Algebra II (Doble grado Informática-Matemáticas)

Mayo- 2020

Tema 8: Grupos finitamente presentados. Clasificación de grupos de orden pequeño.

En las notas que vienen a continuación nos ocupamos de estudiar *Presentaciones de grupos* y daremos la clasificación de todos los grupos de orden ≤ 15.

Antes de definir lo que es dar un grupo por generadores y relaciones y entonces dar una presentación de un grupo, veamos algunos ejemplos ya estudiados.

Hemos estado utilizando que el grupo cíclico de orden n se puede declarar de la forma:

$$C_n = \langle a | a^n = 1 \rangle.$$

Es decir C_n está generado por el elemento a con relación fundamental $a^n = 1$. Con estos datos podemos determinar cuáles son exactamente los elementos del grupo y la tabla de grupo. Recordemos que

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\}$$

y

$$a^r a^s = a^{res(rs;n)}$$

Otro ejemplo que hemos trabajado es el del grupo diédrico

$$D_n = \langle r, s | r^n = 1 = s^2, sr = r^{-1}s \rangle.$$

Decimos que D_n está generado por r y s con relaciones

$$r^n = 1 = s^2; sr = r^{-1}s$$

que nos permite concluir que

$$D_n = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$$

y además conocer completamente la tabla del grupo sin necesidad de recurrir a su descripción original.

Ejemplos análogos a los anteriores son el grupo de Klein o el grupo de los cuaternios. Todos ellos son casos de grupos dados por generadores y relaciones

Definición 0.1. *Sea G un grupo generado por $s_1, s_2, \ldots, s_n$. Cualquier ecuación que satisfagan los generadores la llamaremos una relación del grupo G.*

Por ejemplo $r^n = 1$, $s^2 = 1$ y $sr = r^{n-1}s$ son relaciones de D_n. Además estas tres relaciones, que hemos llamado hasta ahora fundamentales, tiene la propiedad de que cualquier otra relación entre los elementos del grupo puede deducirse a partir de ellas (Esto no es trivial, se sigue del hecho de que podemos decidir exactamente cuando dos elementos del grupo son iguales utilizando sólo estás tres relaciones).

Definición 0.2. *Dar un grupo G por generadores y relaciones es dar un conjunto de generadores $S = \{x_1, \ldots, x_n\}$ de G y un conjunto de relaciones $R_1, \ldots, R_m\}$ (aquí cada R_i es una ecuación en los generadores $x_1, \ldots, x_n$ y el 1) tales que cualquier otra relación entre los elementos de S puede deducirse a partir de ellas. Llamaremos a estos generadores y relaciones una presentación de G y escribiremos:*

$$G = \langle x_1, \ldots, x_n | R_1, \ldots, R_m \rangle.$$

Ejemplo 0.3. Los grupos cíclicos

$$C_n = \langle a | a^n = 1 \rangle,$$

los grupos diédricos

$$D_n = \langle r, s | r^n = 1 = s^2, sr = r^{-1}s \rangle,$$

o el grupo de Klein que puede presentarse por

$$K = \langle a, b | a^2 = 1 = b^2, ab = ba \}.$$

Enunciamos a continuación un teorema muy útil, cuya demostración omitimos pues requiere el estudio de grupos libres que está fuera de los objetivos de este curso.

Teorema 0.4. *Sea $\{x_1, \ldots, x_n\}$ un conjunto de generadores de un grupo G. Sea H un grupo y $a_1, a_2, \ldots, a_n$ elementos de H tales que cualquier relación en G que verifiquen los generadores x_i, también se satisface en H cuando sustituimos cada x_i por a_i. Entonces existe un único homomorfismo*

$$f : G \to H$$

tal que $f(x_i) = a_i$, $i = 1, \ldots, n$.

Corolario 0.5. Teorema de Dyck *Sea G un grupo y*

$$G = \langle x_1, \ldots, x_n | R_1, \ldots, R_m \rangle$$

una presentación de G. Sea H un grupo y $a_1, a_2, \ldots, a_n$ elementos de H tales que las ecuaciones $R_1, \ldots, R_m$ son validas en H al sustituir x_i por a_i. Entonces existe un único homomorfismo

$$f : G \to H$$

tal que $f(x_i) = a_i$, $i = 1, \ldots, n$.

En las hipótesis del corolario si

(1) $H = \langle a_1, \ldots, a_n \rangle$ entonces f es un epimorfismo,

(2) si además de (1) se tiene que $|G| = |H|$ entonces f es un isomorfismo.

Ejemplo 0.6. Haciendo uso del Teorema de Dyck veamos que el grupo de los cuaternios $Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$ puede presentarse de la forma

$$Q_2 = \langle a, b | a^4 = 1, b^2 = a^2, ba = a^3 b \rangle.$$

En efecto, llamemos $G = \langle a, b | a^4 = 1, b^2 = a^2, ba = a^3 b \rangle$. Sabemos que $i^4 = 1$, $i^2 = j^2$ y $ji = -k = (-i)j = i^3 j$. Entonces por el teorema de Dyck, existe un único

$$f : G \to Q_2, \text{ tal que } \ f(a) = i, f(b) = j.$$

Además puesto que $Q_2 = \langle i, j \rangle$, entonces f es un epimorfismo. Para ver que es un isomorfismo veamos que $|G| = 8$. En primer lugar, por el primer teorema de isomorfismo, $G/Ker(f) \cong Q_2$, en particular $|G| = |Q_2| \cdot |Ker(f)| \geq 8$.

Por otro lado, puesto que $a^4 = 1$ entonces $H = \langle a \rangle$ tiene orden ≤ 4. Como $bab^{-1} = a^3 b b^{-1} = a^3 \in H$ entonces $H \trianglelefteq G$ y $G/H = \langle bH \rangle$. Ahora como $(bH)^2 = b^2 H = a^2 H = H$, entonces $|G/H| \leq 2$. Consecuentemente $|G| = |G/H| \cdot |H| \leq 8$, y $G \cong Q_2$.

Definición 0.7. *Para cada $k \geq 1$ se define el k-ésimo grupo <u>dícíclico</u>, como el grupo presentado por*

$$Q_k = \langle a, b | a^{2k} = 1, b^2 = a^k, ba = a^{-1} b \rangle.$$

Como hemos visto, para el caso $k = 2$ tenemos el grupo de los cuaternios. El caso $k = 1$ es fácil ver que se trata del grupo cíclico de orden 4, esto es

$$C_4 \cong \langle a, b | a^2 = 1, b^2 = a, ba = a^{-1} b \rangle.$$

Observación 0.8. En general, para $k \geq 3$, Q_k tiene un cociente isomorfo a D_k y entonces <u>no</u> es abeliano y $2k \leq |Q_k| \leq 4k$. Además si $k = 2r + 1$ entonces $|Q_k| = 4k$.

En efecto, sabemos que $D_k = \langle r, s | r^k = 1 = s^2, sr = r^{-1} s \rangle$ y entonces $r^{2k} = (r^k)^2 = 1$, $s^2 = 1 = r^k$ y $sr = r^{-1} s$. El teorema de Dyck nos asegura

la existencia de un homomorfismo $f : Q_k \to D_k$ tal que $f(a) = r$ y $f(b) = s$. Como r y s generan D_k, entonces f es un epimorfismo con lo que

$$Q_k/Ker(f) \cong D_k.$$

Además $|D_k| = 2k$ es un divisor de $|Q_k|$ y en particular

$$2k \leq |Q_k|.$$

Para la otra desigualdad, puesto que $a^{2k} = 1$ entonces $H = \langle a \rangle$ tiene orden $\leq 2k$. Como $bab^{-1} = a^{-1}bb^{-1} = a^{-1} \in H$ entonces $H \trianglelefteq Q_k$ y $Q_k/H = \langle bH \rangle$. Ahora como $(bH)^2 = b^2H = a^kH = H$, entonces $|Q_k/H| \leq 2$. Consecuentemente $|Q_k| = |Q_k/H| \cdot |H| \leq 4k$.

Supongamos ahora que $k = 2r + 1$. Consideramos el grupo cíclico $C_4 = \langle x | x^4 = 1 \rangle$, puesto que $(x^2)^{2k} = (x^4)^k = 1$, $(x^2)^k = x^{2k} = x^{4r+2} = x^2$ y $x \cdot x^2 = x^3 = x^2 \cdot x = (x^2)^{-1}x$, de nuevo por el teorema de Dyck, existe un epimorfismo $g : Q_k \to C_4$ tal que $g(a) = x^2$ y $g(b) = x$. En particular $Q_k/Ker(g) \cong C_4$, con lo que $4 | |Q_k|$. Como $2k$ también divide a $|Q_k|$ entonces $mcm(4, 2k)$ es un divisor de $|Q_k|$.

Como k es impar entonces $mcm(4, 2k) = 4k$ con lo que $4k \leq |Q_k|$; como la otra desigualdad se tiene para todo k, concluimos que $|Q_k| = 4k$, como queríamos demostrar.

0.1. Clasificación de los grupos abelianos de orden ≤ 15.

(1) Sabemos que todo grupo de orden un número primo es isomorfo al cíclico y entonces los grupos

de orden 2	son isomorfos a	C_2
de orden 3	son isomorfos a	C_3
de orden 5	son isomorfos a	C_5
de orden 7	son isomorfos a	C_7
de orden 11	son isomorfos a	C_{11}
de orden 13	son isomorfos a	C_{13}

(2) Sabemos que todo grupo de orden p^2, p un número primo, es abeliano. Por otro lado, si $|A| = p^2$, sus divisores elementales son $\{p^2\}$ o $\{p, p\}$, es decir

$$A \cong C_{p^2} \text{ ó } A \cong C_p \times C_p.$$

Entonces los grupos

de orden 4	son isomorfos a	C_4 ó $C_2 \times C_2$
de orden 9	son isomorfos a	C_9 ó $C_3 \times C_3$

(3) Nos ocupamos ahora de los grupos de orden 6, 10 y 14. Para ello veamos primero el siguiente resultado

Proposición 0.9. *Si p es un primo impar, todo grupo de orden $2p$ es isomorfo a C_{2p} o a D_p.*

Demostración. Sea G con $|G| = 2p$. Sabemos que el número de p-subgrupos de Sylow, n_p verifica

$$n_p|2 \text{ y } n_p \equiv 1(mod\, p) \Rightarrow n_p = 1.$$

Sea $\mathcal{P}$ el único p-subgrupo de Sylow. Sabemos que $\mathcal{P} \lhd G$ y $|\mathcal{P}| = p$ y entonces $\mathcal{P} = \langle a|a^p = 1\rangle \cong C_p$.

Respecto a los 2-subgrupos de Sylow, como anteriormente sabemos que

$$n_2|p \text{ y } n_2 \equiv 1(mod\, 2) \Rightarrow \begin{cases} n_2 = 1 \\ \text{ó} \\ n_2 = p \end{cases}$$

Caso $n_2 = 1$: Sea $\mathcal{Q}$ el único 2-subgrupo de Sylow, entonces $\mathcal{Q} \cong C_2$, y como $n_p = 1$ entonces

$$G \cong \mathcal{P} \times \mathcal{Q} \cong C_p \times C_2 \cong C_{2p}.$$

Caso $n_2 = p$: Notemos que en este caso el grupo G no es abeliano. Puesto que $[G : \mathcal{P}] = \frac{|G|}{|\mathcal{P}|} = 2$, sólo hay dos clases laterales a derecha y G es la unión de ellas. Esto es

$$G = \mathcal{P} \cup \mathcal{P}b = \{1, a, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b\},$$

siendo $b \notin \mathcal{P}$.

Como $ord(b)|2p = |G|$ entonces $ord(b) = 2, p$, ó $2p$, notemos que no puede ser 1 pues $b \neq 1$. Si $ord(b) = p$ entonces $\langle p\rangle$ es un p-subgrupo de Sylow de G con lo que $\langle p\rangle = \mathcal{P}$ y en particular $b \in \mathcal{P}$ y llegamos a una contradicción. Si $ord(b) = 2p$ entonces $\langle b\rangle = G$ con lo que el grupo G sería abeliano, de nuevo llegamos a una contradicción. Consecuentemente $ord(b) = 2$.

Si consideramos ahora el elemento $ba \in G$ tendremos que $ord(ba) = 1, 2, p$, ó $2p$. Si $ord(ba) = 1$ entonces $ba = 1 \Rightarrow b = a^{-1} \in \mathcal{P}$, contradicción. Si $ord(ba) = p \Rightarrow \langle ba\rangle = \mathcal{P} \Rightarrow ba \in \mathcal{P} \Rightarrow b \in \mathcal{P}$, también contradicción. Finalmente si $ord(ba) = 2p$ entonces G sería abeliano y descartamos por tanto esta posibilidad. Consecuentemente $ord(ba) = 2$ y tendremos:$(ba)^2 = baba = 1 \Rightarrow bab = a^{-1} \Rightarrow ba = a^{-1}b$ y nuestro grupo tiene la siguiente presentació:

$$G = \langle a, b|a^p = 1 = b^2, ba = a^{-1}b\rangle \cong D_p.$$

□

Entonces como consecuencia de la proposición anterior los grupos

de orden 6	son isomorfos a	C_6 ó D_3
de orden 10	son isomorfos a	C_{10} ó D_5
de orden 14	son isomorfos a	C_{14} ó D_7

(4) Veamos que **sólo hay un grupo de orden** 15 **que es** C_{15}:

En efecto si $|G| = 15 = 3 \cdot 5$, entonces si n_3, n_5 denotan el número de 3-subgrupos de Sylow y de 5-subgrupos de Sylow, respectivamente, tenemos

$$n_3|5 \text{ y } n_3 \equiv 1(mod\, 3) \Rightarrow n_3 = 1,$$

sea $\mathcal{P}$ el único 3-subgrupo de Sylow que puesto que $|\mathcal{P}| = 3$, entonces $\mathcal{P} \cong C_3$

$$n_5|3 \text{ y } n_5 \equiv 1(mod\, 5) \Rightarrow n_5 = 1,$$

sea $\mathcal{Q}$ el único 5-subgrupo de Sylow que puesto que $|\mathcal{Q}| = 5$, entonces $\mathcal{Q} \cong C_5$

Consecuentemente G es producto directo interno de $\mathcal{P}$ y $\mathcal{Q}$ y tenemos

$$G \cong \mathcal{P} \times \mathcal{Q} \cong C_3 \times C_5 \cong C_{15}.$$

(5) Grupos de orden 8:

Caso abeliano: Si G es un grupo de orden 8 y abeliano entonces las posibles listas de divisores elementales son

1. $\{2^3\}$ y entonces $G \cong C_8$,
2. $\{2^4, 2\}$ y entonces $G \cong C_4 \times C_2$ y
3. $\{2, 2, 2\}$ y entonces $G \cong C_2 \times C_2 \times C_2$.

Caso no abeliano: Sea G un grupo de orden 8 y no abeliano (notemos que aquí no a lugar a la discusión sobre subgrupos de Sylow pues solo hay uno que es el propio G). En primer lugar, puesto que G no es abeliano entonces no tiene elementos de orden 8 pues sino sería cíclico. Por tanto sus elementos son de orden 4 o 2. Pero no todos los elementos son de orden 2 pues en ese caso sabemos que también sería abeliano, consecuentemente $\exists a \in G$ tal que $ord(a) = 4$.

Sea $H = \langle a \rangle = \{1, a, a^2, a^3\}$. Como $[G : H] = 2$ entonces $H \trianglelefteq G$ y si $b \in G$ es un elemento tal que $b \notin H$ entonces H, Hb son las dos únicas clases laterales a derecha, consecuentemente

$$G = H \cup Hb = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Consideremos el elemento b^2 entonces $b^2 \in H$ ó $b^2 \in Hb$. Si

$$b^2 \in Hb \Rightarrow \begin{cases} b^2 = b & \Rightarrow b = 1 \quad \text{contradicción} \\ b^2 = ab & \Rightarrow b = a \quad \text{contradicción} \\ b^2 = a^2b & \Rightarrow b = a^2 \quad \text{contradicción} \\ b^2 = a^3b & \Rightarrow b = a^3 \quad \text{contradicción} \end{cases}$$

Así pues $b^2 \in H$. Ahora si $b^2 = a \Rightarrow ord(b^2) = ord(a) = 4 \Rightarrow ord(b) = 8$ en contradicción con que G no es abeliano. Análogamente si $b^2 = a^3$ implicaría que $ord(b) = 8$ y tendríamos una contradicción. Consecuentemente $b^2 = 1$ ó $b^2 = a^2$.

Caso $b^2 = 1$. Veamos que $ba = a^3b$.

En efecto, como $H \trianglelefteq G$, entonces $bab^{-1} =\in H$ y como $b^2 = 1 \Rightarrow b = b^{-1}$, así $bab \in H$. Ahora

$bab \neq 1$ pues si $bab = 1 \Rightarrow ba = b \Rightarrow a = 1$ que es una contradicción,

$bab \neq a$ pues si $bab = a \Rightarrow ba = ab \Rightarrow G$ sería abeliano, que es una contradicción,

$bab \neq a^2$ pues si $bab = a^2 \Rightarrow baba = a^3 \Rightarrow ord(ba) = 8 \Rightarrow$ que G es abeliano, que es una contradicción.

Consecuentemente $bab = a^3 \Rightarrow ba = a^3b$ y nuestro grupo es

$$G\langle a, b | a^4 = 1 = b^2, ba = a^3b\rangle \cong D_4.$$

Caso $b^2 = a^2$. Veamos que también en este caso $ba = a^3b$.

En efecto, como $H \trianglelefteq G$, entonces $bab^{-1} =\in H$. Ahora

$bab^{-1} \neq 1$ pues si $bab^{-1} = 1 \Rightarrow ba = b \Rightarrow a = 1$ que es una contradicción,

$bab^{-1} \neq a$ pues si $bab^{-1} = a \Rightarrow ba = ab \Rightarrow G$ sería abeliano, que es una contradicción,

$bab^{-1} \neq a^2$ pues si $bab^{-1} = a^2 \Rightarrow bab^{-1} = b^2 \Rightarrow ab^{-1} = b \Rightarrow a = b^2 \Rightarrow a = a^2 \Rightarrow a = 1$, que es una contradicción.

Consecuentemente $bab^{-1} = a^3 \Rightarrow ba = a^3b$ y nuestro grupo es

$$G\langle a, b | a^4 = 1, a^2 = b^2, ba = a^3b\rangle \cong Q_2.$$

(6) Grupos de orden 12:

Caso abeliano: Si G es un grupo de orden 12 y abeliano entonces las posibles listas de divisores elementales son

1. $\{2^2, 3\}$ y entonces $G \cong C_4 \times C_2 \cong C_{12}$ y
2. $\{2, 2, 3\}$ y entonces $G \cong C_2 \times C_2 \times C_3 \cong C_6 \times C_2$.

Caso no abeliano: Sea G un grupo de orden 12 y no abeliano. Si n_3 denota el número de 3-subgrupos de Sylow, sabemos que $n_3|4$ y $n_3 \equiv 1(mod\,3)$ con lo que $n_3 = 1$ ó $n_3 = 4$.

Si $n_3 = 4$ entonces como ya hemos visto en los ejercicios,

$$G \cong A_4$$

.

Supongamos $n_3 = 1$ y sea $\mathcal{P}$ el único 3-subgrupo de Sylow de G. Sabemos que $\mathcal{P} \trianglelefteq G$ y como $|\mathcal{P}| = 3$ entonces $\mathcal{P} = \langle x|x^3 = 1\rangle = \{1, x, x^2\}$. Veamos que en este caso existe en G un elemento de orden 6.

Para ello consideramos la clase de conjugación de x, $cl(x) = \{gxg^{-1}/g \in G\}$. Como $\mathcal{P} \trianglelefteq G$ entonces $cl(x) \subseteq \mathcal{P}$ y así $cl(x) = \{x\}$ ó $cl(x) = \{x, x^2\}$ (notemos que $cl(x)$ no puede contener al 1 pues $gxg^{-1} = 1 \Rightarrow x = 1$, que es una contradicción). Como $[G : c_G(x)] = |cl(x)|$, siendo $c_G(x) = \{g \in G/gx = xg\}$ el centralizador de x en G, entonces $|c_G(x)| = 6$ ó $|c_G(x)| = 12$. En ambos casos, por el Teorema de Cauchy, existe $z \in c_G(x)$ con $ord(z) = 2$.

Sea $a = xz$. Como $xz = zx$ y $mcd(ord(x), ord(z)) = 1$, entonces $ord(a) = ord(x) \cdot ord(z) = 6$, consideremos $K = \langle a\rangle = \{1, a, a^2, a^3, a^4, a^5\}$. Como $[G : K] = 2$ entonces $K \trianglelefteq G$ y si $b \in G$ es un elemento tal que $b \notin K$ entonces K, Kb son las dos únicas clases laterales a derecha, consecuentemente

$$G = K \cup Kb = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}.$$

Puesto que $bab^{-1} \in K$ y $ord(bab^{-1} = ord(a) = 6 \Rightarrow bab^{-1} = a\,\text{ó}\,a^5$. Pero $bab^{-1} = a \Rightarrow ba = ab$ y G sería abeliano, consecuentemente

$$bab^{-1} = a^5 \Rightarrow ba = a^5b.$$

Consideremos el elemento b^2 entonces $b^2 \in K$ ó $b^2 \in Kb$. Si $b^2 \in Kb \Rightarrow b^2 = a^ib \Rightarrow b = a^i \in K$, lo cual es una contradicción. Así pues, necesariamente $b^2 \in K$. Ahora Si $b^2 = a \Rightarrow ord(b^2) = ord(a) = 5 \Rightarrow ord(b) = 12$ en contradicción con que G no es abeliano. Análogamente si $b^2 = a^5$ implicaría que $ord(b) = 12$ y tendríamos una contradicción.

Si $b^2 = a^2$ entonces

$$(a^{-1})^2 = (bab^{-1})^2 = ba^2b^{-1} = bb^2b^{-1} = b^2 \Rightarrow (a^{-1})^2 = a^2 \Rightarrow a^4 = 1$$

con lo que el orden de a sería 4, en contradicción con que tiene orden 6.

Si $b^2 = a^4$ entonces

$$(a^{-1})^4 = (bab^{-1})^4 = ba^4b^{-1} = b^2 = a^4 \Rightarrow a^8 = a^2 = 1,$$

con lo que el orden de a sería 2, de nuevo una contradicción.

Consecuentemente $b^2 = 1$ ó $b^2 = a^3$.

Caso $b^2 = 1$. , puesto que $ba = a^5b$, nuestro grupo es

$$G = \langle a, b | a^6 = 1 = b^2, ba = a^5b \rangle \cong D_6.$$

Caso $b^2 = a^3$. puesto que $ba = a^5b$, nuestro grupo es

$$G = \langle a, b | a^6 = 1, a^3 = b^2, ba = a^5b \rangle \cong Q_3.$$

Resumimos todo el estudio anterior en la siguiente tabla

orden	N$^{\text{a}}$ de grupos	abelianos	no abelianos
1	1	$\{1\}$	ninguno
2	1	C_2	ninguno
3	1	C_3	ninguno
4	2	$C_4, C_2 \times C_2$	ninguno
5	1	C_5	ninguno
6	2	C_6	D_3
7	1	C_7	ninguno
8	5	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$	D_4, Q_2
9	2	$C_9, C_3 \times C_3$	ninguno
10	2	C_{10}	D_5
11	1	C_{11}	ninguno
12	5	$C_{12}, C_6 \times C_2$	A_4, D_6, Q_3
13	1	C_{13}	ninguno
14	2	C_{14}	D_7
15	1	C_{15}	ninguno

ALGEBRA III (Doble grado Informática-Matemáticas)

1. Preliminares sobre extensiones de cuerpos y raíces de polinomios.

1.1. Sobre extensiones de cuerpos.

(1) Recordemos que por un **cuerpo** K entendemos un anillo conmutativo, no trivial (es decir, con $|K| \geq 2$ o, equivalentemente, donde $1 \neq 0$), en el cual todo elemento no nulo tiene un inverso para el producto. Así, por ejemplo, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, o $\mathbb{Z}_p$ para $p \geq 2$ un primo de $\mathbb{Z}$, son cuerpos bien conocidos.

(2) Dado un cuerpo K, por una **extensión de K entendemos un otro cuerpo E que contiene a K como subcuerpo**, esto es, tal que $K \subseteq E$ como conjunto y sucede que K tiene el mismo 0, el mismo 1, y los cálculos de sumas y productos (y entonces también de opuestos e inversos) se realizan en K como en E. Usualmente representamos la situación de dos formas: escribimos

$$K \leq E$$

cuando queremos enfatizar que "*K es un subcuerpo de E*", y escribimos

$$E/K,$$

expresión que leemos "*E sobre K*", cuando queremos enfatizar que "*E es un cuerpo extensión del cuerpo K*". Significan lo mismo, así que

$$K \leq E \Longleftrightarrow E/K.$$

(3) **Los homomorfismos entre cuerpos son monomorfismos**. Esto es, si K y E son cuerpos, cada aplicación $\sigma : K \to E$ preservando 0 y 1, sumas, y productos (y entonces opuestos e inversos) es inyectiva: Si suponemos que $\sigma(a) = \sigma(b)$ con $a \neq b$, tendríamos por un lado que $a - b \neq 0$, y existiría su inverso $(a-b)^{-1}$, y por otro que $\sigma(a - b) = \sigma(a) - \sigma(b) = 0$. Pero entonces, en el cuerpo E,

$$1 = \sigma(1) = \sigma\big((a-b)(a-b)^{-1}\big) = \sigma(a-b)\sigma(a-b)^{-1} = 0 \cdot \sigma(a-b)^{-1} = 0$$

lo que no puede ocurrir. Debido a esta propiedad, es usual referirse a un homomorfismo de cuerpos $\sigma : K \to E$ como a una **inmersión de K en E**, ya que este homomorfismo establece un isomorfismo de cuerpos entre K y el subcuerpo de E imagen del homomorfismo:

$$K \cong \sigma(K) = \{\sigma(a),\ a \in K\} \leq E, \quad a \mapsto \sigma(a)\,.$$

(4) **Cuando una inmersión $\sigma : K \to E$ es dada y bien conocida, es usual tratarla como una inclusión** (asumiendo de común acuerdo un abuso de lenguaje), identificando cada elemento a de K con su imagen $\sigma(a)$ en E, y K con el subcuerpo de E imagen de σ. De manera asumimos que $K \leq E$ es un subcuerpo (y E/K una extensión).

