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 $yz = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = zy$.

**Proposición 2.40.** *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

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

**Teorema 2.41.** *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, $m = n$.

□

**Definición 2.42.** *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 $|x| = n$.*

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

**Teorema 2.43.** *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 2.40 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 2.43.1.** *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 2.43. Luego $G = H$ tiene orden $p$. Por último, como en un grupo abeliano todos sus subgrupos son normales ya está.

□

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 $x \equiv y \bmod n$.

**Proposición 2.44.** *Si $n \geq 1$, entonces*

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

*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 2.45.** *Si $n$ es un entero positivo, llamamos **función de Euler**, y la denotamos por $\varphi$, a*

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

Notar que por 2.43, $\varphi(n)$ es el número de generadores en un grupo cíclico de orden $n$.

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 $\alpha\beta =\because \alpha$ (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 2.46.** *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 $u + n\mathbb{Z}$ 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 2.47.** *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 2.23.1 y deducimos que $f = f_d$.

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 2.23.1. 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 2.43.

Queda probado así que la aplicación $\mathcal{U}_n \longrightarrow Aut(C_n)$ dada por $d + n\mathbb{Z} \longmapsto f_d$ 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.

Finalmente, veamos el producto directo y semidirecto:

**Proposición 2.48.** *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 $G = N_1N_2$ 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 $G = N_1N_2$, $f$ es suprayectiva. $Kerf = \{(n_1, n_2) \in N_1 \times N_2 : n_1n_2 = 1\}$. Si $n_1n_2 = 1$, entonces $n_2 = n_1^{-1} \in N_1 \cap N_2 = \{1_G\}$. Así, $n_1 = n_2 = 1_G$ y $Kerf = \{1_G\}$ y $f$ es inyectiva. El resultado se sigue del *Primer Teorema de Isomorfía.*

□

**Definición 2.49.** *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 $G = N_1N_2$ y $N_1 \cap N_2 = \{1_G\}$, es un* ***producto directo****.*

**Proposición 2.50.** *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 $\varphi$*** *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 $\varphi$ 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 $\varphi$ 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 $\varphi$ está bien definida y que es un homomorfismo.

Definimos ahora

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

y veamos que $f$ es homomorfismo:

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

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

□

**Proposición 2.51.** *Sea $N = C_n$ un grupo cíclico de orden $n$ y sea $H = \langle x \rangle = C_2$. Entonces definimos*

$$\begin{array}{rccc} \varphi\colon & H & \longrightarrow & Aut(N) \\ & x & \longmapsto & (n \longmapsto n^{-1}), \end{array}$$

*con $\varphi(1) = id$. Entonces $N \times_\varphi H$ es un grupo de $2n$ elementos denominado **grupo diédrico** de $2n$ elementos, y lo escribiremos como $D_{2n}$.*

*Demostración.* La aplicación $n \longrightarrow n^{-1}$ es un automorfismo de $N$ de orden 2. Entonces $\varphi(x) \circ \varphi(x) = id$, y $\varphi(x^2) = \varphi(1) = id$. Así, $\varphi$ es homomorfismo.

□

## 2.2. Grupos de permutaciones

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

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

**Definición 2.52.** *Dados $\alpha_1, \ldots, \alpha_n$ $n$ elementos distintos de $\Omega$, 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**.*

**Definición 2.53.** *Dada una permutación $\sigma \in S_n$, diremos que $\sigma$ **mueve** un $\alpha_i \in \Omega$ si $\sigma(\alpha_i) = \alpha_j$, con $i \neq j$. Por el contrario, diremos que $\sigma$ **fija** un $\alpha_i \in \Omega$ si $\sigma(\alpha_i) = \alpha_i$.*

Del conjunto $\Omega$ 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 $\Omega$ de $n$ elementos en lugar de $S_\Omega$. Veámoslo también así:

**Observación 2.53.1.** *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 $\sigma$ sobre los primeros $n$ enteros positivos y fija los comprendidos entre $n+1$ y $m$. Es decir, la aplicación*

$$\begin{array}{ccc} S_n & \longrightarrow & S_m \\ \sigma & \longmapsto & \sigma' \end{array}$$

   *es un homomorfismo inyectivo de grupos y, por el Primer Teorema de Isomorfía, $S_n$ es isomorfo a su imagen, que es un subgrupo de $S_m$.*

2. *De todo lo visto hasta ahora, lo realmente importante no es la naturaleza del conjunto $\Omega$ como tal, sino el hecho de que tenga $n$ elementos. Así, si $I_n$ es otro conjunto con $n$ elementos, el grupo $Biy(I_n)$ de biyecciones de $I_n$ en sí mismo es isomorfo a $S_n$, y no distinguiremos entre ambos. Para verlo, fijada una biyección cualquiera $\alpha\colon \Omega \longrightarrow I_n$ se comprueba inmediatamente que la aplicación*

$$\begin{array}{ccc} Biy(I_n) & \longrightarrow & S_n \\ \beta & \longmapsto & \alpha \circ \beta \circ \alpha^{-1} \end{array}$$

   *es un isomorfismo de grupos. Es por esta razón por la que hemos introducido la notación de $\Omega$ simplemente para hablar de un conjunto finito de $n$ elementos cualquiera.*

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 $S_\Omega$ actúa sobre $\Omega$ mediante $\sigma \cdot \alpha = \sigma(\alpha)$, con $\sigma \in S_\Omega$, $\alpha \in \Omega$.

**Definición 2.54.** *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 2.55.** *Dado* $\Omega$ *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* $\Omega$ *y las demás órbitas tienen longitud uno.*

*Demostración:* 1. es inmediato a partir de la definición de ciclo.

Para ver 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 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 $w \in \{\beta_1, \ldots, \beta_n\}$.

Ahora veamos 3.. La primera parte es consecuencia directa de lo visto en los apartados anteriores. Tenemos que $\{a_1, \ldots, a_m\} = \{\sigma^r(a_1) : r \geq 0\}, \ldots, \{b_1, \ldots, b_n\} = \{\sigma^r(b_1) : r \geq 0\}$.

□

**Proposición 2.56.** *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 $\sigma G_a$. 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 $\Omega$ de la misma forma que $\sigma$.

Por último, si $\sigma = (a_1, \ldots, a_m) \cdots (b_1, \ldots, b_n)$ se escribe como producto de ciclos disjuntos, entonces por el lema inmediatamente anterior tenemos que $\sigma$ determina unívocamente los ciclos $(a_1, \ldots, a_m), \ldots, (b_1, \ldots, b_n)$, quedando así probada la unicidad.

□

**Corolario 2.56.1.** *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 2.56.2.** *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 $\sigma$ 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 $m$ $\forall i$, luego $h$ divide a $m$.

Como $\tau_i \tau_j = \tau_j \tau_i$ $\forall i, j$, por  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 $(\tau_1)^r \ldots (\tau_k)^r = 1$. Probamos 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 $\Omega$. Dado un $\alpha \in \Omega$, si $\alpha$ es fijado por $\tau_i$, entonces $\alpha$ es fijado por $(\tau_i)^r$. Si $\tau_i$ mueve $\alpha$, entonces $\alpha$ es fijado por $\tau_j$ para $j \neq i$ (en particular por $(\tau_j)^r$). Por tanto $\alpha = (\tau_k)^r \ldots (\tau_1)^r \cdot \alpha = (\tau_i)^r \cdot \alpha$ y deducimos que $(\tau_i)^r$ fija $\alpha$. Concluimos que $(\tau_i)^r = 1$. Por lo tanto, $o(\tau_i)$ divide a $r$ para todo $i$ y tenemos que $h$ divide a $r = o(\sigma)$.

□

**Proposición 2.57.** *Sea $\sigma = (\alpha_1, \ldots, \alpha_k)$ es un $k$-ciclo de $S_n$ y sea $\gamma \in S_n$. Entonces $\sigma^\gamma = (\gamma(\alpha_1), \ldots, \gamma(\alpha_k))$.*

*Demostración:* Sabemos que $\sigma(\alpha_i) = \alpha_{i+1}$, con $i = 1, \ldots, k-1$ 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 $i = 1, \ldots, k-1$ y $(\gamma\sigma\gamma^{-1})(\gamma(\alpha_k)) = \gamma(\alpha_1)$. Finalmente, si $\beta \in \Omega \setminus \{\sigma(\alpha_1), \ldots, \sigma(\alpha_K)\}$ entonces $\gamma^{-1}(\beta) \in \Omega \setminus \{\alpha_1, \ldots, \alpha_k\}$. Por lo que $\sigma \cdot (\gamma^{-1}(\beta)) = \gamma^{-1}(\beta)$ y así $\sigma^\gamma$ fija $\beta$. Luego $\sigma^\gamma$ y $(\gamma(\alpha_1), \ldots, \gamma(\alpha_k))$ actúan igual sobre cada elemento de $\Omega$ y así son iguales.

□

Una consecuencia muy útil de 2.56 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 2.58.** *Dos permutaciones $\sigma, \tau \in S_n$ son conjugadas en $S_n$ si y sólo si tienen el mismo tipo.*

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

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

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

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

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

son dos particiones de $\Omega$. Por lo que existe una única $\sigma \in S_n$ tal que $\sigma(a_i) = a'_i, \ldots, \sigma(b_j) = b'_j$ para $1 \leq i \leq m, \ldots, 1 \leq j \leq n$. 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*** $\sigma$ (ver 2.78) ***está formada por todas las permutaciones del mismo tipo que*** $\sigma$.

**Observación 2.58.1.** *Sea $k > 1$, entonces el número de $k$-ciclos que muevenn $k$ elementos distintos $a_1, \ldots, a_k \in \Omega$ es $(k-1)!$. Si $|\Omega| = n$, el número de $k$-ciclos de $S_n$ es $\binom{n}{k}(k-1)!$.*

*Esto se puede generalizar a permutaciones de determinados tipos: es decir, si queremos saber el número de permutaciones de $S_n$ con $b_j$ ciclos de longitud $j$ tendremos*

$$\frac{n!}{1^{b_1} 2^{b_2} \cdots n^{b_n} b_1! b_2! \cdots b_n!}.$$

*(odio la combinatoria)*

**Ejemplo 2.58.1.** *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 2.58.2.** *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* $\gamma$ *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 2.59.** *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 $S_\Omega$. Ahora, consideremos el conjunto $\mathcal{C}$ de los subconjuntos de $\Omega$ 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 $\sigma$ ***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 $\sigma$ ***invierte*** $X$.

Así, definimos:

**Definición 2.60.** *Dado un $\sigma \in S_n$, su **signatura** es*

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

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

Otra forma de definirla es:

**Definición 2.61.** *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 $f_\sigma$ 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*: $Aut(\mathbb{R}^n) \longrightarrow \mathbb{R}$ *es el homomorfismo determinante. Además el homomorfismo índice es sobreyectivo pues*

$$\varepsilon(id) = det(f_{id}) = det(id_{\mathbb{R}^n}) = +1$$

*y si* $\sigma$ *es una transposición cualquiera, la matriz* $M_{f_\sigma}(B)$ *es aquella en la que se han intercambiado dos columnas de la matriz identidad, y así*

$$\varepsilon(\sigma) = det(f_\sigma) = det(M_{f_\sigma}(B)) = -det(id_{\mathbb{R}^n}) = -1.$$

Así, a partir de la construcción de este *homomorfismo índice* como composición del homomorfismo determinante y $\psi$ antes definido, podemos dar una definición formal de lo que es el *grupo alternado*:

**Definición 2.62.** *El núcleo de* $\varepsilon$ *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* $\varepsilon$ *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 2.63.** *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 2.64.** *La aplicación signatura*

$$\begin{array}{rccc} sig\colon & S_n & \longrightarrow & \{-1, 1\} \\ & \sigma & \longmapsto & sig(\sigma) \end{array}$$

*es un homomorfismo de grupos. Su núcleo, que está formado por las permutaciones pares, es un subgrupo de índice* $2$, *el* ***grupo alternado*** $\mathcal{A}_n$. *Además,*

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

**Observación 2.64.1.** *Para $n \geq 4$ el grupo alternado $\mathcal{A}_n$ no es abeliano puesto que las permutaciones $\sigma = (1,2,3) \in \mathcal{A}_n$ y $\tau = (1,2)(3,4) \in \mathcal{A}_n$, por la proposición anterior y que $\sigma\tau(1) = 1$ y $\tau\sigma(1) = 3$, cumplen $\sigma\tau \neq \tau\sigma$.*

*Además, a partir de la proposición anterior y de 2.56, podemos afirmar que las transposiciones generan el grupo $S_n$, o sea que cada permutación es producto de transposiciones.*

**Ejemplo 2.64.1.** *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 de Niels Henrik Abel.

**Proposición 2.65.** *Si $n \geq 3$, entonces $\mathcal{A}_n$ es transitivo sobre $\Omega = \{1, \ldots, n\}$*

*Demostración:* Si $1 \leq i < j \leq n$, elegimos $k$ distinto de $i$ y de $j$ y tenemos que $(i,j,k)(i) = j$. Claramente $(i,j,k) \in \mathcal{A}_n$.

□

**Teorema 2.66** (***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 2.58.2 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 2.58.2 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 2.53.1 para cada $\sigma \in K$, tenemos definido un $\bar{\sigma} \in S_{n-1}$. Como la descomposición de $\sigma$ y $\bar{\sigma}$ como producto de ciclos disjuntos es la misma entonces $\sigma$ es par si y sólo si $\bar{\sigma}$ lo es. Por lo tanto $K \simeq \mathcal{A}_{n-1}$ 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 $\sigma$ no está en $N$.

Supongamos que $N > 1$ y sea $1 \neq \sigma \in N$. Supongamos primero que en la descomposición de $\sigma$ 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 $\sigma$ 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.

□

## 2.3. Acciones de grupos. Teoremas de Sylow. Resolubilidad

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 2.67.** *Sea $\Omega$ un conjunto no vacío y sea $G$ un grupo. Diremos que $G$ **actúa** sobre $\Omega$ si para todo $\alpha \in \Omega$ y $g \in G$ 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 $\Omega$.*

**Ejemplo 2.67.1.** *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*

$$g \cdot \alpha = \alpha^g.$$

   *Esta es la **acción de $G$ sobre $G$ por conjugación**.*

3. *Sea $\Omega = \{H : H \leq G\}$ el conjunto de 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 $\Omega$ 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 $\Omega$**.*

■

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

**Teorema 2.68.** *Sea $G$ un grupo y $\Omega$ un conjunto no vacío. Entonces:*

1. *Supongamos que $G$ actúa sobre $\Omega$. 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 $\rho_g$ 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 $\Omega$.*

*Demostración:* Veamos primero 1., sea $g \in G$, veamos que $\rho_g$ 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 $\rho_g$ es biyectiva.

Veamos ahora 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 2.69.** *Si un grupo $G$ actúa sobre un conjunto $\Omega$, 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 $\Omega$ 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 2.70.** *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 $g \in K$.

□

Todo grupo finito es subgrupo de un grupo simétrico.

**Teorema 2.71** (***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 $\Omega$ 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 $\Omega$ Por el resultado anterior tenemos que $K \subseteq H$. Por la primera parte de 2.68 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 2.71.1.** *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 $\Omega$. En efecto, si $\alpha, \beta \in \Omega$ escribiremos $\alpha \sim \beta$ si existe $g \in G$ tal que $g \cdot \alpha = \beta$. Es decir, $\alpha$ y $\beta$ van a estar relacionados si existe un elemento de $G$ que actuando sobre $\alpha$ dé $\beta$. 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

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

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

**Definición 2.72.** *Dado un grupo $G$ actuando sobre un conjunto $\Omega$, $\alpha \in \Omega$ y considerando la relación de equivalencia $\sim$ que acabamos de ver, entonces la clase de equivalencia de $\alpha$ es*

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

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

Notar que al tratarse las órbitas de clases de equivalencia para la relación de equivalencia $\sim$ entre elementos de $\Omega$ antes vista, entonces van a formar una partición de $\Omega$. Es decir, que su unión disjunta forman la totalidad de $\Omega$. 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 $\Omega$ 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 || para hablar de cardinal de un conjunto, lo cuál podría considerarse abuso de notación).

**Definición 2.73.** *Dado un grupo $G$ actuando sobre un conjunto $\Omega$, si $\alpha \in \Omega$ entonces definimos el* ***estabilizador*** *de $\alpha$ en $G$ como*

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

**Teorema 2.74** (***Teorema de la órbita-estabilizadora***)**.** *Sea $G$ un grupo que actúa sobre un conjunto $\Omega$ y sea $\alpha \in \Omega$. Entonces $G_\alpha \leq G$ y*

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

*Demostración:* Sea $g, h \in G_\alpha$. Entonces $(gh) \cdot \alpha = g \cdot (h \cdot \alpha) = g \cdot \alpha = \alpha$. Por lo que $gh \in G_\alpha$, además si $g \cdot \alpha = \alpha$ entonces $g^{-1} \cdot \alpha = g^{-1} \cdot (g \cdot \alpha) = (g^{-1}g) \cdot \alpha = \alpha$, luego $g^{-1} \in G_\alpha$ y así $G_\alpha \leq G$.

Ahora, busquemos una aplicación biyectiva $f \colon \{xG_\alpha : x \in G\} \longrightarrow O_\alpha$. Definimos $f(xG_\alpha) = x \cdot \alpha$. Ahora, $xG_\alpha = yG_\alpha$ si y sólo si $x^{-1}y \in G_\alpha$ si y sólo si $(x^{-1}y) \cdot \alpha = \alpha$ si y sólo si $x \cdot ((x^{-1}y) \cdot \alpha) = x \cdot \alpha$ si y sólo si $y \cdot \alpha = x \cdot \alpha$, luego $f$ está bien definida y es inyectiva. Al ser $f$ claramente suprayectiva, ya está.

□

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

**Definición 2.75.** *Dado un grupo $G$ actuando sobre un conjunto $\Omega$, y dado un $\alpha \in \Omega$ decimos que $\alpha$ es un* ***punto fijo*** *de $\Omega$ 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 $\Omega$.*

**Definición 2.76.** *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 2.77.** *Sea $G$ un grupo actuando sobre un conjunto finito $\Omega$. 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 2.74, tendremos que $|O_{\alpha_j}| = [G : G_{\alpha_j}] > 1$, con $j = 1, \ldots, s$. Como $[G : G_{\alpha_j}]$ divide a $|G| = p^n$, ya está.

□

La descomposición del conjunto $\Omega$ 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 2.78.** *Consideremos la acción*

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

*donde ya sabemos que $\alpha_g(x) = x^g = gxg^{-1}$ con $x \in G$. Notar que en este caso el conjunto sobre el que consideramos la acción es $G$, y que también la hemos presentado antes, al comienzo del capítulo concretamente, como la* ***acción conjugación****.*

*Como $\alpha_g \in Aut(G)$ tenemos que en particular es biyectiva. Además es claro que $\alpha_{gh} = \alpha_g\alpha_h$, luego $\varphi$ es homomorfismo.*

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

*El estabilizador, dado un $x \in G$, $G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$ también se presentó en el primer capítulo y lo denominamos* ***centralizador de*** *$x$* ***en*** *$G$ y se escribe como $C_G(x)$. Además, ya que $G_x \leq G$ entonces también $C_G(x) \leq G$.*

*Por último, si $x \in G$, su órbita $O_x$ será entonces $O_x = \{gxg^{-1} : g \in G\}$. La denominaremos* ***clase de conjugación de*** *$x$* ***en*** *$G$. Y, siguiendo el teorema de la órbita estabilizadora vemos que tiene $[G : C_G(x)] = \dfrac{|G|}{|C_G(x)|}$ elementos. En particular, la denotaremos por $Cl_G(x)$, es decir, tendremos:*

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

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

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 $\Omega_0 = Z(G)$.

**Teorema 2.79** (***Ecuación de las clases de conjugación de un grupo***)**.** *Sean $G$ un grupo finito. Sean $K_1, \ldots, K_s$ las clases de conjugación de $G$ de longitud mayor que 1. Entonces*

$$|G| = |Z(G)| + \sum_{j=1}^{s} |K_j|.$$

*Esta fórmula recibe el nombre de* ***ecuación de clases de conjugación de un grupo finito****.*

*Demostración:* Se sigue inmediatamente a partir de lo discutido anteriormente y del teorema 2.77. 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 $\alpha_j$ 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 $x \notin Z(G)$.)

□

**Proposición 2.80.** *Sea $G \neq \{1\}$ un p-grupo finito. Entonces tenemos que $Z(G) \neq \{1\}$.*

*Demostración:* Por 2.77 y 2.79 tenemos que $|G| \equiv |Z(G)| \bmod p$. Como $|G| = p^a$ y $p^a \not\equiv 1 \bmod p$ ya está.

□

**Corolario 2.80.1.** *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 2.43.1.

□

**Definición 2.81.** *Si $H \leq G$ definimos 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. 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 $[G : N_G(H)]$.

**Proposición 2.82.** *Sea $G$ un grupo finito y $H \leq G$ con $|H| = p^a$ para cierto primo $p$. Entonces*

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

*Demostración:* Consideremos el conjunto $\Omega = \{xH : x \in G\}$. Tenemos que $H$ actúa sobre $\Omega$ por multiplicación a izquierda. Calculamos el número de puntos fijos, es decir $\Omega_0$. 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 2.77.

□

**Corolario 2.82.1.** *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.

**Corolario 2.82.2.** *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 2.43.1, 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 2.83.** *Diremos que una acción de un grupo $G$ sobre un conjunto $\Omega$ es* ***transitiva*** *si sólo hay una órbita, es decir, si $\Omega$ es una $G$-órbita. Dicho de otra manera: la acción de $G$ sobre $\Omega$ es transitiva si dados $\alpha, \beta \in \Omega$ existe un $g \in G$ tal que $g \cdot \alpha = \beta$.*

**Proposición 2.84.** *Sea $G$ un grupo actuando sobre un conjunto $\Omega$. Dados $\alpha \in \Omega$ y $g \in G$, entonces*

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

*En particular, si la acción de $G$ sobre $\Omega$ es transitiva, entonces todos los estabilizadores son conjugados.*

*Demostración:* Se tiene que $x \in G_{g\cdot\alpha}$ si y sólo si $x \cdot (g \cdot \alpha) = g \cdot \alpha$ si y sólo si $g^{-1} \cdot (xg \cdot \alpha) = \alpha$ si y sólo si $(g^{-1}xg) \cdot \alpha = \alpha$ si y sólo si $g^{-1}xg \in G_\alpha$ si y sólo si $x \in (G_\alpha)^g$, luego se tiene la igualdad.