Un ejemplo típico de esta asunción es la inmersión

$$\sigma : \mathbb{Q} \to \mathbb{R},$$

del cuerpo de los números racionales en el cuerpo de los números reales, definida por $\sigma(\frac{a}{b}) = ab^{-1}$. Está bien definida, pues

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc \Rightarrow ab^{-1} = cd^{-1}$$

y es ciertamente una inmersión, pues

$$\sigma\Big(\frac{a}{b}+\frac{c}{d}\Big)=\sigma\Big(\frac{ad+cb}{bd}\Big)=(ad+cb)(bd)^{-1}=(ad+cb)b^{-1}d^{-1}$$
$$=adb^{-1}d^{-1}+cbb^{-1}d^{-1}=ab^{-1}+cd^{-1}=\sigma\Big(\frac{a}{b}\Big)+\sigma\Big(\frac{c}{d}\Big),$$
$$\sigma\Big(\frac{a}{b}\frac{c}{d}\Big)=\sigma\Big(\frac{ac}{bd}\Big)=(ac)(bd)^{-1}=acb^{-1}d^{-1}=\sigma\Big(\frac{a}{b}\Big)\sigma\Big(\frac{c}{d}\Big),$$

y claramente $\sigma(\frac{0}{1})=0$ y $\sigma(\frac{1}{1})=1$. Esta inmersión $\sigma:\mathbb{Q}\to\mathbb{R}$ nos es familiar y bien conocida, y es mediante ella que identificamos cada número racional con un número real y vemos a $\mathbb{Q}$ como un subcuerpo de $\mathbb{R}$ y a $\mathbb{R}$ como una extensión de $\mathbb{Q}$.

Veamos otro ejemplo típico en el que usualmente consideramos una cierta inmersión como una inclusión. Supongamos K cualquier cuerpo y $p\in K[x]$ un polinomio de grado ≥ 1 irreducible. Sea

$$K[x]/_p=\{\overline{f}\mid f\in K[x]\},$$

el *cuerpo de clases de congruencias módulo p* (también llamado el *cuerpo de restos módulo p*) donde, recordamos,

$$\begin{aligned}\overline{f}=\overline{g}&\Leftrightarrow f\equiv g \mod p\\ &\Leftrightarrow p\mid f-g\\ &\Leftrightarrow f \text{ y } g \text{ dan el mismo resto al dividirlos por } p,\end{aligned}$$

las operaciones de suma y producto de clases de congruencias son

$$\overline{f}+\overline{g}=\overline{f+g},\ \ \overline{f}\ \overline{g}=\overline{fg},$$

y el zero y el uno son $\overline{0}$ y $\overline{1}$, respectivamente. Puesto que p es irreducible en el Dominio Euclídeo $K[x]$, conocemos que $K[x]/_p$ es un cuerpo: Si $\overline{f}\neq\overline{0}$, será $p\nmid f$ y $mcd(p,f)=1$. Tendremos coeficientes de Bezout $u,v\in K[x]$ tal que $1=fu+pv$, de donde $\overline{1}=\overline{f}\ \overline{u}$, lo que nos asegura que existe $\overline{f}^{\,-1}=\overline{u}$. La asignación $a\mapsto\overline{a}$ nos determina una inmersión estandard

$$K\to K[x]/_p,$$

que miraremos usualmente como una inclusión, considerando a K como un subcuerpo del cuerpo de clases de congruencias módulo p.

Un caso particular es familiar: Tomemos $K=\mathbb{R}$ y $p=x^2+1$, que es irreducible en $\mathbb{R}[x]$ (no tiene raíces). Tenemos, como antes la "inclusión" $\mathbb{R}\leq\mathbb{R}[x]/_{x^2+1}$, después de identificar cada número real a con su clase $\overline{a}$ en $\mathbb{R}[x]/_{x^2+1}$. Analicemos un poco este cuerpo de restos, llamando $i=\overline{x}$. Sea $f\in\mathbb{R}[x]$ cualquier polinomio, sabemos que existen polinomio únicos $q,r\in\mathbb{R}[x]$ tal que $f=(x^2+1)q+r$, donde $gr(r)\leq 1$. Será $r=a+bx$, para ciertos $a,b\in\mathbb{R}$, y tendremos que

$$\overline{f}=\overline{r}=\overline{a}+\overline{b}\,\overline{x}=a+bi.$$

Así que todo elemento de $\mathbb{R}[x]/_{x^2+1}$ se expresa en la forma $a+bi$ para ciertos números reales a y b. Además, de forma única: Supongamos que $a+bi=a'+b'i$. Tendremos que $\overline{a}+\overline{b}\,\overline{x}=\overline{a'}+\overline{b'}\,\overline{x}$, o sea $\overline{a+bx}=\overline{a'+b'x}$. Pero esto significa que x^2+1 divide a $a-a'+(b-b')x$, lo que no es posible si ese último es distinto de

cero, ya que un polinomio no nulo de grado uno no puede ser múltiplo de uno de grado dos. Así que $a - a' = 0$, $b - b' = 0$, y $a = a'$ y $b = b'$.

Observar ahora que

$$i^2 = \overline{x}^{\,2} = \overline{x^2} = \overline{-1} = -1$$

y que

$$\begin{aligned}(a + bi) + (a' + b'i) &= a + a' + (b + b')i,\\ (a + bi)\,(a' + b'i) &= aa' + (ab' + ba')i + bb'i^2 = aa' + (ab' + ba')i - bb'\\ &= aa' - bb' + (ab' + ba')i.\end{aligned}$$

De manera que $\mathbb{R}[x]/_{x^2+1} = \mathbb{C}$, el cuerpo de los números complejos, y la inmersión $\mathbb{R} \to \mathbb{C}$, $a \mapsto a = \overline{a}$, es la ordinaria con que se ve $\mathbb{R}$ como un subcuerpo del cuerpo $\mathbb{C}$ de los complejos.

1.2. Sobre raíces de polinomios y su multiplicidad.

(1) Dada una extensión E/K, recordemos que para cada $\alpha \in E$ hay un homomorfismo de anillos $K[x] \to E$, llamado el **homomorfismo de evaluación en** α, que asigna a cada polinomio $f = \sum_i a_i x^i \in K[x]$, el elemento $f(\alpha) = \sum_i a_i \alpha^i \in E$. Un elemento $\alpha \in E$ tal que $f(\alpha) = 0$ es llamado **una raíz de** f **en** E. Notemos que $K[x] \leq E[x]$ como subanillo, por tanto $f \in E[x]$ y, por el Teorema de Ruffini, el que α sea una raíz de f en E es equivalente a que $(x - \alpha)|f$ en el anillo $E[x]$; esto es, $(x - \alpha)$ es uno de los irreducibles que aparecen en la factorización de f en producto de irreducibles en el anillo $E[x]$. Si en dicha factorización en $E[x]$ aparece el irreducible $x - \alpha$ con exponente m, esto es, si $(x - \alpha)^m$ es la maxima potencia de $x - \alpha$ que divide a f en $E[x]$, decimos que α es una **raíz de** f **en** E **de multiplicidad** m. Decimos que α es una **raíz simple** si es de multiplicidad 1, y que es **raíz múltiple** si es de multiplicidad ≥ 2.

(2) El **criterio del polinomio derivado** es un útil recurso para conocer la inexistencia de raíces múltiples de un polinomio en cuerpos extensión.

Si $f = \sum_i a_i x^i \in K[x]$ es un polinomio con coeficientes es un cuerpo K, se define su **derivado** como el polinomio

$$f' = \sum_i i a_i x^{i-1} = a_1 + 2a_2 x + \cdots \in K[x]\ ^{1}.$$

El cálculo de polinomios derivados tiene las mismas propiedades básicas que las propias del cálculo diferencial:

$$(f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

La primera igualdad es inmediata desde la propia definición. Para la segunda, supongamos ahora que tenemos los polinomios $f = \sum_i a_i x^i$ y $g = \sum_j b_j x^j$. Entonces $fg = \sum_{i,j} a_i b_j x^{i+j}$,

$(fg)' = \left(\sum_{i,j} a_i b_j x^{i+j}\right)' = \sum_{i,j} \left(a_i b_j x^{i+j}\right)' = \sum_{i,j} (i + j) a_i b_j x^{i+j-1}$,

[1] El producto na, de enteros $n \geq 0$ por elementos a de un anillo es el usual: Si $n = 0$, entonces $0a = 0$. Si $n > 0$, entonces $na = a + \overset{n}{\cdots} + a$, la suma reiterada de ese elemento a consigo mismo n veces.

y, finalmente,

$$f'g + fg' = \Big(\sum_i i a_i x^{i-1}\Big)\Big(\sum_j b_j x^j\Big) + \Big(\sum_i a_i x^i\Big)\Big(\sum_j j b_j x^{j-1}\Big)$$
$$= \sum_{i,j} i a_i b_j x^{i+j-1} + \sum_{i,j} j a_i b_j x^{i+j-1} = \sum_{i,j} (i+j) a_i b_j x^{i+j-1} = (fg)'.$$

Por ejemplo,

$$\Big((x-a)^2\Big)' = (x-a)'(x-a) + (x-a)(x-a)' = (x-a) + (x-a) = 2(x-a).$$

Proposición 1.1. *(i) Si $f \in K[x]$ es tal que $mcd(f, f') = 1$ en $K[x]$, entonces todas las raíces de f en cualquier cuerpo extensión de K son simples.*

(ii) Si $f \in K[x]$ es irreducible y $f' \neq 0$, todas las raíces de f en cualquier cuerpo extensión de K son simples.

Demostración.(*i*) Supongamos E/K es una extensión y que α es raíz múltiple de f en E. En el anillo $E[x]$, será $f = (x-\alpha)^2 g$ para un cierto $g \in E[x]$. Pero entonces $f' = 2(x-\alpha)g + (x-\alpha)^2 g'$ y vemos que $f'(\alpha) = 0$. Pero, por el Teorema de Bezout, existen polinomios $u, v \in K[x]$ tal que $1 = fu + f'v$, y evaluando en α, resulta que

$$1 = f(\alpha)u(\alpha) + f'(\alpha)v(\alpha) = 0u(\alpha) + 0v(\alpha) = 0,$$

lo que no es posible.

(*ii*) Como $\mathrm{gr}(f') < \mathrm{gr}(f)$, y f es irreducible, necesariamente $mcd(f, f') = 1$. □

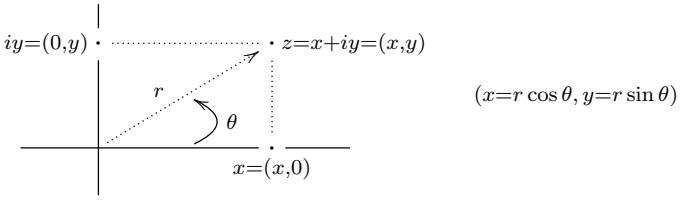
Notar que el polinomio derivado de un polinomio puede ser cero: Si $f = x^2 + 1 \in \mathbb{Z}_2[x]$, entonces $f' = 2x = x + x = (1+1)x = 0x = 0$.

1.3. Raíces n-ésimas de números complejos.

Para todo lo que sigue, es útil el pensar en los puntos del plano como la representación geométrica de los números complejos, así que vamos a identificar cada punto del plano Euclídeo $\mathbb{R}^2$ de coordenadas cartesianas (x, y) con el número complejo $z = x+iy$. Además, sobre todo a efectos de multiplicación, es cómodo usar la expresión de los complejos no nulos, es decir, los del grupo multiplicativo $\mathbb{C}^\times$, en su forma polar

$$z = re^{i\theta}$$

donde $r = |z| = \sqrt{x^2+y^2}$ es el módulo del complejo que coincide con longitud del segmento de extremos 0 y z, $\theta \in \mathbb{R}$ es la amplitud en radianes del ángulo desde el eje de abscisas a la recta que pasa por 0 y z, y $e^{i\theta} = \cos\theta + i\sin\theta$, que es justo el complejo en que la semi-recta que pasa por 0 y z corta a la circunferencia $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$:



$$z = x + iy = r\cos\theta + i\, r\sin\theta = r(\cos\theta + i\sin\theta) = re^{i\theta}.$$

Si $z' = r'e^{i\theta'}$ es otro complejo no nulo, entonces

$$\begin{aligned} zz' = rr'e^{i\theta}e^{i\theta'} &= rr'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') \\ &= rr'\big(\cos\theta\cos\theta' - \sin\theta\sin\theta' + i(\sin\theta\cos\theta' + \cos\theta\sin\theta')\big) \\ &= rr'\big(\cos(\theta+\theta') + i\sin(\theta+\theta')\big) \\ &= rr'e^{i(\theta+\theta')}. \end{aligned}$$

En particular, calculamos las potencias z^n, $n \geq 1$, de un complejo $z = re^{i\theta}$ por la simple fórmula

$$z^n = r^n e^{in\theta}.$$

Si $0 \neq z \in \mathbb{C}$ es cualquier complejo no nulo, para cualquier natural $n \geq 1$, las raíces complejas del polinomio $x^n - z$, esto es, los números complejos x tales que $x^n = z$, son llamadas las **raíces n-ésimas del número** z (cuadradas si $n = 2$, cúbicas si $n = 3$, etc.). Para realizar una descripción de las mismas, procedemos como sigue:

Si $0 < r \in \mathbb{R}$ es un número real positivo, la gráfica de la función real de variable real $y = x^n$ corta exactamente una vez a la recta $y = r$ en el intervalo $(0, +\infty)$, lo que significa que el polinomio $x^n - r$ tiene exactamente una raíz que es real y positiva. Usaremos para ella la notación

$$\sqrt[n]{r}.$$

Las reglas básicas que rigen la extracción de raíces n-ésimas de números reales positivos son las bien familiares: $\sqrt[n]{r}\,\sqrt[n]{r'} = \sqrt[n]{rr'}$, $(\sqrt[n]{r})^m = \sqrt[n]{r^m}$, $\sqrt[m]{\sqrt[n]{r}} = \sqrt[mn]{r}$. Pero hay que manejar los radicales con precaución, pues no todo cálculo con estos se puede hacer en base al uso formal de esas propiedades. Por ejemplo: $\sqrt{5+2\sqrt{6}} = \sqrt{2}+\sqrt{3}$, ya que $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$.

Si ahora $0 \neq z = re^{i\theta} = r(cos\,\theta + i\,sen\,\theta)$ es cualquier complejo no nulo expresado en su forma polar, entonces los n complejos

$$\sqrt[n]{r}e^{i\frac{\theta+2k\pi}{n}} = \sqrt[n]{r}\Big(cos\tfrac{\theta+2k\pi}{n} + i\,sen\tfrac{\theta+2k\pi}{n}\Big), \quad k = 0, \ldots, n-1.$$

son todos ellos raices n-ésimas de z, y por tanto las n-raíces de z (no puede haber más raíces de $x^n - a$). Destacamos entre ellas la raíz que se obtiene cuando $k = 0$, para la que reservamos la notación $\sqrt[n]{z}$, esto es

$$\sqrt[n]{z} = \sqrt[n]{r}\,e^{i\frac{\theta}{n}} = \sqrt[n]{r}\,\big(cos\tfrac{\theta}{n} + i\,sen\tfrac{\theta}{n}\big)\,.$$

Así, por ejemplo,

- $\sqrt[n]{1} = 1$.
- $\sqrt[n]{-1} = cos\frac{\pi}{n} + i\,sen\frac{\pi}{n}$, ya que $-1 = e^{i\pi} = cos\,\pi + i\,sen\,\pi$. Particularmente,

  $$\sqrt{-1} = i, \quad \sqrt[3]{-1} = \tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}, \quad \sqrt[4]{-1} = \tfrac{\sqrt{2}}{2} + i\tfrac{\sqrt{2}}{2}, \quad \ldots$$

  (notar, por ejemplo, que $\sqrt[3]{-1} \neq -1$)
- $\sqrt[2]{i} = \cos\frac{\pi}{4} + i\,sen\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, ya que $i = e^{i\frac{\pi}{2}} = cos\,\frac{\pi}{2} + i\,sen\,\frac{\pi}{2}$.
- $\sqrt[3]{i} = \cos\frac{\pi}{6} + i\,sen\frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i\,.$
- $\sqrt{-2} = \sqrt{2}\cos\frac{\pi}{2} + i\,sen\,\frac{\pi}{2} = i\sqrt{2}$, ya que $-2 = 2\,e^{i\pi} = 2(cos\,\pi + i\,sen\,\pi)$.

En términos de $\sqrt[n]{z}$, las n raíces de $z = e^{i\theta}$ se pueden expresar entonces como $\sqrt[n]{z}\, e^{\frac{2k\pi i}{n}}$, con $0 \leq k \leq n-1$. Por ejemplo, las dos raíces cuadradas de la unidad son 1, -1; las tres raíces cúbicas de la unidad son 1, $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$, y las 4 raíces cuartas de la unidad son 1, i, -1, $-i$.

1.4. **El Teorema Fundamental del Álgebra.**

Si $f \in K[x]$ es un polinomio, decimos que este **descompone totalmente en una extensión** E/K, si en el anillo $E[x]$ el polinomio factoriza como producto de irreducibles de grado uno, esto es, en la forma

$$f = a(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r}.$$

para ciertos $\alpha_i \in E$ con $\alpha_i \neq \alpha_j$ si $i \neq j$, y ciertos enteros $m_i \geq 1$. Es decir, si f tiene todos sus raíces en E.

Un cuerpo K se dice **algebraicamente cerrado** si todo polinomio con coeficientes en K descompone totalmente en K.

Proposición 1.2. *Las siguientes propiedades sobre un cuerpo K son equivalentes:*

(1) *K es algebraicamente cerrado.*
(2) *Todo polinomio de $K[x]$ de grado ≥ 1 tiene una raíz en K.*

Demostración. Es claro que (1) $\Rightarrow$ (2). Para el reciproco, supongamos que $f \in K[x]$ es de grado $n \geq 1$, y hagamos inducción en n. Si $n = 1$, será $f = a_0 + a_1 x$, con $a_1 \neq 0$, y por tanto también $f = a_1\big(x - (-a_0 a_1^{-1})\big)$. Para el caso general $n > 1$, sabemos que existe un $\alpha \in K$ tal que $f(\alpha) = 0$. Por Ruffini, tendremos que $f = (x - \alpha)g$ para un cierto $g \in K[x]$ de grado $n - 1$, y el resultado se deduce de aplicar la hipótesis de inducción a g. □

Teorema 1.3 (Teorema de Gauss)**.** *El cuerpo $\mathbb{C}$ es algebraicamente cerrado.*

Demostración. El cuerpo $\mathbb{C}$ es un espacio vectorial real de dimensión 2, con base $\{1, i\}$, que es métrico con norma el valor absoluto, esto es donde la distancia entre dos complejos a y b es dada por $d(a, b) = |a - b|$. Tiene entonces la topología asociada a dicha métrica, donde una base de entornos abiertos de cualquier punto está formada por las bolas abiertas $B(a, r) = \{z \in \mathbb{C} \mid |z - a| < r\}$, con $0 < r \in \mathbb{R}$. Usaremos el Teorema de Weierstass: *Una función continua $f : \mathbb{C} \to \mathbb{R}$ siempre alcanza su mínimo (y su máximo) en cualquier subconjunto cerrado y acotado de $\mathbb{C}$, particularmente en cualquier bola cerrada $B[a, r] = \{z \in \mathbb{C} \mid |z - a| \leq r\}$.* Usaremos también algunas desigualdades básicas entre módulos, como que $|a| - |b| \leq |a + b| \leq |a| + |b|$.

Sea $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{C}[x]$ un polinomio de grado $n \geq 1$ ($a_n \neq 0$). Se trata de probar que existe un complejo $z \in \mathbb{C}$ tal que $f(z) = 0$. Para ello, comenzamos considerando la función continua $\mathbb{C} \to \mathbb{R}$ definida por $z \mapsto |f(z)|$, y vamos a probar, por inducción en el grado n, el número real $|f(z)|$ se hace más grande que cualquier número real positivo k fuera de cierta bola cerrada $B[0, r]$; es decir vamos a probar que

"Para cada número real $k \geq 0$, existe un real $r \geq 0$ tal que $|z| > r \Rightarrow |f(z)| > k$."

En efecto, escribamos f como

$$f = a_0 + xg, \quad \text{donde } g = a_1 + a_2 x + \cdots + a_n x^{n-1},$$

de manera que, para cualquier $z \in \mathbb{C}$,

$$|f(z)| = |zg(z) + a_0| \geq |z| \cdot |g(z)| - |a_0|.$$

Si $n = 1$, $g = a_1$ es constante y podemos tomar $r = \frac{k+|a_0|}{|a_1|}$, pues si $|z| > r$, entonces

$$|f(z)| \geq |z| \cdot |a_1| - |a_0| > \frac{k + |a_0|}{|a_1|}|a_1| - a_0 = k.$$

Para el caso general $n > 1$, la hipótesis de inducción aplicada al polinomio g y al número real $k' = k + |a_0|$ nos asegura la existencia de un real $r' > 0$ tal que $|g(z)| > k + |a_0|$ siempre que $|z| > r'$. Pero entonces, tomando $r = \text{máx}\{r', 1\}$, para cualquier $z \in \mathbb{C}$ con $|z| > r$, tenemos que $|f(z)| \geq |z| \cdot |g(z)| - |a_0| > 1 \cdot (k + |a_0|) - |a_0| = k$.

En particular, para el caso $k = |a_0|$, concluimos que existe un real $r \geq 0$ tal que $|f(z)| > |a_0|$ siempre que $|z| > r$. Ahora, aplicando el Teorema Weierstrass a la función continua $\mathbb{C} \to \mathbb{R}$ definida por $z \mapsto |f(z)|$, podemos asegurar que existe un $z_0 \in B[0, r]$ tal que $|f(z_0)| \leq |f(z)|$ para todo $z \in B[0, r]$. Pero la misma desigualdad se verifica automáticamente para los $z \notin B[0, r]$, pues si $|z| > r$ entonces $f(z) > |a_0| = |f(0)| \geq |f(z_0)|$. Concluimos así que

"*Existe un* $z_0 \in \mathbb{C}$ *tal que* $|f(z_0)| \leq |f(z)|$*para todo* $z \in \mathbb{C}$".

Es claro que f tiene una raíz en $\mathbb{C}$ si y solo si el polinomio $f(x + z_0)$, que resulta de sustituir x por $x + z_0$ en f tiene una raíz, y este tiene la ventaja notacional de que la función $z \mapsto |f(z + z_0)|$ tiene un mínimo absoluto en el 0. Por tanto, sustituyendo f por $f(x + z_0)$, podemos seguir trabajando con f pero suponiendo que $z_0 = 0$. Esto es, asumimos en lo que sigue que

$$|f(z)| \geq |f(0)| = |a_0| \text{ } \textit{para todo } z \in \mathbb{C}.$$

Si $a_0 = 0$ hemos terminado, pues sería $f(0) = 0$ y f tiene una raíz. Vemos a continuación que suponer $a_0 \neq 0$ nos lleva a una contradicción:

Supuesto $a_0 \neq 0$, si sustituimos f por $\frac{1}{a_0}f$, la función $z \mapsto |\frac{1}{a_0}f(z)|$ también tiene a 0 como mínimo absoluto, así que podemos suponer que $a_0 = 1$, de manera que

$$|f(z)| \geq 1 \text{ } \textit{para todo } z \in \mathbb{C}$$

y, excluyendo los primeros términos de coeficiente nulo, podemos escribir

$$f = 1 + a_m x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n, \qquad \text{con } a_m \neq 0.$$

entonces, sustituyendo x por $\sqrt[m]{-a_m^{-1}}x$, obtenemos el polinomio $f(\sqrt[m]{-a_m^{-1}}x) = 1 - x^m +$ términos de grado mayor que m, es decir,

$$f(\sqrt[m]{-a_m^{-1}}x) = 1 - x^m + x^m g,$$

donde $g \in \mathbb{C}[x]$ es un cierto polinomio con $g(0) = 0$ (pues todos sus términos son de grado ≥ 1). Finalizamos demostrando la existencia de un número real t tal que $f(\sqrt[m]{-a_m^{-1}}t) < 1$ (lo que es imposible pues $f(z) \geq 1$ para todo $z \in \mathbb{C}$): Consideremos la función $\mathbb{R} \to \mathbb{R}$ definida por $t \mapsto |g(t)|$. Su límite en $t = 0$ es $g(0) = 0$ (por continuidad), luego seguro que existe un número real t en el intervalo $(0, 1)$ tal que $|g(t)| < 1$ (tomando $\epsilon = 1$ en la formulación usual de límite, existe un $\delta > 0$ tal que $g(t) < 1$ siempre que $|t| < \delta$,

pues tomemos cualquier $t \in (0,1) \cap (-\delta, \delta)$). Entonces, tanto t^m como $1 - t^m$ están en el intervalo $(0,1)$ y tenemos que

$$|f(\sqrt[m]{-a_m^{-1}}t)| = |1 - t^m + t^m g(t)| \leq |1 - t^m| + |t^m g(t)| < 1 - t^m + t^m \cdot 1 = 1,$$

lo que concluye la demostración. □

1.5. **Sobre existencia de extensiones donde los polinomios tienen todas sus raíces.**

Si $K \leq \mathbb{C}$ es un cuerpo de números, cualquier $f \in K[x]$ descompone totalmente en $\mathbb{C}$, ya que este es algebraicamente cerrado. Para el caso general, tenemos la siguiente hecho.

Proposición 1.4. *Sea K un cuerpo. Dado cualquier polinomio $f \in K[x]$ de grado ≥ 1, existe un cuerpo E extensión de K en el cual f descompone totalmente.*

Demostración. Hagamos inducción sobre el grado del polinomio en cuestión, $f = \sum_i a_i x^i$. Si el grado es 1, basta tomar $E = K$, pues $a_1 x + a_0 = a_1(x - \frac{-a_0}{a_1})$. Supongamos $\mathrm{gr}(f) \geq 2$, y escojamos $p \in K[x]$ un irreducible tal que $p|f$. Sea $E = K[x]/_p$ el cuerpo extensión de K de classes de congruencias de polinomios en $K[x]$ módulo p, y llamemos $\alpha = \overline{x} \in E$. Entonces,

$$f(\alpha) = \textstyle\sum_i a_i \alpha^i = \sum_i a_i \overline{x}^i = \overline{\sum_i a_i x^i} = \overline{f} = 0,$$

y α es una raíz de f en E. Pongamos $f = (x - \alpha)g$, para un cierto $g \in E[x]$. Como g es de grado menor que el de f, existirá un cuerpo extension F/E en el cual g descompone totalmente. Claramente entonces f descompone totalmente en F. □

ALGEBRA III (Doble grado Informática-Matemáticas)

2. Extensiones finitas y algebraicas de cuerpos

2.1. Extensiones algebraicas.

Si E/K es una extensión de cuerpos, un elemento $\alpha \in E$ se dice **algebraico** sobre K si es raíz de algún polinomio no nulo con coeficientes en K. En otro caso, α se dice **trascendente** sobre K.

Por ejemplo, el número real $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$, al ser raíz del polinomio $x^2 - 2$, y el número real π es trascendente sobre $\mathbb{Q}$ (Teorema de Lindemann-Weierstrass).

Notemos que el concepto de algebraicidad de un elemento de un cuerpo E es relativo al cuerpo base. Por ejemplo, aunque π es trascendente sobre $\mathbb{Q}$, es algebraico sobre $\mathbb{R}$ al ser raíz de $x - \pi \in \mathbb{R}[x]$.

Una **extensión** E/K se dice **algebraica** si todo elemento de E es algebraico sobre K.

Ejemplo 2.1. La extensión $\mathbb{C}/\mathbb{R}$ es algebraica. Si $z = a + bi \in \mathbb{C}$, donde $a, b \in \mathbb{R}$, entonces z es raíz del polinomio $x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$:

$$z^2 - 2az + (a^2+b^2) = (a+bi)^2 - 2a(a+bi) + a^2 + b^2 = a^2 + 2abi - b^2 - 2a^2 - 2abi + a^2 + b^2 = 0.$$

Los elementos algebraicos tienen asociado un particular polinomio:

Teorema 2.2. * *Sea E/K una extensión y $\alpha \in E$ algebraico sobre K. Sea $f \in K[x]$ un polinomio mónico*[1] *que tiene a α como raíz.*

1. *Las siguientes propiedades sobre $f \in K[x]$ son equivalentes:*
   - (a) *f es irreducible;*
   - (b) *f es un divisor de cualquier polinomio no nulo en $K[x]$ que tenga a α como raíz;*
   - (c) *f es de grado mínimo entre los polinomios no nulos de $K[x]$ que tienen a α como raíz.*
2. *Existe un único $f \in K[x]$ verificando las condiciones anteriores, que es llamado* **el polinomio irreducible de α sobre K** *y es denotado por*

$$Irr(\alpha, K).$$

Demostración. (1) $(a) \Rightarrow (b)$. Sea $g \in K[x]$ tal que $g(\alpha) = 0$, si ocurriera que $f \nmid g$, sería $mcd(f, g) = 1$ y tendríamos una igualdad de polinomios en $K[x]$ de la forma $1 = uf + vg$. Evaluando en α, obtendríamos que $1 = u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = 0$, lo que es imposible. Luego ha de ser f un divisor de g.

$(b) \Rightarrow (c)$ es inmediato, pues cualquier múltiplo no nulo de f será de grado mayor o igual al de f.

$(c) \Rightarrow (a)$ Supongamos, por el contrario, que $f = gh$ donde g y h son de grado positivo y, por tanto, estrictamente menor que el de f. Como $0 = f(\alpha) = g(\alpha)h(\alpha)$, ha de ser $g(\alpha) = 0$ o $h(\alpha) = 0$. Pero ninguna de esas posibilidades puede darse en virtud de la hipótesis (c).

(2) *Existencia.* Como α es algebraico, existe al menos un polinomio de grado positivo $g \in K[x]$ tal que $g(\alpha) = 0$. Supongamos que la descomposición en irreducibles mónicos de

[1] de coeficiente líder 1, esto es de la forma $x^n + a_{n-1}x^n + \cdots + a_0$.

ese polinomio es $g = af_1^{m_1} \cdots f_r^{m_r}$. Evaluando en α, resulta que $0 = af_1(\alpha)^{m_1} \cdots f_r(\alpha)^{m_r}$, de donde, para algún i, debe ser $f_i(\alpha) = 0$ y el polinomio f_i es el que buscamos.

Unicidad. Es consecuencia inmediata de la propiedad (b). □

Ejemplo 2.3. El número real $1 + \sqrt[3]{2}$ es algebraico sobre $\mathbb{Q}$, y

$$Irr(1 + \sqrt[3]{2}, \mathbb{Q}) = x^3 - 3x^2 + 3x - 3.$$

En efecto, llamemos $\alpha = 1 + \sqrt[3]{2}$. Como $\alpha - 1 = \sqrt[3]{2}$, elevando al cubo obtenemos que $\alpha^3 - 3\alpha^2 + 3\alpha - 1 = 2$, lo que nos asegura que $\alpha = 1 + \sqrt[3]{2}$ es una raíz del polinomio $x^3 - 3x^2 + 3x - 3 \in \mathbb{Q}[x]$, que es mónico e irreducible sobre $\mathbb{Q}$ (por el criterio de Eisenstein para $p = 3$).

Ejemplo 2.4. El número real $\sqrt{5} + \sqrt[4]{5}$ es algebraico sobre $\mathbb{Q}$ y

$$Irr(\sqrt{5} + \sqrt[4]{5}, \mathbb{Q}) = x^4 - 10x^2 - 20x + 20.$$

En efecto, llamemos $\alpha = \sqrt{5} + \sqrt[4]{5}$. De las sucesivas igualdades siguientes $\alpha - \sqrt{5} = \sqrt[4]{5}$, $\alpha^2 - 2\sqrt{5}\alpha + 5 = \sqrt{5}$, $\alpha^2 + 5 = (1 + 2\alpha)\sqrt{5}$, $\alpha^4 + 10\alpha^2 + 25 = (1 + 4\alpha + 4\alpha^2)5$, $\alpha^4 - 10\alpha^2 - 20\alpha + 20 = 0$, vemos que $\sqrt{5} + \sqrt[4]{5}$ es raíz del polinomio $x^4 - 10x^2 - 20x + 20 \in \mathbb{Q}[x]$, que es mónico e irreducible (por el criterio de Eisenstein para el primo $p = 5$). Luego podemos concluir que $Irr(\sqrt{5} + \sqrt[4]{5}, \mathbb{Q}) = x^4 - 10x^2 - 20x + 20$.

El polinomio $Irr(\alpha, K)$ depende tanto de α como de K. Por ejemplo, $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ y $Irr(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$. Una útil observación general es la siguiente.

Proposición 2.5. *Dada una torre $K \leq F \leq E$, si $\alpha \in E$ es algebraico sobre K entonces α es algebraico sobre F y el polinomio $Irr(\alpha, F)$ es un divisor en $F[x]$ del polinomio $Irr(\alpha, K)$.*

Demostración. El polinomio $Irr(\alpha, K) \in F[x]$ y tiene a α como raíz. Luego α es algebraico sobre F y el polinomio $Irr(\alpha, K)$ ha de ser un múltiplo del polinomio $Irr(\alpha, F)$. □

2.2. Extensiones finitas.

Si E/K es una extensión de cuerpos, E es automáticamente un espacio vectorial sobre el cuerpo K. Esto es, los elementos de E pueden ser vistos como vectores sobre el cuerpo de escalares K, con las operaciones de suma $\alpha + \beta$, para $\alpha, \beta \in E$, y multiplicación por escalares $a\alpha$, para $a \in K$ y $\alpha \in E$, dadas por las propias operaciones de suma y multiplicación en E. Es claro que E con su adición es un grupo abeliano, y las igualdades $a(\beta + \gamma) = a\beta + a\gamma$, $(a + b)\alpha = a\alpha + b\alpha$, $(ab)\alpha = a(b\alpha)$, y $1\alpha = \alpha$ son trivialmente consecuencia de ser E un cuerpo y $K \leq E$ un subcuerpo suyo.

Una extensión E/K se dice **finita**, si E es un K-espacio vectorial finitamente generado. Recordemos que cualquier sistema de generadores finito de un espacio vectorial contiene una base, y que la cardinalidad común a todas ellas es la dimensión del espacio vectorial. Usualmente escribimos

$$[E : K]$$

para indicar la dimensión de E como espacio vectorial sobre K, al que llamamos **grado de la extensión**.

Ejemplo 2.6. $[\mathbb{C} : \mathbb{R}] = 2$, pues $1, i$ claramente forman un base de la extensión.

Proposición 2.7. *Todo extensión finita es algebraica.*

DEMOSTRACIÓN. Sea $[E : K] = n$ y $\alpha \in E$. Los elementos $1, \alpha, \alpha^2, \ldots, \alpha^n$ han de ser linealmente dependientes (hay $n+1$). Entonces existen $a_i \in K$, no todos nulos, tal que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Entonces $f(\alpha) = 0$, donde $0 \neq f = \sum_i a_i x^i \in K[x]$. □

Proposición 2.8 (Propiedad multiplicativa del grado)**.** *Sea $K \leq F \leq E$ una torre de extensiones de cuerpos*

(1) *E/K es finita si y solo si E/F y F/K son finitas. En tal caso*

$$[E : K] = [E : F]\,[F : K].$$

(2) *Si $\{\alpha_1, \ldots, \alpha_m\}$ es una base de F/K y $\{\beta_1, \ldots, \beta_n\}$ es una base de E/F, entonces $\{\alpha_i\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ es una base de E/K.*

DEMOSTRACIÓN. Supongamos primero que E/K es finita. Puesto que $K \leq F \leq E$, F es un K-subespacio vectorial de E, se sigue que F/K es finita. Además, cualquier sistema de generadores de E como K-espacio vectorial genera también a E como F-espacio vectorial, luego E/F también es finita. El resto del teorema se sigue de la demostración de la segunda parte:

Sea cualquier $\beta \in E$. Será $\beta = \sum_j z_j\beta_j$ para ciertos $z_j \in F$. Como cada z_j es expresable en la forma $z_j = \sum_i a_{ij}\alpha_i$ donde los $a_{ij} \in K$, obtenemos que $\beta = \sum_j \sum_i a_{ij}\alpha_i\beta_j$. Esto prueba que el conjunto de los productos $\alpha_i\beta_j$ generan E como K-espacio vectorial K. Para probar que son linealmente independientes, supongamos que $0 = \sum_j \sum_i a_{ij}\alpha_i\beta_j$ con $a_{ij} \in K$. Llamando $z_j = \sum_i a_{ij}\alpha_i$, tenemos que $0 = \sum_j z_j\beta_j$ donde los $z_j \in F$. Por la independencia lineal de los β_j concluimos que $z_j = 0$ para todo j, de donde, por la independencia de los α_i que $a_{ij} = 0$ para todo i y todo j. □

Una elemental inducción nos demuestra el siguiente

Corolario 2.9. *Si $K = E_0 \leq E_1 \leq \cdots \leq E_n = E$ es una torre de extensiones de cuerpos, la extensión E/K es finita si y solo si cada peldaño E_i/E_{i-1} es una extensión finita. En tal caso,*

$$[E : K] = \prod_{i=1}^{n} [E_i : E_{i-1}]$$

2.3. Extensiones algebraicas simples.

Sea E/K una extensión de cuerpos. Para cualquier elemento $\alpha \in E$, denotaremos por $K(\alpha)$ al menor subcuerpo de E que contiene a K y a α, y le llamamos el **subcuerpo generado sobre K por α**. Tal cuerpo existe y es único: es la intersección de todos los subcuerpos de E que contienen a K y a α. Si $E = K(\alpha)$, para algún α, la extensión E/K se dice **simple**, y a α un **generador** de la extensión.

Ejemplo 2.10. $\mathbb{C}/\mathbb{R}$ es una extensión simple generada por i, esto es, $\mathbb{C} = \mathbb{R}(i)$. En efecto, puesto que en $\mathbb{R}(i)$ han de estar están todos los números reales y también i, y es un subcuerpo, po tanto cerrado para multiplicación y sumas, se sigue que todo número complejo $a + bi \in \mathbb{R}(i)$.

Ejemplo 2.11. Una extensión simple admite muchos generadores, por ejemplo tenemos las igualdades de subcuerpos de $\mathbb{R}$: $\mathbb{Q}(\frac{1+\sqrt{2}}{3}) = \mathbb{Q}(1 + \sqrt{2}) = \mathbb{Q}(\sqrt{2})$.

En el siguiente teorema se describe completamente una extensión simple de un cuerpo generada por un elemento algebraico en función del polinomio irreducible del generador.

Teorema 2.12 (Estructura de las extensiones algebraicas simples)**.** * *Sea $E = K(\alpha)$ una extensión simple de de un cuerpo K generada por un elemento α algebraico sobre K. Supongamos que $f = Irr(\alpha, K)$ es de grado n. Entonces,*

(1) *La extensión E/K es finita (y por tanto algebraica).*
(2) $[E : K] = n$.
(3) *Los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, forman una base de E/K. Por tanto,*

$$E = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\},$$

donde la expresión de cada elemento de E de tal forma es única.

(4) *Todo elemento de E es expresable como $g(\alpha)$, para algún polinomio $g \in K[x]$. Si $g \in K[x]$ es cualquier polinomio tal que $g(\alpha) = \beta$, entonces la expresión de β en función de la base es*

$$\beta = r(\alpha) = \textstyle\sum_{i=0}^{n-1} c_i\alpha^i,$$

donde $r = \sum_{i=0}^{n-1} c_i x^i$ es el resto de dividir g entre f.

(5) *Si $g, h \in K[x]$ son polinomios tal que $g(\alpha) = \beta$ y $h(\alpha) = \gamma$, entonces*

$$\begin{cases} \beta + \gamma = (g + h)(\alpha), \\ \beta\gamma = (gh)(\alpha). \end{cases}$$

Además, si $0 \neq \beta = g(\alpha)$, existen polinomios $u, v \in K[x]$ tal que $1 = gu + fv$ y se verifica que

$$\beta^{-1} = u(\alpha).$$

Demostración. Sea $F = \{g(\alpha) \mid g \in K[x] \subseteq E$. Observemos que F es un subcuerpo de E: Si $\beta = g(\alpha)$ y $\gamma = h(\alpha)$, para ciertos $g, h \in K[x]$, entonces $\beta + \gamma = g(\alpha) + h(\alpha) = (g + h)(\alpha) \in F$ y $\beta\gamma = g(\alpha)h(\alpha) = (gh)(\alpha) \in F$. Así que F es cerrado para sumas y productos. Claramente contiene a 0 y a 1 (pues $0 = 0(\alpha)$ y $1 = 1(\alpha)$), y es cerrado para opuestos, pues si $\beta = g(\alpha)$, entonces $-\beta = (-g)(\alpha))$. Veamos finalmente que es cerrado para inversos: Supongamos que $0 \neq \beta = g(\alpha)$. Entonces $f \nmid g$ en $K[x]$ y, al ser f es irreducible, $1 = mcd(g, f)$. Por el Teorema de Bezout, existen $u, v \in K[x]$ tal que $1 = gu + fv$, lo que nos asegura que $1 = g(\alpha)u(\alpha) = \beta\, u(\alpha)$; esto es $\beta^{-1} = u(\alpha) \in F$.

Tenemos pues que $F \leq E$ es un subcuerpo. Además $K \leq F$, pues para todo $a \in K$, $a = a(\alpha)$, y $\alpha \in F$, pues $\alpha = x(\alpha)$; luego $E = K(\alpha) \leq F$. Así que $F = E$.

Observemos ahora que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de E/K: Estos elementos son linealmente independientes, pues en otro caso existirían elementos $b_i \in K$, no todos nulos, tal que $b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Pero esto indica que α es raíz del polinomio $b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in K[x]$ cuyo grado es menor que el del polinomio irreducible de α sobre K, lo que es imposible. Finalmente vemos que es un sistema de generadores de E como espacio vectorial sobre K: Sea $\beta \in E$. Será $\beta = g(\alpha)$ para algún $g \in K[x]$. Dividiendo g entre f en $K[x]$, si q es el cociente y r el resto, será $g = fq + r$ donde $r = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, para ciertos $c_i \in K$. Pero entonces

$$\beta = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

Nota. Del teorema anterior se deduce que una extensión simple $K(\alpha)$ generada por un elemento algebraico α, está completamente determinada por el polinomio $f = Irr(\alpha, K)$, pues conocemos como describir sus diferentes elementos y como estos se suman y se multiplican. Podemos expresar esto con otras palabras: Si : $K[x] \to K(\alpha)$, $g \mapsto g(\alpha)$, es el homomorfismo de evaluación en α, este es sobreyectivo (por (4)) y su núcleo es precisamente el ideal principal de $K[x]$ de los múltiplos de f. El Primer Teorema de Isomorfía, nos determina un isomorfismo

$$K[x]/f \cong K(\alpha), \quad [g] \mapsto g(\alpha).$$

Ejemplo 2.13. Puesto que $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, se tiene que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, que $\{1, \sqrt{2}\}$ es una base de la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, y que

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}.$$

Ejemplo 2.14. Puesto que $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, se tiene que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, que $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es una base, y

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

Si queremos expresar en función de esta base, por ejemplo, el elemento $(\sqrt[3]{4} - 1)^{-1}$, podemos proceder así: Consideramos el polinomio $x^2 - 1$ (que al evaluar en $\sqrt[3]{2}$ nos da el elemento $\sqrt[3]{4} - 1$ del cual queremos calcular el inverso). Por el algoritmo de Euclides, obtenemos que

$$3 = -(x + 2)(x^3 - 2) + (x^2 - 1)(x^2 + 2x + 1),$$

de donde, evaluando en $\sqrt[3]{2}$, obtenemos

$$3 = (\sqrt[3]{4} - 1)(\sqrt[3]{4} + 2\sqrt[3]{2} + 1).$$

En definitiva,

$$(\sqrt[3]{4} - 1)^{-1} = \frac{1}{3}\sqrt[3]{4} + \frac{2}{3}\sqrt[3]{2} + \frac{1}{3}.$$

Supongamos ahora que queremos expresar en función de la base el número real

$$(1 - \sqrt[3]{2} + \sqrt[3]{[4]})^3.$$

Podríamos proceder así: Consideramos el polinomio $(1 - x + x^2)^3 = x^6 - 3x^5 + 6x^4 - 7x^3 + 6x^2 - 3x + 1$. Lo dividimos entre $x^3 - 2$ y obtenemos $x^3 - 3x^2 + 6x - 5$ como cociente y $9x - 9$ como resto. Esto es, la igualdad

$$(1 - x + x^2)^3 = (x^3 - 2)(x^3 - 3x^2 + 6x - 5) + 9x - 9,$$

que, evaluando en $\sqrt[3]{2}$ nos dice que

$$(1 - \sqrt[3]{2} + \sqrt[3]{[4]})^3 = 9\sqrt[3]{2} - 9.$$

Supongamos ahora que queremos expresar en función de la base el número real

$$(1 - \sqrt[3]{2} + \sqrt[3]{4})(\sqrt[3]{2} + \sqrt[3]{4}).$$

Podríamos hacerlo así: Consideramos el polinomio $(1 - x + x^2)(x + x^2) = x^4 + x$; lo dividimos entre $x^3 - 2$ y obtenemos la igualdad $(1 - x + x^2)(x + x^2) = (x^3 - 2)x + 3x$; y si evaluamos en $\sqrt[3]{2}$ obtenemos que

$$(1 - \sqrt[3]{2} + \sqrt[3]{4})(\sqrt[3]{2} + \sqrt[3]{4}) = 3\sqrt[3]{2}.$$

Aunque también podríamos haberlo hecho, en este caso, usando simples propiedades de cálculo con radicales:

$$(1-\sqrt[3]{2}+\sqrt[3]{4})(\sqrt[3]{2}+\sqrt[3]{4}) = \sqrt[3]{2}-\sqrt[3]{4}+2+\sqrt[3]{4}-2+2\sqrt[3]{2} = 3\sqrt[3]{2}.$$

□

2.4. **Extensiones algebraicas finitamente generadas.**

Sea E/K una extensión de cuerpos. Para cualesquiera elementos $\alpha_1, \ldots, \alpha_r \in E$, denotaremos por $K(\alpha_1, \ldots, \alpha_r)$ al menor subcuerpo de E que contiene a K y a todos los α_i, $i = 1, \ldots, r$, y le llamamos el **subcuerpo generado sobre** K **por** $\alpha_1, \ldots, \alpha_r$. Tal cuerpo existe y es único: es la intersección de todos los subcuerpos de E que contienen a K y a los α_i. Si $E = K(\alpha_1, \ldots, \alpha_r)$ para ciertos $\alpha_i \in E$, la extensión E/K se dice **finitamente generada**.

Teorema 2.15. *Para E/K una extensión de cuerpos, son equivalentes*

(1) *La extensión es finita.*
(2) *La extensión es algebraica y finitamente generada.*
(3) *La extensión es finitamente generada por elementos algebraicos.*

Demostración. (1) ⇒ (2): Sabemos que toda extensión finita es algebraica. Además, si $\alpha_1, \ldots, \alpha_r$ es una base de E/K, es claro que $E = K(\alpha_1, \ldots, \alpha_r)$.

(2) ⇒ (3): Es obvio.

(3) ⇒ (1): Sea $E = K(\alpha_1, \ldots, \alpha_n)$, donde los α_i son algebraicos sobre K. Hagamos inducción en n. Si $n = 1$, el hecho está probado en el teorema anterior. Suponiendo $n > 1$, y bajo hipótesis de inducción, llamemos $F = K(\alpha_1, \ldots, \alpha_{n-1})$. Entonces tenemos la torre $K \leq F \leq E$, donde F/K es finita. Además $E = F(\alpha_n)$ donde α_n sabemos por hipótesis que es raíz de un polinomio no nulo con coeficientes en K y por tanto en F; esto es, α_n es algebraico sobre F. Luego E/F es finita. Por la transitividad de las extensiones finitas, E/K es finita. □

Corolario 2.16. *Sea E/K una extensión de cuerpos. Si $\alpha, \beta \in E$ son algebraicos sobre K, entonces $-\alpha$, $\alpha+\beta$, $\alpha\beta$ y, si $\alpha \neq 0$, α^{-1} son todos algebraicos sobre K.*

Demostración. La subextension $K(\alpha, \beta)/K$ es finita, luego algebraica. □

En general, manejar extensiones finitamente generadas es algo más complicado que el caso de extensiones simples. Para su tratamiento, lo más útil suele ser el mirar a una tal extensión $E = K(\alpha_1, \cdots, \alpha_r)/K$ como el extremo de una torre de extensiones simples

$$K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) \leq \cdots \leq K(\alpha_1, \cdots, \alpha_{r-1}) \leq K(\alpha_1, \cdots, \alpha_r) = E$$

y estudiar cada eslabón de la cadena.

Ejemplo 2.17. Consideremos la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Es finita, pues es finitamente generada por elementos algebraicos. Tenemos una torre de extensiones

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

donde cada eslabón es una extensión simple, ya que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. Hemos visto antes que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ y que $\{1, \sqrt{2}\}$ es una base de esta extensión. Notemos ahora que $\sqrt{3}$ es raíz del polinomio $x^2 - 3 \in \mathbb{Q}[x] \leq \mathbb{Q}(\sqrt{2})[x]$, por tanto el polinomio

$Irr(\sqrt{3}, \mathbb{Q}(\sqrt{2}))$ es un divisor de $x^2 - 3$, así que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Pero necesariamente ha de ser $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, pues en otro caso sería 1 lo que significaría que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})$, esto es, que $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Pero en tal caso existirían racionales $a, b \in \mathbb{Q}$ de tal manera que $\sqrt{3} = a + b\sqrt{2}$, lo que, elevando al cuadrado, nos llevaría a que $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ y, necesariamente entonces a que $2ab = 0$, $3 = a^2 + 2b^2$. Si $a = 0$, sería $3 = 2b^2$ y b raíz del polinomio $2x^2 - 3$, pero este polinomio es irreducible sobre $\mathbb{Q}$ por el criterio de Eisenstein y no tiene raíces en $\mathbb{Q}$. Análogamente, si es $b = 0$, sería $3 = a^2$ y a una raíz racional del polinomio $x^2 - 3$, lo que es imposible pues este polinomio es irreducible sobre $\mathbb{Q}$. Concluimos entonces que $Irr(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$ y, entonces, que una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{2})$ es $\{1, \sqrt{3}\}$. En definitiva, tenemos que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ como espacio vectorial racional. En conclusión, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ y

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ a, b, c, d \in \mathbb{Q}\}.$$

La siguiente observación es de mucha utilidad práctica.

Proposición 2.18. *Sea $K \leq F \leq E$ una torre de extensiones, donde F/K es finita, y $\alpha \in E$ un elemento algebraico sobre K tal que el grado del polinomio $Irr(\alpha, K)$ es primo relativo con el grado $[F : K]$. Entonces, $Irr(\alpha, K) = Irr(\alpha, F)$.*

Demostración. Supongamos que $[F : K] = m$ y que $Irr(\alpha, K)$ es de grado n. Es claro que $Irr(\alpha, F)$ es un divisor en $F[x]$ del polinomio $Irr(\alpha, K)$ y, en particular, de grado menor o igual. Se trata de ver que son del mismo grado y, por tanto, el mismo polinomio. Consideremos la torre $K \leq F \leq F(\alpha)$. Puesto que $[F(\alpha) : F] = gr(Irr(\alpha, F)) \leq n$, tendremos que

$$[F(\alpha) : K] = [F : K] \cdot [F(\alpha) : F] = m \cdot gr(Irr(\alpha, F)) \leq m \cdot n.$$

De manera que el número $[F(\alpha) : K]$ ha de ser un múltiplo de m y $\leq mn$. Por otra parte, Considerando la torre $K \leq K(\alpha) \leq F(\alpha)$, vemos que $[F(\alpha) : K] = [K(\alpha) : K] \cdot [F(\alpha) : K(\alpha)] = n \cdot [F(\alpha) : K(\alpha)]$ es también un múltiplo de n. Pero entonces resulta que $[F(\alpha) : K]$ es múltiplo del $mcm(m, n) = mn$ y menor o igual que mn. Necesariamente es $[F(\alpha) : K] = mn$ y entonces $gr(Irr(\alpha, F)) = n$.