Supongamos ahora que la acción de $G$ sobre $\Omega$ 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. 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 2.85** (***Teorema de Cauchy para grupos abelianos.***)**.** *Sea $G$ un grupo abeliano finito, y $p$ un número primo que divide al orden de $G$. Entonces existirá $x \in G$ tal que $o(x) = p$.*

*Demostración:* Lo haremos por inducción sobre $|G|$. Sea $H$ un subgrupo propio de $G$ de orden lo mayor posible. Si $p \mid |H|$, por hipótesis de inducción existirá un $x \in H \subset G$ tal que $o(x) = p$. Por lo tanto podemos suponer que $p \nmid |H|$. Como $p \mid |G| = |G/H||H|$ por el *Teorema de Lagrange* (además podemos hacer el cociente porque al ser $G$ abeliano todo subgrupo es normal), y esto quiere decir que $p \mid |G/H|$. Además, como $H$ es de orden lo mayor posible entre los subgrupos de $G$,

por el *Teorema de la correspondencia* $G/H$ no tiene subgrupos propios no triviales y por tanto es simple.

Así, ahora partimos de que $G/H$ es simple y abeliano y que $p \mid |G/H|$. Como los grupos simples abelianos son cíclicos de orden primo tenemos que

$$G/H \simeq C_p.$$

Sea $H \neq xH \in G/H$. Entonces es claro que $o(xH) = p$. Tenemos un elemento de orden $p$ dentro del cociente y queremos encontrar un elemento de orden $p$ dentro del grupo. Para ello construiremos el homomorfismo sobreyectivo que ya conocemos

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

y de las propiedades de los homomorfismos sabemos que $p = o(xH) = o(\pi(x)) \mid o(x)$. Esto quiere decir que $p \mid o(x)$ y así $x^{o(x)/p} \in G$ de orden $p$, ese es el elemento que buscábamos.

□

Ahora, el resultado general:

**Teorema 2.86** (***Teorema de Cauchy.***)**.** *Sea $G$ un grupo finito y $p$ un número primo que divide al orden de $G$. Entonces existirá un $x \in G$ tal que $o(x) = p$.*

*Demostración:* Por inducción nuevamente sobre $|G|$. Si existe un subgrupo propio $H$ de $G$ tal que $p \mid |H|$ ya hemos terminado, puesto que existirá un $x \in H \subset G$ tal que $o(x) = p$. Así, podemos suponer que $p \nmid |H|$ para todo $H$ subgrupo propio de $G$. Ahora, de la ecuación de clases:

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)]$$

sabemos que como $1 < [G : C_G(x_i)]$ entonces $p \nmid |C_G(x_i)|$ $\forall i$, pero a la vez también $p \mid |G|$, esto quiere decir que $p \mid [G : C_G(x_i)]$ $\forall i$.

Como $p \mid |G|$ y $p \mid [G : C_G(x_i)]$ entonces necesariamente $p \mid |Z(G)|$, pero como $p$ no divide al cardinal de ningún subgrupo propio tenemos que $Z(G) = G$ y así $G$ es abeliano. Por el resultado para grupos abelianos tenemos éste.

□

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

**Definición 2.87.** *Sea $G$ un grupo finito, y $p$ un número primo que divide al orden de $G$. Por tanto $|G| = p^n m$, con $m$ y $n$ enteros positivos tales que $p$ no divide a $m$, es decir, $mcd(p, m) = 1$. Notar que $n = 0$. Sea $H$ subgrupo de $G$. Entonces:*

1. *Diremos que $H$ es un $p$-**subgrupo** de $G$ si el orden de $H$ es potencia de $p$, es decir, $|H| = p^r$ con $r \geq 0$.*

2. *Diremos que $H$ es un $p$-**subgrupo de Sylow** de $G$ si $H$ es un $p$-subgrupo de $G$ y $[G:H]$ no es múltiplo de $p$, es decir, $|H| = p^n$ (la máxima potencia de $p$ que divide al orden de $G$). Al conjunto de todos los $p$-subgrupos de Sylow de $G$ los denotaremos por*

$$Syl_p(G) = \{H \leq G : |H| = p^n\}.$$

El objetivo fundamental de esta sección es demostrar que los subgrupos de Sylow siempre existen ($Syl_p(G) \neq \{\emptyset\}$, $\forall p$) y que son conjugados entre sí.

**Teorema 2.88** (***Primer Teorema de Sylow***)**.** *Sea $G$ es un grupo finito y $p$ un número primo, entonces $G$ tiene un $p$-subgrupo de Sylow.*

*Demostración:* Lo haremos por inducción sobre el orden de $G$. Si $|G| = 1$, entonces es evidente. Supongamos ahora que todos los grupos de orden menor que $|G|$ tienen $p$-subgrupos de Sylow y veamos que $G$ también los tiene. Si $p \nmid |G|$ entonces el subgrupo trivial es un $p$-subgrupo de Sylow de $G$. Por lo que supongamos que $p \mid |G|$, así $|G| = p^n m$ con $p$ no dividiendo a $m$ ($mcd(p, m) = 1$). Entonces, podemos distinguir dos casos:

Primero, que exista un subgrupo $H \leq G$ tal que $p \nmid [G:H]$. Entonces es claro que $p^n \mid |H|$ y por hipótesis de inducción se tiene que $H$ tiene un $p$-subgrupo de Sylow de orden $p^n$, que llamaremos $P$ y que también será $p$-subgrupo de Sylow de $G$ .

Segundo, que para todo subgrupo $H$ de $G$, $p \mid [G:H]$. Entonces, por la ecuación de clases tenemos que $p \mid |Z(G)|$, y como éste es un grupo abeliano entonces tiene un elemento de orden $p$, ó equivalentemente tiene un subgrupo $H \leq Z(G)$ de orden $p$. Como todos los elementos de $H$ conmutan con todos los elementos de $G$ entonces es claro que $H^g = H$ para todo $g \in G$, es decir, $H \trianglelefteq G$. Se cumple que $[G:H] = p^{n-1}m$ y tiene un subgrupo de Sylow $P/H$ que cumplirá $[P:H] = p^{n-1}$, por lo que $|P| = p^n$ y así $P$ es un $p$-subgrupo de Sylow de $G$.

□

**Teorema 2.89** (***Segundo Teorema de Sylow***)**.** *Si $G$ es un grupo finito, entonces todo $p$-subgrupo de $G$ está contenido en un $p$-subgrupo de Sylow y dos $p$-subgrupos de Sylow cualesquiera son conjugados.*

*Demostración:* Sea $P$ un $p$-subgrupo de Sylow de $G$ y sea $H$ un $p$-subgrupo arbitrario. Entonces $H$ actúa sobre $X = G/R^P$ por multiplicación a izquierda como vimos en **??**. Por el teorema de la órbita estabilizadora tenemos que las órbitas de $\Omega$ 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 $\Omega$, que es $[G:P]$, sería suma de potencias (no triviales) de $p$, así sería múltiplo de $p$.

Por lo tanto, existirá un $g \in G$ tal que la clase de conjugación $x = gP$ formará una órbita trivial, con $x$ como único elemento. Concretamente $hgP = gP$ para todo $h \in H$. En particular $hg \in gP$ y así $h \in P^g$ para todo $h \in H$. De aquí $H \leq P^g$ y así $P^g$ es también $p$-subgrupo de Sylow.

En caso de que $H$ sea un $p$-subgrupo de Sylow de $G$, entonces ha de darse la igualdad $H = P^g$, puesto que tenemos una inclusión y ambos tienen el mismo orden.

□

Por lo tanto, queda claro que los $p$-subgrupos de Sylow forman una órbita en la acción de $G$ sobre el conjunto de todos sus subgrupos por conjugación. Luego, si $P$ es un $p$-subgrupo de Sylow entonces el número total es $[G : N_G(P)]$. Éste número es un divisor del orden de $G$ y también de $[G : P]$.

**Corolario 2.89.1.** *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 2.90.** *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 2.91** (***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 $\Omega$ el conjunto de sus $p$-subgrupos de Sylow. Sea un $P \in \Omega$ y consideremos la acción de $P$ en $\Omega$ por conjugación. Es claro que $P^g = P$ para todo $g \in P$, luego la órbita de $P$ es trivial. Veamos que es única. Dado otro $Q \in \Omega$, entonces se tiene que $Q^g = Q$ para todo $g \in P$, entonces $P \leq N_G(Q)$ y así $P$ y $Q$ son $p$-subgrupos de Sylow de $N_G(Q)$, luego son conjugados en $N_G(Q)$. Así, existe un $g \in N_G(Q)$ tal que $P = Q^g = Q$.

Las órbitas que $P$ forma en $\Omega$ 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 $G$.

## 2.5. Resolubilidad

**Definición 2.92.** *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 todos $x, y \in G_{i+1}$, concluimos que $G_{i+1}/G_i$ es abeliano si y sólo $xyx^{-1}y^{-1} \in G_i$ para todo $x, y \in G_{i+1}$.*

**Proposición 2.93.** *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 **??**. Por tanto, $NG_i/N \trianglelefteq NG_{i+1}/N$ por 2.32. 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 2.94.** *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 unn $p$-grupo, por 2.82.2 podemos hallar subgrupos

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

tales que $[G_{i+1} : G_i] = p$, con $i = 0, \ldots, k-1$. Por 2.82.1, 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 2.95.** *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 2.43.1 tenemos que $G/M$ es cíclico de orden primo. Ahora, por la primera parte de 2.93, $M$ es resoluble y aplicamos la hipótesis de inducción.

□

**Proposición 2.96.** *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 2.93. Por tanto, existe $N \trianglelefteq A_n$, con $N < A_n$, 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****, es decir que dados $a, b, c \in A$, tenemos que*

$$(a + b)c = ac + bc, \quad a(b + c) = ab + ac.$$

*Además es importante matizar que el elemento neutro para la suma, el cero, podrá escribirse como $0_A$ ó simplemente $0$. Denotaremos por $A^* = A \setminus \{0\}$. Y, como en grupos, la operación conocida como producto podrá denotarse con un $\cdot$ en ocasiones ó con simple yuxtaposición.*

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

**Definición 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.*

**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*

$$ab = ba.$$

**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 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*

$$ab = ba.$$

**Definición 3.5.** *Si $A$ es un anillo, podemos construir el* ***anillo de polinomios*** *$A[x]$ sobre $A$.*

*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 $a_m = 1$ 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:*

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

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

**Definición 3.6.** *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.*

**Definición 3.7.** *Llamaremos* ***dominio de integridad****, ó D.I, a un anillo unitario y conmutativo sin divisores de cero.*

*Importante remarcar una propiedad fundamental de los dominios de integridad, y también de los cuerpos: se pueden simplificar factores comunes en las igualdades ya que si tenemos $ab = ac$, con $a \neq 0$, entonces $a(b-c) = 0$, y al no ser $a$ un divisor de cero, tenemos que $b - c = 0$ y de aquí $b = c$. Esto se conoce como* ***ley cancelativa*** *y también puede darse en estructuras de anillos, siempre y cuando los elementos implicados no sean divisores de cero.*

**Definición 3.8.** *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* $x \longrightarrow x/1$*.*

**Definición 3.9.** *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).*

**Definición 3.10.** *Algunas definiciones de especial interés:*

1. *El conjunto* $\{0\}$ *es un ideal de* $A$*, denominado* ***ideal nulo****. También* $A$ *cumple con las condiciones, así que también es ideal de* $A$*, y tanto este como el ideal nulo son los llamados* ***ideales impropios*** *de* $A$*. Esto sirve para distinguirlos de aquellos ideales* $\{0\} \neq I \neq A$*, 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.*

**Definición 3.11.** ***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 la denotaremos $A/I$ y la clase de equivalencia de un elemento $x \in A$ será:*

$$x + I = \{x + a : \ a \in I\}.$$

*Que un elemento $y$ esté en la clase de equivalencia de $x$ significa que existirá un elemento $a \in I$ de la forma $a = y - x$. Además,*

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

*Ahora, dotaremos a $A/I$ de dos operaciones que lo convertirán en un anillo, dados $x, y \in A$:*

$$\begin{array}{rccl} +: & A/I \times A/I & \longrightarrow & A/I \\ & ((x+I),(y+I)) & \longmapsto & (x+I)+(y+I) = (x+y)+I, \end{array}$$

*que le confiere a $A/I$ estructura de grupo abeliano (conmutativo), y*

$$\begin{array}{rccl} \cdot: & A/I \times A/I & \longrightarrow & A/I \\ & ((x+I),(y+I)) & \longmapsto & (x+I)\cdot(y+I) = xy+I. \end{array}$$

*Esta última operación además no depende de los representantes elegidos. Supongamos que $x + I = x' + I$ (es decir, $x - x' \in I$) y que $y + I = y' + I$ ($y - y' \in I$). Entonces $xy + I = x'y' + I$, ya que*

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y') \in I$$

*esto último es así por la segunda condición que deben cumplir los ideales.*

*Una vez visto esto, las propiedades asociativa y conmutativa del producto, así como la distributiva, son inmediatas. El* ***elemento neutro*** *de $A/I$ será $1 + I$. Así, $A/I$ dotado con las dos operaciones, suma y producto respectivamente, y las demás propiedades enunciadas tiene estructura de anillo conmutativo unitario, que denominaremos* ***anillo cociente ó anillo de clases de restos módulo*** *$I$.*

*Finalmente, los ideales del cociente $A/I$ serán aquellos ideales de $A$ que contengan a $I$, de hecho se puede establecer fácilmente una biyección entre ambos conjuntos. Sea $L$ un ideal del anillo cociente y consideremos el conjunto*

$$J = \{x \in A : x + I \in L\}.$$

*Entonces es claro que $J$ es un ideal de $A$ y que contiene a $I$, puesto que si $x \in I$ entonces $x + I = 0 + I \in L$. Luego la biyección se establece entre los conjuntos de la forma $L$ y de la forma $J$, es decir, entre los ideales de $A/I$ y los ideales de $A$ que contienen a $I$ respectivamente.*

**Definición 3.12.** *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 3.13.** *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 3.14.** *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 falso.

Recíprocamente, sea $x + I$ un elemento no nulo de $A/I$. Entonces $x \in A \setminus I$, es decir, será un elemento de $A$ que no estará en $I$, por lo que el ideal $I + xA$ contiene estrictamente a $I$. Como este último es maximal tendremos que $I + xA = A$, es decir que existirá $b \in I$ e $y \in A$ tal que $b + xy = 1$. Así que $1 - xy \in I$, es decir,

$$xy + I = (x + I)(y + I) = 1 + I,$$

por lo que $A/I$ es un cuerpo.

□

**Proposición 3.15.** *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.

□

**Definición 3.16.** *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. $f(1_A) = 1_B$.

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 $p(b) = a_k b^k + \ldots + a_1 b + a_0$.

**Proposición 3.17** (***Homomorfismo evaluación***)**.** *Sea $A$ un anillo conmutativo y unitario, y supongamos que $a \in A$. Entonces, la aplicación*

$$\begin{array}{rccc} e_a\colon & A[x] & \longrightarrow & A \\ & p & \longmapsto & p(a) \end{array}$$

*es un homomorfismo de anillos.*

*Demostración:* Observar que $e_a(1) = 1$. Si $p(x) = \sum_n a_n x^n$ y $q(x) = \sum_n b_n x^n$ hay que comprobar que $(p+q)(a) = p(a) + q(a)$ y que $pq(a) = p(a)q(a)$. Es un simple ejercicio.

□

**Definición 3.18.** *Sea $f\colon A \longrightarrow B$ un homomorfismo de anillos conmutativos y unitarios. Entonces:*

1. *Llamaremos* ***núcleo*** *de $f$ y lo denotaremos $kerf$ al ideal*

   $$kerf = \{x \in A : f(x) = 0\}.$$

   *Es un ideal ya que, si $x, y \in kerf$, $a \in A$, tenemos que*

   $$f(x+y) = f(x) + f(y) = 0 + 0 = 0,$$
   $$f(ax) = f(a)f(x) = f(a) \cdot 0 = 0.$$

2. *Llamaremos* ***imagen*** *de $f$ y la denotaremos $Imf$ al anillo*

   $$Imf = \{y \in B :\ \exists x \in A,\ y = f(x)\}.$$

   *Es un anillo conmutativo y unitario con las operaciones heredadas de $B$, ya que si $y = f(x)$, $v = f(u)$, $x, u \in A$, tenemos que*

   $$y - v = f(x) - f(u) = f(x-u) \in imf,$$
   $$y \cdot v = f(x)f(u) = f(xu) \in imf,$$
   $$1_B = f(1_A) \in imf.$$

**Proposición 3.19.** *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.

□

**Definición 3.20.** *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.*

**Teorema 3.21 (*Primer Teorema de Isomorfía*).** *Sea $f\colon A \longrightarrow B$ un homomorfismo de anillos conmutativos y unitarios. Consideremos el diagrama siguiente:*

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

*con $A/Kerf$ el anillo de clases módulo $Kerf$ y*

$$\begin{array}{rccc} \pi\colon & A & \longrightarrow & A/Kerf \\ & x & \longmapsto & x + Kerf, \end{array}$$

*la proyección canónica, que es suprayectiva.*

$$\begin{array}{rccc} \bar{f}\colon & A/Kerf & \longrightarrow & Imf \\ & x + Kerf & \longmapsto & f(x), \end{array}$$

*la aplicación que nos induce, que será biyectiva, es decir, un isomorfismo:*

$$A/Kerf \cong Imf.$$

*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

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

□

**Definición 3.22.** *Sean $x, y$ elementos de $A$ tales que $x \neq 0$. Se dice que $x$* ***divide a $y$, que $x$ es un divisor de $y$, que $y$ es divisible por $x$ ó que $y$ es un múltiplo de*** *$x$ si existe $a \in A$ tal que $y = ax$. Se escribe $x \mid y$. Si $x$ no divide a $y$ se escribe $x \nmid y$.*

*En otras palabras, $x \mid y \Leftrightarrow y \in (x)$, ó equivalentemente $(y) \subseteq (x)$.*

Esto nos presenta la divisibilidad como una relación de orden parcial que será inmediata para ideales pero que para entenderla entre elementos habrá que describir la relación de igualdad asociada:

$$x \text{ está relacionado con } y \text{ si } x \mid y \text{ e } y \mid x, \text{ o sea si } (x) = (y).$$

Estas condiciones son equivalentes a:

1. Existe una unidad $a \in \mathcal{U}(A)$ tal que $y = ax$. Esto es así ya que si $(y) = (x)$ tendremos que $y \in (x), x \in (y)$, luego $y = ax$ y $x = by$. Luego $y = aby$ y como $A$ es un dominio de integridad podremos simplificar y obtener $1 = ab$, y así $a$ es unidad.

2. Si $y \in A^*$ no es unidad, denotaremos $div(y)$ el conjunto de todos los divisores de $y$. Es claro que los conjuntos $y \cdot \mathcal{U}(A)$ y $\mathcal{U}(A)$ están contenidos en $div(y)$. Así, si $y$ no tiene más divisores que las unidades y los productos del propio $y$ por unidades, es decir asociados, diremos que $y$ es ***irreducible***.

3. Si $y \in A^*$ genera un ideal primo diremos que $y$ es primo. ***Todo elemento primo es irreducible***. Veámoslo.

*Demostración:* Sea $y = ax$. Si $y$ es primo entonces $(y)$ es primo y se tendrá que $a \in (y)$ ó $x \in (y)$. Si $a \in (y)$ tendremos que $a = zy$, luego $y = zyx$ y $1 = zx$. Así, $x \in \mathcal{U}(A)$ y $a = yx^{-1} \in y \cdot \mathcal{U}(A)$. Análogo si $x \in (y)$.

□

El recíproco en general no se cumple, aunque esto lo desarrollaremos más adelante.

**Definición 3.23.** *Dos elemento $x, y \in A$ se dirán **asociados** en $A$ si $x \mid y$ e $y \mid x$. 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 $x$ cualquiera (sus asociados) estará formada por elementos de la forma $ux$, con $u \in \mathcal{U}(A)$.*

## 3.2. Algunas estructuras algebraicas

**Definición 3.24.** *Diremos que $A$ es un **dominio euclídeo**, escrito $DE$, si existe una aplicación*

$$\|\cdot\| \colon A \longrightarrow \mathbb{N}$$

*con $\mathbb{N}$ el conjunto de los enteros no negativos, 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:

**Proposición 3.25.** *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.

□

**Proposición 3.26.** *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 todos los dominios euclídeos tienen todos sus ideales generados por un sólo elemento, si definimos a éstos como una nueva clase de dominios habremos encontrado otra estructura que nos facilitará mucho el trabajo con ideales.

**Definición 3.27.** *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 $DIP$.*

**Proposición 3.28.** *Sea $A$ un $DIP$. Entonces todo elemento irreducible $a \in A^*$ genera un ideal maximal.*

*Demostración:* Sea $I \subseteq A$ un ideal que contiene al ideal principal $(a)$, generado por el elemento irreducible $a$. Veamos que ó bien $I = (a)$ ó $I = A$. Pero por ser $A$ un $DIP$, existirá un $b \in A$ tal que $I = (b)$. En consecuencia, $(a) \subseteq I = (b)$ y $b \mid a$. Como $a$ es irreducible, tendremos dos opciones:

1. O bien $b = u \cdot a$, con $u \in \mathcal{U}(A)$, y entonces $(a) = (b) = I$.
2. O bien $b \in \mathcal{U}(A)$, y entonces $A = (b) = I$.