Ejemplo 2.19. Consideremos la extensión $\mathbb{Q}(\sqrt[3]{5}, \sqrt{2})/\mathbb{Q}$. Tenemos la torre la torre $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{5}) \leq \mathbb{Q}(\sqrt[3]{5}, \sqrt{2})$. La primera extensión es simple con $Irr(\sqrt[3]{5}, \mathbb{Q}) = x^3 - 5$, de manera que es de grado 3 y $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ es una base. Puesto que $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ y $mcd(2, 3) = 1$, por la proposición anterior, conocemos que también $Irr(\sqrt{2}, \mathbb{Q}(\sqrt[3]{5}) = x^2 - 2$ y la segunda extensión es de grado 2 con $\{1, \sqrt{2}\}$ una base de la misma. Entonces, la extensión $\mathbb{Q}(\sqrt[3]{5}, \sqrt{2})/\mathbb{Q}$ es de grado 6, con base

$$\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}, \sqrt[3]{5}\sqrt{2}, \sqrt[3]{25}\sqrt{2}\}.$$

Queremos ahora expresar en función de ella el elemento $(\sqrt[3]{5}+\sqrt{2})^{-1}$. Para ello, vamos a utilizar de nuevo la torre $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{5}) \leq \mathbb{Q}(\sqrt[3]{5}, \sqrt{2})$ y, en primera instancia expresaremos $(\sqrt[3]{5} + \sqrt{2})^{-1}$ como combinación lineal de $\{1, \sqrt{2}\}$ con coeficientes en $\mathbb{Q}(\sqrt[3]{5})$ y, después expresaremos cada coeficiente de esa combinación en la base $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ de la extensión $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$:

Para la primera cuestión, consideramos el polinomio $x+\sqrt[3]{5}$ (que al ser evaluado en $\sqrt{2}$ nos da el número del cual queremos calcular el inverso). Aplicamos entonces el algoritmo extendido de Euclides a los polinomios x^2-2 y $x+\sqrt[3]{5}$,obteniendo la igualdad

$$\sqrt[3]{25}-2=(x^2-2)+(x+\sqrt[3]{5})(\sqrt[3]{5}-x),$$

de donde, por evaluación en $\sqrt{2}$, deducimos que $\sqrt[3]{25}-2=(\sqrt{2}+\sqrt[3]{5})(\sqrt[3]{5}-\sqrt{2})$. Así que

$$(\sqrt[3]{5}+\sqrt{2})^{-1}=(\sqrt[3]{25}-2)^{-1}(\sqrt[3]{5}-\sqrt{2}).$$

Calculamos ahora el inverso de $\sqrt[3]{25}-2$ en $\mathbb{Q}(\sqrt[3]{5})$ en su base natural $\{1,\sqrt[3]{5},\sqrt[3]{25}\}$. Para ello, consideramos el polinomio x^2-2 y, utilizando de nuevo el algoritmo extendido de Euclides, obtenemos que

$$\frac{17}{4}=-\left(\frac{1}{2}x+\frac{5}{4}\right)(x^3-5)+\left(\frac{1}{2}x^2+\frac{5}{4}x+1\right)(x^2-2).$$

Evaluando en $\sqrt[3]{5}$, obtenemos que

$$\frac{17}{4}=\left(\frac{1}{2}\sqrt[3]{25}+\frac{5}{4}\sqrt[3]{5}+1\right)(\sqrt[3]{25}-2),$$

de donde

$$(\sqrt[3]{25}-2)^{-1}=\frac{2}{17}\sqrt[3]{25}+\frac{5}{17}\sqrt[3]{5}+\frac{4}{17}.$$

En conclusión,

$$\begin{aligned}(\sqrt[3]{5}+\sqrt{2})^{-1}&=(\sqrt[3]{5}-\sqrt{2})\left(\frac{2}{17}\sqrt[3]{25}+\frac{5}{17}\sqrt[3]{5}+\frac{4}{17}\right)\\&=\frac{10}{17}+\frac{4}{17}\sqrt[3]{5}+\frac{5}{17}\sqrt[3]{25}-\frac{4}{17}\sqrt{2}-\frac{5}{17}\sqrt[3]{5}\sqrt{2}-\frac{2}{17}\sqrt[3]{25}\sqrt{2}\,.\end{aligned}$$

□

La siguientes observaciones nos será de utilidad en el siguiente capítulo.

Lema 2.20. *Sea $E=K(\alpha_1,\ldots,\alpha_n)$ una extensión finita generada por elementos algebraicos $\alpha_1,\ldots,\alpha_n$. Si dos homomorfismos de cuerpos $\sigma,\sigma':E\to E'$ son tales que $\sigma|_K=\sigma'|_K$ y $\sigma(\alpha_i)=\sigma'(\alpha_1)$ para $i=1,\ldots n$, entonces $\sigma=\sigma'$.*

Demostración. Procedemos por inducción en r. Supongamos primero que $r=1$, esto es, que $E=K(\alpha)$ una extensión simple generada por un elemento algebraico α. Si r es el grado del polinomio $Irr(\alpha,K)$, cada elemento $\beta\in E$ se expresa de la forma $\beta=\sum_{i=0}^{r-1}a_i\alpha^i$, donde $a_i\in K$. Tenemos entonces que

$$\sigma(\beta)=\sum_i\sigma(a_i)\sigma(\alpha)^i=\sum_i\sigma'(a_i)\sigma'(\alpha)^i=\sigma'(\beta)$$

y $\sigma=\sigma'$. Supongamos ahora que $n>1$. Sea $F=K(\alpha_1,\ldots,\alpha_{r-1})$. Por hipótesis de inducción será $\sigma|_F=\sigma'|_F$. Como $E=F(\alpha_r)$, la conclusión $\sigma=\sigma'$ sigue por el caso $n=1$ antes visto. □

Lema 2.21. *Sea $E=K(\alpha_1,\ldots,\alpha_n)$ una extensión finita generada por elementos algebraicos $\alpha_1,\ldots,\alpha_r$. Si $\sigma:E\to F$ es un homomorfismo de cuerpos, entonces*

$$\sigma(E)=\sigma(K)(\sigma(\alpha_1),\ldots,\sigma(\alpha_n))\,.$$

Demostración. Hacemos inducción sobre el número de generadores de la extensión. Supongamos $n = 1$, o sea $E = K(\alpha)$ una extensión simple algebraica. El cuerpo $\sigma(E)$ contiene a $\sigma(K)$ y a $\sigma(\alpha)$ y por tanto al cuerpo $\sigma(K)(\sigma(\alpha))$. Para la inclusión recíproca, supongamos que $Irr(\alpha, K)$ es de grado r. Sabemos entonces que $\{1, \alpha, \ldots, \alpha^{r-1}\}$ es una base de E como espacio vectorial sobre K, por tanto cualquier elemento β de este cuerpo es expresable de la forma $\beta = \sum a_i \alpha^i$, con los $a_i \in K$. Pero entonces $\sigma(\beta) = \sigma(\sum a_i \alpha^i) = \sum \sigma(a_i)\sigma(\alpha)^i \in \sigma(K)(\sigma(\alpha))$. El resto de la demostración se sigue entonces por inducción:

$$\begin{aligned}\sigma(E) &= \sigma(K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)) = \sigma(K(\alpha_1, \ldots, \alpha_{n-1}))(\sigma(\alpha_n)) \\ &= \sigma(K)(\sigma(\alpha_1), \ldots, \sigma(\alpha_{n-1}))(\sigma(\alpha_n)) = \sigma(K)(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)).\end{aligned}$$

□

ALGEBRA III (Doble grado Informática-Matemáticas)

3. Teoría de Galois

En todo lo que sigue, trabajaremos con **cuerpos de números**, esto es, con subcuerpos del cuerpo $\mathbb{C}$ de los números complejos, como $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}$, o el propio $\mathbb{C}$. A continuación empezaremos a familiarizarnos con otros cuerpos de números, que surgen de forma natural asociados a ecuaciones polinómicas. De momento, simplemente observemos que **cualquier cuerpo de números es extensión del cuerpo $\mathbb{Q}$ de los racionales**: Si K es un tal cuerpo de números, como $1 \in K$, se sigue por una obvia inducción que $\mathbb{N} \leq K$, y como K es cerrado para opuestos, que $\mathbb{Z} \leq K$. Si $\frac{n}{m} \in \mathbb{Q}$ es cualquier número racional, entonces $\frac{n}{m} = nm^{-1} \in K$, puesto que K es cerrado para productos e inversos. Luego $\mathbb{Q} \leq K$.

3.1. Inmersiones complejas.

En este capítulo, usaremos la siguiente terminología sobre inmersiones de cuerpos números en el cuerpo $\mathbb{C}$ de los complejos.

Sea E/K una extensión de cuerpos de números. Si $\tau : K \to \mathbb{C}$ es una inmersión dada, llamamos **τ-inmersión** de E en $\mathbb{C}$, a toda inmersión $\sigma : E \to \mathbb{C}$ tal que $\sigma(a) = \tau(a)$ para todo $a \in K$; esto es, tal que $\sigma|_K = \tau$. Usualmente también nos referimos a σ como una **extensión de** τ a E, y representamos la relación entre σ y τ por el diagrama

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & \mathbb{C} \\ {\scriptstyle in}\uparrow & \nearrow_{\tau} & \\ K & & \end{array}$$

donde $in : K \to E$ es la inmersión de inclusión, $a \mapsto a$. Cuando $\tau = in$, a las τ-inmersiones usualmente las llamamos **K-inmersiones**; esto es, una K-inmersión $\sigma : E \to \mathbb{C}$ es una inmersión tal que tal que $\sigma(a) = a$ para todo $a \in K$ (o, en otros términos, tal que $\sigma|_K = id_K$).

Ejemplo 1. Si E es cualquier cuerpo de números, **toda inmersión $\sigma : E \to \mathbb{C}$ es una $\mathbb{Q}$-inmersión**: Como $\sigma(1) = 1$, por inducción vemos que $\sigma(n) = n$ para todo $n \in \mathbb{N}$, y como σ preserva opuestos, vemos que $\sigma(n) = n$ para todo $n \in \mathbb{Z}$. Como preserva productos e inverso, también preserva los racionales

$$\sigma(\tfrac{n}{m}) = \sigma(nm^{-1}) = \sigma(n)\sigma(m)^{-1} = mn^{-1} = \tfrac{n}{m}.$$

Ejemplo 2. La aplicación $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ definida por $\sigma(a+b\sqrt{2}) = a-b\sqrt{2}$, donde $a, b \in \mathbb{Q}$, es una $\mathbb{Q}$-inmersión compleja del cuerpo $\mathbb{Q}(\sqrt{2})$. En efecto, es inmediato que sigma respeta sumas, el 0 y el 1, y también productos:

$$\begin{aligned} \sigma\big((a+b\sqrt{2})(c+d\sqrt{2})\big) &= \sigma\big(ac+2bd+(ad+bc)\sqrt{2}\big) = ac+2bd-(ad+bc)\sqrt{2} \\ &= (a-b\sqrt{2})(c-d\sqrt{2}) = \sigma(a+b\sqrt{2})\sigma(c+d\sqrt{2}). \end{aligned}$$

El siguiente teorema es clave para determinar las diferentes τ-inmersiones complejas de una extensión finita de cuerpos de números E/K. Resaltemos primero que, si K es un cuerpo de números, cada inmersión $\tau : K \to \mathbb{C}$ nos determina un monomorfismo de anillos

$$K[x] \to \mathbb{C}[x], \quad f = \sum a_i x^i \mapsto f^\tau = \sum \tau(a_i) x^i,$$

y se verifica que

Lema 3. *Sea K un cuerpo de números y $\tau : K \to \mathbb{C}$ una inmersión compleja. Sea E/K una extensión de cuerpos de números y $\sigma : E \to \mathbb{C}$ una τ-inmersión. Para cualquier $\alpha \in E$ y cualquier polinomio $f \in K[x]$ se verifica que*

$$\sigma(f(\alpha)) = f^\tau(\sigma(\alpha)).$$

En particular, si $\alpha \in E$ es raíz de un polinomio $f \in K[x]$, entonces $\sigma(\alpha)$ es raíz de f^τ.

Demostración. Supongamos $f = \sum a_i x^i$. Entonces,

$$f^\tau(\sigma(\alpha)) = \sum \tau(a_i)\sigma(\alpha)^i = \sum \sigma(a_i)\sigma(\alpha)^i = \sigma\Big(\sum a_i \alpha^i\Big) = \sigma(f(\alpha)). \quad \square$$

Corolario 4. *Sea E/K una extensión de cuerpos de números y $\sigma : E \to \mathbb{C}$ una K-inmersión. Si $\alpha \in E$ es raíz de un polinomio $f \in K[x]$, entonces $\sigma(\alpha)$ también es raíz de f.*

El siguiente teorema nos dice como "construir" las diferentes τ-inmersiones de una extensión simple algebraica.

Teorema 5. * *Sea K un cuerpo de números y $\tau : K \to \mathbb{C}$ una inmersión compleja. Sea $\alpha \in \mathbb{C}$ un número complejo algebraico sobre K, y supongamos que $f = Irr(\alpha, K)$ y es de grado n. Entonces,*

1. *El polinomio f^τ tiene n raíces complejas distintas.*
2. *Si $\beta_1, \ldots, \beta_n$ son las raíces de f^τ en $\mathbb{C}$, entonces para cada i, con $1 \le i \le n$, existe una única τ-inmersión compleja $\sigma_i : K(\alpha) \to \mathbb{C}$ tal que $\sigma_i(\alpha) = \beta_i$.*
3. *Estas $\sigma_1, \ldots, \sigma_n : K(\alpha) \to \mathbb{C}$ listan todas las τ-inmersiones complejas de $K(\alpha)$.*
4. *El número de diferentes τ-inmersiones complejas de $K(\alpha)$ coincide con el grado $[K(\alpha) : K]$ de la extensión.*

Demostración. (1) Denotemos $K' = \tau(K)$, el subcuerpo de $\mathbb{C}$ imagen de K por τ. Puesto que $\tau : K \cong K'$ es un isomorfismo de cuerpos, este determina un isomorfismo entre los correspondientes anillos de polinomios $K[x] \cong K'[x]$, $g \mapsto g^\tau$. En particular, como f es irreducible en $K[x]$, f^τ es irreducible en $K'[x]$ y, por tanto, no tiene raíces múltiples en $\mathbb{C}$ (claramente el polinomio derivado de un polinomio de grado ≥ 1 con coeficientes en $\mathbb{C}$ es no nulo).

(2) Sea $\beta = \beta_i$ una cualquiera de las raíces del polinomio f^τ. Conocemos que cada elemento $u \in K(\alpha)$ se expresa en la forma $u = g(\alpha)$, con $g \in K[x]$. Definimos

$$\sigma(u) = g^\tau(\beta).$$

Esto es, si $u = \sum a_i \alpha^i$, entonces $\sigma(\alpha) = \sum \tau(a_i)\beta^i$.

Veamos que está bien definida: Si $u = h(\alpha)$ para un otro polinomio $h \in K[x]$, entonces $(g-h)(\alpha) = u-u = 0$ y $f|(g-h)$. Esto es, $g-h = fq$ para cierto $q \in K[x]$. Pero entonces

$$\begin{aligned} g^\tau(\beta) - h^\tau(\beta) &= (g^\tau - h^\tau)(\beta) = (g-h)^\tau(\beta) = (fq)^\tau(\beta) \\ &= (f^\tau g^\tau)(\beta) = f^\tau(\beta)\, q^\tau(\beta) = 0\ q^\tau(\beta) = 0 \end{aligned}$$

y vemos que $g^\tau(\beta) = h^\tau(\beta)$.

Claramente $\sigma|_K = \tau$ (en particular, $\sigma(0) = 0$ y $\sigma(1) = 1$) y $\sigma(\alpha) = \beta$. Veamos que respeta sumas y productos: Sean $u = g(\alpha)$ y $v = h(\alpha)$, para ciertos polinomios $g, h \in K[x]$, dos elementos de $K(\alpha)$; entonces $u + v = (g+h)(\beta)$, $uv = (gh)(\beta)$ y

$$\begin{cases} \sigma(u+v) = (g+h)^\tau(\beta) = (g^\tau + h^\tau)(\beta) = g^\tau(\beta) + h^\tau(\beta) = \sigma(u) + \sigma(v), \\ \sigma(uv) = (gh)^\tau(\beta) = (g^\tau h^\tau)(\beta) = g^\tau(\beta)\ h^\tau(\beta) = \sigma(u)\sigma(v). \end{cases}$$

Así que $\sigma : K(\alpha) \to \mathbb{C}$ es una τ-inmersión con $\sigma(\alpha) = \beta$; y es la única, pues si $\sigma' : K(\alpha) \to \mathbb{C}$ es otra τ-inmersión con $\sigma'(\alpha) = \beta$, tendríamos que $\sigma|_K = \tau = \sigma'|_K$ y $\sigma(\alpha) = \sigma'(alpha)$ lo que sabemos implica que $\sigma = \sigma'$.

(3) Si $\sigma : K(\alpha) \to \mathbb{C}$ una supuesta τ-inmersión compleja. Entonces $\sigma(\alpha)$ será una raíz de f^τ, así que $\sigma(\alpha) = \beta_i$ para algún i y, por tanto, $\sigma = \sigma_i$.

(3) Es inmediato, pues $[K(\alpha) : K] = n$. □

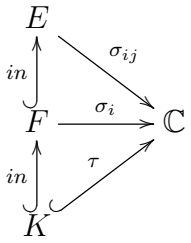
Para "construir" las diferentes τ-inmersiones de una extensión finita no simple, digamos $E = K(\alpha_1, \ldots, \alpha_r)/K$, lo más útil suele ser el mirar a una tal extensión como el extremos de una torre de extensiones simples

$$K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) \leq \cdots \leq K(\alpha_1, \cdots, \alpha_{r-1}) \leq K(\alpha_1, \cdots, \alpha_r) = E$$

y aplicar la construcción anterior a cada eslabón simple de la torre. Previamente a ilustrar esto, establecemos la siguiente observación general.

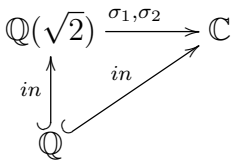
Teorema 6. *Sea E/K es una extensión finita de cuerpos de numeros y $\tau : K \to \mathbb{C}$ una inmersión. Si $[E : K] = n$, existen exactamente n diferentes τ-inmersiones $\sigma : E \to \mathbb{C}$.*

Demostración. La extensión es finitamente generada, supongamos que $E = K(\alpha_1, \ldots, \alpha_r)$ y procedemos por inducción en $r \geq 1$. El caso $r = 1$ está explícito en el teorema anterior. Supongamos $r \geq 2$ y consideremos $F = K(\alpha_1, \ldots, \alpha_{r-1})$, de manera que tenemos la torre de extensiones finitas $K \leq F \leq E$, donde $E = F(\alpha_r)$. Sea $[F : K] = p$ y $[E : F] = q$, de manera que $n = pq$. Por hipótesis de inducción existen exactamente p diferentes τ-inmersiones complejas $\sigma_1, \ldots, \sigma_p : F \to \mathbb{C}$. Por al caso $r = 1$, para cada $i = 1, \ldots, p$, existen exactamente q diferentes σ_i-inmersiones, $\sigma_{i1}, \ldots, \sigma_{iq} : E \to \mathbb{C}$. Todas estas listan $pq = n$ diferentes τ-inmersiones $\sigma_{ij} : E \to \mathbb{C}$.



Y no hay más: si $\sigma : E \to \mathbb{C}$ es cualquier supuesta τ-inmersión, su restricción $\sigma|_F : F \to \mathbb{C}$ sería una τ-inmersión y, por tanto, debe ser una de las σ_i, pero entonces σ es una σ_i-inmersión y debe ser ella misma una de las σ_{ij}. □

Ejemplo 7. *(a)* Consideremos la extensión simple $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Queremos determinar las $\mathbb{Q}$-inmersiones complejas de $\mathbb{Q}(\sqrt{2})$. La inmersión a extender es por tanto la inclusión $\tau = in : \mathbb{Q} \to \mathbb{C}$. Como $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, la extensión es de grado dos, con base $\{1, \sqrt{2}\}$, y habrá exactamente dos $\mathbb{Q}$-inmersiones complejas de $\mathbb{Q}(\sqrt{2})$



que estarán en correspondencia con las raíces complejas del polinomio

$$(x^2 - 2)^{in} = x^2 - 2.$$

Como las raíces de este polinomio son $\pm\sqrt{2}$, las dos $\mathbb{Q}$-inmersiones resultan caracterizadas por que $\sigma_1(\sqrt{2}) = \sqrt{2}$ y $\sigma_2(\sqrt{2}) = -\sqrt{2}$, información que podemos sintetizar en el cuadro

$$\begin{array}{r|c|c} & \sigma_1 & \sigma_2 \\ \hline \sqrt{2} \mapsto & \sqrt{2} & -\sqrt{2} \end{array},$$

y que explícitamente, están dadas por

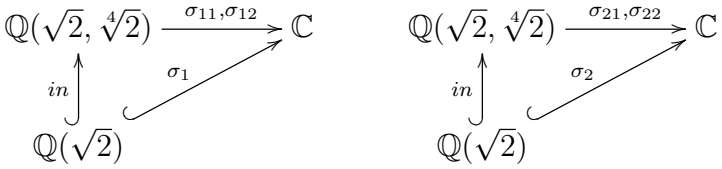
$$\begin{cases} \sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}, \\ \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}. \end{cases}$$

Notemos que σ_1 es simplemente la inclusión $in : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$.

(b) Consideremos ahora la extensión $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$, y queremos determinar las σ_1-inmersiones ($= \mathbb{Q}(\sqrt{2})$-inmersiones) y las σ_2-inmersiones.

La extensión es de grado 2, con $Irr(\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})) = x^2 - \sqrt{2}$ y $\{1, \sqrt[4]{2}\}$ una base: En efecto, $\sqrt[4]{2}$ es raíz del polinomio $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ y la extensión será por tanto de grado 1 o 2. Pero si la suponemos de grado 1, sería $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt{2})$ que es tanto como decir que $\sqrt[4]{2} \in \mathbb{Q}\sqrt{2}$, lo que es falso: En otro caso sería $\sqrt[4]{2} = a + b\sqrt{2}$ para ciertos $a, b \in \mathbb{Q}$. Elevando al cuadrado, sería $\sqrt{2} = a^2 + 2b^2 + 2ab\sqrt{2}$; o sea

que $a^2+2b^2=0$ y $2ab=1$. Lo primero obliga a que $a=0=b$ y concluiríamos que $1=0$. Luego habrá dos σ_1-inmersiones y otras dos σ_2-inmersiones



Para conocer las σ_1-inmersiones, debemos determinar las raíces del polinomio

$$(x^2-\sqrt{2})^{\sigma_1}=x^2-\sqrt{2},$$

que son $\pm\sqrt[4]{2}$. Por tanto, las dos σ_1-inmersiones $\sigma_{11},\sigma_{12}:\mathbb{Q}(\sqrt{2},\sqrt[4]{2})\to\mathbb{C}$ son las determinadas por que la imagen del generador es la indicada en el cuadro

	σ_{11}	σ_{12}
$\sqrt[4]{2}\mapsto$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$

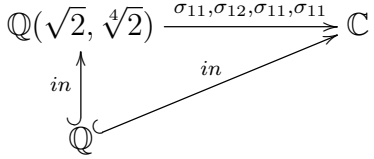
Para conocer las σ_2-inmersiones, debemos determinar las raíces del polinomio

$$(x^2-\sqrt{2})^{\sigma_2}=x^2+\sqrt{2},$$

que son $\pm i\sqrt[4]{2}$. Por tanto, las dos σ_2-inmersiones $\sigma_{21},\sigma_{22}:\mathbb{Q}(\sqrt{2},\sqrt[4]{2})\to\mathbb{C}$ son las determinadas por que la imagen del generador es la indicada en el cuadro

	σ_{21}	σ_{22}
$\sqrt[4]{2}\mapsto$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$

(c) Consideremos ahora la extensión $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})/\mathbb{Q}$, y queremos determinar las $\mathbb{Q}$-inmersiones complejas de $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})$. Puesto que la extensión es de grado 4, habrá 4. Pero entonces ya las tenemos todas descritas por el apartado anterior: Son las inmersiones



cuyos respectivos efectos sobre los generadores son indicados en el cuadro

	σ_{11}	σ_{12}	σ_{21}	σ_{22}
$\sqrt{2}\mapsto$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\sqrt[4]{2}\mapsto$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$

Podemos ser más explícitos. Una base de $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es $\{1,\sqrt{2}\}$ y una base de $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ es $\{1,\sqrt[4]{2}\}$, luego una base de $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})/\mathbb{Q}$ es $\{1,\sqrt{2},\sqrt[4]{2},\sqrt{2}\sqrt[4]{2}\}$ y

$$\begin{cases}\sigma_{11}(a+b\sqrt{2}+c\sqrt[4]{2}+d\sqrt{2}\sqrt[4]{2}) &= a+b\sqrt{2}+c\sqrt[4]{2}+d\sqrt{2}\sqrt[4]{2},\\ \sigma_{12}(a+b\sqrt{2}+c\sqrt[4]{2}+d\sqrt{2}\sqrt[4]{2}) &= a+b\sqrt{2}-c\sqrt[4]{2}-d\sqrt{2}\sqrt[4]{2},\\ \sigma_{21}(a+b\sqrt{2}+c\sqrt[4]{2}+d\sqrt{2}\sqrt[4]{2}) &= a-b\sqrt{2}+c\sqrt[4]{2}\,i-d\sqrt{2}\sqrt[4]{2}\,i,\\ \sigma_{22}(a+b\sqrt{2}+c\sqrt[4]{2}+d\sqrt{2}\sqrt[4]{2}) &= a-b\sqrt{2}-c\sqrt[4]{2}\,i+d\sqrt{2}\sqrt[4]{2}\,i.\end{cases}$$

Notemos que $\sigma_{11} = in : \mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) \to \mathbb{C}$, es la inclusión.