□

**Definición 3.29.** *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.*

**Proposición 3.30.** *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

$$xy/u = (x/u)y = cy, \;\; xy/u = (y/u)x = dx,$$

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 3.31.** *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 $zt = xy$.

□

Anteriormente vimos que todo elemento primo es irreducible, ahora veremos que dadas unas condiciones también se cumple el recíproco.

**Proposición 3.32.** *Supongamos que en un dominio de integridad $A$ se cumple cualquiera de las condiciones de 3.31. Entonces todo elemento irreducible de $A$ es primo.*

*Demostración:* Sean $a \in A$ irreducible e $I = (a)$. Para comprobar que $I$ es primo consideremos $x, y \in A$ con $xy \in I$. Entonces $xy = ab$ con $b \in A$. Por la hipótesis existen

$$\alpha = mcm(y, b)$$

$$\beta = mcd(y, b)$$

y se verifica $\alpha\beta = yb$. Observemos ahora que $xy$ es múltiplo de $b$ y de $y$, luego $\alpha \mid xy$. En consecuencia, podemos escribir

$$a = \frac{xy}{\alpha} \cdot \frac{\alpha}{b};\ \ \frac{xy}{\alpha}, \frac{\alpha}{b} \in A.$$

Por ser $a$ irreducible existe una unidad $u \in A$ tal que se verifica una de las dos condiciones siguientes:

1. $xy/\alpha = ua$. Entonces $x = u(\alpha/y)a$, con lo que $x \in (a) = I$. (Notar que $y \mid \alpha$, luego $\alpha/y \in A$.)
2. $\alpha/b = ua$. Entonces $y = \alpha\beta/b = u\beta a$ y así $y \in (a) = I$.

□

**Proposición 3.33** (***Identidad de Bézout***)**.** *Sean $x, y \in A^*$, y supongamos que generan un ideal principal. Entonces existe $z = mcd(x, y)$ y*

$$z = ax + by$$

*con $a, b \in A$.*

*Demostración:* Sea $z \in A$ un generador de $(x) + (y)$. Entonces:

1. $x, y \in (z)$, luego $z$ es un divisor común de $x$ e $y$.
2. $z = ax + by$ para ciertos $a, b \in A$.

Por último, además, si $t \mid x$ y $t \mid y$, es claro que $t \mid z$. Por lo que tendremos que $z = mcd(x, y)$.

□

**Definición 3.34.** *Dos elementos $x, y \in A^*$ se denominan **primos entre sí** cuando no comparten más divisores comunes que las unidades, es decir, cuando $mcd(x, y) = 1$.*

**Definición 3.35.** *Un **dominio de factorización única**, escrito $DFU$ es un dominio de integridad en el que se cumple:*

1. *Todo elemento irreducible es primo.*
2. *Todo elemento no nulo que no sea unidad es producto de elementos irreducibles.*

Los $DFU$ satisfacen la condición de cadena ascendente para ideales principales.

**Observación 3.35.1.** *Algunas observaciones:*

1. *Que todo elemento no nulo que no sea unidad sea producto de elementos irreducibles no garantiza la unicidad de dicha factorización. Es necesaria también la primera condición, ya que la unicidad se desprende de que ésta se cumple sobre un dominio de ideales principales.*

2. *En un DFU siempre existen mcd y mcm. Efectivamente, puesto que el mcd es el producto de los factores irreducibles comunes elevados al menor exponente y el mcm es el producto de todos los factores irreducibles (comunes y no comunes) elevados al mayor exponente.*

3. *Las relaciones entre las distintas estructuras algebraicas estudiadas se puede resumir en:*

$$Cuerpos \subseteq DE \subseteq DIP \subseteq DFU \subseteq DI \subseteq Anillo.$$

*Por ejemplo, las matrices constituyen un anillo pero no un DI,* $\mathbb{Z}[\sqrt{-3}]$ *es un DI que no es DFU (puesto que* $(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$*), el anillo de los polinomios con coeficientes enteros* $\mathbb{Z}[X]$ *es un DFU que no es DIP o* $\mathbb{Z}$ *es un DE que no es un cuerpo.*

*Los anillos* $\mathbb{Z}$ *y* $\mathbb{Z}[i]$ *son DE y por tanto DFU. Es precisamente en* $\mathbb{Z}$ *donde éste resultado se manifiesta como el* ***teorema fundamental de la Aritmética****: todo número entero positivo* $n$ *se escribe de modo único como producto de números primos positivos* $p_1, \ldots, p_r$ *de la forma* $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$.

## 3.3. Anillos de restos

Primero, el resultado central de la sección, y a partir del cual desarrollaremos el resto.

**Proposición 3.36.** *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:

$$n = p_1^{\alpha_1} \ldots p_s^{\alpha_s},$$

con $p_i$ números primos conocidos como factores primos de $n$.

Con esto ya podemos pasar a describir los cocientes de $\mathbb{Z}$:

**Definición 3.37.** *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 $[-8] = [1] = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, \ldots\}$ (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,*

$$\mathbb{Z}/(n) = \{[0], [1], \ldots, [n-1]\}.$$

*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: $[1] + \ldots + [1] = [n] = [0]$, 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 3.38.** *Sea $n > 1$. Ya vimos en 3.11 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 $I = (-m) = (m)$).*

Podemos dar una versión alternativa del teorema chino de los restos:

**Teorema 3.39.** *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 $ker f = \{0\}$ y $f$ es inyectiva.

Como es una aplicación inyectiva entre dos conjuntos finitos de igual cardinal $ab$ entonces también será biyectiva, y así isomorfismo.

□

Veamos las unidades de los anillos de restos:

**Proposición 3.40.** *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 3.41.** *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 $\phi$ 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. Polinomios

**Definición 3.42.** *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 3.43.** *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*

$$f(X)\cdot g(X)=\sum_{k=1}^{n+m}c_kX^k,\ \ c_k=\sum_{i+j=k}a_ib_j,$$

*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 3.43.1.** *Este nuevo anillo,* $A[X]$*, contiene a* $A$ *ya que los elementos de* $A$ *son polinomios de la forma* $a=a+0X+\ldots+0X^n$*.*

A partir de ahora supondremos que $A$ es un dominio de integridad.

**Definición 3.44.** *Si* $0\neq f(X)=\sum_{i=0}^{n}a_nX^n\in A[X]$*, el* ***grado*** *de* $f(X)$ *es el mayor entero* $n\geq 0$ *tal que* $a_n\neq 0$ *y se denota* $\delta(f)$*. Los polinomios de grados* $0,1,2,3,4$ *los llamaremos constantes, lineales, cuadráticos, cúbicos y cuárticos respectivamente.*

*Diremos que un* $a_iX^i$ *es el término de grado* $i$*. El de grado* $0$ *se denomina* ***término independiente****. El coeficiente del término de mayor grado lo llamaremos* ***coeficiente director de*** $f(X)$*. Diremos que un* $f(X)$ *es mónico si su coeficiente director es una unidad del anillo.*

Ahora, dado $0\neq f(X_1,\ldots,X_n)\in A[X_1,\ldots,X_n]$ el $grado_{X_i}(f)$ 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 3.45.** *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 $A[X]$:

$$f=a_0+a_1X+\ldots+a_pX^p,\ \ g=b_0+b_1X+\ldots+b_qX^q,$$

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:

$$fg=\sum_{r}^{p+q}c_rX^r=a_0b_0+\ldots+(a_{p-1}b_q+a_pb_{q-1})X^{p+q-1}+a_pb_qX^{p+q}.$$

Por tanto, $c_{p+q}=a_pb_q\neq 0$ 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 $DI$.

□

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 general vamos a tener que $\delta(f \cdot g) \leq \delta(f) + \delta(g)$, pero como $A[X]$ es dominio de integridad entonces:

$$\delta(f \cdot g) = \delta(f) + \delta(g).$$

Además,

**Corolario 3.45.1.** *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 $A$.

□

La división en $A[X]$ está regulada por la conocida como ***pseudodivisión***.

**Proposición 3.46.** *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 $r(x) = r'(x)$.

□

**Corolario 3.46.1.** *SI $K$ es un cuerpo, $K[x]$ es un dominio euclídeo.*

*Demostración:* En este caso, el grado es una función euclídea.

□

**Corolario 3.46.2** (***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 3.46 con $f(x)$ como dividendo y $x - a$ como divisor y después sustituir $x = a$.

□

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 3.47.** *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 3.48.** *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 $n > 1$.*

## 3.5. Cuerpos y polinomios

En esta sección presentaremos las bases para luego desarrollar lo que serán las conocidas *extensiones de cuerpos*. Para ello, en lugar de sobre un anillo $A$, en esta sección estudiaremos polinomios sobre un cuerpo $K$.

**Proposición 3.49.** *Dado un cuerpo $K$ y $p \in K[x]$. Entonces $p$ es irreducible si y sólo si $K[x]/(p)$ es un cuerpo.*

*Demostración:* Veamos la primera implicación. Sea $f+(p) \neq (p)$. Veamos que $f+(p)$ tiene inverso. Como $p$ es irreducible, el máximo común divisor de $f$ y $p$ es 1. Por Bézout, existen $a, b \in K[x]$ tales que $1 = af + bp$. Tendríamos así que

$$1 + (p) = (a + (p))(f + (p)) + (b + (p))(p + (p)) = (a + (p))(f + (p))$$

ya que $p+(p) = 0$. Así, $a+(p)$ es el inverso de $f+(p)$. Luego, $K[x]/(p)$ es un cuerpo.

Recíprocamente, supongamos que $p$ no es irreducible y sea $p = fg$, con $\delta(f) < \delta(p)$ y $\delta(g) < \delta(p)$. $0 = p + (p) = (f + (p))(g + (p))$. Entonces $f + (p)$ y $g + (p)$ serían divisores de cero en $K[x]/(p)$, lo que es imposible porque se trata de un cuerpo. Así, $p$ es irreducible.

□

**Proposición 3.50.** *Sea $p \in K[x]$ irreducible. Entonces $K$ está contenido en un cuerpo en el que $p$ tiene alguna raíz.*

*Demostración:* Sea $E = K[x]/(p)$. Entonces sabemos que $E$ es un cuerpo por el resultado anterior. Consideramos la aplicación

$$\begin{array}{ccc} K[x] & \longrightarrow & K[x]/(p) \\ f & \longmapsto & f + (p) \end{array}$$

Si $0 \neq a \in K$ y $\bar{a}$ es su imagen en $K[x]/(p)$ por la aplicación anterior, $\bar{a} \neq 0$. Así, $K$ es isomorfo a $\bar{K} = \{\bar{a} : a \in K\}$ y podemos identificar $K$ con $\bar{K}$. Si $p = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, $p$ considerado como polinomio en $\bar{K}[x]$ es $\bar{p} = x^n + \bar{a}_{n-1}x^{n-1} + \ldots + \bar{a}_1x + \bar{a}_0$.

Ahora, $\bar{x} = x+(p)$ es raíz del polinomio $\bar{p}$ en $E = K[x]/(p)$, es decir, $\bar{p}(\bar{x}) = p+(p) = (p) = 0 + (p)$, el cero de $K[x]/(p)$. $((x^n + \bar{a}_{n-1}x^{n-1} + \ldots + \bar{a}_1x + \bar{a}_0) + (p) = (p))$.

□

**Ejemplo 3.50.1.** *Un ejemplo claro y sencillo de lo que nos dice la proposición anterior es el caso de $p(x) = x^2 + 1$. Está claro que $p(x) \in \mathbb{Q}[x]$ y que es irreducible. Entonces, de acuerdo al resultado que acabamos de ver, este cuerpo $\mathbb{Q}$ va a estar contenido en otro en el que $p(x)$ sí tenga alguna raíz. En efecto, en este caso dicho cuerpo va a ser*

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

*Además,*

$$\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i).$$

■

**Proposición 3.51.** *Sea $p \in K[x]$ y $a \in K$. Entonces $p(a) = 0$ si, y sólo si $x - a \mid p$.*

*Demostración:* Aplicamos el algoritmo de la división a $p$ y $x - a$: $p = (x - a)q + r$, donde $r = 0$ ó $\delta(r) < \delta(x - a)$. Si $r = 0$ ya está, si no entonces es una constante y como $p(a) = 0 \Leftrightarrow r(a) = 0$ entonces $r = 0$ y así $x - a \mid p$.

□

**Proposición 3.52.** *Sea $K$ un cuerpo y $E$ un cuerpo que contenga a $K$. Sea $f \in K[x]$ y $f'$ la derivada de $f$. Supongamos que $f' \neq 0$. Entonces:*

1. *Sea $a \in E$ raíz de $f$. Entonces $a$ es raíz múltiple de $f$ si y sólo si $f'(a) = 0$.*
2. *Si $f$ y $f'$ son primos entre sí, $f$ no tiene raíces múltiples en $E$.*
3. *Si $f \in K[x]$ es irreducible, $f$ no tiene raíces múltiples en $E$.*
4. *Si $charK = 0$, los polinomios irreducibles de $K[x]$ no tienen raíces múltiples en $E$.*
5. *Si $charK = p$, los polinomios irreducibles de $K[x]$ cuyo grado no es múltiplo de $p$ no tienen raíces múltiples en $E$.*

*Demostración:*

1. Sea $a$ raíz múltiple de $f$, entonces $f = (x - a)^n g$, con $n > 1$ y un $g \in K[x]$. Entonces $f' = n(x - a)^{n-1} g + (x - a)^n g'$ y así $f'(a) = 0$. Recíprocamente, si $a$ no fuera raíz múltiple entonces $f = (x - a)g$, con $g(a) \neq 0$ y $f' = g + (x - a)g'$ y $f'(a) = g(a) \neq 0$, absurdo.
2. Por Bézout, existen $g, h \in K[x]$ tales que $1 = fg + f'h$. Si fuera $f(a) = f'(a) = 0$ entonces $1(a) = 0$, absurdo. Por el punto 1. $f$ no tiene raíces múltiples.
3. Como $f$ es irreducible y $f' \neq 0$, entonces $f$ y $f'$ son primos entre sí y aplicamos el punto anterior.
4. Si $charK = 0$ y $g$ es un polinomio irreducible en $K[x]$, $g$ es no constante y $g' \neq 0$. Aplicamos el punto anterior.
5. Si $charK = p$ y $g$ es un polinomio irreducible en $K[x]$ tal que $p$ no divide a $\delta(g)$, $g' \neq 0$ y aplicamos el punto 3.

□

**Proposición 3.53** (***Criterio de Eisenstein***)**.** *Sea $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$. Supongamos que existe $p$ primo tal que $p \mid a_i$, con $0 \leq i \leq n - 1$, $p \nmid a_n$ y $p^2 \nmid a_0$. Entonces $f$ es irreducible en $\mathbb{Q}[x]$.*

## 3.6. Raíces de la unidad

A las raíces del polinomio $f(x) = x^n - z \in \mathbb{C}[x]$, con $z \in \mathbb{C}$ y $n \geq 1$ las denominamos ***raíces complejas de la unidad***. Como, para $n \geq 2$, el polinomio derivado

$f'(x) = nx^{n-1}$ tiene como única raíz el cero y los polinomios $f(x)$ y $f'(x)$ no tienen raíces en común, entonces todas las raíces $n$-ésimas de $z$ son todas distintas. Para determinarlas, usaremos la conocida como ***fórmula de De Moivre*** para la multiplicación de números complejos en forma trigonométrica:

$$(\cos(x) + i\sin(x))^n = \cos(nx) + i\sin(nx).$$

Si

$$z_1 = \rho_1(\cos(\theta_1) + i\sin(\theta_1)) \;\; z_2 = \rho_2(\cos(\theta_2) + i\sin(\theta_2)),$$

con $\rho_1, \rho_2$ reales positivos, ahora usando propiedades de las funciones trigonométricas tenemos que:

$$z_1 z_2 = \rho_1\rho_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)).$$

Ahora podemos simplificar y hacer que $z = \rho(\cos(\theta) + i\sin(\theta))$, con $\rho > 0$. Si $\zeta = \sigma(\cos(\varphi) + i\sin(\varphi))$ es una raíz $n$-ésima de $z$, entonces tiene que ser que

$$\sigma^n(\cos(n\varphi) + i\sin(n\varphi)) = \rho(\cos(\theta) + i\sin(\theta)),$$

de lo que deducimos que $\sigma^n = \rho$ y $n\varphi = \theta + 2k\pi$, con $k \in \mathbb{Z}$, es decir,

$$\sigma = \sqrt[n]{\rho}, \;\; \varphi = \frac{\theta + 2k\pi}{n}.$$

De todo esto concluimos que las raíces complejas $n$-ésimas de $z = \rho(\cos(\theta) + i\sin(\theta))$ se obtienen para $k = 0, 1, \ldots, n-1$ y son precisamente los números complejos

$$(*) \;\; \zeta_k = \sqrt[n]{\rho}\left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\sin\left(\frac{\theta + 2k\pi}{n}\right)\right).$$

Por ejemplo, si tenemos $z = 3i = 3\left(\cos\left(\frac{\pi}{2})\right) + i\sin\left(\frac{\pi}{2}\right)\right)$ y queremos calcular sus raíces cuadradas, entonces

$$\zeta_0 = \sqrt{3}\left(\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)\right) = \frac{\sqrt{6}}{2} + \frac{\sqrt{6}}{2}i, \;\; \zeta_1 = \sqrt{3}\left(\cos\left(\frac{5\pi}{4}\right) + i\sin\left(\frac{5\pi}{4}\right)\right) = -\frac{\sqrt{6}}{2} - \frac{\sqrt{6}}{2}i.$$

Otro ejemplo, las raíces terceras de $1 + i = \sqrt{2}\left(\cos\left(\frac{\pi}{4})\right) + i\sin\left(\frac{\pi}{4}\right)\right)$ entonces se tiene que

$$\zeta_0 = \sqrt[6]{2}\left(\cos\left(\frac{\pi}{12})\right) + i\sin\left(\frac{\pi}{12}\right)\right),$$

$$\zeta_1 = \sqrt[6]{2}\left(\cos\left(\frac{3\pi}{4})\right) + i\sin\left(\frac{3\pi}{4}\right)\right),$$

$$\zeta_2 = \sqrt[6]{2}\left(\cos\left(\frac{17\pi}{12})\right) + i\sin\left(\frac{17\pi}{12}\right)\right).$$

Ahora, hemos visto (o más bien recordado brevemente) cómo se calculan las raíces en general de cualquier número complejo. Pero las que nos van a interesar a lo largo del

texto van a ser las raíces de $z = 1$, es decir, las ***raíces complejas $n$-ésimas de la unidad***. Vamos, por tanto, a tener el número complejo $z = 1 = \cos(2\pi) + i\sin(2\pi)$. Utilizando ahora $(*)$ llegamos a la fórmula para calcular las raíces de la unidad:

$$\zeta_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right), \;\; k = 1, \dots n.$$

Notar que $k$ va de 1 hasta $n$ y que sería equivalente a que fuera desde 0 hasta $n-1$. Notar también que la fórmula de los $\zeta_k$ la podemos reescribir como $e^{2\pi ki/n}$.

De esto, lo primero que observamos es que empleando nuevamente la fórmula de De Moivre, resulta que $\zeta_1^k = \zeta_k$, donde

$$\zeta_1 = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) = \xi,$$

y así podemos llegar a escribir todas las $n$-ésimas raíces de la unidad como

$$\zeta_1 = \xi,\ \zeta_2 = \xi^2, \dots,\ \zeta_{n-1} = \xi^{n-1},\ \zeta_n = \xi^n = 1.$$

Así, es claro cómo las raíces forman un grupo cíclico de orden $n$.

# 4. Extensiones de Cuerpos

Nos encuadramos en una área de las matemáticas donde las estructuras algebraicas son fundamentales de conocer, en este caso, y durante todo el texto, conocer los grupos y anillos es imprescindible. Y como ya sabemos, un tipo concreto de anillo son los cuerpos, en los que se cumple que todo elemento no nulo es una unidad, o dicho de otra manera, el grupo de las unidades es el propio anillo a excepción del cero.

Nosotros nos vamos a parar a estudiar estas estructuras, cómo se relacionan entre ellas (veremos similitudes con grupos en algunos casos) y cómo se relacionan con la *Teoría de Galois*. Sin más comencemos:

## 4.1. Generalidades

**Definición 4.1.** *Dados dos cuerpos $E, K$, diremos que $E$ es una extensión de un cuerpo $K$ si existe un monomorfismo de cuerpos $\varphi\colon K \longrightarrow E$. Dicho de otra forma, si $K$ es un subcuerpo de $E$. A las extensiones las denotaremos por $E/K$. Además, se cumplirá que $E$ es un $K-$espacio vectorial. A la dimensión de este $K-$espacio vectorial la denotaremos por $dim_K E$. Si $dim_K E$ es finita, se dice que la extensión $E/K$ es **finita** y $dim_K E$ se escribirá como $|E : K|$ y se denominará **grado** de la extensión.*

Dada una extension $E/K$, $E$ tendrá una estructura de espacio vectorial sobre $K$. Para ver esto simplemente hay que considerar las operaciones $+$, $\cdot$ y partir de un grupo

abeliano $(E,+)$. Al ser $K$ un subcuerpo de $E$ las operaciones anteriores inducen las de $K$. En este grupo definimos la siguiente operación:

$$(\lambda, a) \longmapsto \lambda a = \lambda \cdot a, \ \ \lambda \in K, a \in E,$$

con $\lambda \cdot a$ el producto de elementos habitual en $E$. Como además, $1_K = 1_E$ por ser $K$ subcuerpo, entonces se va a tener que $1_K \cdot x = x \ \forall x$. Así es fácil ver que, con lo anterior, tenemos una estructura de espacio vectorial.

**Ejemplo 4.1.1.** *Veamos algunos ejemplos de extensiones conocidas:*

1. $|\mathbb{R} : \mathbb{Q}| = \infty$*, pues en caso de que fuese un natural* $n$ *cualquiera entonces* $\mathbb{R} \simeq \mathbb{Q}^n$ *y* $\mathbb{R}$ *sería numerable.*
2. $|\mathbb{C} : \mathbb{R}| = 2$*, puesto que* $\{1, i\}$ *es una base de* $\mathbb{C}$ *como* $\mathbb{R}$*-espacio vectorial.*
3. *Si* $E$ *es una extensión de* $K$*, entonces* $|E : K| = 1$ *si y sólo si* $E = K$*.*

■

Veamos que ocurre si intentamos encadenar extensiones:

**Proposición 4.2.** *Sea* $E$ *una extensión de* $L$*, y a su vez* $L$ *una extensión de* $K$*. Diremos entonces que* $L$ *es un cuerpo intermedio, ya que se tiene que* $K \subseteq L \subseteq E$*. Entonces* $E/K$ *es finita si y sólo si* $E/L$ *y* $L/K$ *lo son. En este caso, se tiene*

$$|E : K| = |E : L||L : K|.$$

*Demostración:* Partimos primero de que $E/K$ es finita, entonces $|E : K|$ es finita y que $L$ como $K$-espacio vectorial esté contenido en $E$ $K$-espacio vectorial implica que $dim_K L \leq dim_K E < \infty$, es decir, $|L : K|$ es finito. Por otro lado, si $B = \{u_1, \ldots, u_n\}$ es una base de $E$ como $K$-espacio vectorial y $v \in E$, entonces $v = \sum_i k_i u_i$, con los $k_i \in K \subseteq L$. Así, $B$ genera $E$ como $L$-espacio vectorial, es decir, $dim_L E$ es finita y así $|E : L|$ también.

Recíprocamente, si $|L : K| = s$ y $|E : L| = r$, sean $\{l_1, \ldots, l_s\}$ y $\{e_1, \ldots, e_r\}$ bases de $L$ como $K$-espacio vectorial y $E$ como $L$-espacio vectorial respectivamente. Veamos ahora que $U = \{v_{ij} : v_{ij} = l_i e_j, \ \forall i, j\}$ es una base de $E$ como $K$-espacio vectorial. En efecto, si $m \in E$, $m = \sum_j^r d_j e_j$, con $d_j \in L$, y a su vez $d_j = \sum_i^s c_{ji} l_i$, con los $c_{ji} \in K$. Por lo tanto,

$$m = \sum_{j=1}^{r} \left( \sum_{i=1}^{s} c_{ji} l_i \right) e_j = \sum_{j=1}^{r} \sum_{i=1}^{s} c_{ji} v_{ij}, \ \ c_{ji} \in K.$$

Con esto, $U$ genera el $E$ $K$-espacio vectorial. Ahora veamos que $U$ es también linealmente independiente, para ello supongamos que

$$0 = \sum_{j=1}^{r} \sum_{i=1}^{s} c_{ji} v_{ji} = \sum_{j=1}^{r} \left( \sum_{i=1}^{s} c_{ji} l_i \right) e_j, \ \ c_{ji} \in K.$$

Como $\{e_1, \ldots, e_r\}$ es una base de $E$ como $L$-espacio vectorial tenemos que $\sum_i^s c_{ji} l_i = 0$ para todo $j = 1, \ldots, r$. Y como $\{l_1, \ldots, l_s\}$ es una base de $L$ como $K$-espacio

vectorial entonces $c_{ji} = 0$ también para todo $i = 1, \ldots, s$. Así, es linealmente independiente, y además

$$|E : K| = rs = |E : L||L : K|.$$

□

**Proposición 4.3.** *Sean $E_1/K_1$, $E_2/K_2$ extensiones, y $\sigma\colon E_1 \longrightarrow E_2$ un isomorfismo de cuerpos. Si $K_2 = \sigma(K_1)$, entonces*

$$|E_1 : K_1| = |E_2 : K_2|.$$

Veamos ahora alguna definiciones:

**Definición 4.4.** *Sea $E$ una extensión de $K$, y sean $f(x) = \sum_i k_i x^i \in K[x]$ y $a \in E$. Diremos que $a$ es una **raíz** de $f$ si $f(a) = \sum_i k_i a^i = 0$.*

Llegados a este punto hay que aclarar que, como una extensión la hemos definido al fin y al cabo como un monomorfismo (una inyección) de un cuerpo en otro, estamos cometiendo un abuso de notación al identificar los $k_i$ anteriores con los $\varphi(k_i)$. En realidad deberíamos poner $f(a)$ como $f^{\varphi}(a) = \sum_i \varphi(k_i)a^i$.

Ahora, una observación que ya conocemos del capítulo anterior:

**Observación 4.4.1.** *Sea $E/K$ una extensión, y $a \in E$ una raíz de un polinomio $f$ de $K[x]$. Entonces $f(x) = (x - a)g(x)$, con $g \in E[x]$.*

**Definición 4.5.** *Sea $E/K$ una extensión y $X \subseteq E$. Entonces $K(X)$ es la intersección de los subcuerpos de $E$ que contienen a $K$ y a $X$, es decir, el menor subcuerpo de $E$ que contiene a $K$ y a $X$.*

**Proposición 4.6.** *Sea $E/K$ una extensión y $\alpha \in E$. Entonces*

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}.$$

Además, por inducción podemos definir $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.

Un resultado que se desprenden de forma inmediata de la transitividad del grado de las extensiones y de la noción que acabamos de ver es el siguiente:

**Proposición 4.7.** *Sea $E/K$ una extensión de cuerpos, finita, y $|E : K|$ un número primo. Entonces cada elemento $\alpha \in E \setminus K$ cumple que $E = K(\alpha)$.*

*Demostración:* Aplicando 4.2 a los cuerpos $K \subseteq K(\alpha) \subset E$ tenemos que

$$|E : K| = |E : K(\alpha)||K(\alpha) : K|$$

y como $|E : K|$ es un número primo y $|K(\alpha) : K| \neq 1$ ya que $\alpha \notin K$, entonces se tiene que $|E : K(\alpha)| = 1$, es decir, que $E = K(\alpha)\ \forall \alpha \in E \setminus K$.

□

**Definición 4.8.** *Sea $E/K$ una extensión y $\alpha \in E$. Diremos que $\alpha$ es* ***algebraico*** *sobre $K$ si existe un $p \in K[x]$ no nulo tal que $p(\alpha) = 0$, es decir, que $\alpha$ sea una raíz de $p$. Si $\alpha$ no es algebraico sobre $K$ se dice entonces que es* ***trascendente****. La extensión $E/K$ se dirá* ***algebraica*** *si todo elemento de $E$ es algebraico sobre $K$.*

**Ejemplo 4.8.1.** *Algunos ejemplos:*

1. *Si $\alpha \in K$, entonces $\alpha$ es algebraico sobre $K$. En particular, será raíz de $f(x) = x - \alpha$.*
2. *$\sqrt{2}$ es algebraico sobre $\mathbb{Q}$, ya que es raíz de $x^2 - 2$.*
3. *Los números $e$ y $\pi$ son trascendentes sobre $\mathbb{Q}$.*
4. *El número $\alpha = \sqrt{2 + \sqrt{5}}$ es algebraico sobre $Q$, pues $\alpha^2 = 2 + \sqrt{5}$, es decir, $\alpha^2 - 2 = \sqrt{5}$, y entonces $\alpha^4 - 4\alpha^2 - 1 = 0$. Por tanto, $\alpha$ es raíz del polinomio $p(x) = x^4 - 4x^2 - 1 \in \mathbb{Q}[x]$.*

■

**Proposición 4.9.** *Toda extensión finita es algebraica.*

*Demostración:* Sea $E/K$ finita y $n = |E : K|$. Si $\alpha \in E$, la familia $\{1, \alpha, \ldots, \alpha^n\}$ tiene $n + 1$ elementos (iguales o repetidos). Como $dim_K E = n$, dicha familia tiene que ser linealmente dependiente. Así, existen $t_0, t_1, \ldots, t_n \in K$ no todos nulos tales que $t_0 1 + t_1\alpha + \ldots + t_n\alpha^n = 0$. Sea $p(x) = t_0 + t_1 x + \ldots + t_n x^n$. Entonces $p(x) \in K[x]$, $p(x) \neq 0$ y $p(\alpha) = 0$.

□

Es interesante ver que, como hemos dicho, dada una extensión $E/K$ de grado $n$ y un $\alpha \in E$, entonces la familia $\{1, \alpha, \ldots, \alpha^n\}$ va a ser linealmente dependiente. Más adelante veremos qué significa esta familia, qué hay que hacer para convertirla en linealmente independiente y si será base de algo, ya que al fin y al cabo estamos hablando de espacios vectoriales.

Ahora, estudiaremos un resultado que nos dice que a cada cuerpo le podemos asignar una extensión que contendrá una raíz de un polinomio de su anillo de polinomios.

**Proposición 4.10.** *Sea $K$ un cuerpo y sea $f \in K[x]$, con $\delta(f) > 0$. Entonces existen una extensión $E$ de $K$ y $\alpha \in E$ tal que $\alpha$ es raíz de $f$.*

*Demostración:* Como $K[x]$ es un dominio de factorización única, factorizamos $f$ como producto de polinomios irreducibles en $K[x]$. Sea $p(x) = \sum_i^n a_i x^i$ uno de los factores irreducibles de $f$ y consideremos el ideal $I$ generado por $p$ en $K[x]$. Entonces $E = K[x]/I$ es un cuerpo y podemos ver que el homomorfismo

$$\begin{array}{rccc} \varphi\colon & K & \longrightarrow & E \\ & a & \longmapsto & a + I, \end{array}$$

es un monomorfismo de cuerpos. En efecto, $\varphi(a) = 0$ quiere decir que $a \in I$, es decir, que $p(x)$ divide a $a$. Como $\delta(p) \geq 1$ y $a \in K$, tenemos que $a = 0$.

Ahora, veamos que existe $\alpha \in E$ tal que $p(\alpha) = 0$ (o dicho de otra forma, que $p^{\varphi}(\alpha) = I$). En efecto, sea $\alpha = x + I \in E$. Entonces $p^{\varphi}(\alpha) = \sum_i^n \varphi(a_i)\alpha^i = \sum_i^n (a_i + I)(x + I)^i = \sum_i^n (a_i + I)(x^i + I) = \sum_i^n a_i x^i + I = p(x) + I = I$, es decir, $p(\alpha) = 0$. Como $p$ divide a $f$, $f(\alpha) = 0$.

□

**Corolario 4.10.1.** *Sea $K$ un cuerpo y sea $f \in K[x]$, con $\delta(f) > 0$. Entonces existe una extensión $E$ de $K$ tal que $f$ tiene todas sus raíces en $E$.*

*Demostración:* Por el resultado anterior existen una extensión $K_1$ de $K$ y $\alpha_1 \in K_1$ tal que $f(\alpha_1) = 0$. Luego $f(x) = (x - \alpha_1)f_1(x)$ en $K_1[x]$. Si aplicamos nuevamente el resultado anterior a $f_1(x)$ obtendremos una extensión $K_2$ de $K_1$ y $\alpha_2 \in K_2$ tal que $f_1(\alpha_2) = 0$ (es decir, $f(\alpha_2) = 0$). Si continuamos haciendo esto obtendremos

$$f(x) = e(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

Donde $\alpha_i \in K_i$, $e \in K$, con los $K_i$ las sucesivas extensiones, que cumplen:

$$K \subseteq K_1 \subseteq \dots \subseteq K_{n-1} \subseteq K_n.$$

□

Veremos más adelante que este tipo de descomposiciones serán de gran importancia, y cuando ocurra diremos que $E$ es un *cuerpo de escisión de $f$ sobre $K$*.

**Corolario 4.10.2.** *Si $K$ es un cuerpo, y $\{f_1, f_2, \dots, f_m\} \subseteq K[x]$, con $\delta(f_i) \geq 1 \ \forall$ $i$, entonces existirá una extensión $E$ de $K$ que contiene a todas las raíces de $f_i \ \forall \ i$.*

Ahora, dada una extensión $E/K$ y un elemento $\alpha \in E$, una forma alternativa a 4.6 de ver $K(\alpha)$ es como la intersección de todos los cuerpos intermedios que contengan a ese elemento, es decir

$$K(\alpha) = \bigcap \{L : L \text{ cuerpo} : K \subseteq L \subseteq E, \ \alpha \in L\}.$$

Ahora para ver qué pasa si $|K(\alpha) : K| = \infty$ recordemos que, dado un cuerpo cualquiera $K$, su cuerpo de fracciones $K(x)$ es de la forma:

$$K(x) = \left\{ \frac{f}{g} : f, g \in K[x], g \neq 0 \right\}.$$

**Proposición 4.11.** *Sea $E/K$ una extensión, $\alpha \in E$ trascendente, entonces $|K(\alpha) : K| = \infty$ y $K(\alpha) \cong K(x)$.*

*Demostración:* Consecuencia de que, en este caso al ser $\alpha$ trascendente, la aplicación

$$\begin{array}{rccc} \theta\colon & K(x) & \longrightarrow & K(\alpha) \\ & \dfrac{p(x)}{q(x)} & \longmapsto & \dfrac{p(\alpha)}{q(\alpha)} \end{array}$$

es un isomorfismo de cuerpos y de espacios vectoriales sobre $K$.

□

Sabemos que si $K$ es un cuerpo, entonces también será un dominio de ideales principales ($DIP$), es decir, que cualquier ideal de $K$ estará generado por un sólo elemento, que será mónico.

**Definición 4.12.** *Sea $E/K$ y $\alpha \in K$ algebraico sobre $K$, llamaremos* ***polinomio irreducible de $\alpha$ sobre $K$*** *al único generador mónico del ideal $I = \{f \in K[x] : f(\alpha) = 0\}$. Este polinomio se denotará por $Irr(\alpha, K)$ y su grado se denomina* ***grado de $\alpha$ sobre $K$.***

Es importante observar que $Irr(\alpha, K)$ siempre existe, ya que $K[x]$ es $DIP$. Además, su grado es el menor posible entre los polinomios no nulos de $K[x]$ de los cuales $\alpha$ es raíz. Es decir, $Irr(\alpha, K)$ ***es el polinomio mónico irreducible de menor grado posible de $K[x]$ que tiene a $\alpha$ por raíz.***

Recordemos antes de ver el siguiente resultado que, dado un anillo conmutativo y unitario $A$, un elemento cualquiera $f$ de $A[x]$ es irreducible en $A[x]$ si:

1. $f$ no es invertible en $A[x]$.
2. Si $f = qp$, con $q, p \in A[x]$, entonces $q$ es invertible o $p$ lo es.

**Proposición 4.13.** *Sea $E/K$ una extensión, $\alpha \in K$ algebraico sobre $K$ y $Irr(\alpha, K)$. Entonces:*

1. *$Irr(\alpha, K)$ es irreducible sobre $K$.*
2. *Si $\delta(Irr(\alpha, K)) = n$, entonces $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es base de $K(\alpha)$ sobre $K$. Así, $K(\alpha) = K + \alpha K + \ldots + \alpha^{n-1}K$.*
3. *$|K(\alpha) : K| = n = \delta(Irr(\alpha, K))$.*
4. *Si $q$ es un polinomio mónico irreducible en $K[x]$ y $\alpha$ es raíz de $q$, entonces $q = Irr(\alpha, K)$.*

*Demostración:* Vamos a llamar a $Irr(\alpha, K) = p(x)$ y a definir que $I = \{f \in K[x] : f(\alpha) = 0\} = (p)$.

1. $p(x) \notin K$ pues es no nulo. Además, si $p(x) = h(x)g(x)$ en $K[x]$, se tendría que $0 = p(\alpha) = h(\alpha)g(\alpha)$ y por ejemplo tomemos $h(\alpha) = 0$. Entonces $h \in I$, es decir, que existiría $f \in K[x]$ tal que $pf = h$, por lo que $p = pfg$ en $K[x]$. De esto se deduce que $1 = fg$ y así $g$ es invertible, por tanto $p$ irreducible. Análogo si $g(\alpha) = 0$.
2. Si $\sum_{i=0}^{n-1} c_i\alpha^i = 0$, con $c_i \in K$ y algún $c_i$ es no nulo, entonces $\alpha$ sería raíz de $k(x) = \sum_{i=0}^{n-1} c_i x^i$, es decir, $k \in I$ , lo cual es absurdo, ya que $\delta(k) \leq n-1$. Por lo tanto, $c_i = 0\ \forall i$ y así la familia $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es linealmente independiente (esto tiene sentido con lo que vimos al demostrar que toda extensión finita es algebraica). Veamos ahora que genera $K(\alpha)$. Como

$$K \subseteq T = K + \alpha K + \ldots + \alpha^{n-1}K \subseteq K(\alpha),$$

para ver que $K(\alpha) \subseteq K + \alpha K + \ldots + \alpha^{n-1}K$ bastará con ver que esto último, $T$, es un cuerpo. Lo veremos en dos partes:

Primero, $p(\alpha) = 0$ y si $p(x) = x^n + k_{n-1}x^{n-1} + \ldots + k_0$, entonces $\alpha^n = -k_0 - k_1\alpha - \ldots - k_{n-1}\alpha^{n-1} \in T$. Luego $\alpha^{n+1} \in \alpha T \subseteq \alpha K + \ldots + \alpha^{n-1}K + \alpha^n K \subseteq T + \alpha^n K \subseteq T + TE \subseteq T + T \subseteq T$. En general se tiene así que los $\alpha^i \in T$ $\forall i \geq n$, y como $1, \alpha, \ldots, \alpha^{n-1} \in T$ entonces $\alpha^i \in T$ $\forall i \geq 0$.

Segundo, de lo que acabamos de ver se deduce que $T$ es cerrado para la suma y el producto, y es fácil ver que es anillo unitario. Ahora, si $0 \neq t \in T$, $t = \lambda_0 + \lambda_1\alpha + \ldots + \lambda_{n-1}\alpha^{n-1}$, con $\lambda_i \in K$, veamos que $t$ es invertible en $T$. Si $v(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1}x^{n-1}$, entonces $v(\alpha) = t \neq 0$ y $v(x) \notin I$, es decir, $p$ no divide a $v(x)$. Como $p$ es irreducible, resulta que $p$ y $v(x)$ son coprimos, y por Bézout existirán $q, r \in K[x]$ tales que $1 = rv + qp$. Ahora, $1 = r(\alpha)v(\alpha) + q(\alpha)p(\alpha) = r(\alpha)t$, con $r(\alpha) \in T$, y así $t$ es invertible en $T$.

3. De la segunda parte del apartado anterior se tiene que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es base de $K(\alpha)$ sobre $K$, con $n = \delta(Irr(\alpha K))$, por lo que $|K(\alpha) : K| = n = \delta(Irr(\alpha, K))$.

4. Como $q \in I$, $q = rp$ con $r \in K[x]$. Al ser $q$ irreducible en $K[x]$ se tiene que cumplir que $\delta(q) = \delta(p)$ ó bien $\delta(q) = \delta(r)$. En el primer caso, $r$ es constante y como $q$ y $p$ son ambos mónicos entonces son iguales. En el segundo caso, $p$ sería constante y así reducible, lo cual es absurdo.

□

De lo último además se puede deducir que, dado un $q \in K[x]$ cualquiera, $q(\alpha) = 0$ si y sólo si $Irr(\alpha, K) \mid q$.

Ahora, bajo las mismas condiciones que en el anterior resultado, se va a tener que $K(\alpha) = \{f(\alpha) : f \in K[x]\}$. En efecto, si consideramos una aplicación

$$\begin{array}{rccc} \varphi\colon & K[x] & \longrightarrow & E \\ & f & \longmapsto & f(\alpha). \end{array}$$

Como $Ker\,\varphi = (p)$ (el pol. irreducible) y $p$ es irreducible, $K[x]/Ker\,(\varphi)$ es un cuerpo. Por el *Primer Teorema de Isomorfía de anillos*, $\varphi(K[x])$ también será un cuerpo, y $\varphi(K[x]) = \{f(\alpha) : f \in K[x]\}$. Como $\{f(\alpha) : f \in K[x]\} \subseteq K(\alpha)$, entonces $K(\alpha) = \{f(\alpha) : f \in K[x]\}$.