(d) La anterior conclusión podríamos haberla obtenido de forma más directa si hubieramos observado previamente que $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$ (ya que $\sqrt{2} = (\sqrt[4]{2})^2 \in \mathbb{Q}(\sqrt[4]{2})$) y hubiéramos seguido el procedimiento usual para las extensiones simples: Tenemos que $Irr(\sqrt[4]{2}, \mathbb{Q}) = x^4 - 2$ y $(x^4 - 2)^{in} = x^4 - 2$, cuyas raíces en $\mathbb{C}$ son $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. Luego hay 4 $\mathbb{Q}$-inmersiones $\tau_i : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{C}$ que están determinadas por que la imagen del generador es la indicada en el cuadro

	τ_1	τ_2	τ_3	τ_4
$\sqrt[4]{2} \mapsto$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$

Así que $\tau_1 = \sigma_{11}$= inclusión, $\tau_2 = \sigma_{12}$, $\tau_3 = \sigma_{21}$ y $\tau_4 = \sigma_{22}$. Observar que, al ser $\sqrt{2} = (\sqrt[4]{2})^2$ el efecto de las inmersiones sobre $\sqrt{2}$ está determinado por el efecto sobre $\sqrt[4]{2}$. Así $\tau_1(\sqrt{2}) = (\sqrt[4]{2})^2 = \sqrt{2}$, $\tau_2(\sqrt{2}) = (-\sqrt[4]{2})^2 = \sqrt{2}$, $\tau_3(\sqrt{2}) = (i\sqrt[4]{2})^2 = -\sqrt{2}$ y $\tau_4(\sqrt{2}) = (-i\sqrt[4]{2})^2 = -\sqrt{2}$. Si hubiéramos determinado directamente estas τ_i, para su descripción explícita determinaríamos la base

$$\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2 = \sqrt{2}, (\sqrt[4]{2})^3 = \sqrt[4]{8} = \sqrt{2}\sqrt[4]{2}\} = \{1, \sqrt{2}, \sqrt[4]{2}, \sqrt{2}\sqrt[4]{2}\}$$

y tendríamos que, por ejemplo,

$$\begin{aligned}\tau_3(a + b\sqrt{2} + c\sqrt[4]{2} + d\sqrt{2}\sqrt[4]{2}) &= a + b\,\tau_3(\sqrt{2}) + c\,\tau_3(\sqrt[4]{2}) + d\,\tau_3(\sqrt{2})\,\tau_3(\sqrt[4]{2}) \\ &= a + b(-\sqrt{2}) + c\,i\sqrt[4]{2} + d\,(-\sqrt{2})(i\sqrt[4]{2}) \\ &= a - b\,\sqrt{2} + c\,\sqrt[4]{2}\,i - d\,\sqrt{2}\sqrt[4]{2}\,i,\end{aligned}$$

y procediendo análogamente para los otros casos podemos concluir que

$$\begin{cases} \tau_1(a + b\sqrt{2} + c\sqrt[4]{2} + d\sqrt{2}\sqrt[4]{2}) &= a + b\sqrt{2} + c\sqrt[4]{2} + d\sqrt{2}\sqrt[4]{2}, \\ \tau_2(a + b\sqrt{2} + c\sqrt[4]{2} + d\sqrt{2}\sqrt[4]{2}) &= a + b\sqrt{2} - c\sqrt[4]{2} - d\sqrt{2}\sqrt[4]{2}, \\ \tau_3(a + b\sqrt{2} + c\sqrt[4]{2} + d\sqrt{2}\sqrt[4]{2}) &= a - b\sqrt{2} + c\sqrt[4]{2}\,i - d\sqrt{2}\sqrt[4]{2}\,i, \\ \tau_4(a + b\sqrt{2} + c\sqrt[4]{2} + d\sqrt{2}\sqrt[4]{2}) &= a - b\sqrt{2} - c\sqrt[4]{2}\,i + d\sqrt{2}\sqrt[4]{2}\,i. \end{cases}$$

(e) El conocimiento de las inmersiones $\tau_i : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{C}$ proporciona información sobre otras cuestiones. Por ejemplo, considerar el número $\alpha = \sqrt{2} + \sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$. Si desarrollamos la igualdad $(\alpha - \sqrt{2})^2 = \sqrt{2}$, vemos que $\alpha^2 + 2 = \sqrt{2}(1 + 2\alpha)$ y, elevando al cuadrado, obtenemos que $\alpha^4 - 6\alpha^2 - 8\alpha + 2 = 0$. Esto es, $\sqrt{2} + \sqrt[4]{2}$ es raíz del polinomio $x^4 - 4x^2 - 8x + 2$. Pero entonces, por el Corolario 4, cada $\tau_i(\sqrt{2} + \sqrt[4]{2})$ es también raíz de $x^4 - 4x^2 - 8x + 2$. Así conocemos que las 4 raíces de $x^4 - 4x^2 - 8x + 2$ son

$$\sqrt{2} + \sqrt[4]{2},\ \sqrt{2} - \sqrt[4]{2},\ -\sqrt{2} + i\sqrt[4]{2},\ -\sqrt{2} - i\sqrt[4]{2}.$$

3.2. **Normalidad.**

Sea E/K una extensión finita de cuerpos de números.

- Si $\sigma : E \to \mathbb{C}$ es una K-inmersión, el cuerpo imagen $\sigma(E)$ es llamado **el conjugado de E sobre K por σ**. Puesto que $K \leq E \Rightarrow K = \sigma(K) \leq$

$\sigma(E)$, $\sigma(E)/K$ es también una extensión, a la que llamamos **extensión conjugada de E/K por σ**.

- La extensión E/K se dice **normal** si coincide con todas sus conjugadas; es decir, si para toda K-inmersión compleja $\sigma : E \to \mathbb{C}$ se verifica que $\sigma(E) = E$.

Una importante observación es que las extensiones conjugadas son del mismo grado:

Proposición 8. *Sea E/K una extensión finita de cuerpos de números y $\sigma : E \to \mathbb{C}$ una K-inmersión. Se verifica que $[\sigma(E) : K] = [E : K]$.*

Demostración. Puesto que $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ y $\sigma(a\alpha) = \sigma(a)\sigma(\alpha) = a\sigma(\alpha)$, para $a \in K$ y $\alpha, \beta \in E$, ocurre que σ es un monomorfismo de K-espacios vectoriales y, en consecuencia, la dimensión de E como K-espacio vectorial es igual a la dimensión de su imagen $\sigma(E)$; esto es, $[E : K] = [\sigma(E) : K]$. □

Corolario 9. *Sea E/K una extensión finita de cuerpos de números. Si $\sigma : E \to \mathbb{C}$ es una K-inmersión, entonces*

$$\sigma(E) = E \Leftrightarrow \sigma(E) \leq E.$$

Demostración. Si $\sigma(E) \leq E$, necesariamente será $\sigma(E) = E$ al tener ambos igual dimensión como K-espacios vectoriales. □

Podemos decir entonces que **la extensión es normal si y solo si contiene a todas sus conjugadas**. La siguiente observación es muy práctica.

Corolario 10. *Sea $E = K(\alpha_1, \ldots, \alpha_n)/K$ una extensión finita de cuerpos de números. Si $\sigma : E \to \mathbb{C}$ es una K-inmersión, entonces*

$$\sigma(E) = E \Leftrightarrow \sigma(\alpha_i) \in E, \text{ para todo } i = 1, \ldots, n.$$

Demostración. Puesto que $\sigma(E) = \sigma(K)(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$, si cada $\sigma(\alpha_i) \in E$ se deduce que $\sigma(E) \leq E$. y basta utilizar el corolario anterior. □

Ejemplo 11. La extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es normal. En efecto, hemos visto que hay exactamente dos $\mathbb{Q}$-inmersiones $\sigma_1, \sigma_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$, caracterizadas por que $\sigma_1(\sqrt{2}) = \sqrt{2}$ y $\sigma_2(\sqrt{2}) = -\sqrt{2}$, y vemos que las imágenes del generador por ambas pertenece a la propia extensión.

Ejemplo 12. La extensión $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es normal. En efecto, sabemos que hay una $\mathbb{Q}$-inmersión $\sigma : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{C}$, tal que $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$.

En el estudio de las extensiones normales, el siguiente concepto es fundamental.

Definición 13. *Si $f \in K[x]$, donde K es un cuerpo de números, y $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ son sus diferentes raíces en $\mathbb{C}$, el cuerpo $K(f) = K(\alpha_1, \ldots, \alpha_n)$ es llamado* **el cuerpo de descomposición de f sobre K.**

Ejemplo 14. El cuerpo de descomposición del polinomio $x^2 + 1$ sobre $\mathbb{R}$ es

$$\mathbb{R}(x^2 + 1) = \mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C},$$

mientras que el cuerpo de descomposición de ese mismo polinomio sobre $\mathbb{Q}$ es

$$\mathbb{Q}(x^2+1) = \mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\}.$$

Ejemplo 15. El cuerpo de descomposición de x^2-3 sobre $\mathbb{Q}$ es

$$\mathbb{Q}(x^2-3) = \mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3} \mid a,b \in \mathbb{Q}\},$$

mientras que su cuerpo de descomposición sobre $\mathbb{Q}(\sqrt{2})$ es

$$\mathbb{Q}(\sqrt{2})(x^2-3) = \mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6},\ a,b,c,d \in \mathbb{Q}\}.$$

Ejemplo 16. Consideremos el polinomio $x^3-1 \in \mathbb{Q}[x]$, cuyas raíces en $\mathbb{C}$ son llamadas las **raíces cúbicas de la unidad**. El polinomio tiene a 1 como raíz, y dividiéndolo por $x-1$, vemos que $x^3-1 = (x-1)(x^2+x+1)$. Las raíces del polinomio x^2+x+1, es decir, las otras dos raíces cúbicas de la unidad, son $\frac{-1\pm i\sqrt{3}}{2}$. El número complejo

$$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\frac{2\pi}{3} = e^{\frac{2\pi i}{3}}$$

es llamado **la raíz cúbica primitiva de la unidad**. Puesto que $\omega^2 = \frac{1}{4} - \frac{3}{4} - i\frac{\sqrt{3}}{2} = \frac{-1-i\sqrt{3}}{2}$ y $\omega^3 = 1$, vemos que las tres raíces cúbicas de la unidad son

$$\begin{cases} \omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\ \omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \overline{\omega} = \omega^{-1} \\ \omega^3 = 1. \end{cases}$$

El cuerpo de descomposición de x^3-1 sobre $\mathbb{Q}$ es entonces

$$\mathbb{Q}(x^3-1) = \mathbb{Q}(\omega).$$

Se tiene que $Irr(\omega,\mathbb{Q}) = x^2+x+1$, y $\mathbb{Q}(\omega)/\mathbb{Q}$ es una extensión de grado 2, con base $\{1,\omega\}$.

Ejemplo 17. Los polinomios x^3-1 y x^2+3 tienen el mismo cuerpo de descomposición sobre $\mathbb{Q}$, pues

$$\mathbb{Q}(w) = \mathbb{Q}(i\sqrt{3}).$$

Ejemplo 18. Las raíces complejas de x^3-2 son $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, por tanto su cuerpo de descomposición sobre $\mathbb{Q}$ es

$$\mathbb{Q}(x^3-2) = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2}).$$

Es una extensión de $\mathbb{Q}$ de grado 6, con base $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$.

Teorema 19 (Caracterización de Extensiones finitas normales)**.** * *Sea E/K una extensión finita de cuerpos de números. Son equivalentes:*

(1) *E/K es una extensión normal.*
(2) *Existe un polinomio $f \in K[x]$ tal que $E = K(f)$.*
(3) *Si $f \in K[x]$ es cualquier polinomio irreducible con una raíz en E, entonces todas las raíces de f están en E, esto es, f descompone totalmente en E.*

(4) *Existen* $\alpha_1, \ldots, \alpha_n \in E$, *tal que* $E = K(\alpha_1, \ldots, \alpha_n)$ *y cada polinomio* $Irr(\alpha_i, K)$ *descompone totalmente en* E, $i = 1, \ldots, n$.
(5) *Existen* $\alpha_1, \ldots, \alpha_n \in E$, *tal que* $E = K(\alpha_1, \ldots, \alpha_n)$ *y, para cada* $i = 1, \ldots, n$ *existe un polinomio* $f_i \in K[x]$ *tal que* $f_i(\alpha_i) = 0$ *y descompone totalmente en* E.

DEMOSTRACIÓN. (2) $\Rightarrow$ (1). Supongamos que $E = K(\beta_1, \ldots, \beta_r)$, donde los $\beta_i \in \mathbb{C}$ son las diferentes raíces del polinomio $f \in K[x]$, y sea $\sigma : E \to \mathbb{C}$ cualquier K-inmersión compleja. Puesto que $f(\beta_j) = 0$, será $f(\sigma(\beta_j)) = 0$. Así que $\sigma(\beta_j) \in \{\beta_1, \ldots, \beta_r\} \subset E$ para todo j. Por el Corolario 10, $\sigma(E) = E$ y la extensión es normal.

(1) $\Rightarrow$ (3). Supongamos que $f \in K[x]$ es un polinomio irreducible con una raíz $\alpha \in E$, y sea $\beta \in \mathbb{C}$ cualquier otra raíz de ese mismo polinomio. No perdemos generalidad en suponer que f es mónico, y por tanto en suponer que $f = Irr(\alpha, K)$. Sabemos entonces que existe exactamente una K-inmersión $\tau : K(\alpha) \to \mathbb{C}$ tal que $\tau(\alpha) = \beta$, y también que esta τ admite al menos una extensión a E, es decir que existe una τ-inmersión $\sigma : E \to \mathbb{C}$ (en realidad, habrá tantas como indique el grado $[E : K(\alpha)]$). Obviamente, σ es una K-inmersión y consecuentemente será $\sigma(E) = E$. Esto nos permite concluir que $\beta = \sigma(\alpha) \in E$.

(3) $\Rightarrow$ (4). Esto es trivial, basta considerar cualquier sistema de generadores de la extensión y aplicar la hipótesis a sus correspondientes irreducibles sobre K.

(4) $\Rightarrow$ (5). Obvio, tomemos $f_i = Irr(\alpha_i, K)$.

(5) $\Rightarrow$ (2). Sea $f = \prod_i f_i$. El cuerpo de descomposición $K(f)$ será la extensión de K generada por todas las raíces de todos los polinomios f_i, $i = 1, \ldots, n$. Como por hipótesis todas esas raíces están en E, será $K(f) \leq E$. Pero que cada α_i es raíz de f, por tanto $E = K(\alpha_1, \ldots, \alpha_n) \leq K(f)$. En conclusión $E = K(f)$. □

Ejemplo 20. La extensión $\mathbb{Q}(\sqrt{5}, i\sqrt{3}, \sqrt[3]{2})/\mathbb{Q}$ es normal, pues $Irr(\sqrt{5}, \mathbb{Q}) = x^2 - 5$ cuyas raíces, $\pm\sqrt{5}$, están en el cuerpo extensión, $Irr(i\sqrt{3}, \mathbb{Q}) = x^2 + 3$ cuyas raíces son $\pm i\sqrt{3}$, ambas también en el cuerpo extensión, y $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, cuyas raíces son $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ y $\omega^2\sqrt[3]{2}$, donde $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, y las tres están también en el cuerpo extensión.

Ejemplo 21. La extensión $\mathbb{Q}(\sqrt{5}, \sqrt{3}, \sqrt[3]{2})/\mathbb{Q}$ no es normal, pues las dos de las raíces complejas no reales de $x^3 - 2$ no están en el cuerpo $\mathbb{Q}(\sqrt{5}, \sqrt{3}, \sqrt[3]{2})$ (que está contenido en $\mathbb{R}$).

3.3. **El grupo de Galois de una extensión.**

Si E es un cuerpo de números y $\sigma : E \to \mathbb{C}$ es cualquier inmersión, sabemos que esta produce un isomorfismo de cuerpos, que denotamos igual, $\sigma : E \cong \sigma(E)$, $x \mapsto \sigma(x)$. Si ocurre que $\sigma(E) = E$, entonces σ produce lo que llamamos un **automorfismo** de E, es decir, un isomorfismo de E en sí mismo, $\sigma : E \cong E$. Y recíprocamente, si $\sigma : E \cong E$ es cualquier automorfismo, al componerlo con la inclusión $in : E \to \mathbb{C}$, obtenemos una inmersión, que denotamos igual, $\sigma : E \to \mathbb{C}$, $x \mapsto \sigma(x)$, con $\sigma(E) = E$. De esta manera, desde ahora en adelante, *convenimos en*

no distinguir entre un automorfismo σ de un cuerpo de números E, y una inmersión compleja σ de este cuerpo tal que $\sigma(E) = E$. Denotaremos por $Aut(E)$ al conjunto de sus automorfismos. De manera que

$$Aut(E) = \{\text{isomorfismos } \sigma : E \cong E\} = \{\text{inmersiones } \sigma : E \to \mathbb{C} \mid \sigma(E) = E\}.$$

Y resaltemos ahora que $Aut(E)$ **es un grupo**, al que nos referimos como **el grupo de automorfismos del cuerpo** E. La multiplicación en este grupo es la operación de composición: Si $\sigma, \tau \in Aut(E)$, su producto $\sigma\tau$ es el automorfismo definido por

$$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)), \text{ para cada } \alpha \in E.$$

El elemento neutro de este grupo es el automorfismo identidad, $id_E : E \to E$, $\alpha \mapsto \alpha$, y, para cada $\sigma \in Aut(E)$, su inverso en el grupo de automorfismos es justamente el automorfismo de E definido por la aplicación inversa $\sigma^{-1} : E \to E$, que asigna a cada $\alpha \in E$ el único elemento de E cuya imagen por σ es α. Es claro que $\sigma^{-1}(0) = 0$ y $\sigma^{-1}(1) = 1$; además, para cualesquiera $\alpha, \beta \in E$, las igualdades $\sigma(\sigma^{-1}(\alpha) + \sigma^{-1}(\beta)) = \alpha + \beta$ y $\sigma(\sigma^{-1}(\alpha)\sigma^{-1}(\beta)) = \alpha\beta$, prueban que $\sigma^{-1}(\alpha + \beta) = \sigma^{-1}(\alpha) + \sigma^{-1}(\beta)$ y $\sigma^{-1}(\alpha\beta) = \sigma^{-1}(\alpha)\sigma^{-1}(\beta)$. Así que, efectivamente, la aplicación inversa σ^{-1} de cualquier automorfismo σ de E es también un automorfismo.

Si E/K una extensión finita de cuerpos números, se define su **grupo de Galois**, denotado por $G(E/K)$, como el subgrupo del grupo $Aut(E)$ definido por

$$G(E/K) = \{\sigma \in Aut(E) \mid \sigma(a) = a \ \forall a \in K\} = \{\sigma \in Aut(E) \mid \sigma|_K = id_K\}.$$

Usualmente nos referiremos a los elementos del grupo de Galois $G(E/K)$ como **K-automorfismos de** E. En términos equivalentes, podemos decir que

$$G(E/K) = \{K\text{-inmersiones } \sigma : E \to \mathbb{C} \mid \sigma(E) = E\}$$

o también que (ver Corolario 9)

$$G(E/K) = \{K\text{-inmersiones } \sigma : E \to \mathbb{C} \mid \sigma(E) \leq E\}$$

y, si $E = K(\alpha_1, \ldots, \alpha_r)$, que (ver Corolario 10)

$$G(E/K) = \{K\text{-inmersiones } \sigma : E \to \mathbb{C} \mid \sigma(\alpha_i) \in E, i = 1, \ldots, r\}.$$

Ejemplo 22. Consideremos la extensión $\mathbb{C}/\mathbb{R}$. Como $\mathbb{C} = \mathbb{R}(i)$ y $Irr(i, \mathbb{R}) = x^2 + 1$, es una extensión de grado dos, con base $\{1, i\}$. Como las raíces de $x^2 + 1$ son $\pm i$, hay exactamente dos $\mathbb{R}$-inmersiones $\sigma_1, \sigma_2 : \mathbb{C} \to \mathbb{C}$, caracterizadas por que $\sigma_1(i) = i$ y $\sigma_2(i) = -i$. Puesto que

$$\sigma_1(\mathbb{C}) = \sigma_1(\mathbb{R}(i)) = \mathbb{R}(\sigma_1(i)) = \mathbb{R}(i) = \mathbb{C},$$
$$\sigma_2(\mathbb{C}) = \sigma_2(\mathbb{R}(i)) = \mathbb{R}(\sigma_2(i)) = \mathbb{R}(-i) = \mathbb{R}(i) = \mathbb{C},$$

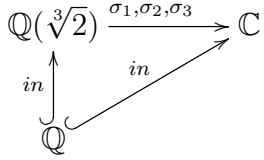
concluimos que $G(\mathbb{C}/\mathbb{R})$ es un grupo de orden dos con $G(\mathbb{C}/\mathbb{R}) = \{\sigma_1, \sigma_2\}$ donde, explícitamente,

$$\begin{cases} \sigma_1(a + bi) = a + bi, \\ \sigma_2(a + bi) = a - bi. \end{cases}$$

Notemos que $\sigma_1 = id_{\mathbb{C}}$ es simplemente identidad y $\sigma_2 = C$ es el automorfismo de conjugación $C : \mathbb{C} \to \mathbb{C}$, $z = a + bi \mapsto \overline{z} = a - bi$. Como todo grupo de orden 2, este grupo es cíclico generado por su elemento no trivial, esto es

$$G(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}}, C\} = \langle C \mid C^2 = id_{\mathbb{C}} \rangle$$

Ejemplo 23. Consideremos la extensión simple $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Puesto que las raíces complejas del polinomio $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ son $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ y $\omega^2\sqrt[3]{2}$, hay exactamente tres $\mathbb{Q}$-inmersiones complejas



determinadas por que las respectivas imágenes del generador son las indicadas en el cuadro

	σ_1	σ_2	σ_3
$\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$

Puesto que $\sigma_1(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$, pero $\sigma_2(\sqrt[3]{2}) \notin \mathbb{Q}(\sqrt[3]{2})$ y $\sigma_3(\sqrt[3]{2}) \notin \mathbb{Q}(\sqrt[3]{2})$, concluimos que $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ tiene un solo elemento, el automorfismo $\sigma_1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ tal que $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, que es precisamente el automorfismo identidad en $\mathbb{Q}(\sqrt[3]{2})$. Así que

$$G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$$

es un grupo trivial.

Proposición 24. *Sea E/K una extensión finita de cuerpos de números. Entonces*

(1) $|G(E/K)| \leq [E : K]$.
(2) $|G(E/K)| = [E : K] \iff E/K$ *es normal.*

Demostración. (1) Es consecuencia de que número total de las diferentes K-inmersiones complejas de E es igual al grado de la extensión.

(2) La igualdad $|G(E/K)| = [E : K]$ significa que todas las K-inmersiones $\sigma : E \to \mathbb{C}$ verifican la condición $\sigma(E) = E$, pero esto dice exactamente que la extensión E/K coincide con todas sus conjugadas; es decir, que E/K es normal. □

Definición 25. *Si $f \in K[x]$ es un polinomio con coeficientes en un cuerpo numérico K, su grupo de Galois sobre K, denotado por $G(f/K)$ es el grupo de Galois de su cuerpo de descomposición sobre K; esto es,*

$$G(f/K) = G(K(f)/K).$$

Puesto que la extensión $K(f)/K$ siempre es normal, tenemos el siguiente hecho.

Proposición 26. *Si $f \in K[x]$, donde K es un cuerpo de números, entonces*

$$|G(f/K)| = [K(f) : K].$$

Ejemplo 27. El cuerpo de descomoposición del polinomio x^3-1 sobre $\mathbb{R}$ es

$$\mathbb{R}(x^3-1)=\mathbb{R}(\omega)=\mathbb{R}(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2})=\mathbb{R}(i)=\mathbb{C}\ .$$

Luego $G(x^3-1/\mathbb{R})=G(\mathbb{C}/\mathbb{R})$, que es cíclico de orden 2 consistente del automorfismo $id_{\mathbb{C}}$ y del automorfismo de conjugación compleja (ver Ejemplo 22).

Ejemplo 28. Vamos a describir explicitamente el grupo de Galois $G=G(x^3-2/\mathbb{Q})$.

(1) *El cuerpo de descomposición del polinomio.* Como ya comentamos en el Ejemplo 18, las raíces complejas de x^3-2 son $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ y $\omega^2\sqrt[3]{2}$ donde, recordemos, $\omega=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$ es la raíz cúbica primitiva de la unidad. Por tanto, su cuerpo de descomposición sobre $\mathbb{Q}$ es $\mathbb{Q}(x^3-2)=\mathbb{Q}(\sqrt[3]{2},\omega)$ y

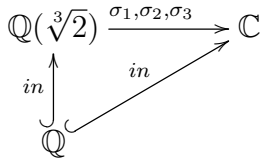
$$G=G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}).$$

(2) *Tamaño del grupo.* Para determinar el orden del grupo G, determinemos el grado de la extensión $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$. Considerando la torre de extensiones $\mathbb{Q}\leq\mathbb{Q}(\sqrt[3]{2})\leq\mathbb{Q}(\sqrt[3]{2},\omega)$, vemos sin dificultad que la primera es de grado 3, siendo $Irr(\sqrt[3]{2},\mathbb{Q})=x^3-2$, y la segunda es de grado 2, siendo $Irr(\omega,\mathbb{Q}(\sqrt[3]{5}))=Irr(\omega,\mathbb{Q})=x^2+x+1$, ya que $mcd(2,3)=1$ (ver Ejemplo 16). Así, Concluimos entonces que la extension $\mathbb{Q}(\sqrt[3]{2}),\omega)/\mathbb{Q}$ es de grado 6 y, por tanto, $|G|=6$.

(3) *Descripción de los elementos del grupo.* El grupo de Galois $G=G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ consistirá de los seis automorfismos en $\mathbb{Q}(\sqrt[3]{2},\omega)$ definidos por las seis $\mathbb{Q}$-inmersiones $\mathbb{Q}(\sqrt[3]{2},\omega)\to\mathbb{C}$. Para describirlas, consideremos de nuevo la torre

$$\mathbb{Q}\leq\mathbb{Q}(\sqrt[3]{2})\leq\mathbb{Q}(\sqrt[3]{2},\omega),$$

y buscamos primero las $\mathbb{Q}$-inmersiones $\mathbb{Q}(\sqrt[3]{2})\to\mathbb{C}$: Tal como se comentó en el Ejemplo 23, puesto que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ es de grado 3, habrá tres tales inmersiones complejas

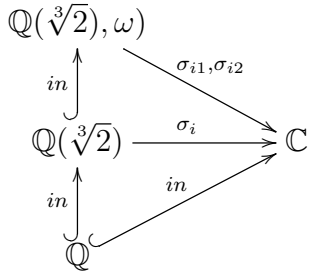


que están determinadas por que su respectiva imagen del generador es cada una de las raíces en $\mathbb{C}$ del polinomio x^3-2, esto es, según se índica en el cuadro

	σ_1	σ_2	σ_3
$\sqrt[3]{2}\mapsto$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$

.

Y ahora buscamos, para cada $i = 1, 2, 3$, las σ_i-inmersiones $\mathbb{Q}(\sqrt[3]{2}), \omega) \to \mathbb{C}$. Puesto que la extensión $\mathbb{Q}(\sqrt[3]{2}), \omega)/\mathbb{Q}(\sqrt[3]{2})$ es de grado dos, habrá 2 tales σ_i-inmersiones



en correspondencia con las dos raíces de $(x^2 + x + 1)^{\sigma_i} = x^2 + x + 1$, que son ω y ω^2. Así que, las dos σ_i-inmersiones $\sigma_{i1}, \sigma_{i2} : \mathbb{Q}(\sqrt[3]{2}, \omega) \to \mathbb{C}$ son las determinadas por las asignaciones al generador ω indicadas en el cuadro

	σ_{i1}	σ_{i2}
$\omega \mapsto$	ω	ω^2

.