**Corolario 4.13.1.** *Sea $E/K$ una extensión y $\alpha \in E$, entonces $\alpha$ es algebraico sobre $K$ si y sólo si $|K(\alpha) : K|$ es finito.*

**Corolario 4.13.2.** *Sea $E/K$ una extensión, $\alpha \in E$ y $|E : K| = m$, entonces el grado de $\alpha$ sobre $K$ divide a $m$.*

Visto ya cómo conseguir una base de una extensión, y que para ello necesitaremos encontrar un polinomio irreducible sobre un cuerpo, importante remarcar el hecho de que sea irreducible, para comprobarlo disponemos de algunos criterios como el visto anteriormente, el criterio de Eisenstein. Ahora unos ejemplos:

**Ejemplo 4.13.1.** *Veamos algunos casos de polinomios irreducibles:*

1. *Si consideramos la extensión $\mathbb{Q}(i)/\mathbb{Q}$, entonces $x^2+1 \in \mathbb{Q}[x]$ es irreducible, mónico y tiene a $i$ por raíz, luego es el polinomio irreducible de $i$ sobre $\mathbb{Q}$. Por la proposición anterior $\{1, i\}$ es una base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$, así*

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

2. $x^2 - 2 = Irr(\sqrt{2}, \mathbb{Q})$, $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$ *y* $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
3. $x^2 - 3 = Irr(\sqrt{3}, \mathbb{Q})$, $|\mathbb{Q}(\sqrt{3}) : \mathbb{Q}| = 2$ *y* $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.
4. *El polinomio irreducible de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$ tiene que tener a $\sqrt{3}$ por raíz, sabemos que $x^2 - 3$ lo tiene y podemos intentar ver si es irreducible sobre $\mathbb{Q}(\sqrt{2})[x]$ (lo es en $\mathbb{Q}[x]$ pero eso no nos asegura nada).*

   *Si fuera reducible tendría que tener alguna raíz en $\mathbb{Q}(\sqrt{2})$, luego $\pm\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ y así $\sqrt{3} = a + b\sqrt{2}$, con $a, b \in \mathbb{Q}$, es decir, que $\sqrt{3} - b\sqrt{2} = a \in \mathbb{Q}$. Si elevamos al cuadrado:*

$$3 + 2b^2 - 2b\sqrt{6} = a^2 \in \mathbb{Q},$$

   *de lo que deducimos que $b\sqrt{6} \in \mathbb{Q}$, ya que $\mathbb{Q}$ es un cuerpo. Pero como $\sqrt{6} \notin \mathbb{Q}$ sólo puede ser $b = 0$, y así $\sqrt{3} = a \in \mathbb{Q}$, lo cual es absurdo. Por lo tanto, $x^2 - 3$ es irreducible en $\mathbb{Q}(\sqrt{2})[x]$, y así $Irr(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$, luego $|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})| = 2$. Notar que así:*

$$|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2 \cdot 2 = 4.$$

■

**Ejemplo 4.13.2.** *Analizaremos ahora otra extensión que veremos que guarda relación con el ejemplo anterior, la extensión $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$. Y es que se tiene que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, esto es así ya que $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ es evidente y para ver el otro contenido simplemente basta comprobar que $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Para ver esto último tengamos en cuenta que*

$$11\sqrt{2} + 9\sqrt{3} = (\sqrt{2} + \sqrt{3})^3 \in \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$

*de lo que deducimos que*

$$\sqrt{2} = \frac{(11\sqrt{2} + 9\sqrt{3} - 9(\sqrt{2} + \sqrt{3}))}{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$\sqrt{3} = \frac{-(11\sqrt{2} + 9\sqrt{3}) + 11(\sqrt{2} + \sqrt{3})}{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

*Así, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ y por tanto tenemos la igualdad: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.*

*Una consecuencia de esto es que:*

$$|\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2 \cdot 2 = 4.$$

■

**Ejemplo 4.13.3.** *Sea* $\alpha = \sqrt{5} + \sqrt{-5}$ *y* $\beta = \sqrt[4]{5}$. *Vamos a calcular el grado de la extensión* $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$.

*Notar primero que* $\beta^2 = \sqrt{5}$ *y que* $\alpha = \sqrt{5} + \sqrt{5}i$, *es decir,* $\alpha = \beta^2 + \beta^2 i$. *Así,* $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta^2 + \beta^2 i, \beta) = \mathbb{Q}(\beta^2 i, \beta) = \mathbb{Q}(i, \beta) = \mathbb{Q}(\beta)(i)$.

*Ahora, al estar claramente* $\mathbb{Q}(\beta) \subseteq \mathbb{R}$ *pero* $i \notin \mathbb{R}$, *el polinomio irreducible de* $i$ *sobre* $\mathbb{Q}(\beta)$ *va a ser el mismo que sobre* $\mathbb{Q}$, *es decir,* $x^2+1$. *Así, va a ser* $|\mathbb{Q}(i, \beta) : \mathbb{Q}(\beta)| = 2$.

*Por otro lado, es claro que* $|\mathbb{Q}(\beta) : \mathbb{Q}| = 4$ *ya que el polinomio irreducible de* $\beta = \sqrt[4]{5}$ *sobre* $\mathbb{Q}$ *es* $x^4 - 5$. *(por el criterio de Eisenstein). Así,*

$$|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| = |\mathbb{Q}(i, \beta) : \mathbb{Q}| = |\mathbb{Q}(i, \beta) : \mathbb{Q}(\beta)||\mathbb{Q}(\beta) : \mathbb{Q}| = 2 \cdot 4 = 8.$$

■

**Proposición 4.14.** *Dada* $E/K$ *una extensión, y* $L$ *un cuerpo intermedio. Sea* $a \in E$ *algebraico sobre* $K$. *Entonces* $a$ *también será algebraico sobre* $L$ *y*

$$Irr(a, L) \mid Irr(a, K).$$

*Demostración:* Si $a \in E$ es algebraico sobre $K$ entonces existe un $f \in K[x]$ tal que $f(a) = 0$. Como $f$ también pertenecerá a $L[x]$, $a$ también será algebraico sobre $L$. Recordemos que el polinomio irreducible de un elemento es el de menor grado (mónico) que lo anula y cualquier otro que lo anule es múltiplo suyo. Como $Irr(a, K) \in L[x]$ y anula a $a$ entonces $Irr(a, L) \mid Irr(a, K)$.

□

**Proposición 4.15.** *Dada una extensión* $E/K$ *de cuerpos, y* $u, v \in E$ *elementos algebraicos sobre* $K$. *Sea* $m = \delta(Irr(u, K))$ *y* $n = \delta(Irr(v, K))$, *entonces son equivalentes:*

1. $|K(u, v) : K(v)| = m$.
2. $|K(u, v) : K(u)| = n$.

*Además, ambas se cumplen si* $mcd(m, n) = 1$.

*Demostración:* Está claro que $|K(u) : K| = m$ y que $|K(v) : K| = n$, luego

$$\frac{|K(u, v) : K(u)|}{|K(u, v) : K(v)|} = \frac{|K(u, v) : K|/|K(u) : K)|}{|K(u, v) : K|/|K(v) : K|} = \frac{|K(v) : K|}{|K(u) : K|} = \frac{n}{m}.$$

De lo que se desprende la equivalencia entre 1. y 2. Ahora, si $mcd(m, n) = 1$, la fracción $\dfrac{n}{m}$ no se puede simplificar, luego existirá un entero positivo $a$ tal que

$$|K(u, v) : K(u)| = an, \;\; |K(u, v) : K(v)| = am.$$

Ahora,

$$n \leq an = |K(u,v) : K(u)| = \delta(Irr(v, K(u))) \leq \delta(Irr(v, K)) = n,$$

donde la última desigualdad se desprende de lo visto en el anterior resultado, como $K \subseteq K(u)$ el polinomio $Irr(v, K)$ es múltiplo de $Irr(v, K(u))$. Así, $an = n$ y $a = 1$. Luego:

$$|K(u,v) : K(u)| = n, \;\; |K(u,v) : K(v)| = m.$$

□

Hay que tener en cuenta que el resultado dice que si se cumple una se cumple la otra, pero en general no tiene por qué ocurrir ninguna. Ocurrirá cuando $m, n$ sean coprimos.

Vamos a ver un caso donde podamos aplicar esto que acabamos de ver:

**Ejemplo 4.15.1.** *Sea $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $\alpha = \sqrt[5]{2}$. Vamos a calcular $Irr(\alpha, E)$.*

*Para empezar, si tomamos $x^5 - 2$, por el criterio de Eisenstein, es irreducible en $\mathbb{Q}[x]$. Así, $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 5$. Ahora, ya hemos visto en ejemplos anteriores que si $v = \sqrt{2} + \sqrt{3}$ entonces $E = \mathbb{Q}(v)$, y que $|\mathbb{Q}(v) : \mathbb{Q}| = 4$. Como $mcd(4, 5) = 1$ entonces podemos aplicar el resultado que acabamos de ver:*

$$|E(\alpha) : E| = |\mathbb{Q}(\alpha, v) : \mathbb{Q}(v)| = \delta(Irr(\alpha, \mathbb{Q})) = 5.$$

*Así, al ser $x^5 - 2$ un polinomio de grado 5 en $E[x]$ que tiene por raíz a $\alpha$, entonces*

$$Irr(\alpha, E) = x^5 - 2.$$

■

**Definición 4.16.** *Sea una extensión $E/K$, llamaremos **clausura algebraica** de $K$ en $E$ al conjunto de los elementos algebraicos de una extensión, y la denotaremos por $Cl_K^E = \{\alpha \in E : \alpha$ es algebraico sobre $K\}$.*

**Proposición 4.17.** *Sea $E/K$ una extensión, entonces la clausura algebraica de $K$ en $E$ es un subcuerpo de $E$.*

*Demostración:* Si $\alpha, \beta \in Cl_K^E$, entonces $|K(\alpha, \beta) : K(\beta)|$ es finito pues $\alpha$ es algebraico sobre $K$ y por lo tanto sobre $K(\beta)$. Además, como $\beta$ es algebraico sobre $K$, $|K(\beta) : K|$ es finito. Así, $|K(\alpha, \beta) : K|$ es finito y por 4.13.1 $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta \in Cl_K^E$, también $1/\alpha \in Cl_K^E$ si $\alpha \neq 0$.

□

**Proposición 4.18.** *Sea $E/K$ una extensión, y $K$ numerable, entonces $Cl_K^E$ es numerable.*

*Demostración:* Como $K[x]$ es numerable, contiene numerables polinomios y cada uno de ellos tiene un número finito de raíces en cualquier extensión de $K$, y por lo tanto en $E$. Así, $Cl_K^E$ es numerable.

□

**Corolario 4.18.1.** $\mathbb{R}$ *contiene más elementos trascendentes que algebraicos sobre* $\mathbb{Q}$.

*Demostración:* $Cl_{\mathbb{Q}}^{\mathbb{R}}$ (todos los $\alpha \in \mathbb{R}$ algebraicos sobre $\mathbb{Q}$) es numerable, pero $\mathbb{R}$ es no numerable. Si el conjunto $T$ de los $\beta \in \mathbb{R}$ trascendentes sobre $\mathbb{Q}$ fuese también numerable, entonces $\mathbb{R} = Cl_{\mathbb{Q}}^{\mathbb{R}} \cup T$ sería numerable.

□

**Proposición 4.19.** *Sea* $E/K$ *una extensión. Si* $\alpha_1, \ldots, \alpha_n \in E$ *son algebraicos sobre* $K$, $K(\alpha_1, \ldots, \alpha_n)/K$ *es finita, luego algebraica.*

*Demostración:* La haremos por inducción sobre $n$. Si $n = 1$, ya sabemos que $|K(\alpha_1) : K|$ es finito. Supongamos el resultado cierto para $n-1$ y probémoslo para $n$. Como $\alpha_n$ es algebraico sobre $K$, también es algebraico sobre $K(\alpha_1, \ldots, \alpha_{n-1})$. Así, $|K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})|$ es finito. Por inducción, $|K(\alpha_1, \ldots, \alpha_{n-1}) : K|$ es finito. Pero $K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\alpha_1, \ldots, \alpha_n)$. Por 4.2

$$|K(\alpha_1, \ldots, \alpha_n) : K| = |K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})||K(\alpha_1, \ldots, \alpha_{n-1}) : K|$$

es finito.

□

Un resultado que puede parecer obvio pero que es interesante es la "transitividad" de las extensiones algebraicas, es decir,

**Proposición 4.20.** *Si* $E$ *es una extensión algebraica de* $K$ *y* $F$ *es una extensión algebraica de* $E$, *entonces* $F$ *es una extensión algebraica de* $K$.

*Demostración:* Si $\alpha \in F$ existirá en $E[x]$ un elemento no nulo $f = \sum_{i=0}^{n} a_i x^i$ tal que $f(\alpha) = 0$. Por hipótesis $a_i$ es algebraico sobre $K$, $\forall\ i$. Si $L = K(a_0, a_1, \ldots, a_n)$ se tiene

$$|L : K| = |L : K(a_0, a_1, \ldots, a_{n-1})||K(a_0, a_1, \ldots, a_{n-1}) : K(a_0, a_1, \ldots, a_{n-2})| \ldots |K(a_0 : K|.$$

Como $a_i$ es algebraico sobre $K(a_0, a_1, \ldots, a_{i-1})$ $\forall i$, cada factor es finito y por lo tanto $|L : K|$ es finito. Además, $\alpha$ es algebraico sobre $L$, pues $f \in L[x]$ y $f(\alpha) = 0$, por lo que $|L(\alpha) : L|$ es finito y así $|L(\alpha) : K|$ es finito. Luego, $L(\alpha)$ es una extensión algebraica de $K$ y $\alpha$ es algebraico sobre $K$.

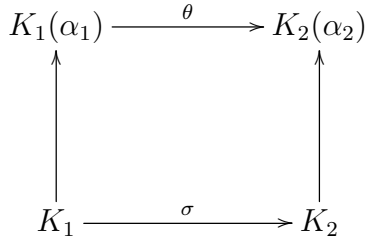
□

**Lema 4.20.1.** *Sea* $\sigma\colon K_1 \longrightarrow K_2$ *un isomorfismo de cuerpos. Entonces* $\sigma$ *se extiende a un isomorfismo de* $K_1[x]$ *en* $K_2[x]$ *haciendo que, si* $f \in K_1[x]$ *con* $f = a_0 + a_1 x + \ldots + a_k x^k$, *entonces* $\sigma(f) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_k)x^k$. *En particular,*

$$f \text{ es irreducible} \Longleftrightarrow \sigma(f) \text{ es irreducible.}$$

Esta extensión se produce de manera natural siempre, por lo que muchas veces se obviará. Además hay que puntualizar una cuestión de notación, tal y como comentamos al principio (tras 4.4) en este caso a $\sigma(f)$ se le denotará en ocasiones $f^\sigma$, ya que estrictamente hablando $\sigma$ es un isomorfismo de cuerpos y $f \in K_1[x]$.

**Proposición 4.21.** *Sean $E_1/K_1$ y $E_2/K_2$ dos extensiones. Sean $\sigma\colon K_1 \longrightarrow K_2$ un isomorfismo. Sea $p_1 \in K_1[x]$ irreducible. Sea $p_2 = \sigma(p_1)$. Sea $\alpha_i$ raíz de $p_i$, $i = 1, 2$. Entonces $\sigma$ se extiende a un isomorfismo de cuerpos $\theta\colon K_1(\alpha_1) \longrightarrow K_2(\alpha_2)$ tal que $\theta(\alpha_1) = \alpha_2$.*




*Demostración:* Supongamos que $p_1$ es mónico, con lo que $p_2$ también lo es. Entonces, como $p_1$ y $p_2$ son irreducibles,

$$p_1 = Irr(\alpha_1, K_1),$$

$$p_2 = Irr(\alpha_2, K_2).$$

Ahora, $K_1(\alpha_1) = \{f(\alpha_1) : f \in K_1[x]\}$, $K_2(\alpha_2) = \{f(\alpha_2) : f \in K_2[x]\}$. Definimos

$$\begin{array}{rccc} \theta\colon & K_1(\alpha_1) & \longrightarrow & K_2(\alpha_2) \\ & f(\alpha_1) & \longmapsto & \sigma(f)(\alpha_2). \end{array}$$

Y ahora veamos que está bien definida: si $f, g \in K_1[x]$, $f(\alpha_1) = g(\alpha_1) \Leftrightarrow (f - g)(\alpha_1) = 0 \Leftrightarrow p_1 \mid f - g \Leftrightarrow \sigma(p_1) \mid \sigma(f - g) \Leftrightarrow p_2 \mid \sigma(f) - \sigma(g) \Leftrightarrow (\sigma(f) - \sigma(g))(\alpha_2) = 0 \Leftrightarrow \sigma(f)(\alpha_2) = \sigma(g)(\alpha_2)$.

Es inyectiva: $\theta(f(\alpha_1)) = \sigma(f)(\alpha_2) = 0 \Rightarrow f(\alpha_1) = 0$. Es fácil ver que también es suprayectiva.

Y es claro que $\theta$ es homomorfismo de cuerpos:

$$\theta(f(\alpha_1) + g(\alpha_1)) = \theta((f + g)(\alpha_1)) = \sigma(f + g)(\alpha_2) = (\sigma(f) + \sigma(g))(\alpha_2) = \sigma(f)(\alpha_2) + \sigma(g)(\alpha_2) = \theta(f(\alpha_1)) + \theta(g(\alpha_1)).$$

Igual con el producto.

□

**Corolario 4.21.1.** *Sea $p \in K[x]$ irreducible, $\alpha$ y $\beta$ raíces de $p$ en una extensión $E$ de $K$. Existe un isomorfismo $\theta\colon K(\alpha) \longrightarrow K(\beta)$ tal que $\theta|_K = id, \theta(\alpha) = \beta$. Recíprocamente, si $\alpha, \beta \in E$, siendo $E/K$ una extensión, y existe un isomorfismo $\theta\colon K(\alpha) \longrightarrow K(\beta)$ tal que $\theta|_K = id, \theta(\alpha) = \beta$, entonces $Irr(\alpha, K) = Irr(\beta, K)$.*

*Demostración:* La primera parte se deduce del anterior resultado, tomando $K_1 = K_2$ y $\sigma = id$. Sea ahora $Irr(\alpha, K) = x^k + a_{k-1}x^{k-1} + \ldots + a_1x + a_0$. Entonces,

$$\alpha^k + a_{k-1}\alpha^{k-1} + \ldots + a_1\alpha + a_0 = 0.$$

Aplicando $\theta$ tenemos: $\theta(\alpha)^k + a_{k-1}\theta(\alpha)^{k-1} + \ldots + a_1\theta(\alpha) + a_0 = \beta^k + a_{k-1}\beta^{k-1} + \ldots + a_1\beta + a_0 = 0$ (ya que $\theta|_K = id$). Luego, $Irr(\alpha, K) = Irr(\beta, K)$.

□

Recordemos la necesidad de que $p \in K[x]$ sea irreducible. Entonces, dadas $\alpha$ y $\beta$ raíces en una extensión $E$ de $K$,

$$\begin{array}{rccc} \theta\colon & K(\alpha) & \longrightarrow & K(\beta) \\ & \alpha & \longmapsto & \beta \\ & k & \longmapsto & k \end{array}$$

Respecto al resultado anterior tenemos la siguiente definición:

**Definición 4.22.** *Si $E$ es una extensión algebraica de $K$, $\alpha, \beta \in E$, diremos que $\alpha$ y $\beta$ son **conjugados sobre** $K$ si $Irr(\alpha, K) = Irr(\beta, K)$, o equivalentemente si $\alpha$ es raíz de $Irr(\beta, K)$. Lo denotaremos por $\alpha\ conj_K\ \beta$.*

Así, el anterior corolario nos viene a decir que todo eso ocurre si y sólo si $\alpha$ y $\beta$ son conjugados.

**Definición 4.23.** *Sea $E/K$ una extensión. Diremos que $\varphi\colon E \longrightarrow E$ es un **$K$-homomorfismo de cuerpos** si*

1. *$\varphi$ es un homomorfismo de cuerpos.*
2. *$\varphi|_K = id_K$, es decir, $\varphi(k) = k\ \forall k \in K$.*

Un simple ejemplo de esto podría ser, dada la extensión $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$

$$\begin{array}{rccc} \varphi\colon & \mathbb{Q}(\sqrt{5}) & \longrightarrow & \mathbb{Q}(\sqrt{5}) \\ & a + b\sqrt{5} & \longmapsto & a - b\sqrt{5} \end{array}$$

es un $\mathbb{Q}$-homomorfismo de cuerpos.

**Ejemplo 4.23.1.** *Vamos a describir ahora el subcuerpo $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ de $\mathbb{C}$.*

*Lo primero, notar que $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5})(\sqrt{7})$, luego $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{5})(\sqrt{7}) \subseteq \mathbb{C}$.*

*Calculemos primero $|\mathbb{Q}(\sqrt{5}) : \mathbb{Q}|$. $\sqrt{5}$ es algebraico sobre $\mathbb{Q}$ porque es raíz de $x^2 - 5$, $x^2 - 5$ es irreducible en $\mathbb{Q}[x]$ y es mónico, luego $Irr(\sqrt{5}, \mathbb{Q}) = x^2 - 5$ y así $|\mathbb{Q}(\sqrt{5}) : \mathbb{Q}| = 2$ y $\{1, \sqrt{5}\}$ es una base de $\mathbb{Q}(\sqrt{5})$.*

*Calculemos ahora $|\mathbb{Q}(\sqrt{5})(\sqrt{7}) : \mathbb{Q}(\sqrt{5})|$, para lo cual necesitaremos $Irr(\sqrt{7}, \mathbb{Q}(\sqrt{5}))$. Sabemos que $x^2 - 7 = Irr(\sqrt{7}, \mathbb{Q})$ y que $x^2 - 7 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt{5})[x]$. Las únicas raíces del polinomio son $\sqrt{7}$ y $-\sqrt{7}$. Si dichas raíces no pertenecen a $\mathbb{Q}(\sqrt{5})$ entonces $x^2 - 7$ será también irreducible sobre $\mathbb{Q}(\sqrt{5})[x]$.*

*Ahora, recordemos que $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$. Si $\sqrt{7} \in \mathbb{Q}(\sqrt{5})$ entonces existen $a, b \in \mathbb{Q}$ tales que $\sqrt{7} = a + b\sqrt{5}$, es decir, $7 = a^2 + 2ab\sqrt{5} + 5b^2$. Con esto tenemos que:*

1. *Si $a = 0$, entonces $7 = 5b^2$ y de aquí $b = \pm\dfrac{\sqrt{7}}{5} \notin \mathbb{Q}$. Absurdo*

2. *Si* $b = 0$, *entonces* $7 = a^2$ *y de aquí* $a = \pm\sqrt{7} \notin \mathbb{Q}$. *Absurdo.*

3. *Si* $a, b \neq 0$, *entonces* $\sqrt{5} = \dfrac{7 - a^2 - 5b^2}{2ab}$, *pero esto último es racional, luego absurdo también.*

*Luego, como las raíces no pertenecen a* $\mathbb{Q}(\sqrt{5})$, *tenemos que* $Irr(\sqrt{7}, \mathbb{Q}(\sqrt{5})) = x^2 - 7$, *por lo que* $|\mathbb{Q}(\sqrt{5})(\sqrt{7}) : \mathbb{Q}(\sqrt{5})| = 2$. *Así* $|\mathbb{Q}(\sqrt{5})(\sqrt{7}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{5})(\sqrt{7}) : \mathbb{Q}(\sqrt{5})||\mathbb{Q}(\sqrt{5}) : \mathbb{Q}| = 2 \cdot 2 = 4$. *Por tanto, podemos ver a* $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ *como un* $\mathbb{Q}$*-e.v de dimensión* 4. *Calcularemos ahora una base:*

$$\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \{c + d\sqrt{7} : c, d \in \mathbb{Q}(\sqrt{5})\} = \{(a_0 + b_0\sqrt{5}) + (a_1 + b_1\sqrt{5})\sqrt{7} : a_0, b_0, a_1, b_1 \in \mathbb{Q}\} = \{a_0 + a_1\sqrt{7} + b_0\sqrt{5} + b_1\sqrt{5}\sqrt{7} : a_0, b_0, a_1, b_1 \in \mathbb{Q}\}.$$

*De lo que deducimos que, por ejemplo,* $\{1, \sqrt{5}, \sqrt{7}, \sqrt{5}\sqrt{7}\}$ *es una base de* $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.

■

**Ejemplo 4.23.2.** *Sea* $a \in \mathbb{C}$ *raíz de* $x^3 + x + 1$. *Veamos que* $\mathbb{Q}(a\sqrt{2}) = \mathbb{Q}(a, \sqrt{2})$. *Lo veremos por doble inclusión:*

*Primero veamos que* $\mathbb{Q}(a\sqrt{2}) \subseteq \mathbb{Q}(a, \sqrt{2})$. *Como* $a$ *y* $\sqrt{2} \in \mathbb{Q}(a, \sqrt{2})$ *y* $\mathbb{Q}(a, \sqrt{2})$ *es un cuerpo entonces* $a\sqrt{2} \in \mathbb{Q}(a, \sqrt{2})$ *y como* $\mathbb{Q}(a\sqrt{2})$ *es el menor subcuerpo de* $\mathbb{Q}$ *conteniendo al mismo* $\mathbb{Q}$ *y a* $a\sqrt{2}$, *concluimos que*

$$\mathbb{Q}(a\sqrt{2}) \subseteq \mathbb{Q}(a, \sqrt{2}).$$

*Ahora veamos que* $\mathbb{Q}(a, \sqrt{2}) \subseteq \mathbb{Q}(a\sqrt{2})$. *Para esto basta ver que* $a \in \mathbb{Q}(a\sqrt{2})$ *(y así* $\sqrt{2}$ *ya que* $\sqrt{2} = a^{-1}(a\sqrt{2})$*) ya que como* $\mathbb{Q}(a, \sqrt{2})$ *es el menor cuerpo conteniendo a ambos elementos se tendrá que*

$$\mathbb{Q}(a, \sqrt{2}) \subseteq \mathbb{Q}(a\sqrt{2}).$$

*Como* $x^3 + x + 1$ *es irreducible en* $\mathbb{Q}[x]$ *entonces se tiene que* $Irr(a, \mathbb{Q}) = x^3 + x + 1$ *y* $|\mathbb{Q}(a) : \mathbb{Q}| = 3$. *Así,* $\mathbb{Q}(a) = \{d + ba + ca^2 : b, c, d \in \mathbb{Q}\}$. *Luego ó* $\mathbb{Q}(a^2) = \mathbb{Q}(a)$ *ó* $\mathbb{Q}(a^2) = \mathbb{Q}$. *Pero esto último no puede ser ya que si* $\mathbb{Q}(a^2) = \mathbb{Q}$ *entonces* $a^2 \in \mathbb{Q}$ *y así* $a^2 = t \in \mathbb{Q}$ *y* $x^2 - t$ *tiene como raíz* $a$. *Absurdo porque* $x^3 + x + 1$ *es su polinomio irreducible. Con esto, tenemos que* $a^2 = \dfrac{(a\sqrt{2})^2}{2} \in \mathbb{Q}(a\sqrt{2})$ *y así* $\mathbb{Q}(a) = \mathbb{Q}(a^2) \subseteq \mathbb{Q}(a\sqrt{2})$.

$$\mathbb{Q}(a, \sqrt{2}) \subseteq \mathbb{Q}(a\sqrt{2}) \subseteq \mathbb{Q}(a, \sqrt{2}) \Rightarrow \mathbb{Q}(a\sqrt{2}) = \mathbb{Q}(a, \sqrt{2}).$$

■

## 4.2. Clausura Algebraica

Como ya vimos en 4.10.2, dado un cuerpo $K$ y un subconjunto $M$ finito de polinomios no constantes de $K[x]$, entonces existe una extensión $E$ de $K$ que contienen a todas las raíces de todos los elementos de $M$. Ahora veremos que esto es cierto aunque $M$ no sea finito.

**Definición 4.24.** *Diremos que un cuerpo $K$ es* ***algebraicamente cerrado*** *si contiene a todas las raíces de los polinomios no constantes de $K[x]$.*

**Proposición 4.25.** *Si $K$ es un cuerpo algebraicamente cerrado y $E$ es un extensión algebraica de $K$, entonces $E = K$.*

*Demostración:* Si $\alpha \in E$, $f(x) = Irr(\alpha, K)$ es un polinomio no constante de $K[x]$. En consecuencia $\alpha$ es raíz de $f$, con $f \in K[X]$. Como $K$ es algebraicamente cerrado, $\alpha \in K$.

□

Anteriormente ya definimos lo que era la clausura algebraica a partir de los elementos algebraicos de una extensión, pero ahora adaptaremos el concepto usando los cuerpos algebraicamente cerrados.

**Definición 4.26.** *Sea $E/K$ una extensión de cuerpos, se dice que $E$ es una* ***clausura algebraica*** *de $K$ si*

1. *$E$ es algebraico sobre $K$.*
2. *$E$ es algebraicamente cerrado.*

Ahora, se presentará el resultado más importante de esta sección:

**Teorema 4.27.** *Todo cuerpo admite una clausura algebraica.*

*Demostración:* La idea de la demostración va a consistir en que para cada $f \in K[x]$ con $\delta(f) \geq 1$, y $x_f$ una indeterminada formaremos un conjunto infinito $S = \{x_f : f \in K[x],\ \delta(f) \geq 1\}$. Entonces, sea $K[S]$ el anillo de polinomios en las indeterminadas $x_f$ de $S$, y sea $I$ el ideal de $K[S]$ generado por el conjunto $\{f(x_f) : f \in K[x]\}$. Construiremos cuerpos $E_i$ con $K \subseteq E_1 \subseteq E_2 \subseteq \ldots$ tales que todo $g \in E_i[x]$ con $\delta(g) \geq 1$ tenga raíces en $E_{i+1}$, y luego formaremos $E = \cup_{i=1}^{\infty} E_i$ que resultará un cuerpo algebraicamente cerrado con $K \subseteq E$. Finalmente, si $L = Cl_K^E$ demostraremos que $L$ es una clausura algebraica de $K$ y se habrá probado el teorema.

Comenzaremos entonces construyendo los $E_i$. El ideal $I$ está propiamente contenido en $K[S]$, ya que si $I = K[S]$ se tiene

$$(*)\ \ 1 = g_1 f_1(x_{f_1}) + \ldots + g_k f_k(x_{f_k}),\ \ g_i \in K[S].$$

Por 4.10.2 existe una extensión $E$ de $K$ en la cual $f_1, \ldots, f_k$ tienen todas sus raíces. Sea $\alpha_i \in E$ una raíz de $f_i$, $i = 1, \ldots, k$. Haciendo en $(*)$ $x_{f_i} = \alpha_i$ para $1 \leq i \leq k$, y $x_t = 0\ \forall t \neq f_i$, se obtiene $1 = 0$, que es una contradicción. Luego $I \subset K[S]$ y por lo tanto existe un ideal maximal $M$ de $K[S]$ tal que $I \subseteq M$. Sea $\varphi = \pi|_K$, siendo $\pi$ la proyección canónica de $K[S]$ en $K[S]/M$. Entonces, $\varphi\colon K \longrightarrow K[S]/M$ es un monomorfismo, pues si $k \in K$ y $\varphi(k) = M$, entonces $k \in M$ por lo que $k$ debe ser no invertible, es decir, $k = 0$. Veamos ahora que $\forall f \in K[x]$ con $\delta(f) \geq 1$, $f$ tiene raíces en $E_1 = K[S]/M$. Efectivamente, si $a_0 + a_1 x + \ldots + a_n x^n = f(x) \in K[x]$, entonces $f(x_f) = a_0 + a_1 x_f + \ldots + a_n x_f^n \in M$ y se tiene que

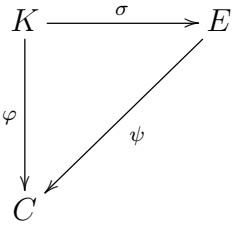
$$M = \pi(f(x_f)) = f(x_f) + M = (a_0 + M) + (a_1 x_f + M) + \ldots + (a_n x_f^n) + M) = \varphi(a_0)(1 + M) + \varphi(a_1)(x_f + M) + \ldots + \varphi(a_n)(x_f + M)^n.$$

Si ahora $\bar{1} = 1 + M$ y $\bar{x}_f = x_f + M$, obtenemos que $\bar{x}_f \in E_1$ y es raíz del polinomio $h(x) = \sum_{i=0}^{n} \varphi(a_i)x^i$. Si repetimos el razonamiento anterior tomando $E_1$ en lugar de $K$, tendremos que $E_2 \supseteq E_1 \supseteq K$ tal que todo $g \in E_1[x]$ con $\delta(g) \geq 1$ tiene raíces en $E_2$. Continuando con este proceso se obtiene $K \subseteq E_1 \subseteq E_2 \subseteq E_3 \ldots$, tales que todo $g \in E_i[x]$ con $\delta(g) \geq 1$ tiene raíces en $E_{i+1}$, Evidentemente, $E = \cup_i E_i$ es un cuerpo que contiene a $K$. Veamos que $E$ es algebraicamente cerrado: en efecto, si $p(t) = \sum_{i=0}^{n} e_i t^i \in E(t)$, entonces $p(t) \in E_m(t)$ para algún $m$ y por lo tanto tiene raíces en $E_{m+1}$. Por lo tanto, $p$ tiene una raíz $\alpha$ en $E$, y así $p(t) = (t - \alpha)h(t)$, con $h(t) \in E[t]$. Si aplicamos este razonamiento con $h(t)$ y los sucesivos polinomios que vayan saliendo obtendremos que $p(t)$ tiene todas sus raíces en $E$.

Probaremos ahora que $L = Cl_K^E$ es una clausura algebraica de $K$. Obviamente $L$ es algebraico sobre $K$. Para ver que es algebraicamente cerrado tomaremos $f \in L[x]$ con $\delta(f) \geq 1$. Entonces $f \in E[x]$, y como $E$ es algebraicamente cerrado existirá un $\alpha \in E$ con $f(\alpha) = 0$. Entonces $L(\alpha)$ es una extensión finita de $L$, luego algebraica sobre $L$. Como además $L$ es algebraico sobre $K$, y así también extension algebraica, tenemos que también $L(\alpha)$ es una extensión algebraica de $K$, luego $\alpha$ es algebraico sobre $K$. Entonces $\alpha \in Cl_K^E = L$. Hemos probado así que todo polinomio no constante de $L[x]$ tiene alguna raíz en $L$, es decir, que $L$ es algebraicamente cerrado.

□

**Proposición 4.28.** *Sea $C/K$ una extensión algebraica. Si $C$ es una clausura algebraica de $K$, entonces dada cualquier extensión algebraica $E$ de $K$, existirá un monomorfismo $\psi\colon E \longrightarrow C$ tal que $\psi\sigma = \varphi$, es decir, el siguiente diagrama es conmutativo*




*Demostración:* Sea $\sigma\colon K \longrightarrow E$ una extensión algebraica y consideremos el conjunto

$$S = \{(F, F', \psi) : \sigma(K) \subseteq F \subseteq E,\ \ \varphi(K) \subseteq K' \subseteq C,\ \ \psi\colon F \longrightarrow F' \text{ isomorfismo }, \psi\sigma = \varphi\}.$$

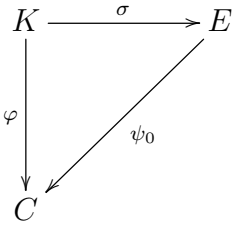
Notar que $S \neq \emptyset$, ya que $(\sigma(K), \varphi(K), \varphi\sigma^{-1}) \in S$. Definiremos en $S$ un orden parcial de la siguiente manera:

$$(F, F', \psi) \leq (L, L', \phi) \Longleftrightarrow F \subseteq L,\ \phi|_F = \psi.$$

Visto esto, es claro que se puede aplicar el lema de Zorn para obtener un elemento maximal de $S$, $(F_0, F_0', \psi_0)$. Veamos que $F_0 = E$. Es evidente que $F_0 \subseteq E$, así que solo tendremos que ver el contenido contrario $E \subseteq F_0$. Supongamos que existe $\alpha \in E \setminus F_0$ y sean $f_1 = Irr(\alpha, F_0) \in F_0[x]$ y $f_2 = f_1^{\psi_0} \in F_0'[x] \subseteq C[x]$.

Como $C$ es algebraicamente cerrado, existirá un $\alpha' \in C$ tal que $f_2(\alpha') = 0$ y, por 4.21, existirá un único isomorfismo de cuerpos $\psi_1\colon F_0(\alpha) \longrightarrow F_0'(\alpha')$ tal que $\psi_1(\alpha) = \alpha'$

y $\psi_1|_{F_0} = \psi_0$, es decir, que extiende $\psi_0$. Además, $\psi_0\sigma = \varphi$ y $\sigma(K) \subseteq F_0$, por lo que $\forall u \in K$, $\sigma(u) \in F_0$ y $\psi_1\sigma(u) = \psi_0\sigma(u) = \varphi(u)$, es decir, $\psi_1\sigma = \varphi$. Entonces $(F_0(\alpha), F_0'(\alpha'), \psi_1) \in S$, lo cual contradice la maximalidad de $(F_0, F_0', \psi_0)$. Por lo tanto, $F_0 = E$ y $(E, F_0', \psi_0) \in S$, y como $\psi_0 \colon E \longrightarrow F_0' \subseteq C$, se tiene que el siguiente diagrama es conmutativo:




□

## 4.3. Cuerpo de escisión de un polinomio

De lo que se trata de ver en esta sección es la existencia y unicidad (salvo isomorfismo como siempre) de los cuerpos de escisión. Pero primero vamos a definir lo que son:

**Definición 4.29.** *Sea $f \in K[x]$ un polinomio y $E/K$ una extensión. Diremos que $f$* ***se escinde*** *en $E$ si existen $a_1, \ldots, a_n \in E$ tales que $f = a(x - a_1) \ldots (x - a_n)$, con $a \in K$. Si además $E = K(a_1, \ldots, a_n)$ decimos que $E$ es un* ***cuerpo de escisión de $f$ sobre*** *$K$.*

Una definición más general (la anterior sólo sirve para casos finitos) sería: *diremos que un cuerpo $E$ es un* ***cuerpo de escisión*** *de un $f$ sobre un cuerpo $K$ si $f$ se puede descomponer como producto factores lineales en $E$.*

**Observación 4.29.1.** *Algunas observaciones:*

1. *Todo polinomio de grado* 1 *de $K[x]$ se escinde en $K$.*
2. *$f \in K[x]$ se escinde en $K$ si, y sólo si todos los polinomios irreducibles que aparecen en su descomposición son de grado* 1.
3. *Si $f \in K[x]$ se escinde en $K$ y $g \mid f$, entonces $g$ también se escinde en $K$.*

Pasemos ahora a probar la existencia:

**Teorema 4.30** (***Existencia de cuerpos de escisión***)**.** *Si $f \in K[x]$, existe un cuerpo de escisión de $f$ sobre $K$.*

*Demostración:* Lo haremos por inducción sobre el grado de $f$: Si $f$ se escinde en $K$ (en particular, si $\delta(f) = 1$), entonces $K$ es un cuerpo de escisión de $f$ sobre $K$. Supongamos que no es así y sea $f_1$ un factor irreducible de $f$ de grado mayor que 1. Por 3.50, existe una extensión $E$ de $K$ en la que $f_1$ tiene una raíz $a$. Entonces $f(a) = 0$ ya que $f_1(a) = 0$. Por 3.51 $x - a \mid f$ y así $f = (x - a)g$, con $g \in K(a)[x]$. Como $\delta(g) < \delta(f)$, por la hipótesis de inducción tenemos que existe un cuerpo de escisión de $g$ sobre $K(a)$. Será $g = b(x - b_1) \ldots (x - b_m)$ y el cuerpo de escisión de $g$ (sobe $K(a)$) será $K(a)(b_1, \ldots, b_m) = K(a, b_1, \ldots, b_m)$. Ahora, $f = b(x - a)(x - b_1) \ldots (x - b_m)$ y su cuerpo de escisión sobre $K$ es $K(a, b_1, \ldots, b_m)$.

□

**Ejemplo 4.30.1.** *Hallar un cuerpo de escisión de* $f(x) = x^4 - 5x^2 + 5 \in \mathbb{Q}[x]$ *sobre* $\mathbb{Q}$.

*Sabemos que* $f(x)$ *es irreducible por Eisenstein, sus raíces son:*

$$x = \pm\sqrt{\frac{5 \pm \sqrt{25-20}}{2}}, \quad \alpha = \sqrt{\frac{5+\sqrt{5}}{2}},\ \beta = \sqrt{\frac{5-\sqrt{5}}{2}},\ , -\alpha, -\beta.$$

*Es inmediato ver que* $\alpha\beta = \sqrt{5}$. *Notar que tanto* $\alpha$ *como* $\beta$ *son reales. El cuerpo de escisión será* $\mathbb{Q}(\alpha, \beta, -\alpha, -\beta) = \mathbb{Q}(\alpha, \beta)$.

*Ahora,* $\alpha^2 = \dfrac{5+\sqrt{5}}{2}$, *luego* $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{5})$ *ó* $\sqrt{5} \in \mathbb{Q}(\alpha)$. *Así,* $\beta = \alpha/\sqrt{5} \in \mathbb{Q}(\alpha)$, *luego* $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ *y así el cuerpo de escisión es* $\mathbb{Q}(\alpha)$. *Y* $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \delta(f) = 4$, *ya que* $f = Irr(\alpha, \mathbb{Q})$.

■

De este ejemplo podemos ver que en estos casos, en los polinomios bicuadrados de la forma $x^4 + ax^2 + b$, las raíces van a ser de la forma:

$$\alpha = \sqrt{\frac{-a+\sqrt{a^2-4b}}{2}},\ \beta = \sqrt{\frac{-a-\sqrt{a^2-4b}}{2}},\ -\alpha,\ , -\beta,$$

y van a cumplir que $\alpha\beta = \sqrt{b}$. Luego, el cuerpo de escisión de estos polinomios será de la forma $\mathbb{Q}(\alpha, \beta)$.

**Ejemplo 4.30.2.** *Hallar el cuerpo de escisión de* $f(x) = x^4 + 3x^2 - 3 \in \mathbb{Q}[x]$ *sobre* $\mathbb{Q}$.

$$\alpha = \sqrt{\frac{-3+\sqrt{21}}{2}},\ \beta = \sqrt{\frac{-3-\sqrt{21}}{2}},\ \alpha\beta = \sqrt{-3},\ \mathbb{Q}(\alpha^2) = \mathbb{Q}(21).$$

*Notar que* $\beta \notin \mathbb{Q}(\alpha)$ *ya que* $\beta \notin \mathbb{R}$ *pero* $\alpha \in \mathbb{R}$. *Así, el cuerpo de escisión de* $f(x)$ *sobre* $\mathbb{Q}$ *es* $\mathbb{Q}(\alpha, \beta)$. *Se tiene que* $\beta^2 \in \mathbb{Q}(\sqrt{21}) = \mathbb{Q}(\alpha^2)$, *luego* $\beta^2 = t \in \mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$ *y así* $Irr(\beta, \mathbb{Q}(\alpha)) = x^2 - t$, *luego* $|\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\beta)| = 2$, *y*

$$|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| = |\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)||\mathbb{Q}(\alpha) : \mathbb{Q}| = 8.$$

■

**Proposición 4.31.** *Sea* $\sigma\colon K_1 \longrightarrow K_2$ *un isomorfismo,* $f_1 \in K_1[x]$ *y* $f_2 = \sigma(f_1) \in K_2[x]$. *Sean* $E_i$, *con* $i = 1, 2$ *cuerpos de escisión de* $f_i$ *sobre* $K_i$, $i = 1, 2$. *Entonces existe un isomorfismo* $\tau\colon E_1 \longrightarrow E_2$ *que extiende* $\sigma$, *es decir,* $\tau|_{K_1} = \sigma$.

*Demostración:* Inducción sobre $|E_1 : K_1|$ :

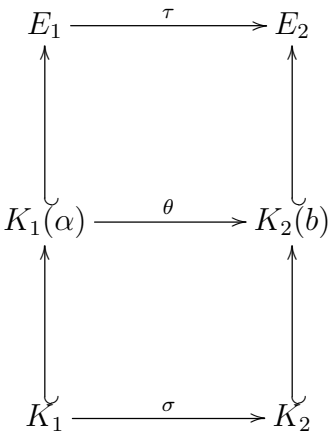
Si $|E_1 : K_1| = 1$, entonces $E_1 = K_1$ es cuerpo de escisión de $f_1$ sobre $K_1$. Como $\sigma\colon K_1[x] \longrightarrow K_2[x]$ es isomorfismo de anillos, también $\sigma(f_1)$ $(= f_2)$ se escindirá sobre $K_2$. Así $E_2 = K_2$ y basta tomar $\tau = \sigma$.