Tenemos así las seis $\mathbb{Q}$-inmersiones complejas de $\mathbb{Q}(\sqrt[3]{2}, \omega)$, caracterizadas por su efecto sobre los generadores tal como se indica en el cuadro de asignaciones

	σ_{11}	σ_{12}	σ_{21}	σ_{22}	σ_{31}	σ_{32}
$\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$
$\omega \mapsto$	ω	ω^2	ω	ω^2	ω	ω^2

que, debido a la normalidad de la extensión, nos muestran también los seis automorfismos del grupo de Galois

$$G = G(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = \{\sigma_{11} = id, \sigma_{12}, \sigma_{21}, \sigma_{22}, \sigma_{31}, \sigma_{32}\},$$

donde, recordamos, la multiplicación es por composición.

(4) *¿De qué órdenes son los diferentes elementos de G?.* Claramente $\sigma_{11} = id$, que es de orden 1. Para los demás, estudiemos sus potencias mostrando su efecto sobre los generadores:

$$\begin{cases} \sigma_{12}^2(\sqrt[3]{2}) = \sigma_{12}(\sqrt[3]{2}) = \sqrt[3]{2}, \\ \sigma_{12}^2(\omega) = \sigma_{12}(\omega^2) = (\sigma_{12}(\omega))^2 = (\omega^2)^2 = \omega^4 = \omega. \end{cases}$$

Luego $\sigma_{12}^2 = id$ y, por tanto, $or(\sigma_{12}) = 2$.

$$\begin{cases} \sigma_{21}^2(\sqrt[3]{2}) = \sigma_{21}(\omega\sqrt[3]{2}) = \sigma_{21}(\omega)\sigma_{21}(\sqrt[3]{2}) = \omega\,\omega\sqrt[3]{2} = \omega^2\sqrt[3]{2}, \\ \sigma_{21}^2(\omega) = \sigma_{21}(\omega) = \omega. \end{cases}$$

Luego $\sigma_{21}^2 = \sigma_{31}$.

$$\begin{cases} \sigma_{21}^3(\sqrt[3]{2}) = \sigma_{21}(\omega^2\sqrt[3]{2}) = \omega^2\omega\sqrt[3]{2} = \sqrt[3]{2}, \\ \sigma_{21}^3(\omega) = \omega. \end{cases}$$

Luego $\sigma_{21}^3 = id$ y, por tanto, $or(\sigma_{21}) = 3$. Como $\sigma_{31} = \sigma_{21}^2 = \sigma_{21}^{-1}$, podemos asegurar que $or(\sigma_{31}) = 3$.

$$\begin{cases} \sigma_{22}^2(\sqrt[3]{2}) = \sigma_{22}(\omega\sqrt[3]{2}) = \omega^2\omega\sqrt[3]{2} = \sqrt[3]{2}, \\ \sigma_{22}^2(\omega) = \sigma_{22}(\omega^2) = \omega^4 = \omega. \end{cases}$$

Luego $\sigma_{22}^2 = id$ y, por tanto, $or(\sigma_{22}) = 2$. Finalmente,

$$\begin{cases} \sigma_{32}^2(\sqrt[3]{2}) = \sigma_{22}(\omega^2\sqrt[3]{2}) = \omega^4\omega^2\sqrt[3]{2} = \sqrt[3]{2}, \\ \sigma_{32}^2(\omega) = \sigma_{32}(\omega^2) = \omega^4 = \omega. \end{cases}$$

Luego $\sigma_{32}^2 = id$ y, por tanto, $or(\sigma_{32}) = 2$.

(4) *¿Conocemos el grupo G?* Sí. Es isomorfo al grupo Diédrico D_3, el grupo de simetrías del triángulo equilátero (que a su vez es isomorfo al grupo de permutaciones S_3). Recordemos que este grupo es de orden seis, sus elementos se listan usualmente como

$$D_3 = \{1, r, r^2, s, rs, r^2s\},$$

donde r representa al giro de amplitud $\frac{2\pi}{3}$ radianes ($= 120^o$) respecto al baricentro del triángulo y s la simetría es la reflexión respecto al eje que pasa por el baricentro y uno de los vértices. Este grupo D_3 tiene una presentación por generadores y relaciones de la forma

$$D_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2s\rangle$$

lo que significa (Teorema de Dyck) que *"para todo grupo G y para todo par de elementos $\sigma, \tau \in G$ tales que $\sigma^3 = 1$, $\tau^2 = 1$ y $\tau\sigma = \sigma^2\tau$ existe un único homomorfismo de grupos $\phi : D_3 \to G$ tal que $\phi(r) = \sigma$ y $\phi(s) = \tau$".*

Fijándonos en nuestro grupo $G = G(x^3 - 2/\mathbb{Q})$, puesto que $\sigma_{21}^3 = 1 = \sigma_{12}^2$ y comprobamos también que $\sigma_{12}\sigma_{21} = \sigma_{21}^2\sigma_{12}$ $(= \sigma_{32})$:

$$\begin{cases} \sigma_{12}\sigma_{21}(\sqrt[3]{2}) = \sigma_{12}(\omega\sqrt[3]{2}) = \omega^2\sqrt[3]{2}, \\ \sigma_{12}\sigma_{21}(\omega) = \sigma_{12}(\omega) = \omega^2, \end{cases}$$

$$\begin{cases} \sigma_{21}^2\sigma_{12}(\sqrt[3]{2}) = \sigma_{31}(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}, \\ \sigma_{21}^2\sigma_{12}(\omega) = \sigma_{31}(\omega^2) = \omega^2, \end{cases}$$

concluimos que hay un homomorfismo $\phi : D_3 \to G$ tal que $\phi(r) = \sigma_{21}$ y $\phi(s) = \sigma_{12}$. El subgrupo imagen de este homomorfismo contiene al menos un elemento de orden 3 y otro de orden 2, luego su orden ha de ser al menos 6 y es necesariamente todo G. Como ambos grupos son de orden 6, necesariamente es un isomorfismo (una aplicación sobreyectiva o inyectiva entre dos conjuntos finitos con el mismo cardinal necesariamente es biyectiva). Así que $D_3 \cong G$. □

3.4. **El Teorema Fundamental de la Teoría de Galois.**

Sea F/E una extensión de cuerpos (no necesariamente numéricos). Si $\sigma : E \to F$ es cualquier inmersión, el subconjunto

$$E^\sigma = \{\alpha \in E \mid \sigma(\alpha) = \alpha\}$$

es un subcuerpo de E, al que nos referimos como **el subcuerpo fijo** por σ. Más en general, si $S = \{\sigma_1, \ldots, \sigma_n : E \to F\}$ es un conjunto de homomorfismos, el subcuerpo fijo por S es el subcuerpo

$$E^S = \{\alpha \in E \mid \sigma_i(\alpha) = \alpha \text{ para todo } i = 1, \ldots, n\} = \textstyle\bigcap_{i=1}^n E^{\sigma_i} \, .$$

En particular, si E es un cuerpo y $G \leq Aut(E)$ es cualquier subgrupo finito de su grupo de automorfismos, entonces el subcuerpo fijo por G es

$$E^G = \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ para todo } \sigma \in G\}.$$

Observaciones inmediatas son, por ejemplo, que

$$H \leq G \implies E^G \leq E^H \, ,$$

o que que si $\{\sigma_1, \cdots, \sigma_n\}$ es un sistema de generadores de G (es decir, si todo elemento de G es un producto reiterado de los σ_i), entonces

$$E^G = E^{\{\sigma_1, \cdots, \sigma_n\}} = \textstyle\bigcap_{i=1}^n E^{\sigma_i} \, .$$

Teorema 29 (Lema de Artin)**.** *Sea E un cuerpo de números y $G \leq Aut(E)$ un subgrupo finito de su grupo de automorfismos. Entonces,*

(1) $[E : E^G] = |G|$.
(2) $G(E/E^G) = G$.

Demostración. Denotemos por $K = E^G$, al subcuerpo fijo por G. Como $G \leq G(E/K)$, tenemos que $|G| \leq |G(E/K)| \leq [E : K]$. Si probamos que $[E : K] \leq |G|$, concluiremos que $[E : K] = |G|$ y que $G = G(E/K)$, lo que prueba el teorema.

Supongamos, por el contrario, que $|G| = n$ y $[E : K] > n$.

Sean $\{\alpha_1, \ldots, \alpha_{n+1}\}$ elementos de E linealmente independientes sobre K, y consideremos el sistema homogéneo de n ecuaciones lineales con $n + 1$ incógnitas sobre el cuerpo E:

$$\begin{cases} \sigma(\alpha_1)x_1 + \cdots + \sigma(\alpha_{n+1})x_{n+1} = 0 \, , \\ \sigma \in G \, . \end{cases}$$

Existirá una solución no trivial $(\beta_1, \ldots, \beta_{n+1}) \in E^{n+1}$. Sea r el mínimo de componentes no nulas presentes entre las diferentes soluciones no triviales del sistema. No habrá por tanto soluciones con menos de r componentes no nulas. Notemos que ese r es necesariamente > 1, ya que en otro caso tendríamos una solución de la forma $(0, \ldots, 0, \beta_i, 0 \ldots, 0)$, con $\beta_i \neq 0$, y, por la ecuación para $\sigma = id_E$, la igualdad que $\alpha_i\beta_i = 0$, siendo $\alpha_i \neq 0 \neq \beta_i$.

Bien, para simplificar, renumerando los α_i si es necesario, podemos suponer que hay una tal solución en la que todas las componentes no nulas están al principio, esto es de la forma $(\beta_1, \ldots, \beta_r, 0, \ldots, 0)$ con $\beta_i \neq 0$. Además, multiplicando por su inverso si es necesario, podemos también suponer que $\beta_r = 1$.

Observamos ahora que no puede ocurrir que todos los β_i estén en K, pues en ese caso la ecuación correspondiente a $\sigma = id_E \in G$ violaría la supuesta independencia

lineal de $\{\alpha_1, \ldots, \alpha_{n+1}\}$. Entonces, existe un i tal que $\beta_i \notin K$. Como $K = E^G$, existe entonces $\tau \in G$ con $\tau(\beta_i) \neq \beta_i$, y aplicando este τ a las igualdades

$$(1) \qquad \begin{cases} \sigma(\alpha_1)\beta_1 + \cdots + \sigma(\alpha_{r-1})\beta_{r-1} + \sigma(\alpha_r) = 0\,, \\ \sigma \in G\,. \end{cases}$$

obtenemos las igualdades

$$\begin{cases} \tau\sigma(\alpha_1)\tau(\beta_1) + \cdots + \tau\sigma(\alpha_{r-1})\tau(\beta_{r-1}) + \tau\sigma(\alpha_r) = 0, \\ \sigma \in G. \end{cases}$$

Pero como G es un grupo, la aplicación de multiplicar por τ, $\sigma \mapsto \tau\sigma$, es una permutación entre los elementos de G, así que $\{\tau\sigma,\ \sigma \in G\} = G$, y las anteriores igualdades nos dicen simplemente que

$$(2) \qquad \begin{cases} \sigma(\alpha_1)\tau(\beta_1) + \cdots + \sigma(\alpha_{r-1})\tau(\beta_{r-1}) + \sigma(\alpha_r) = 0, \\ \sigma \in G. \end{cases}$$

Substrayendo ahora cada una de estas igualdades en (2) a la correspondiente igualdad en (1), obtenemos las igualdades

$$\begin{cases} \sigma(\alpha_1)[\beta_1 - \tau(\beta_1)] + \cdots + \sigma(\alpha_{r-1})[\beta_{r-1} - \tau(\beta_{r-1})] = 0, \\ \sigma \in G. \end{cases}$$

para todo $\sigma \in G$. Como $\beta_i - \tau(\beta_i) \neq 0$, hemos encontrado una solución no trivial del sistema original,

$$(\beta_1 - \tau(\beta_1), \ldots, \beta_{r-1} - \tau(\beta_{r-1}), 0 \ldots, 0)$$

teniendo menos de r componentes no nulas. He aquí la contradicción. □

Una importante consecuencia es observada en el siguiente teorema.

Teorema 30. *Una extensión finita de cuerpos de números E/K es normal si y solo si $K = E^{G(E/K)}$.*

Demostración. Supongamos primero que $K = E^{G(E/K)}$. Entonces, por el Lema de Artin, $[E : K] = |G(E/K)|$ y, por la Proposición 24, la extensión es normal.

Recíprocamente, asumamos que E/K es normal. Entonces $[E : K] = |G(E/K)|$. Consideremos el subcuerpo fijo por el grupo de Galois $E^{G(E/K)}$, tendremos la situación

$$K \leq E^{G(E/K)} \leq E\,,$$

de donde

$$\begin{aligned} [E : K] &= [E : E^{G(E/K)}] \cdot [E^{G(E/K)} : K] = |G(E/K)| \cdot [E^{G(E/K)} : K] \\ &= [E : K]\,[E^{G(E/K)} : K] \end{aligned}$$

y concluimos que $[E^{G(E/K)} : K] = 1$. Esto es, $E^{G(E/K)} = K$. □

Y ya tenemos todos los ingredientes para establecer con facilidad el resultado cumbre de esta teoría. **Una notación**: Si E/K es una extensión de cuerpos números, denotamos $Sub(E/K)$ al conjunto, ordenado por inclusión, de los cuerpos de números F intermedios entre K y E, esto es,

$$Sub(E/K) = \{\text{cuerpos } F \mid K \leq F \leq E\}.$$

También, denotamos por $Sub(G(E/K))$ al conjunto, también ordenado por inclusión, de los subgrupos de su grupo de Galois, esto es,

$$Sub(G(E/K)) = \{\text{ grupos } G \mid G \leq G(E/K)\}.$$

Observemos que, si $G \in Sub(G(E/K))$, entonces $E^G \in Sub(E/K)$, esto es, $K \leq E^G \leq E$. Además, si $G, G' \in Sub(G(E/K))$ y $G \leq G'$, entonces $E^{G'} \leq E^G$.

También, si $F \in Sub(E/K)$, entonces $G(E/F) \leq G(E/K)$, esto es, $G(E/F) \in Sub(G(E/K))$. Además, si $F, F' \in Sub(E/K)$ y $F \leq F'$, entonces $G(E/F') \leq G(E/F)$.

Teorema 31 (Teorema Fundamental de la Teoría de Galois)**.** * *Sea E/K una extensión finita y normal de cuerpos de números.*

(1) *Las aplicaciones*

$$Sub(G(E/K)) \to Sub(E/K), \quad G \mapsto E^G,$$

$$Sub(E/K) \to Sub(G(E/K)), \quad F \mapsto G(E/F)$$

son inversas una de la otra.

Esto es, para cada cuerpo de números F con $K \leq F \leq E$, se verifica que $E^{G(E/F)} = F$ y, para cada subgrupo $G \leq G(E/K)$, se verifica que $G(E/E^G) = G$. Estas biyecciones (que invierten el orden de inclusión) entre el conjunto de subgrupos del grupo de Galois de la extensión y el conjunto de subcuerpos intermedios, establecen lo que se conoce como **La Conexión de Galois** *para la extensión E/K.*

(2) *Sean $F, F' \in Sub(E/K)$. Entonces*

$$F \leq F' \Leftrightarrow G(E/F') \leq G(E/F).$$

Si $F \leq F'$,

$$[F' : F] = [G(E/F) : G(E/F')],$$

y F'/F es normal $\Leftrightarrow G(E/F') \trianglelefteq G(E/F)$, y en tal caso

$$G(F'/F) \cong \frac{G(E/F)}{G(E/F')}.$$

(3) *Sean $G, G' \in Sub(G(E/K))$. Entonces*

$$G \leq G' \Leftrightarrow E^{G'} \leq E^G.$$

Si $G \leq G'$,

$$[G' : G] = [E^G : E^{G'}],$$

y $E^G/E^{G'}$ *es normal* $\Leftrightarrow G \trianglelefteq G'$*, y en tal caso*

$$G(E^G/E^{G'}) \cong \frac{G'}{G}.$$

Demostración.(1) Ya conocemos que, para cada subgrupo $G \leq G(E/K)$, se verifica que $G(E/E^G) = G$. Por otro lado, para F cualquier cuerpo de números con $K \leq F \leq E$, se verifica que la extensión E/F es normal, pues si $\sigma : E \to \mathbb{C}$ es cualquier F-inmersión, como $K \leq F$, se tiene que σ es también una K-inmersión y, por tanto, $\sigma(E) = E$. Entonces $F = E^{G(E/F)}$. Esas igualdades $G(E/E^G) = G$ y $E^{G(E/F)} = F$ prueban que las aplicaciones $F \mapsto G(E/F)$ y $G \mapsto E^G$ son inversas una de la otra.

(2) Si $F \leq F'$, es claro que $G(E/F') \leq G(E/F)$. Y recíprocamente, si $G(E/F') \leq G(E/F)$, es claro que $E^{G(E/F)} \leq E^{G(E/F')}$, o sea que $F \leq F'$.

Supongamos que $F \leq F'$. Entonces

$$[F' : F] = \frac{[E : F]}{[E : F']} = \frac{|G(E/F)|}{|G(E/F')|} = [G(E/F) : G(E/F')]\,.$$

Supongamos ahora que F'/F es normal. Dado cualquier $\sigma \in G(E/F)$, la restricción de σ a F' nos define una F-inmersión $\sigma|_{F'} : F' \to \mathbb{C}$, $\alpha \mapsto \sigma(\alpha)$, que, por la normalidad de F' sobre F, tendrá como imagen el propio cuerpo F', así que $\sigma(F') = F'$. Luego $\sigma|_{F'} \in G(F'/F)$. Tenemos así la aplicación

$$G(E/F) \to G(F'/F), \quad \sigma \mapsto \sigma|_{F'}\,.$$

que es un homomorfismo de grupos $((\sigma\tau)|_{F'} = \sigma|_{F'}\tau|_{F'})$, cuyo núcleo es precisamente $G(E/F')$. Por tanto $G(E/F') \trianglelefteq G(E/F)$. Pero, más aun, es un epimorfismo: En efecto, supongamos cualquier $\tau \in G(F'/F)$. Mirando a τ como una F-inmersión compleja de F', $\tau : F' \to \mathbb{C}$, podemos escoger una τ-inmersión compleja de E, digamos $\sigma : E \to \mathbb{C}$ (de hecho, habrá tantas como el grado $[E : F']$). Como E/F es normal, será $\sigma(E) = E$ y tenemos así un $\sigma \in G(E/F)$ que, claramente, verifica que $\sigma|_{F'} = \tau$. El Primer Teorema de Isomorfía nos determina entonces el isomorfismo anunciado:

$$\frac{G(E/F)}{G(E/F')} \cong G(F'/F), \quad [\sigma] \mapsto \sigma|_{F'}\,.$$

Vemos ahora que si $G(E/F') \trianglelefteq G(E/F)$ entonces la extensión F'/F es normal. Sea $\tau : F' \to \mathbb{C}$ una F-inmersión. Vamos a ver que $\tau(F') \leq F'$. Para ello, seleccionemos cualquier τ-inmersión compleja de E, digamos $\sigma : E \to \mathbb{C}$. Puesto que E/F es normal y σ es una F-inmersión será $\sigma(E) = E$; esto es, $\sigma \in G(E/F)$. Supongamos ahora cualquier $\beta \in F'$. Puesto que $\sigma(\beta) = \tau(\beta)$, será $\beta = \sigma^{-1}(\tau(\beta))$. Entonces, $\sigma^{-1}(\tau(\beta)) \in F' = E^{G(E/F')}$ y por tanto, para todo $\gamma \in G(E/F')$, será $\gamma\sigma^{-1}(\tau(\beta)) = \sigma^{-1}(\tau(\beta))$. Aplicando σ, vemos que $\sigma\gamma\sigma^{-1}(\tau(\beta)) = \tau(\beta)$, de donde concluimos que $\tau(\beta) \in E^{\sigma\gamma\sigma^{-1}}$, para todo $\gamma \in G(E/F')$; así que $\tau(\beta) \in E^{\sigma G(E/F')\sigma^{-1}}$. Pero, por la hipótesis de normalidad, $\sigma\, G(E/F')\, \sigma^{-1} = G(E/F')$ y se deduce que $\tau(\beta) \in E^{G(E/F')} = F'$.

(3) Todo se deduce de (2) considerando los cuerpos E^G y $E^{G'}$: Sean $G, G' \in G(E/K)$. Entonces

$$E^{G'} \leq E^G \Leftrightarrow G(E/E^G) \leq G(E/E^{G'}) \Leftrightarrow G \leq G'.$$

Supuesto que $G \leq G'$, entonces $[E^G : E^{G'}] = [G(E/E^{G'}) : G(E/E^G)] = [G' : G]$ y $E^G/E^{G'}$ es normal $\Leftrightarrow G(E/E^G) \trianglelefteq G(E/E^{G'}) \Leftrightarrow G \trianglelefteq G'$, en cuyo caso

$$G(E^G/E^{G'}) \cong \frac{G(E/E^{G'})}{G(E/E^G)} = \frac{G'}{G}.$$

Ejemplo 32. Volvamos al Ejemplo 28, donde se ha estudiado el grupo de Galois

$$G = G(x^3 - 2/\mathbb{Q}) = G(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}).$$

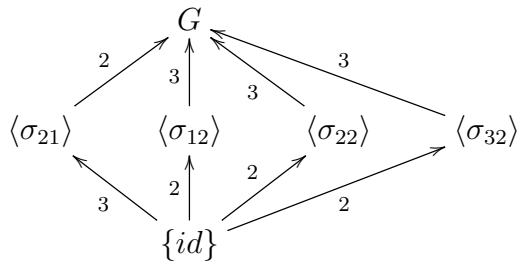
(1) *Descripción del retículo de subgrupos del grupo de Galois.* Puesto que $|G| = 6$, Los subgrupos propios serán de orden 3 y de orden 2. Puesto que 3 es la máxima potencia de 3 que divide al orden del grupo, los subgrupos de orden 3 serán los 3-subgrupos de Sylow de G y, por los Teoremas de Sylow, el número de estos, n_3, verificará que $n_3|2$ y $n_3 \equiv 1 \mod (3)$. Concluimos que $n_3 = 1$, así que G tiene un único subgrupo de orden 3, que será normal. Además, un grupo de orden 3 es necesariamente cíclico y generado por un elemento de orden 3. Puesto que el automorfismo $\sigma_{21} \in G$ tiene orden 3, este genera el único subgrupo de orden 3 de G:

$$\langle \sigma_{21} \rangle = \{id, \sigma_{21}, \sigma_{21}^2 = \sigma_{31}\}.$$

Los subgrupos de orden 2, que serán cíclicos generados por elementos de orden 2, serán los 2-subgrupos de Sylow de G, y el número de estos, n_2, verificará que $n_2|3$ y $n_2 \equiv 1 \mod (2)$. Así que será $n_2 = 1$ o $n_2 = 3$. En este caso es $n_2 = 3$, pues en G hay tres elementos distintos de orden 2, y cada uno de ellos genera un subgrupo distinto, a saber:

$$\langle \sigma_{12} \rangle = \{id, \sigma_{12}\}, \quad \langle \sigma_{22} \rangle = \{id, \sigma_{22}\}, \quad \langle \sigma_{32} \rangle = \{id, \sigma_{32}\}.$$

El retículo de subgrupos se representaría así:



donde se muestran las relaciones de inclusión entre ellos y sus correspondientes índices.

(2) *Descripción del retículo de subcuerpos intermedios.* Por la conexión de Galois, los cuerpos de números F con $\mathbb{Q} \leq F \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$ serán los correspondientes subcuerpos fijos de $\mathbb{Q}(\sqrt[3]{2}, \omega)$ por los subgrupos de $G = G(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$.