Supongamos que $|E_1 : K_1| > 1$ y que el resultado es cierto para extensiones de menor grado. Como $|E_1 : K_1| > 1$, $f_1$ no se escinde en $K_1$ y existe un factor irreducible (importante esto!) $p$ de $f_1$ tal que $\delta(p) > 1$. Como $f_1$ se escinde en $E_1$, también $p$ se escinde en $E_1$ y $\sigma(p)$ se escinde en $E_2$. Sea $a \in E_1$, raíz de $p$ y sea $b \in E_2$ raíz de $\sigma(p)$. Por existe un isomorfismo $\theta\colon K_1(a) \longrightarrow K_2(b)$ que extiende $\sigma$, es decir $\theta|_{K_1} = \sigma$.

Ahora, $E_1$ es cuerpo de escisión de $f_1$ sobre $K_1(a)$. Y $E_2$ es cuerpo de escisión de $f_2$ $(= \sigma(f_1))$ sobre $K_2(b)$. Además,

$$|E_1 : K_1| = |E_1 : K_1(a)||K_1(a) : K_1| > |E_1 : K_1(a)|, \text{ ya que } a \notin K_1 \ .$$

Por inducción, existe $\tau\colon E_1 \longrightarrow E_2$ isomorfismo que extiende $\theta$, luego también extiende $\sigma$.




□

**Corolario 4.31.1** (***Unicidad de los cuerpos de escisión***)**.** *Si $E_1, E_2$ son cuerpos de escisión de un mismo polinomio $f$ de $K[x]$ sobre $K$, existe entonces $\tau\colon E_1 \longrightarrow E_2$ isomorfismo tal que $\tau|_K = id$.*

*Demostración:* Basta hacer $K_1 = K_2 = K$ y $\sigma = id$ en la proposición anterior.

□

## 4.4. Extensiones normales

**Definición 4.32.** *Una extensión de cuerpos $E/K$ es una **extensión normal** si existe $f \in K[x]$ tal que $E$ sea cuerpo de escisión de $f$ sobre $K$.*

**Observación 4.32.1.** *Un par de observaciones:*

1. *Si $E/K$ es normal, $E/K$ es finita. Esto es así ya que $E$ lo vamos a obtener adjuntando a $K$ un número finito de elementos algebraicos y aplicar 4.19.*
2. *Si $E/K$ es normal y $K \subseteq L \subseteq E$, $E/L$ también es normal. En este caso, ya que $E$ es cuerpo de escisión de un $f \in K[x]$ sobre $K$, también es cuerpo de escisión de $f \in L[x]$ sobre $L$.*

**Proposición 4.33.** *Toda extensión de grado 2 es normal.*

*Demostración:* $E/K$ es algebraica ya que es finita. Sea ahora $f \in K[x]$ irreducible con una raíz $\alpha$ en $E$. Veamos que $f$ se escinde en $E$. $\alpha$ es algebraico sobre $K$ y $|K(\alpha) : K| = \delta(Irr(\alpha, K)) = \delta(f)$. Como $K \subseteq K(\alpha) \subseteq E$, entonces $|K(\alpha) : K| \leq |E : K| = 2$. Luego $\delta(f) = 1$ ó 2.

Si $\delta(f) = 1$ entonces $f$ se escinde en $K$. Si $\delta(f) = 2$, como sabemos que $x - \alpha$ divide a $f$ en $E[x]$ existe un $g \in E[x]$ tal que $f = (x - \alpha)g$, y como $\delta(f) = 2$ entonces $\delta(g) = 1$ y $f$ se escinde en $E$.

□

**Proposición 4.34.** *Sea $E/K$ una extensión normal y $K \subseteq M_1, M_2 \subseteq E$ cuerpos intermedios. Sea $\sigma\colon M_1 \longrightarrow M_2$ un isomorfismo tal que $\sigma|_K = id$. Entonce existe un isomorfismo $\tau\colon E \longrightarrow E$ que extiende $\sigma$.*

*Demostración:* Por definición de extensión normal, $E$ es cuerpo de escisión de un $f \in K[x]$ sobre $K$. Como hemos observado, $E$ también es cuerpo de escisión de $f$ sobre $M_i$, con $i = 1, 2$. Además, $\sigma(f) = f$ ya que $\sigma|_K = id$. Aplicamos ahora 4.31 y tenemos $\tau\colon E \longrightarrow E$ tal que $\tau$ extiende $\sigma$.

□

**Proposición 4.35.** *Sea $E/K$ una extensión normal, $p \in K[x]$ irreducible, $a, b \in E$ raíces de $p$ en $E$. Entonces existe $\tau\colon E \longrightarrow E$ isomorfismo tal que $\tau(a) = b$ y $\tau|_K = id$.*

*Demostración:* Por 4.21.1, existe $\theta\colon K(a) \longrightarrow K(b)$ isomorfismo tal que $\theta(a) = b$ y $\theta|_K = id$. Por la proposición anterior existe $\tau\colon E \longrightarrow E$ que extiende $\theta$. Entonces $\tau(a) = \theta(a) = b$ y $\tau|_K = id$.

□

**Ejemplo 4.35.1.** *Veamos el cuerpo de escisión de $x^3 - 2 \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$.*

**Proposición 4.36.** *Sea $E/K$ una extensión finita. Entonces $E/K$ es normal si y sólo si todo polinomio irreducible de $K[x]$ que tenga una raíz en $E$ se escinde en $E$.*

*Demostración:* Como $E/K$ finita entonces $\{a_1, \ldots, a_n$ es una base de $E$ como $K - e.v$. Entonces $E = K(a_1, \ldots, a_n)$. Sea ahora $p_i = Irr(a_i, K)$, con $i = 1, \ldots, n$. Entonces, por hipótesis, $p_i$ se escinde en $E$, $i = 1, \ldots, n$. Sea $f = p_1 \ldots p_n$. Claramente $E$ es un cuerpo de escisión de $f$ sobre $K$ ($E = K(a_1, \ldots, a_n) = K(Ker f)$, ya que los $a_1, \ldots, a_n$ anulan a $f$). Así que $E/K$ es normal.

Recíprocamente, como $E/K$ es normal, $E$ es cuerpo de escisión de un polinomio $f \in K[x]$ sobre $K$. Sea $p \in K[x]$ irreducible con una raíz $a$ en $E$. Sea $b$ otra raíz de $p$ en un cuerpo de escisión de $p$ ($p \in K[x]$ luego también está en $E[x]$) sobre $E$. Tenemos que ver que $b \in E$. Para ello, por 4.21.1 existe un isomorfismo $\theta\colon K(a) \longrightarrow K(b)$ tal que $\theta|_K = id$. Ahora, $E$ es un cuerpo de escisión de $f$ sobre $K(a)$ (lo era sobre $K$). También $E(b)$ es cuerpo de escisión de $f$ sobre $K(b)$. Además, como $f \in K[x]$ y $\theta$ fija $K$, tenemos que $\theta(f) = f$. Por 4.31, existe un isomorfismo $\tau\colon E \longrightarrow E(b)$ que

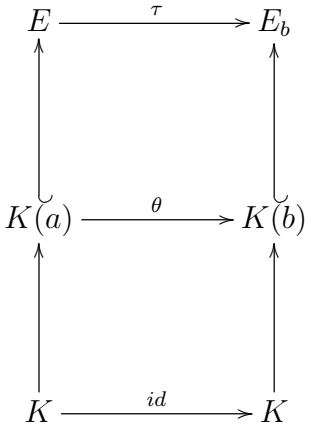
extiende $\theta$. Por 4.3, se tiene que

$$|E : K(a)| = |E(b) : K(b)|.$$

Como $a$ y $b$ son raíces de $p \in K[x]$ irreducible, $|K(a) : K| = |K(b) : K| = \delta(p)$. Así,

$$|E(b) : E||E : K| = |E(b) : K| = |E(b) : K(b)||K(b) : K| = |E : K(a)||K(a) : K| = |E : K|,$$

luego $|E(b) : E| = 1$, es decir, $b \in E$.




□

## 4.5. Extensiones separables

**Definición 4.37.** *Una extensión $E/K$ se dice **separable** si todo $f \in K[x]$ irreducible que tenga una raíz en $E$ no tiene raíces múltiples en $E$. Es decir, todas sus raíces son distintas.*

De igual forma podremos definir:

**Definición 4.38.** *Dado un cuerpo $K$, un polinomio $f \in K[x]$ diremos que es **separable** si el máximo común divisor de $f$ y su derivada $f'$ es* 1.

**Definición 4.39.** *Sea $E/K$ una extensión. Un elemento algebraico $a \in E$ se dice que es **separable** si su polinomio irreducible lo es. Evidentemente si todo $a \in E$ es separable entonces la extensión será separable.*

Por ejemplo, el polinomio $x^2 - 1 \in \mathbb{Q}[x]$ es separable, pero $(x-1)^2 \in \mathbb{Q}[x]$ no.

Toda extensión de cuerpos de característica 0 es separable por 3.52. Recordemos que es así porque entonces $Irr(a, K)$ de un elemento $a \in E$ es irreducible y así el máximo común divisor con su derivada sólo puede ser 1.

**Proposición 4.40.** *Sea $E/K$ una extensión algebraica y separable y $L$ un cuerpo intermedio de la extensión. Entonces $E/L$ y $L/K$ son separables.*

*Demostración:* La extensión $L/K$ es separable ya que $L \subseteq E$ y todo elemento de $E$ es separable sobre $K$.

Sea ahora $\alpha \in E$ y $f \in K[x]$ su polinomio irreducible. Entonces $q = Irr(\alpha, L) \mid f$. Si $q$ no fuera separable, cualquier factor común entre $q$ y su derivada sería también un factor común entre $f$ y su derivada, por lo que $f$ no sería separable.

□

**Definición 4.41.** *Una extensión $E/K$ se dice* ***extensión de Galois*** *si es normal y separable.*

# 5. La correspondencia de Galois

## 5.1. El grupo de Galois

Lo que a continuación vamos a definir será el objeto de estudio del resto del texto, imprescindible para entender lo que venga en adelante y eje vertebrador de la *Teoría de Galois*. Empezaremos definiendo el grupo de Galois.

Recordemos que, dado un cuerpo $E$, denotaremos por $Aut(E)$ al grupo de los automorfismos de $E$, es decir, al grupo de los isomorfismos $\sigma\colon E \longrightarrow E$ con la operación composición de aplicaciones.

**Definición 5.1.** *Sea $E/K$ una extensión de cuerpos. Llamaremos* ***grupo de Galois de*** *$E/K$, y lo denotaremos por $Gal(E/K)$, a*

$$Gal(E/K) = \{\sigma\colon E \longrightarrow E :\ \sigma \text{ es isomorfismo}, \sigma|_K = id_K\}.$$

*Es decir, que $\sigma \in Aut(E)$ y $\sigma(k) = k$, $\forall k \in K$. Además, va a ser un subgrupo de $Aut(E)$ con la composición de aplicaciones:*

$$(\sigma \circ \tau)(e) = \sigma(\tau(e)),\ \ \forall e \in E.$$

**Definición 5.2.** *Si $\sigma \in Aut(E)$, definimos el* ***cuerpo fijo de*** *$\sigma$, escrito $C_E(\sigma)$, como*

$$C_E(\sigma) = \{a \in E : \sigma(a) = a\}.$$

**Observación 5.2.1.** *$C_E(\sigma)$ es un subcuerpo de $E$. Esto es así ya que, dados $a, b \in C_E(\sigma)$, se tiene que $\sigma(a-b) = \sigma(a) - \sigma(b) = a - b$. Luego $a - b \in C_E(\sigma)$. Y si $b \neq 0$ entonces $\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1}$, y $ab^{-1} \in C_E(\sigma)$.*

**Ejemplo 5.2.1.** *El grupo de Galois de $\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q})$, escrito $Gal(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q})$. Sabemos que $x^3 - 2 = Irr(\sqrt[3]{2}, \mathbb{Q})$, y que sus raíces son $\sqrt[3]{2}$, $\sqrt[3]{2}w$, $\sqrt[3]{2}w^2$, con*

$$w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$$

*(recordar la fórmula de las raíces de la unidad).*

*Sea $\sigma \in Gal(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q})$, debe llevar $\sqrt[3]{2}$ a otra raíz de $Irr(\sqrt[3]{2}, \mathbb{Q})$. Sabemos también que $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, sin embargo $\sqrt[3]{2}w$, $\sqrt[3]{2}w^2$ no pertenecen a $\mathbb{R}$. Por lo tanto, $\sigma(\sqrt[3]{2}) =$*

$\sqrt[3]{2}$ *y* $\sigma(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2) = a+b\sqrt[3]{2}+c\sqrt[3]{2}^2$, *ya que ha de fijar* $\mathbb{Q}$ *(como el irreducible es de grado* 3 *entonces una base de la extensión es esa). Así,* $\sigma = id$ *y* $Gal(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q}) = 1$.

■

**Proposición 5.3.** *Sea* $E_1/K_1$ *una extensión de cuerpos y* $\sigma\colon E_1 \longrightarrow E_2$ *isomorfismo. Si* $K_2 = \sigma(K_1)$*, se cumple que* $Gal(E_1/K_1)$ *y* $Gal(E_2/K_2)$ *son isomorfos.*

**Definición 5.4.** *Dado un* $f \in K[x]$ *definimos el* ***grupo de Galois de*** $f$ *como* $Gal(E/K)$*, siendo* $E$ *un cuerpo de escisión de* $f$ *sobre* $K$.

*Notar que si* $E_1, E_2$ *son cuerpos de escisión de* $f$ *sobre* $K$*, sabemos que por 4.31.1 existe* $\tau\colon E_1 \longrightarrow E_2$ *isomorfismo tal que* $\tau|_K = id$*. Por 5.3,* $Gal(E_1/K)$ *es isomorfo a* $Gal(E_2/K)$*. Luego el concepto de grupo de Galois de* $f$ *está bien definido.*

**Proposición 5.5.** *Sea* $E = K(a_1, \ldots, a_n)$*. Sean* $\sigma, \tau \in Gal(E/K)$ *tal que* $\sigma(a_i) = \tau(a_i)$*,* $i = 1, \ldots, n$*. Entonces* $\sigma = \tau$.

*Demostración:* Por hipótesis, $\sigma(a_i) = \tau(a_i)$, con $i = 1, \ldots, n$. Es decir, que $(\sigma \circ \tau^{-1})(a_i) = a_i$, con $i = 1, \ldots, 0$. Entonces $a_i \in C_E(\sigma\tau^{-1})$. Además, $K$ es subcuerpo de $C_E(\sigma\tau^{-1})$. Como a su vez $C_E(\sigma\tau^{-1})$ es subcuerpo de $E$ y $K(a_1, \ldots, a_n)$ es el menor subcuerpo de $E$ que contiene a $K$ y a $a_1, \ldots, a_n$ entonces $E = K(a_1, \ldots, a_n) \in C_E(\sigma\tau^{-1})$. Asi, $\sigma = \tau$.

□

Básicamente esto quiere decir que un elemento de $Gal(E/K)$ queda unívocamente determinado por las imágenes de los $a_i$.

**Proposición 5.6.** *Sea* $f \in K[x]$ *y sea* $a$ *una raíz de* $f$ *en una extensión* $E$ *de* $K$*. Si* $\sigma \in Gal(E/K)$*, también* $\sigma(a)$ *es raíz de* $f$*. Sea* $\Omega = \{$*raíces de* $f$ *en* $E\}$*. La aplicación*

$$\begin{array}{rccc} \varphi\colon & Gal(E/K) & \longrightarrow & S_\Omega \\ & \sigma & \longmapsto & \sigma|_\Omega \end{array}$$

*es una acción de* $Gal(E/K)$ *sobre* $\Omega$*. Si* $E$ *es cuerpo de escisión de* $f$ *sobre* $K$*, dicha acción es fiel, es decir, cumple que* $Ker\,\varphi = 1$*. Si además* $f$ *es irreducible, dicha acción es transitiva, es decir, tiene sólo una órbita.*

*Demostración:* Veamos que $\sigma(a)$ es también una raíz de $f$. Sea $f = a_0 + a_1x + \ldots + a_kx^k$, entonces $a_0 + a_1a + \ldots + a_ka^k = 0$, y de aquí $\sigma(a_0 + a_1a + \ldots + a_ka^k) = \sigma(0) = 0$. Pero $\sigma(a_0 + a_1a + \ldots + a_ka^k) = \sigma(a_0) + \sigma(a_1)\sigma(a) + \ldots + \sigma(a_k)\sigma(a)^k = 0$. Como $\sigma|_K = id$ tenemos que $a_0 + a_1\sigma(a) + \ldots + a_k\sigma(a)^k = 0$, es decir, que $\sigma(a)$ es raíz de $f$.

Ahora, supongamos que $E$ es un cuerpo de escisión de $f$ sobre $K$. Luego $E = K(a_1, \ldots, a_n)$ siendo $\Omega = \{a_1, \ldots, a_n\}$. Si $\sigma \in Ker\,\varphi$, $\sigma$ fijará $a_1, \ldots, a_n$. Por el resultado anterior 5.5 $\sigma = id$. Supongamos que además $f$ es irreducible. Por 4.35, dados $a, b \in \Omega$, existe $\sigma\colon E \longrightarrow E$ isomorfismo, $\sigma|_K = id$ y $\sigma(a) = b$. Entonces $\sigma \in Gal(E/K)$ y $a, b$ están en la misma órbita, luego hay sólo 1 órbita y la acción es transitiva.

□

**Proposición 5.7.** *Sea $E/K$ una extensión, $a_1, \ldots, a_n \in E$. Sea $L$ un cuerpo cualquiera y $\sigma\colon E \longrightarrow L$ un isomorfismo. Entonces tenemos que $\sigma(K(a_1, \ldots, a_n)) = \sigma(K)(\sigma(a_1), \ldots, \sigma(a_n))$.*

*Demostración:* $\sigma(K(a_1, \ldots, a_n))$ es un cuerpo y contiene a $\sigma(K)$ y a $\sigma(a_1), \ldots, \sigma(a_n)$. Como $\sigma(K)(\sigma(a_1), \ldots, \sigma(a_n))$ es el menor subcuerpo de $L$ que contiene a $\sigma(K)$ y a $\sigma(a_1), \ldots, \sigma(a_n)$, será

$$\sigma(K)(\sigma(a_1), \ldots, \sigma(a_n)) \subseteq \sigma(K(a_1, \ldots, a_n)).$$

$\sigma^{-1}(\sigma(K)(\sigma(a_1), \ldots, \sigma(a_n)))$ es un cuerpo y contiene a $K, a_1, \ldots, a_n$. Por el mismo argumento tenemos que

$$\sigma^{-1}(\sigma(K)(\sigma(a_1), \ldots, \sigma(a_n))) \supseteq K(a_1, \ldots, a_n).$$

Aplicando $\sigma$ :

$$\sigma(K)(\sigma(a_1), \ldots, \sigma(a_n)) \supseteq \sigma(K(a_1, \ldots, a_n)).$$

□

**Proposición 5.8.** *Sean $K \subseteq L \subseteq E$.*

1. *$Gal(E/L) \leq Gal(E/K)$.*
2. *Si $L/K$ es normal, entonces $\sigma(L) = L\ \forall \sigma \in Gal(E/K)$.*
3. *Supongamos que $E/K$ es normal. Entonces $L/K$ es normal si y sólo si $\sigma(L) = L\ \forall \sigma \in Gal(E/K)$. Si $L/K$ es normal, $Gal(E/L) \trianglelefteq Gal(E/K)$ y*

$$Gal(L/K) \cong \frac{Gal(E/K)}{Gal(E/L)}.$$

*Demostración:*

1. Si $\sigma$ fija a $L$ también fija a $K$, ya que $K \subseteq L$.
2. Si $L/K$ es normal, $L = K(a_1, \ldots, a_n)$, siendo $\Omega = \{a_1, \ldots, a_n\}$ el conjunto de raíces de un $f \in K[x]$. Vimos en 5.6 que si $\sigma \in Gal(E/K)$, $\sigma$ permuta las raíces de $f$ y $\sigma(\Omega) = \Omega$. Por 5.7

   $$\sigma(K(a_1, \ldots, a_n)) = \sigma(K)(\sigma(a_1), \ldots, \sigma(a_n)).$$

   Como $\{\sigma(a_1), \ldots, \sigma(a_n)\} = \{a_1, \ldots, a_n\}$ entonces $\sigma(L) = L$.
3. Veamos que si $\sigma(L) = L\ \forall \sigma \in Gal(E/K)$ se tiene que $L/K$ es normal. Por 4.36 bastará ver que si $p \in K[x]$ es irreducible y tiene una raíz $a \in L$, entonces $p$ se escinde en $L$. Como $E/K$ es normal, de nuevo por 4.36, todas las raíces de $p$ están en $E$. Sea $b \in E$ otra raíz de $p$. Por 4.35 existe $\sigma \in Gal(E/K)$ tal que $\sigma(a) = b$. Como, por hipótesis, $\sigma(L) = L$, tenemos que $b \in L$. Así, $L/K$ es normal.

Ahora, consideremos la aplicación (suponiendo que $L/K$ es normal)

$$\begin{array}{ccc} Gal(E/K) & \longrightarrow & Gal(L/K) \\ \sigma & \longmapsto & \sigma|_L \end{array}$$

Por 2. $\sigma(L) = L$, luego $\sigma|_L : L \longrightarrow L$ y la aplicación está bien definida. Es evidentemente homomorfismo. Si $\tau\colon L \longrightarrow L$ es un isomorfismo tal que $\tau|_K = id$, por 4.34 y por ser $E/K$ normal, existe $\sigma\colon E \longrightarrow E$ isomorfismo con $\sigma|_K = id$. Así, $\sigma \in Gal(E/K)$ y $\sigma|_L = \tau$. Así, la aplicación es suprayectiva. Su núcleo es $Gal(E/L)$. Así $Gal(E/L) \trianglelefteq Gal(E/K)$. Luego, por el *Primer Teorema de Isomorfía*

$$Gal(L/K) \cong \frac{Gal(E/K)}{Gal(E/L)}.$$

□

**Definición 5.9.** *Sea $E$ un cuerpo y $H \leq Aut(E)$. Definimos el cuerpo fijo de $H$ como*

$$C_E(H) = \bigcap_{\sigma \in H} C_E(\sigma).$$

*Que es un subcuerpo de $E$, por serlo cada $C_E(\sigma)$ ($C_E(\sigma) = \{a \in E : \sigma(a) = a\}$).*

**Definición 5.10.** *Una extensión $E/K$ se dice* ***extensión de Galois*** *si es normal y separable.*

**Proposición 5.11.** *Sea $K \subseteq L \subseteq E$. Si $E/K$ es de Galois, $E/L$ es de Galois.*

*Demostración:* Recordar que una extensión se dice de Galois si es normal y separable. Por lo tanto, partiremos de que $E/K$ es normal y separable. Veamos que $E/L$ también lo es.