Claramente

$$\mathbb{Q}(\sqrt[3]{2},\omega)^G = \mathbb{Q}$$

(pues la extensión $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$) es normal) y

$$\mathbb{Q}(\sqrt[3]{2},\omega)^{id} = \mathbb{Q}(\sqrt[3]{2},\omega).$$

Conocemos que $[\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{21}} : \mathbb{Q}] = 2$. Puesto que $\sigma_{21}(\omega) = \omega$, tenemos que $\mathbb{Q}(\omega) \leq \mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{21}}$. Como $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, concluimos que

$$\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{21}} = \mathbb{Q}(\omega).$$

Conocemos que $[\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{12}} : \mathbb{Q}] = 3$. Puesto que $\sigma_{12}(\sqrt[3]{2}) = \sqrt[3]{2}$, tenemos que $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{12}}$. Como $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, concluimos que

$$\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{12}} = \mathbb{Q}(\sqrt[3]{2}).$$

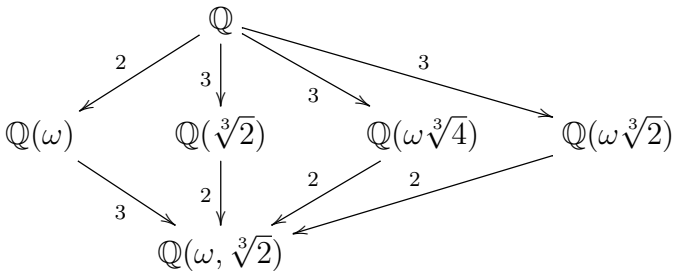
Conocemos que $[\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{22}} : \mathbb{Q}] = 3$. Puesto que $\sigma_{22}(\omega\sqrt[3]{4}) = \omega^2\omega^2\sqrt[3]{4} = \omega\sqrt[3]{4}$, tenemos que $\mathbb{Q}(\omega\sqrt[3]{4}) \leq \mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{22}}$. Como $[\mathbb{Q}(\omega\sqrt[3]{4}) : \mathbb{Q}] = 3$, ya que $Irr(\omega\sqrt[3]{4},\mathbb{Q}) = x^3 - 4$, concluimos que

$$\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{22}} = \mathbb{Q}(\omega\sqrt[3]{4}).$$

Conocemos que $[\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{32}} : \mathbb{Q}] = 3$. Puesto que $\sigma_{32}(\omega\sqrt[3]{2}) = \omega^2\omega^2\sqrt[3]{2} = \omega\sqrt[3]{2}$, tenemos que $\mathbb{Q}(\omega\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{32}}$. Como $[\mathbb{Q}(\omega\sqrt[3]{2}) : \mathbb{Q}] = 3$, ya que $Irr(\omega\sqrt[3]{2},\mathbb{Q}) = x^3 - 2$, concluimos que

$$\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{32}} = \mathbb{Q}(\omega\sqrt[3]{2}).$$

El retículo de subcuerpos de $\mathbb{Q}(\omega, \sqrt[3]{2})$ se escribiría entones en la forma



El cálculo anterior de los subcuerpos fijos podemos abordarlo de otra forma, menos ligada a una feliz inspección. Por ejemplo, para calcular $\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{32}}$, tengamos en cuenta que una base de la extensión $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ es $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$. Sea entonces

$$\alpha = a + a'\sqrt[3]{2} + a''\sqrt[3]{4} + b\,\omega + b'\omega\sqrt[3]{2} + b''\omega\sqrt[3]{4}$$

cualquier elemento de $\mathbb{Q}(\sqrt[3]{2},\omega)$ expresado como combinación lineal con coeficientes en $\mathbb{Q}$ de los elementos de la base. Tendremos que (recordar que $\omega^2+\omega+1=0$)

$$\begin{aligned}\sigma_{32}(\alpha) &= a+a'\omega^2\sqrt[3]{2}+a''\omega\sqrt[3]{4}+b\,\omega^2+b'\omega\sqrt[3]{2}+b''\sqrt[3]{4}\\ &= a+a'(-\omega-1)\sqrt[3]{2}+a''\omega\sqrt[3]{4}+b(-\omega-1)+b'\omega\sqrt[3]{2}+b''\sqrt[3]{4}\\ &= a-a'\omega\sqrt[3]{2}-a'\sqrt[3]{2}+a''\omega\sqrt[3]{4}-b\,\omega-b+b'\omega\sqrt[3]{2}+b''\sqrt[3]{4}\\ &= (a-b)-a'\sqrt[3]{2}+b''\sqrt[3]{4}-b\,\omega+(b'-a')\omega\sqrt[3]{2}+a''\omega\sqrt[3]{4},\end{aligned}$$

y vemos que

$$\sigma_{32}(\alpha)=\alpha \Leftrightarrow \begin{cases} a-b=a\\ a'=-a'\\ b''=a''\\ b=-b\\ b'-a'=b'\\ b''=a'' \end{cases} \Leftrightarrow \begin{cases} b=0\\ a'=0\\ b''=a'' \end{cases} \Leftrightarrow$$

$$\begin{aligned}\alpha &= a+a''\sqrt[3]{4}+b'\omega\sqrt[3]{2}+a''\omega\sqrt[3]{4}\\ &= a+b'\omega\sqrt[3]{2}+a''(1+\omega)\sqrt[3]{4}\\ &= a+b'\omega\sqrt[3]{2}-a''\omega^2\sqrt[3]{4}\end{aligned}$$

donde a,b',a'' son arbitrarios en $\mathbb{Q}$. Vemos así que $\sigma_{32}(\alpha)=\alpha \Leftrightarrow \alpha\in\mathbb{Q}(\omega\sqrt[3]{2})$, pues $Irr(\omega\sqrt[3]{2},\mathbb{Q})=x^3-2$ y $\{1,\omega\sqrt[3]{2},\omega^2\sqrt[3]{4}\}$ es la base standard de $\mathbb{Q}(\omega\sqrt[3]{2})/\mathbb{Q}$. □

(3) **¿Qué cuerpo de los anteriores es $\mathbb{Q}(\omega^2\sqrt[3]{2})$?.**

Determinemos el grupo de Galois $G(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}(\omega^2\sqrt[3]{2}))$, que será el subgrupo de G consistente de los σ_{ij} tales que $\sigma_{ij}(\omega^2\sqrt[3]{2})=\omega^2\sqrt[3]{2}$. Puesto que

$$\begin{aligned}&\sigma_{11}(\omega^2\sqrt[3]{2})=\omega^2\sqrt[3]{2},\\ &\sigma_{21}(\omega^2\sqrt[3]{2})=\sqrt[3]{2},\\ &\sigma_{31}(\omega^2\sqrt[3]{2})=\omega\sqrt[3]{2},\\ &\sigma_{12}(\omega^2\sqrt[3]{2})=\omega\sqrt[3]{2},\\ &\sigma_{22}(\omega^2\sqrt[3]{2})=\omega^2\sqrt[3]{2},\\ &\sigma_{32}(\omega^2\sqrt[3]{2})=\sqrt[3]{2},\end{aligned}$$

vemos que

$$G(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}(\omega^2\sqrt[3]{2}))=\{\sigma_{11}=id,\sigma_{22}\}=\langle\sigma_{22}\rangle=G(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}(\omega\sqrt[3]{4})),$$

y podemos concluir que $\mathbb{Q}(\omega^2\sqrt[3]{2})=\mathbb{Q}(\omega\sqrt[3]{4})$.

(3) **¿Qué cuerpo de los anteriores es $\mathbb{Q}(\omega+\sqrt[3]{2})$?.** Determinemos el grupo de Galois $G(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}(\omega+\sqrt[3]{2}))$, que será el subgrupo de G consistente de los

$\sigma_{ij} \in G$ tales que $\sigma_{ij}(\omega + \sqrt[3]{2}) = \omega + \sqrt[3]{2}$. Puesto que

$$\begin{aligned}
\sigma_{11}(\omega + \sqrt[3]{2}) &= \omega + \sqrt[3]{2},\\
\sigma_{21}(\omega + \sqrt[3]{2}) &= \omega + \omega\sqrt[3]{2},\\
\sigma_{31}(\omega + \sqrt[3]{2}) &= \omega - \sqrt[3]{2} - \omega\sqrt[3]{2},\\
\sigma_{12}(\omega + \sqrt[3]{2}) &= -1 - \omega + \sqrt[3]{2},\\
\sigma_{22}(\omega + \sqrt[3]{2}) &= -1 - \omega + \omega^2\sqrt[3]{2},\\
\sigma_{32}(\omega + \sqrt[3]{2}) &= -1 - \omega - \sqrt[3]{2} - \omega\sqrt[3]{2},
\end{aligned}$$

vemos que

$$G(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega^2\sqrt[3]{2})) = \{\sigma_{11} = id\} = G(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega, \sqrt[3]{2})),$$

y podemos concluir que $\mathbb{Q}(\omega + \sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2})$.

Estas observaciones siempre tienen otras consecuencias interesantes. Por ejemplo, el grado del polinomio $Irr(\omega + \sqrt[3]{2}, \mathbb{Q})$ es seis, etc. □

ÁLGEBRA III (Doble grado Informática-Matemáticas)

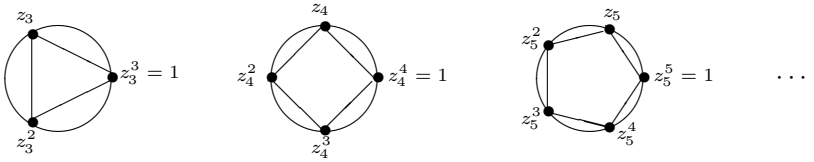
4. Extensiones Ciclotómicas, Radicales y Cíclicas

4.1. **Extensiones ciclotómicas.**

Recordar que, si $a \in \mathbb{C}$ es cualquier complejo no nulo, para cualquier natural $n \geq 2$, las raíces complejas del polinomio $x^n - a$, esto es, los números complejos z tales que $z^n = a$, son llamadas las **raíces n-ésimas del número** a (cuadradas si $n = 2$, cúbicas si $n = 3$, etc.). Un caso particular de especial interés, son las **raíces n-ésimas de la unidad**, esto es las raíces del polinomio $x^n - 1$. Para cada entero $n \geq 1$, estas conforman un subgrupo de orden n del grupo multiplicativo de los complejos

$$\mathbb{C}_n = \{z \in \mathbb{C}^\times \mid z^n = 1\} \leq \mathbb{C}^\times$$

En efecto, si $z, z' \in \mathbb{C}_n$, entonces $(zz')^n = z^n z'^n = 1 \cdot 1 = 1$. Además $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$. Así que $\mathbb{C}_n$ es cerrado para productos, inversos, y contiene al 1. Es por tanto un grupo. Podemos ser más explícitos en la descripción de las raíces n-ésimas de la unidad: Con la representación geométrica de los números complejos como puntos del plano $\mathbb{R}^2$ en mente, si dividimos el círculo de radio 1 en n sectores circulares de igual amplitud, esto es, todos de amplitud $\frac{2\pi}{n}$, y ubicamos el primero de ellos sobre el eje positivo de abscisas se nos determinan los n vértices de un polígono regular de n lados inscrito en la circunferencia $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$,



que corresponderían justo a los n números complejos $e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i\,\sin\frac{2k\pi}{n}$, para $k = 1, \ldots, n$. Todos estos listan las n raíces n-ésimas de la unidad, pues $(e^{\frac{2k\pi i}{n}})^n = e^{2k\pi i} = \cos 2k\pi + i \sin 2k\pi = 1$, así que

$$\mathbb{C}_n = \{e^{\frac{2k\pi i}{n}},\ 1 \leq k \leq n\}.$$

Entre esas n diferentes raíces complejas de la unidad hay una especial, que es llamada la **raíz n-ésima primitiva de la unidad**:

$$z_n = e^{\frac{2\pi i}{n}} = cos\frac{2\pi}{n} + i\,sen\frac{2\pi}{n},$$

que tiene la propiedad de ser un generador del grupo $\mathbb{C}_n$, ya que $z_n^k = e^{\frac{2k\pi i}{n}}$ y, por tanto, $\mathbb{C}_n = \{1, z_n, z_n^2, \ldots, z_n^{n-1}\} = \langle z_n \mid z_n^n = 1\rangle$ *es un grupo cíclico de orden n generado por* z_n.

Definición 1. *Si $K \leq \mathbb{C}$ es cualquier cuerpo de números, para cada entero $n \geq 1$, el cuerpo extensión $K(z_n)$ es llamado el n-ésimo* **cuerpo ciclotómico sobre** *K, o la n-ésima* **extension ciclotómica de** *K. Particularmente nos referimos a $\mathbb{Q}(z_n)$ como al n-ésimo* **cuerpo ciclotómico**.

Los siguientes son los primeros ejemplos de extensiones ciclotómicas,

- $z_1 = 1$, así que $K(z_1) = K$.
- $z_2 = -1$, luego $K(z_2) = K$.
- $z_3 = \omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, por tanto $K(z_3) = K(\omega) = K(i\sqrt{3})$.
- $z_4 = i$, luego $K(z_4) = K(i)$.

Notemos que $K(z_n) = K(x^n - 1)$, el cuerpo de descomposición del polinomio $x^n - 1$ sobre K. Por tanto la extensión ciclotómica $K(z_n)/K$ **es una extensión de normal**, cuyo grado será el grado del polinomio $Irr(z_n, K)$ que, al ser un divisor de $x^n - 1$, siempre ser $\leq n$. Intentamos a continuación conocer más información sobre el polinomio $Irr(z_n, K)$ y el grupo de Galois $G(K(z_n)/K) = G(x^n - 1/K)$.

Sabemos que, en el grupo $\mathbb{C}_n$, $or(z_n^k) = \frac{n}{(k,n)}$. En particular, $or(z_n^k) = n$, esto es, z_n^k es un generador de $\mathbb{C}_n$, si y solo si $(k, n) = 1$. Entonces,

$$Gen(\mathbb{C}_n) = \{z \in \mathbb{C}_n \mid or(z) = n\} = \{z_n^k \mid 1 \leq k \leq n,\, mcd(k, n) = 1\}$$

y $\mathbb{C}_n$ tiene exactamente $\varphi(n)$ generadores, donde φ es la función de Euler. Recordar que, si $p_1, \ldots, p_r$ son los diferentes primos positivos que dividen al natural n, digamos que $n = p_1^{e_1} \cdots p_r^{e_r}$, entonces

$$\begin{aligned}\varphi(n) &= p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1) = p_1^{e_1-1} p_1 \Big(1 - \frac{1}{p_1}\Big) \cdots p_r^{e_r-1} p_r \Big(1 - \frac{1}{p_r}\Big) \\ &= p_1^{e_1} \Big(1 - \frac{1}{p_1}\Big) \cdots p_r^{e_1} \Big(1 - \frac{1}{p_r}\Big) = p_1^{e_1} \cdots p_r^{e_r} \Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big) \\ &= n\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big).\end{aligned}$$

Definición 2. *Se define el* n**-ésimo polinomio ciclotómico** Φ_n *por la fórmula*

$$\Phi_n = \prod_{z \in Gen(\mathbb{C}_n)} (x - z) = \prod_{\substack{1 \leq k \leq n \\ (k,\, n) = 1}} (x - z_n^k)\,.$$

Esto es, Φ_n es el polinomio mónico de grado $\varphi(n)$ cuya raíces son las raíces n-ésimas de la unidad de orden n. Los siguientes son unos primeros ejemplos

- $Gen(\mathbb{C}_1) = \{1\}$, y $\Phi_1 = x - 1$.
- $Gen(\mathbb{C}_2) = \{-1\}$, y $\Phi_2 = x + 1$.
- $Gen(\mathbb{C}_3) = \{\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \omega^2 = \overline{\omega}\}$, por tanto
$$\Phi_3 = (x - \omega)(x - \overline{\omega}) = x^2 - (\omega + \overline{\omega})x + \omega\overline{\omega} = x^2 + x + 1\,.$$
- $Gen(\mathbb{C}_4) = \{i, i^3 = -i\}$, y $\Phi_4 = (x - i)(x + i) = x^2 + 1$.

El siguiente hecho es muy útil para el cálculo recursivo de los polinomios ciclotómicos.

Proposición 3. *Para todo natural* $n \geq 1$ *se verifica que*

$$x^n - 1 = \prod_{d|n} \Phi_d\,.$$

Demostración. Trabajando en el grupo multiplicativo $\mathbb{C}^\times$, tenemos que

$$\begin{aligned}\mathbb{C}_n = \{z \in \mathbb{C}^\times \mid z^n = 1\} = \{z \in \mathbb{C}^\times \mid or(z) | n\} &= \bigcup_{d|n} \{z \in \mathbb{C}^\times \mid or(z) = d\} \\ &= \bigcup_{d|n} Gen(\mathbb{C}_d)\,,\end{aligned}$$

siendo esa unión disjunta. Entonces,

$$x^n - 1 = \prod_{z \in \mathbb{C}_n} (x - z) = \prod_{\substack{d|n \\ z \,\in\, Gen(\mathbb{C}_d)}} (x - z) = \prod_{d|n} \prod_{z \in Gen(\mathbb{C}_d)} (x - z) = \prod_{d|n} \Phi_d\,.$$

□

Los siguientes ejemplos ilustran el uso de la anterior relación para cálculos:

- $x-1=\Phi_1$.
- $x^2-1=\Phi_1\Phi_2$, de donde $\Phi_2=x+1$.
- $x^3-1=\Phi_1\Phi_3$, de donde $\Phi_3=\frac{x^3-1}{x-1}=x^2+x+1$.
- Si p es un primo, $x^p-1=\Phi_1\Phi_p$, de donde

$$\Phi_p=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1.$$

- $x^6-1=\Phi_1\Phi_2\Phi_3\Phi_6=(\Phi_1\Phi_3)\Phi_2\Phi_6=(x^3-1)(x+1)\Phi_6$, de donde

$$\Phi_6=\frac{x^6-1}{(x^3-1)(x+1)}=\frac{x^3+1}{x+1}=x^2-x+1.$$

El siguiente teorema muestra que los polinomios ciclotómicos tienen sus coeficientes números enteros, y entonces $\Phi_n\in K[x]$ para todo cuerpo de números K, de manera que $Irr(z_n,K)|\Phi_n$ en $K[x]$. Para su demostración usaremos el siguiente lema:

Lema 4. *1) Sea $g\in\mathbb{Q}[x]$ mónico, entonces $g=\frac{1}{a}g_1$ donde $a\geq 1$ y $g_1\in\mathbb{Z}[x]$ es primitivo. 2) Sea $f\in\mathbb{Z}[x]$ mónico. Si $f=gh$ con $g,h\in\mathbb{Q}[x]$ mónicos, entonces $g,h\in\mathbb{Z}[x]$.*

Demostración. 1) Supongamos $g=\frac{a_0}{b_0}+\cdots+\frac{a_{n-1}}{b_{n-1}}x^{n-1}+x^n$. Sea $b=mcd(b_i)$. Claramente entonces $c_i=\frac{ba_i}{b_i}\in\mathbb{Z}$ para todo $i=0,\ldots,n-1$, y $bg=c_0+\cdots+c_{n-1}x^{n-1}+bx^n\in\mathbb{Z}[x]$. Siendo $c=mcd(c_0,\ldots,c_{n-1},b)$ su contenido, será $bg=cg_1$ con $g_1\in\mathbb{Z}[x]$ primitivo. Puesto que $c|b$, será $b=ac$ para un cierto $a\geq 1$. Pero entonces

$$g=\frac{1}{b}bg=\frac{1}{b}cg_1=\frac{1}{ac}cg_1=\frac{1}{a}g_1.$$

2) Pongamos $g=\frac{1}{a}g_1$ y $h=\frac{1}{b}h_1$, con $a,b\geq 1$ y $g_1,h_1\in\mathbb{Z}[x]$ primitivos. Entonces $f=\frac{1}{ab}g_1h_1$ y $abf=g_1h_1$. Puesto que f es primitivo (es mónico) y g_1 y h_1 también, por el Lema de Gauss (*"El contenido de un producto es el producto de los contenidos"*), concluimos que $ab=1$ y consecuentemente que $a=b=1$. □

Teorema 5. * *Para todo $n\geq 1$, $\Phi_n\in\mathbb{Z}[x]$.*

Demostración. Probamos primero que $\Phi_n\in\mathbb{Q}[x]$. Notemos que $\mathbb{C}_n\subseteq\mathbb{Q}(z_n)$. Supongamos cualquier $\sigma\in G(\mathbb{Q}(z_n)/\mathbb{Q})$. Entonces para todo $z\in\mathbb{C}_n$ se verifica que $\sigma(z)\in\mathbb{C}_n$, pues $\sigma(z)^n=\sigma(z^n)=\sigma(1)=1$. Se sigue que σ restringe definiendo un automorfismo del grupo $\mathbb{C}_n$, $\sigma:\mathbb{C}_n\cong\mathbb{C}_n$, y entonces también restringe a una permutación $\sigma:Gen(\mathbb{C}_n)\cong Gen(\mathbb{C}_n)$. Notemos que, por construcción, $\Phi_n\in\mathbb{Q}(z_n)[x]$. Si suponemos entonces que $\Phi_n=\sum a_ix^i$ con $a_i\in\mathbb{Q}(z_n)$, de la cadena de igualdades

$$\Phi_n^\sigma=\sum\sigma(a_i)x^i=\prod_{z\in Gen(\mathbb{C}_n)}(x-z)^\sigma=\prod_{z\in Gen(\mathbb{C}_n)}(x-\sigma(z))=\prod_{z\in Gen(\mathbb{C}_n)}(x-z)=\Phi_n(x)\,,$$

deducimos que $\sigma(a_i)=a_i$ para todo i y todo $\sigma\in G(\mathbb{Q}(z_n)/\mathbb{Q})$. De donde todo coeficiente $a_i\in\mathbb{Q}(z_n)^{G(\mathbb{Q}(z_n)/\mathbb{Q})}=\mathbb{Q}$. Así que $\Phi_n\in\mathbb{Q}[x]$.

Finalmente, puesto que $x^n-1=\Phi_n\prod_{d|n,d\neq n}\Phi_d$, el lema anterior nos permite concluir que, efectivamente, $\Phi_n\in\mathbb{Z}[x]$. □

Nuestro objetivo a continuación es probar que $\Phi_n = Irr(z_n, \mathbb{Q})$. Para ello, necesitamos unos resultados auxiliares. Entre ellos, el significado de los términos binomiales

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} = \frac{n(n-1)\cdots(n-i+1)}{i(i-1)\cdots 2\cdot 1}.$$

y que, en cualquier anillo conmutativo, digamos A, se verifica la fórmula binomial

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i},$$

donde el producto na de enteros $n \geq 0$ por elementos $a \in A$ es el usual: Si $n = 0$, entonces $0a = 0$; si $n > 0$, entonces $na = \sum_{i=1}^{n} a$ es la suma reiterada de ese elemento a consigo mismo n veces. En efecto, para $n = 1$ es fácil

$$\binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = b + a = a + b = (a+b)^1.$$

Y, para $n > 1$, su demostración es inductiva apoyándose en la igualdad

$$\begin{aligned}\binom{n}{j} + \binom{n}{j-1} &= \frac{n!}{j!(n-j)!} + \frac{n!}{(j-1)!(n-j+1)!} = \frac{n!(n-j)!(j-1)!(n-j+1+j)}{j!(n-j)!(j-1)!(n-j+1)!} \\ &= \frac{n!(n+1)}{j!(n-j+1)!} = \binom{n+1}{j}.\end{aligned}$$

Supuesta la validez para un n, entonces

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} \\ &= \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n+1-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} \\ &= \sum_{i=1}^{n+1} \binom{n+1}{i} a^i b^{n+1-i} + b^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}.\end{aligned}$$

Necesitamos también recordar que, para cada entero $n \geq 2$, tenemos el anillo de clases de congruencia módulo n,

$$\mathbb{Z}_n = \{[m] \mid m \in \mathbb{Z}\}$$

donde

$$\begin{aligned}[m] = [m'] &\Leftrightarrow m \equiv m' \mod n \\ &\Leftrightarrow n \mid m - m' \\ &\Leftrightarrow m - m' \in n\mathbb{Z} \\ &\Leftrightarrow m \text{ y } m' \text{ dan el mismo resto al dividirlos por } n,\end{aligned}$$

con las operaciones ordinarias de suma y producto de clases

$$[m] + [m'] = [m + m'],\ [m][m'] = [mm'].$$

Este sabemos que es efectivamente un anillo con exactamente n elementos distintos, que se listan como las clases módulo n de los n diferentes restos que se obtienen al dividir todos los enteros enteros entre n; esto es, las clases $[0], [1], \ldots, [n-1]$ que solemos denotar también simplemente por $0, 1, \ldots, n-1$. Así, es usual simplificar la notación y poner

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

con las operaciones

$$m + m' = \text{ resto de dividir en } \mathbb{Z} \text{ el entero m+m' entre } p,$$
$$mm' = \text{ resto de dividir en } \mathbb{Z} \text{ el entero producto de } mm' \text{ entre } p,$$

para cuales quiera $0 \leq m, m' \leq n-1$.

Haremos uso del epimorfismo de anillos **reducción módulo** n,

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}_n, \qquad m \mapsto \overline{m} = \text{ resto de dividir } m \text{ entre } n,$$

y del correspondiente inducido,

$$\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}_n[x], \qquad f = \textstyle\sum_i m_i x^i \mapsto \overline{f} = \sum_i \overline{m}_i x^i \ .$$

También haremos uso del grupo multiplicativo $\mathbb{Z}_n^\times$ de las unidades (elementos inversibles) del anillo $\mathbb{Z}_n$. Explícitamente,

$$\mathbb{Z}_n^\times = \{k \in \mathbb{Z}_n,\ mcd(k,n) = 1\} = \{k \mid 1 \leq k \leq n,\ mcd(k,n) = 1\}.$$

En efecto, supongamos que $k \in \mathbb{Z}_n$ con $mcd(k,n) = 1$. por el Teorema de Bezout, existirán $u, v \in \mathbb{Z}$ tal que $1 = uk + vn$. Pero entonces

$$1 = \overline{1} = \overline{uk} + \overline{vn} = \overline{uk} + 0 = \overline{u}\overline{k} = \overline{u}k$$

y concluimos que k es invertible en $\mathbb{Z}_n$, con $k^{-1} = \overline{u}$. Y recíprocamente, supongamos que $k \in \mathbb{Z}_n^\times$. Será $ku = 1$ (en $\mathbb{Z}_n$) para un cierto $u \in \mathbb{Z}_n$, lo que significa que 1 es el resto de dividir en $\mathbb{Z}$ el producto de los enteros k y u; esto es, si q es el correspondiente cociente, será $1 = ku - qn$. Y esta última igualdad implica que $mcd(k,n) = 1$ (pues si $d > 1$ fuese un divisor común, digamos que $k = dk'$ y $n = un'$, entonces $1 = d(k'u - qn')$ lo que en $\mathbb{Z}$ es imposible).

Para el siguiente lema auxiliar, supondremos que $p > 0$ es cualquier primo positivo de $\mathbb{Z}$. Notemos que, en este caso, $\mathbb{Z}_p^\times = \{1, \ldots, p-1\}$ y $\mathbb{Z}_p$ es un cuerpo.

Lema 6. *Sea* $\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}_p[x]$, $f = \sum_i m_i x^i \mapsto \overline{f} = \sum_i \overline{m}_i x^i$, *el epimorfismo de reducción módulo un primo* p.

(*i*) *Para cualesquiera* $f, g \in \mathbb{Z}[x]$, *se verifica que*

$$(\overline{f} + \overline{g})^p = \overline{f}^p + \overline{g}^p.$$

(*ii*) *Para cualquier* $m \in \mathbb{Z}$, $\overline{m}^p = \overline{m}$.

(*iii*) *Para cualesquiera* $m_1, \ldots, m_r \in \mathbb{Z}$ *y* $f_1, \ldots, f_r \in \mathbb{Z}[x]$, *se verifica que*

$$(\overline{m}_1\overline{f}_1 + \cdots + \overline{m}_r\overline{f}_r)^p = \overline{m}_1\overline{f}_1^p + \cdots + \overline{m}_r\overline{f}_r^p.$$

(*iv*) *Para cualquier* $g \in \mathbb{Z}[x]$, *se verifica que*

$$\overline{g}^p = \overline{g}(x^p),$$

donde $\overline{g}(x^p)$ *es el polinomio resultante de sustituir* x *en* $\overline{g}$ *por* x^p.

Demostración. (*i*):

$$(\overline{f} + \overline{g})^p = \overline{(f+g)^p} = \overline{\sum_{i=0}^{p} \binom{p}{i} f^i g^{p-i}} = \sum_{i=0}^{p} \overline{\binom{p}{i}}\overline{f}^i\overline{g}^{p-i} = \overline{f}^p + \overline{g}^p.$$

(*ii*) Este es el Pequeño Teorema de Fermat: El grupo $\mathbb{Z}_p^\times$ es de orden $p-1$, por tanto, si $\overline{m} \neq 0$, se tendrá que $\overline{m}^{p-1} = 1$. Luego $\overline{m}^p = \overline{m}$ sea m cualquiera.

(*iii*) Es consecuencia de (*i*) y (*ii*), y se argumenta por una simple inducción en r.