Recordar también que una extensión $E/K$ es normal si existe un $f \in K[x]$ tal que $E$ es cuerpo de escisión de $f$ sobre $K$. Pero si $E/K$ es normal entonces $E$ es un cuerpo de escisión también de un $f \in L[x]$ sobre $L$ (si lo es de $f \in K[x]$, también $f$ estará en $L$).

Para ver que es separable (todo $f \in K[x]$ irreducible que tenga una raíz en $E$ no tiene raíces múltiples en $E$) sea $p \in L[x]$ irreducible con una raíz $a \in E$. Podemos suponer que $p$ es mónico y así $p = Irr(a, L)$. Entonces, por 4.14

$$Irr(a, L) \mid Irr(a, K).$$

Como $E/K$ es separable, $Irr(a, K)$ no tiene raíces múltiples en $E$, y así $Irr(a, L)$ tampoco. Luego $E/L$ es separable y de Galois.

□

**Proposición 5.12.** *Sea $E/K$ una extensión de Galois. Entonces*

$$|E : K| = |Gal(E/K)|.$$

*Demostración:* Lo haremos por inducción sobre $|E : K|$. Si $|E : K| = 1$, $E = K$ y $Gal(E/K) = 1$ y ya está.

Supongamos que $|E : K| > 1$. Sea $a \in E \setminus K$ y $p = Irr(a, K)$. Entonces $\delta(p) > 1$. Como $E/K$ es normal, por 4.36 tenemos que todas las raíces de $p$ están en $E$. Como $E/K$ es separable, todas las raíces son distintas entre sí.

Sea $\Omega = \{\text{raíces de p en E}\}$. Entonces $|\Omega| = \delta(p)$. Por 5.6 $Gal(E/K)$ actúa sobre $\Omega$. Por 4.35, dadas dos raíces de $p$ en $E$ existe $\sigma \in Gal(E/K)$ que lleva una a la otra. Esto significa que hay sólo una órbita en esta acción, es decir, que la acción es transitiva. El estabilizador de $a$ en esta acción

$$\begin{array}{ccc} Gal(E/K) & \longrightarrow & S_\Omega \\ \sigma & \longmapsto & \sigma|_\Omega \end{array}$$

es $Gal(E/K(a))$ puesto que $\sigma(a) = a$ si y sólo si $\sigma(x) = x \quad \forall x \in K(a)$. Entonces $|\Omega| = |Gal(E/K)|/|Gal(E/K(a))|$. Pero $|\Omega| = \delta(p) = |K(a) : K|$. $|Gal(E/K)| = |Gal(E/K(a))||\Omega| = |Gal(E/K(a))||K(a) : K|$. Por 5.11, $E/K(a)$ es de Galois. Por inducción, $|E : K(a)| = |Gal(E/K(a))|$.

Sustituyendo:

$$|Gal(E/K)| = |E : K(a)||K(a) : K| = |E : K|.$$

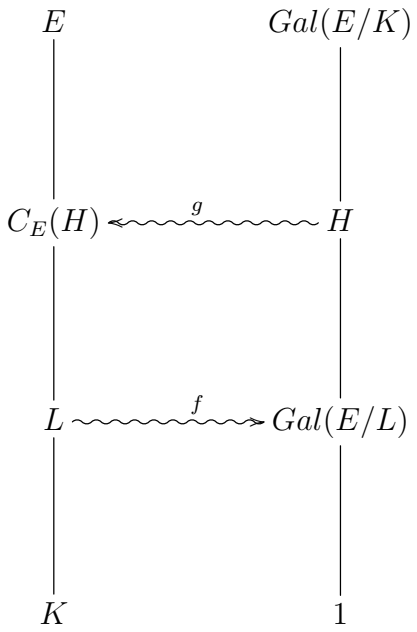
□

**Ejemplo 5.12.1.** *Sea* $E = \mathbb{Q}(\sqrt[4]{2})$. *Entonces* $|E : \mathbb{Q}| = 4$, $|Gal(E/\mathbb{Q})| = 2$. *Si* $\sigma \in Gal(E/\mathbb{Q})$, $\sigma(\sqrt[4]{2})$ *será raíz de* $x^4 - 2$, $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$, $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$, *pero también están* $\sqrt[4]{2}i \notin \mathbb{Q}(\sqrt[4]{2})$ *y* $-\sqrt[4]{2}i \notin \mathbb{Q}(\sqrt[4]{2})$.

■

## 5.2. El Teorema Fundamental de la Teoría de Galois

Vamos a partir de una extensión $E/K$, con sus respectivos cuerpos intermedios $L$ tales que $K \subseteq L \subseteq E$, y su grupo de Galois $Gal(E(K)$, con sus respectivos subgrupos $H$. Entonces, si $E/k$ es de Galois vamos a poder establecer una biyección entre los subgrupos de $Gal(E/K)$ y los respectivos cuerpos intermedios de la extensión $E/K$. En esto consiste el teorema fundamental de la *Teoría de Galois*.




**Proposición 5.13.** *Sea $E/K$ de Galois. Entonces $C_E(Gal(E/K)) = K$.*

*Demostración:* Podemos suponer que $E \neq K$. Sea $a \in E \setminus K$ y sea $p = Irr(a, K)$. Entonces $\delta(p) > 1$. Como la extensión $E/K$ es normal, por 4.36 $p$ se escinde en $K$. Como $E/K$ es separable, todas las raíces de $p$ son distintas. Sea $a \neq b$ una raíz de $p$. Ahora, por 4.35, existe $\sigma \in Gal(E/K)$ tal que $\sigma(a) = b$. Así, $a \notin C_E(Gal(E/K))$ y $C_E(Gal(E/L)) = K$.

□

**Observación 5.13.1.** *Sea $K \subseteq L \subseteq E$ y $E/K$ de Galois. Entonces $C_E(Gal(E/L)) = L$. Recordemos que $E/L$ también es de Galois.*

**Proposición 5.14.** *Sea $E/K$ extensión de Galois y $H \leq Gal(E/K)$. Entonces $Gal(E/C_E(H)) = H$.*

*Demostración:* Claramente $H \leq Gal(E/C_E(H))$. Por 5.11, $E/C_E(H)$ es de Galois. Por 5.12, $|Gal(E/C_E(H))| = |E : C_E(H)|$. Así, $|H| \leq |E : C_E(H)|$. Bastará ver que $|E : C_E(H)| \leq |H|$.

Sea $H = \{id = \sigma_1, \sigma_2, \ldots, \sigma_n\}$. Así, $|H| = n$. Sea $F = C_E(H)$. Tenemos que probar que cualesquiera $n+1$ elementos de $E$ son $F$-linealmente dependientes. Sean $a_1, \ldots, a_{n+1} \in E$. Vamos a considerar el sistema de $n$ ecuaciones lineales con $n+1$ incógnitas

$$\sigma_1(a_1)x_1 + \ldots + \sigma_1(a_{n+1})x_{n+1} = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n(a_1)x_1 + \ldots + \sigma_n(a_{n+1})x_{n+1} = 0$$

Como es un sistema homogéneo y hay más incógnitas que ecuaciones existe alguna solución no trivial, es decir, que no todo son 0. Elegimos una solución no trivial

$x_i = t_i$, con $i = 1, \ldots, n+1$ que tenga el menor número posible de $t_i$'s no nulos. Veamos que $t_i \in F$, con $i = 1, \ldots, n+1$. Ahora, como $\sigma_1 = id$ la primera ecuación es $t_1 a_1 + \ldots + t_{n+1} a_{n+1} = 0$ y $\{a_1, \ldots, a_{n+1}\}$ será linealmente dependiente, como queríamos. Reordenando los $a_i$'s podemos suponer que $t_1 \neq 0$ y, dividiendo por él, que $t_1 = 1$. Por reducción al absurdo y reordenando de nuevo puedo suponer que $t_2 \in E \setminus F$. Como $F = C_E(H)$, existe algún $\sigma_i \in H$ tal que $\sigma_i(t_2) \neq t_2$. Como $H$ es un grupo, $\{\sigma_i \sigma_j : 1 \leq j \leq n\} = H$. El sistema de ecuaciones

$$(\sigma_i\sigma_1)(a_1)x_1 + \ldots + (\sigma_i\sigma_1)(a_{n+1})x_{n+1} = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(\sigma_i\sigma_n)(a_1)x_1 + \ldots + (\sigma_i\sigma_n)(a_{n+1})x_{n+1} = 0$$

es el mismo sistema de antes (sólo cambian el orden de las ecuaciones). Entonces $x_j = \sigma_i(t_j)$, con $j = 1, \ldots, n+1$, es solución del sistema:

$$\sigma_1(a_1)t_1 + \ldots + \sigma_1(a_{n+1})t_{n+1} = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n(a_1)t_1 + \ldots + \sigma_n(a_{n+1})t_{n+1} = 0$$

ya que si hacemos

$$\sigma_i(\sigma_1(a_1)t_1 + \ldots + \sigma_1(a_{n+1})t_{n+1}) = \sigma_i(0) = 0$$

con todas las ecuaciones entonces:

$$(\sigma_i\sigma_1)(a_1)\sigma_i(t_1) + \ldots + (\sigma_i\sigma_1)(a_{n+1})\sigma_i(t_{n+1}) = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(\sigma_i\sigma_n)(a_1)\sigma_i(t_1) + \ldots + (\sigma_i\sigma_n)(a_{n+1})\sigma_i(t_{n+1}) = 0.$$

Y como toda combinación lineal de soluciones de un sistema homogéneo es también solución entonces una nueva solución será restarle a la primera la segunda:

$$x_1 = 1 - \sigma_i(1) = 0$$

$$x_2 = t_2 - \sigma_i(t_2) \neq 0$$

$$\ldots\ldots$$

$$x_{n+1} = t_{n+1} - \sigma_i(t_{n+1}).$$

Si un $t_j = 0$ entonces $t_j - \sigma_i(t_j) = 0$. Luego esta nueva solución (la obtenida de restar) tiene como mínimo un 0 más que la original. Absurdo.

□

**Proposición 5.15.** *Sea $K \subseteq L \subseteq E$. Sea $H = Gal(E/L) \leq Gal(E/K)$. Dado un $\tau \in Gal(E/K)$ entonces $H^\tau = Gal(E/\tau(L))$.*

*Demostración:* Sea $\sigma \in Gal(E/K)$. $\sigma \in Gal(E/\tau(L))$ si y sólo si $\sigma(\tau(l)) = \tau(l)$ $\forall l \in L$ si y sólo si $(\tau^{-1}\sigma\tau)(l) = l$ $\forall l \in L$ si y sólo si $\tau^{-1}\sigma\tau \in Gal(E/L) = H$ si y sólo si $\sigma \in \tau H \tau^{-1} = H^\tau$.

□

**Teorema 5.16** (***Teorema fundamental de la teoría de Galois.***). *Sea $E/K$ extensión de Galois y $G = Gal(E/K)$. Consideremos los siguientes conjuntos $\mathcal{G} = \{$subgrupo de $G\}$ y $\mathcal{K} = \{$cuerpos intermedios de $E/K\}$. Entonces:*

1. *Las aplicaciones*

$$\begin{array}{rccc} f\colon & \mathcal{G} & \longrightarrow & \mathcal{K} \\ & H & \longmapsto & C_E(H) \end{array}$$

$$\begin{array}{rccc} g\colon & \mathcal{K} & \longrightarrow & \mathcal{G} \\ & L & \longmapsto & Gal(E/L) \end{array}$$

   *son inversas una de la otra, por lo que ambas son biyectivas. Esto quiere decir que $Gal(E/C_E(H)) = H$, con $H \in \mathcal{G}$ y $L = C_E(Gal(E/L))$, con $L \in \mathcal{K}$.*

2. *Sea $L \in \mathcal{K}$. Entonces $L/K$ es normal si y sólo si $Gal(E/L) \trianglelefteq Gal(E/K)$. En este caso*

$$Gal(L/K) \simeq \frac{Gal(E/K)}{Gal(E/L)}.$$

*Demostración:*

1. Sea $H \in \mathcal{G}$. Vimos en 5.14 que $Gal(E/C_E(H)) = H$ y así $(g \circ f)(H) = H$. Luego $g \circ f = id$. Sea ahora $L \in \mathcal{L}$. Como $E/K$ es de Galois, $E/L$ también lo será por 5.11. Por 5.13, $C_E(Gal(E/L)) = L$, luego $(f \circ g)(L) = L$ y $f \circ g = id$. Por lo que $f = g^{-1}$ y $g = f^{-1}$ y ambas son biyectivas.

2. Sea $H = Gal(E/L)$. Por 5.15, si $\tau \in G$ tenemos que $H^\tau = Gal(E/\tau(L))$. Ahora $H \trianglelefteq G$ si y sólo si $H^\tau = H$ $\forall \tau \in G$ si y sólo si $Gal(E/\tau(L)) = Gal(E/L)$ $\forall \tau \in G$ si y sólo si $g(\tau(L)) = g(L)$ $\forall \tau \in G$ ($g$ es inyectiva) si y sólo si $\tau(L) = L$ $\forall \tau \in G$ si y sólo si $L/K$ es normal.

   Ahora, si suponemos que $L/K$ sea normal, 5.8 (c) nos dice que

$$Gal(L/K) \simeq \frac{Gal(E/K)}{Gal(E/L)}.$$

□

Es decir, el conjunto de los subgrupos de un grupo de Galois y el de los cuerpos intermedios de la extensión de Galois de la parte son biyectivos.

**Corolario 5.16.1.** *Sea $E/K$ una extensión de Galois, $G = Gal(E/K)$ y $H \leq G$. Entonces $|E : C_E(H)| = |H|$. Además, como la aplicación $f$ de antes es suprayectiva, todo cuerpo intermedio de la extensión $E/K$ es de la forma $C_E(H)$ para un cierto $H \leq G$. Es decir, conociendo los subgrupos de $G$ y sus cuerpos fijos conozco todos los cuerpos intermedios de la extensión.*

*Demostración:* Por 5.11, como $E/K$ es de Galois, $E/C_E(H)$ también es de Galois. Además $Gal(E/C_E(H)) = H$ por el *Teorema fundamental*. Ahora, por 5.12, $|E/C_E(H)| = |Gal(E/C_E(H))| = |H|$.

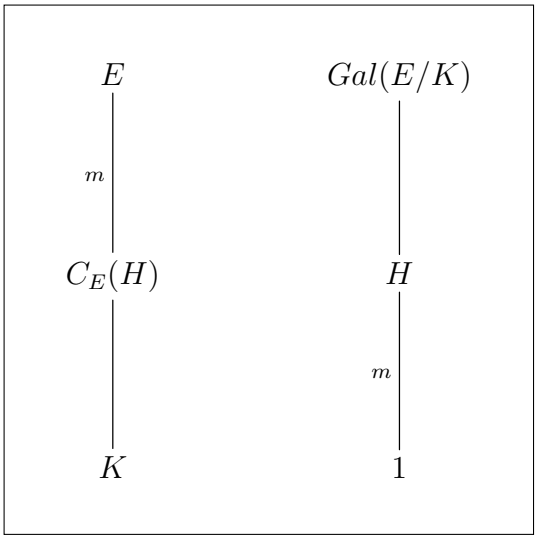
Para la segunda parte,

$$\begin{array}{rccc} f\colon & \mathcal{G} & \longrightarrow & \mathcal{K} \\ & H & \longmapsto & C_E(H) \end{array}$$

y como $f$ es suprayectiva, si $L \in \mathcal{K}$, $L = f(H) = C_E(H)$ para algún $H \in \mathcal{G}$.

□

Este resultado lo podemos esquematizar tal que así:




donde $E/K$ es de Galois.

# 6. Polinomios resolubles por radicales

## 6.1. Extensiones radicales

**Definición 6.1.** *Una extensión $E/K$ se dice **radical** si existen subcuerpos*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = E$$

*tales que $K_{i+1} = K_i(a_i)$ y $a_i^{n_i} \in K_{i+1}$, para algún $a_i$ y $n_i$ con $i = 1, \ldots, n-1$. Dicho de otro modo, diremos que una extensión $E/K$ es **radical** si existen $a_1, \ldots, a_r$ y naturales $n_1, \ldots, n_r$ tales que $E = K(a_1, \ldots, a_r)$, $a_1^{n_1} \in K$ y $a_j^{n_j} \in K(a_1, \ldots, a_{j-1})$ $\forall j \geq 2$.*

*Un polinomio $f \in K[x]$ se dice que es **resoluble por radicales** si existe una extensión radical $E/K$ que contenga un cuerpo de escisión de $f$ sobre $K$.*

Por ejemplo, la extensión $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5+\sqrt{2}})/\mathbb{Q}$ es radical.

**Proposición 6.2.** *Toda extensión radical $E/K$ es finita.*

*Demostración:* Como $a_1^{n_1} = \alpha_1 \in K$, $a_1$ es una raíz de $x^{n_1} - \alpha_1 \in K[x]$ y por ello $K(a_1)/K$ es una extensión de grado finito. En general, tendremos que $a_j$ es algebraico sobre $K(a_1, \ldots, a_{j-1})$, con $j = 2, \ldots, r$, lo cual garantiza que $|K(a_1, \ldots, a_r) : K| = |E : K| < \infty$.

□

De lo que se trata de ver es que, si tenemos un $f \in K[x]$ y $E$ un cuerpo de escisión de $f$ sobre $K$ entonces:

1. $f$ es resoluble por radicales $\Rightarrow Gal(E/K)$, el grupo de Galois de $f$, es resoluble.
2. Si el grupo de Galois de $f$ es resoluble $\Rightarrow$ $f$ es resoluble por radicales.

Y así poder establecer el si y sólo si.

Necesitaremos que $K$ contenga a las $n$ raíces de la unidad, para un cierto $n$. Tal y como se vió en 3.6 las $n-$raíces de la unidad forman un grupo cíclico, por lo que podemos definir:

**Definición 6.3.** *Una* ***n-raíz primitiva de la unidad*** *es un generador del grupo multiplicativo generado por ellas:*

$$\{\textit{raíces de } x^n\text{-}1\} = \{1, \xi, \ldots, \xi^{n-1}\},$$

*con $\xi$ una $n-$raíz primitiva.*

Es claro que si tenemos una $n-$ésima raíz primitiva de la unidad $\xi$ sobre un cuerpo $K$, entonces la extensión $K(\xi)/K$ también será una extensión radical.

**Proposición 6.4.** *Sea $E/K$ una extensión y supongamos que existe una raíz $n$-ésima primitiva de la unidad $\xi$ en $E$. Entonces $K(\xi)/K$ es de Galois y con grupo de Galois abeliano.*

*Demostración.* Las raíces de $x^n - 1$ son $H = \{1, \xi, \ldots, \xi^{n-1}\}$. Entonces $K(\xi)$ es cuerpo de escisión de $x^n - 1$ sobre $K$, luego $K(\xi)/K$ es normal, luego de Galois. Si $\sigma \in Gal(K(\xi)/K)$, entonces, por 5.6, $\sigma(H) \subseteq H$. Como $\sigma$ es biyectiva y $H$ es finito, tendremos $\sigma(H) = H$. Además, $\sigma$ es automorfismo de $H$ como grupo multiplicativo. Si $\sigma|_H = id$, tendremos $\sigma(\xi) = \xi$ y por 5.5, $\sigma = id$. Así, $Gal(K(\xi)/K)$ es un subgrupo del grupo de automorfismos de un grupo cíclico que ya sabemos que es abeliano.

□

**Proposición 6.5.** *Sea $E/K$ una extensión. Supongamos que $E = K(a)$ y que existe un $n$ tal que $a^n \in K$ y que $K$ contiene una raíz $n$-ésima primitiva de la unidad. Entonces $E/K$ es de Galois con grupo de Galois cíclico de orden divisor de $n$.*

*Demostración.* Si $a = 0$, es evidente. Supongamos que $a \neq 0$ y consideremos el polinomio $x^n - a^n$. Sea $\xi \in K$ una raíz $n$-ésima primitiva de la unidad. Las raíces de $x^n - a^n$ son $\xi^i a$, con $i = 0, \ldots, n-1$. Ahora, $E = K(a)$ es cuerpo de escisión de

$x^n - a^n$ sobre $K$, luego $E/K$ es normal, y así de Galois. Si $\sigma \in Gal(E/K)$, por 5.6, $\sigma(a) = \xi^i a$ para algún $i$. Definimos así una aplicación

$$\begin{array}{ccc} Gal(E/K) & \longrightarrow & \langle \xi \rangle \\ \sigma & \longmapsto & \xi^i \end{array}$$

con $\sigma(a) = \xi^i a$. Es homomorfismo de grupos: $\sigma_1(a) = \xi^i a$, $\sigma_2(a) = \xi^j a$. Así

$$(\sigma_1\sigma_2)(a) = \sigma_1(\xi^j a) = \sigma_1(\xi^j)\sigma_1(a) = \xi^j \sigma_1(a) = \xi^{j+i} a,$$

teniendo en cuenta que $\xi^j \in K$. Ahora, si la imagen de $\sigma$ es 1 entonces $\sigma(a) = a$ y así $\sigma = id$ por 5.5, luego es inyectiva. Así, $Gal(E/K)$ es isomorfo a un subgrupo de un grupo cíclico de orden $n$, luego es cíclico de orden divisor de $n$.

□