(iv) Supongamos $g = \sum_{i=0}^{n} m_i x^i$. Entonces

$$\overline{g}^p = (\sum_i \overline{m}_i x^i)^p = (\sum_i \overline{m}_i \overline{x^i})^p = \sum_i \overline{m}_i \overline{x^{ip}} = \sum_i \overline{m}_i (x^p)^i = \overline{g}(x^p). \quad \square$$

Con todo lo anterior, podemos ya abordar el siguiente

Teorema 7. *Para todo natural $n \geq 1$ el polinomio Φ_n es irreducible en $\mathbb{Q}[x]$. Entonces,*

$$\Phi_n = Irr(z_n, \mathbb{Q}).$$

Demostración. Pongamos $f = Irr(z_n, \mathbb{Q})$. Probaremos a continuación que, para toda raíz z de f y cualquier primo p con $p \nmid n$ se tiene que z^p es también una raíz de f. Un uso reiterado de esta propiedad nos conduce a que $z_n^{p_1^{m_1} \cdots p_r^{m_r}}$ es una raíz de f para todos los primos $p_1, \ldots p_r$ que no dividan a n; esto es, a que z_n^k es una raíz de f siempre que $(k, n) = 1$. Pero esto implica que f tiene a todo elemento del conjunto $Gen(\mathbb{C}_n)$ como una de sus raíces, lo que implica que $gr(f) \geq \varphi(n)$; puesto que $f | \Phi_n$ y ambos son mónicos, concluimos que $f = \Phi_n$. Así que, $\Phi_n = Irr(z_n, \mathbb{Q})$.

Supongamos entonces que $f(z) = 0$ y que p es un primo con $p \nmid n$.

Notemos que ha de ser $x^n - 1 = fg$ para un cierto polinomio $g \in \mathbb{Q}[x]$, y el Lema 4 nos asegura que $f, g \in \mathbb{Z}[x]$. Como $z^p \in \mathbb{C}_n$, $0 = (z^p)^n - 1 = f(z^p)g(z^p)$ y, por tanto, $f(z^p) = 0$ o $g(z^p) = 0$. La demostración se reduce a ver que no es posible que $g(z^p) = 0$: Supongamos, por contrario, que $g(z^p) = 0$. Consideremos el polinomio $g(x^p)$, que tiene entonces a z como raíz. Como $f = Irr(z, \mathbb{Q})$, ha de ser $f | g(x^p)$ (necesariamente en $\mathbb{Z}[x]$, de nuevo por el Lema 4). Considerando ahora el epimorfismo de reducción módulo p, $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $h(x) \mapsto \overline{h}(x)$, tenemos que $\overline{f} | \overline{g}(x^p)$ en el anillo $\mathbb{Z}_p[x]$. Puesto que $\overline{g}(x^p) = \overline{g}^p$, concluimos que $\overline{f} | \overline{g}^p$ en el anillo $\mathbb{Z}_p[x]$, lo que particularmente implica que toda raíz del polinomio $\overline{f}$ (en cualquier cuerpo extensión de $\mathbb{Z}_p$) es también una raíz del polinomio $\overline{g}$. Pero, dada la igualdad $x^n - 1 = \overline{f}(x)\overline{g}(x)$ en $\mathbb{Z}_p[x]$, esto nos lleva a que el polinomio $x^n - 1 \in \mathbb{Z}_p[x]$ tiene raíces múltiples. Pero esto es contradictorio (ver Proposición 1.1 en Tema 1), ya que el derivado de este polinomio es

$$nx^{n-1} = x^{n-1} + \overset{n}{\cdots} + x^{n-1} = (1 + \overset{n}{\cdots} + 1)x^{n-1} = \overline{n}x^{n-1},$$

que es asociado de x^{n-1} (recordemos que $p \nmid n$ y por tanto $\overline{n} \neq 0$), y claramente primo relativo con $x^n - 1$. $\square$

Nos centramos ahora en el grupo de Galois de una extensión ciclotómica.

Teorema 8. * *Para cualquier cuerpo de números K, hay un monomorfismo de grupos*

$$G(K(z_n)/K) \to \mathbb{Z}_n^\times, \quad \sigma \mapsto k \text{ si } \sigma(z_n) = z_n^k.$$

En particular, $G(\mathbb{Q}(z_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$.

Demostración. Sea $\sigma \in G(K(z_n)/K)$. Puesto que z_n es raíz de Φ_n que es un polinomio de $\mathbb{Q}[x]$ (también entonces $\Phi \in K[x]$, pues $\mathbb{Q} \leq K$) y por tanto $\Phi_n^\sigma = \Phi_n$, necesariamente $\sigma(z_n)$ será otra raíz de Φ_n (ver Lema 3 en Tema 3), esto es $\sigma(z_n) = z_n^k$ para un cierto $k \in \mathbb{Z}_n^\times$. Podemos definir así la aplicación

$$f : G(K(z_n)/K) \to \mathbb{Z}_n^\times, \quad \sigma \mapsto f(\sigma) = k \text{ si } \sigma(z_n) = z_n^k.$$

Esta aplicación es inyectiva, pues cada σ está totalmente determinada por quien sea la imagen del generador $\sigma(z_n)$. Y es efectivamente un monomorfismo de grupos: Sean $\sigma, \tau \in$

$G(K(z_n)/K)$ con $f(\sigma) = k$ y $f(\tau) = j$. Supongamos que $j\,k = q\,n + r$, con $0 \leq r \leq n-1$. entonces $f(\sigma)f(\tau) = r$, y como

$$\sigma\tau(z_n) = \sigma(z_n^j) = \sigma(z_n)^j = (z_n^k)^j = z_n^{kj} = z_n^{qn+r} = (z_n^n)^q z_n^r = z_n^r\,,$$

concluimos que $f(\sigma\tau) = r = f(\sigma)f(\tau)$ en el anillo $\mathbb{Z}_n$.

En el caso particular $K = \mathbb{Q}$, el resultado se sigue dado que ambos grupos $G(\mathbb{Q}(z_n)/K)$ y $\mathbb{Z}_n^\times$ son del mismo orden, $\varphi(n)$. □

Corolario 9. *Toda extensión ciclotómica tiene grupo de Galois abeliano.*

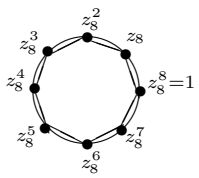
Ejemplo 10. *Sea z_8 la raíz octava primitiva de la unidad.*

(1) *Describir los complejos z_8^k, $1 \leq k \leq 8$, en la forma a+bi y representarlos geométricamente como puntos en el plano Euclídeo.*
(2) *Calcular Φ_8.*
(3) *Describir el grupo $G(\mathbb{Q}(z_8)/\mathbb{Q})$ y probar que es isomorfo al grupo de Klein $K = \langle u, v \mid u^2 = 1, v^2 = 1, uv = vu\rangle$ ($\cong \mathbb{C}_2 \times \mathbb{C}_2$).*
(4) *Describir su retículo de subgrupos de $G(\mathbb{Q}(z_8)/\mathbb{Q})$.*
(5) *Describir el retículo de subcuerpos de $\mathbb{Q}(z_8)$.*

Solución: (1) Puesto que $z_8 = cos(\pi/4) + i\,sen(\pi/4)$, tenemos que

$$\begin{cases} z_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, & z_8^2 = i, & z_8^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, & z_8^4 = -1, \\ z_8^5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, & z_8^6 = -i, & z_8^7 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, & z_8^8 = 1. \end{cases}$$

Su representación geométrica en el plano consiste de los 8 vértices del octógono inscrito en la circunferencia S^1



(2) Puesto que $x^8 - 1 = \Phi_1\Phi_2\Phi_4\Phi_8$ y $\Phi_1\Phi_2\Phi_4 = x^4 - 1$, concluimos que

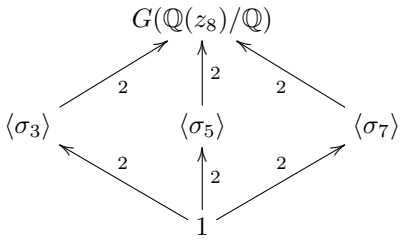
$$\Phi_8 = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1.$$

(3) Conocemos que que el grupo de Galois $G(\mathbb{Q}(z_8)/\mathbb{Q})$ es isomorfo al grupo de las unidades del anillo de restos módulo 8, $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. Analizando este grupo, donde $j \cdot k = \overline{j\,k}$ (= resto de dividir el producto de j y k en $\mathbb{Z}$ entre 8), vemos que es un grupo de orden 4 tipo Klein, pues es abeliano y todos sus elementos no triviales son de orden 2: $3^2 = 1$, $5^2 = 1$, $7^2 = 1$. Entonces

$$G = \{\sigma_j \mid :\ \sigma_j(z_8) = z_8^j,\ j = 1, 3, 5, 7\},$$

con multiplicación $\sigma_j\sigma_k = \sigma_{\overline{j\cdot k}}$. Por el Teorema de Dyck (ya que $\sigma_3^2 = id = \sigma_5^2$ y $\sigma_3\sigma_5 = \sigma_5\sigma_3$) existe un homomorfismo $\phi : K \to G$ tal que $\phi(u) = \sigma_3$ y $\phi(v) = \sigma_5$. Su imagen también contiene a $\sigma_7 = \sigma_3\sigma_5 = \phi(uv)$ y, obviamente, a $\sigma_1 = id$, y es por tanto un epimorfismo. Puesto que K y G tiene ambos cuatro elementos, $\phi : K \cong G$ es un isomorfismo.

(4) El grupo de Galois tiene entonces tres subgrupos propios, todos cíclicos de orden 2: $\langle\sigma_3\rangle$, $\langle\sigma_5\rangle$ y $\langle\sigma_7\rangle$. Y el retículo de subgrupos será de la forma



(5) Por el Teorema Fundamental de la Teoría de Galois, existen exactamente tres cuerpos intermedios, que serán los subcuerpos fijos correspondientes a los tres subgrupos anteriores. Para determinar el subcuerpo fijo bajo σ_3, discutamos la ecuación $\sigma_3(\alpha) = \alpha$, con $\alpha = a_0 + a_1 z_8 + a_2 z_8^2 + a_3 z_8^3$, donde los $a_j \in \mathbb{Q}$. Como $\sigma_3(\alpha) = a_0 + a_1 z_8^3 + a_2 z_8^6 + a_3 z_8^9$, si tenemos en cuenta que $z_8^8 = 1$ y que $z_8^4 = -1$, resulta que $\sigma_3(\alpha) = \alpha$ si y solo si

$$a_0 + a_1 z_8^3 - a_2 z_8^2 + a_3 z_8 = a_0 + a_1 z_8 + a_2 z_8^2 + a_3 z_8^3.$$

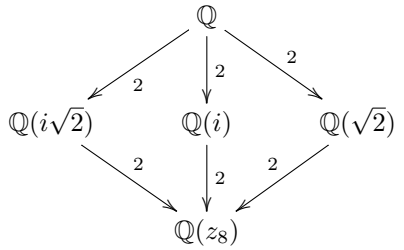
Lo que se verifica si y solo si $a_1 = a_3$ y $a_2 = 0$. Por tanto

$$\mathbb{Q}(z_8)^{\sigma_3} = \{a + b(z + z^3),\, a, b \in \mathbb{Q}\}.$$

Ahora,como $z + z^3 = (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) + (-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = i\sqrt{2}$, concluimos que

$$\mathbb{Q}(z_8)^{\sigma_3} = \mathbb{Q}(i\sqrt{2})\,.$$

Procediendo del mismo modo, calculamos los otros dos subcuerpos fijos y concluimos el retículo de subcuerpos es



4.2. **Extensiones radicales y cíclicas.**

Recordemos que, si $0 \neq a = re^{i\theta} = r(cos\,\theta + i\,sen\,\theta)$ es cualquier complejo no nulo expresado en su forma polar, entonces el complejo $\sqrt[n]{r}\, e^{i\frac{\theta}{n}}$ es una particular raíz n-ésima de a a la que denotaremos por $\sqrt[n]{a}$. Esto es,

$$\sqrt[n]{a} = \sqrt[n]{r}\, e^{i\frac{\theta}{n}} = \sqrt[n]{r}\,\left(cos\frac{\theta}{n} + i\,sen\frac{\theta}{n}\right).$$

Y también que el conjunto de las n diferentes n raíces n-ésimas de a (es decir, raíces complejas de $x^n - a$) es

$$\{\sqrt[n]{a},\ \sqrt[n]{a}\, z_n,\ \sqrt[n]{a}\, z_n^2,\ \ldots,\ \sqrt[n]{a}\, z_n^{n-1}\},$$

donde $\sqrt[n]{a}\, z_n^k = \sqrt[n]{r}\, e^{i\frac{\theta+2k\pi}{n}}$ para cada $k = 1, \ldots, n$.

Por una **extensión radical** de un cuerpo de números $K \leq \mathbb{C}$ se entiende una extensión simple de este cuerpo, que es generada por una raíz n-ésima, para algún $n \geq 1$, de algún número $a \in K$. Dicho de otra forma, una extensión radical de K es un cuerpo de la forma

$K(\alpha)$, donde $\alpha^n = a \in K$ para algún $n \geq 1$. Alternativamente, también podemos decir que una extensión radical de un cuerpo de números K es un cuerpo de números de la forma $K(\sqrt[n]{a}z_n^k)$ para algún $a \in K$, algún $n \geq 1$ y algún k con $1 \leq k \leq n$. Por ejemplo, las extensiones ciclotómicas son extensiones radicales.

Las extensiones radicales están muy relacionadas con las llamadas **extensiones cíclicas**, esto es, extensiones normales E/K cuyo grupo de Galois $G(E/K)$ es cíclico. Para establecer esta relación, haremos uso del siguiente resultado conocido como el Lema de independencia de Dedekind.

Lema 11 (Dedekind)**.** *Sean $\sigma_1, \ldots, \sigma_n : E \to \mathbb{C}$ son diferentes inmersiones de un cuerpo de números E. Si $a_1, \ldots, a_n \in \mathbb{C}$ son tales que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$ para todo $\alpha \in E$, entonces $a_1 = \cdots = a_n = 0$.*

Demostración. Procedemos por inducción en n. Si $n = 1$, tenemos la igualdad $0 = a_1\sigma_1(1) = a_1$ que prueba el lema. Supongamos entonces $n > 1$ y que el lema es cierto para el caso de $n-1$ inmersiones complejas E. Si $a_1 = 0$, el resultado se deduce de la hipótesis de inducción. Veamos que la alternativa no se puede dar, así que supongamos que $a_1 \neq 0$.

Poniendo $b_j = -a_j a_1^{-1}$, tendremos la igualdad

$$\sigma_1(\alpha) = \sum_{j=2}^{n} b_j\sigma_j(\alpha) = b_2\sigma_2(\alpha) + \cdots + b_n\sigma_n(\alpha), \quad \text{para todo } \alpha \in E.$$

Siendo $\alpha, \beta \in E$ cualesquiera dos elementos, puesto que $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$, tenemos por un lado la igualdad

$$\sigma_1(\alpha\beta) = \sum_{j=2}^{n} b_j\sigma_j(\alpha)\sigma_j(\beta) = b_2\sigma_2(\alpha)\sigma_2(\beta) + \cdots + b_n\sigma_n(\alpha)\sigma_n(\beta),$$

y por otro lado, puesto que $\sigma_1(\alpha\beta) = \sigma_1(\alpha)\sigma_1(\beta)$, tenemos la igualdad

$$\sigma_1(\alpha\beta) = \sum_{j=2}^{n} b_j\sigma_j(\alpha)\sigma_1(\beta) = b_2\sigma_2(\alpha)\sigma_1(\beta) + \cdots + b_n\sigma_n(\alpha)\sigma_1(\beta)\,.$$

Restando ambas expresiones, obtenemos que para todo $\alpha, \beta \in E$ se da la igualdad

$$0 = \sum_{j=2}^{n} b_j\big(\sigma_j(\beta) - \sigma_1(\beta)\big)\sigma_j(\alpha) = b_2\big(\sigma_2(\beta) - \sigma_1(\beta)\big)\sigma_2(\alpha) + \cdots + b_n\big(\sigma_n(\beta) - \sigma_1(\beta)\big)\sigma_n(\alpha).$$

Como es para todo $\alpha \in E$, aplicando la hipótesis de inducción, concluimos que ha de ser $b_j\big(\sigma_j(\beta) - \sigma_1(\beta)\big) = 0$, y esto para cualquier $\beta \in E$. Pero, como las inmersiones son diferentes, para cada $j = 2, \cdots, n$ es posible encontrar un $\beta \in E$ tal que $\sigma_j(\beta) \neq \sigma_1(\beta)$ y concluimos que ha de ser $b_j = 0$ para todo $j = 2, \cdots, n$. Esto nos lleva a que $\sigma_1(\alpha) = 0$ para todo $\alpha \in E$, lo que imposible ya que $\sigma_1(1) = 1$. □

El siguiente Teorema de Lagrange muestra que, en presencia de adecuadas raíces de la unidad en el cuerpo base, una extensión es radical si y solo si es cíclica.

Teorema 12. ⋆ *Sea E/K una extensión finita de cuerpos de números, donde $\mathbb{C}_n \subseteq K$ ($\sim z_n \in K$). Son equivalentes:*
(1) *E es una extensión radical de K generada por una raíz n-ésima de un elemento de K.*
(2) *E/K es una extensión cíclica y de grado un divisor de n.*

Demostración. (1) $\Rightarrow$ (2): Por hipótesis $E = K(\sqrt[n]{a}z)$, para algún $a \in K$ y algún $z \in \mathbb{C}_n$. Como $z \in K$, resulta que $E = K(\sqrt[n]{a})$. Además, como el cuerpo de descomposición del polinomio $x^n - a$ sobre K es $K(\{\sqrt[n]{a}z,\, z \in \mathbb{C}_n\}) = K(\sqrt[n]{a}) = E$, ya que $\mathbb{C}_n \subseteq K$, la extensión E/K es normal.

Ahora, cada $\sigma \in G(E/K)$ está determinado por quien sea $\sigma(\sqrt[n]{a})$, que sabemos ha de ser otra raíz del polinomio $(x^n - a)^\sigma = x^n - a$. Así que que ha de ser $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\, z$ para algún $z \in \mathbb{C}_n$. Tenemos entonces una aplicación inyectiva

$$f : G(E/K) \to \mathbb{C}_n, \quad \sigma \mapsto f(\sigma) = z \;\text{ si }\; \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\, z\,.$$

Esta aplicación es realmente un monomorfismo de grupos, pues si $\sigma' \in G(E/K)$ es tal que $\sigma'(\sqrt[n]{a}) = \sqrt[n]{a}z'$, entonces

$$\sigma\sigma'(\sqrt[n]{a}) = \sigma(\sqrt[n]{a}z') = \sigma(\sqrt[n]{a})\sigma'(z') = \sqrt[n]{a}\, zz'\,,$$

de manera que $f(\sigma\sigma') = zz' = f(\sigma)f\sigma')$. El grupo $G(E/K)$ es entonces isomorfo a un subgrupo del grupo cíclico $\mathbb{C}_n$ y por tanto también cíclico y de orden un divisor de $n = |\mathbb{C}_n|$.

(2) $\Rightarrow$ (1): Supongamos que E/K es normal, con $[E : K] = d$, donde $d \mid n$, y que $G(E/K)$ es un grupo cíclico generado por σ. Notemos que la hipótesis de que $\mathbb{C}_n \subseteq K$ implica que $\mathbb{C}_d \subseteq K$. De hecho, si $n = dd'$, entonces $z_n^{d'} = e^{i\frac{2\pi d'}{dd'}} = e^{i\frac{2\pi}{d}} = z_d$ y $z_d \in K$. Para cada $x \in E$, formemos el elemento de E, llamado su **resolvente de Lagrange**,

$$\alpha_x = x + \sigma(x)z_d^{d-1} + \sigma^2(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d\,.$$

Por el Lema de independencia de Dedekind, ha de ser $\alpha_x \neq 0$ para algún $x \in E$. Fijemos un tal x y sea $\alpha = \alpha_x$. Observamos entonces que

$$\begin{aligned}
\sigma(\alpha) &= \sigma(x) + \sigma^2(x)z_d^{d-1} + \sigma^3(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d^2 + \sigma^d(x)z_d \\
&= \sigma(x)z_d^d + \sigma^2(x)z_d^{d-1} + \sigma^3(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d^2 + xz_d \\
&= z_d\Big(x + \sigma(x)z_d^{d-1} + \sigma^2(x)z_d^{d-2} + \cdots + \sigma^{d-1}(x)z_d\Big) \\
&= \alpha\, z_d.
\end{aligned}$$

Así $0 \neq \alpha \in E$ y $\sigma(\alpha) = z_d\alpha$.

Vemos entonces, recursivamente, que $\sigma^k(\alpha) = z_d^k\alpha$, lo que nos lleva a que $\sigma^k(\alpha) \neq \alpha$, para $k = 1, \ldots, d-1$. Pero entonces $G(E/K(\alpha)) = \{id\} = G(E/E)$ y concluimos por el Teorema Fundamental de la Teoría de Galois, concluimos que $E = K(\alpha)$.

Vemos finalmente que $\sigma(\alpha^n) = \sigma(\alpha)^n = z_d^n\alpha^n = \alpha^n$, ya que $z_d^n = 1$ al ser d un divisor de n. De manera que $\alpha^n \in E^{G(E/K)} = K$, y concluimos que, efectivamente, la extensión E/K es radical y está generada por una raíz n-ésima de un elemento de K.

5. Resolución de ecuaciones polinómicas por radicales

Sea $f \in K[x]$ un polinomio con coeficientes en un cuerpo de números $K \leq \mathbb{C}$. Nos plantemos el problema de saber si es posible determinar sus raíces mediante un uso reiterado de las operaciones algebraicas básicas de suma, resta, multiplicación, división y extracción de radicales desde números del cuerpo de coeficientes K. En caso positivo, diremos que **el polinomio f es resoluble por radicales sobre** K, o también que **la ecuación polinómica** $f(x) = 0$ **es resoluble por radicales** sobre K. Más formalmente, establecemos que

Definición 1. *Sea $f \in K[x]$, donde K es un cuerpo de números. Se dice que f* **es resoluble por radicales sobre** *K si existe una torre de cuerpos de números*

$$K = K_0 \leq K_1 \leq \cdots \leq K_r\,,$$

tal que cada extensión K_{i+1}/K_i es una extensión radical, y tal que su extremo K_r contenga a todas las raíces del polinomio f (lo que equivale a decir que $K(f) \leq K_r$). Una tal torre se llama una **torre radical** *de origen K en cuyo extremo el polinomio f descompone totalmente.*

Este concepto de resolubilidad de f es relativo al cuerpo K, y bien podría ser que un polinomio f sea resoluble sobre un cuerpo de números y no sobre otro. Aunque es fácil argumentar que si f es resoluble por radicales sobre un cuerpo K, entonces lo es sobre cualquier cuerpo E extensión de K: Si E/K es una extensión y $K = K_0 \leq K_1 \leq \cdots \leq K_r$ es una torre radical en cuyo extremo descompone f, donde $K_{i+1} = K_i(\alpha_i)$ con $\alpha_i^{n_i} \in K_i$, entonces, definiendo $E_0 = E$ y $E_{i+1} = E_i(\alpha_i)$, obtenemos una torre radical $E = E_0 \leq E_1 \leq \cdots \leq E_r$, en cuyo extremo están todas las raíces de f. Así que $f \in E[x]$ y f es resoluble por radicales sobre E.

Ilustramos la definición con algunos ejemplos:

- El polinomio $x^2+x-\frac{1}{2}$ es resoluble sobre $\mathbb{Q}$ (y entonces sobre cualquier cuerpo de números). Sus raíces son $\frac{-1\pm\sqrt{3}}{2}$, y ambas están en el extremo de la torre radical
$$\mathbb{Q} \leq \mathbb{Q}\big(\sqrt{3}\,\big)\,.$$
- Los polinomios $x^n - 1$ y Φ_n son resolubles sobre $\mathbb{Q}$. Su cuerpo de descomposición es la extensión ciclotómica $\mathbb{Q}(z_n)$, que es una extensión radical de $\mathbb{Q}$.
- Para cualquier $a \in K$, el polinomio $x^n - a$ es resoluble sobre K, pues todos sus raíces están en extremo de la torre radical: $K \leq K(z_n) \leq K(z_n, \sqrt[n]{a})$.
- El polinomio $x^3 - 6x^2 + 12x - 12 = (x-2)^3 - 4$ es resoluble sobre $\mathbb{Q}$. Sus raíces son
$$2 + \sqrt[3]{4},\ 2 - \frac{1 - i\sqrt{3}}{\sqrt[3]{2}},\ 2 - \frac{1 + i\sqrt{3}}{\sqrt[3]{2}}$$
y las cuatro están en el extremo de la torre radical
$$\mathbb{Q} \leq \mathbb{Q}\big(\sqrt[3]{2}\,\big) \leq \mathbb{Q}\big(\sqrt[3]{2}, i\sqrt{3}\,\big)\,.$$
- El polinomio $x^4 - 4x^3 + 7x^2 - 6x + 4 = (x-1)^4 + (x-1)^2 + 2$ es resoluble por radicales sobre $\mathbb{Q}$. Sus raíces son
$$\frac{2 \pm \sqrt{2(-1 \pm i\sqrt{7}\,)}}{2}\,,$$

y las cuatro están en el extremo de la torre radical

$$\mathbb{Q} \le \mathbb{Q}\big(\sqrt{2}\,\big) \le \mathbb{Q}\big(\sqrt{2}, i\sqrt{7}\,\big) \le \mathbb{Q}\Big(\sqrt{2}, \sqrt{-1+i\sqrt{7}}\Big) \le \mathbb{Q}\Big(\sqrt{2}, \sqrt{-1+i\sqrt{7}}, \sqrt{-1-i\sqrt{7}}\Big)\,.$$

El siguiente hecho nos prepara para el resultado fundamental sobre resolución de ecuaciones polinómicas.

Lema 2. *Si $K \le K_1 \le \cdots \le K_r$ es cualquier torre radical, entonces existe una otra torre radical $K \le E_1 \le \cdots \le E_s$, tal que $K_r \le E_s$ y E_s/K es normal.*

Demostración. Procedemos inductivamente en r.

Caso $r = 1$. Tenemos $K \le K_1$, donde $K_1 = K\big(\sqrt[n]{a}\, z_n^k\big)$, para algún $a \in K$, $n \ge 1$ y $1 \le k \le n$. Consideremos la torre

$$K \le K(z_n) \le K\big(z_n, \sqrt[n]{a}\,\big)\,.$$

Es evidente que $K_1 \le K\big(z_n, \sqrt[n]{a}\,\big)$, y puesto que $K\big(z_n, \sqrt[n]{a}\,\big)$ es justamente el cuerpo de descomposición sobre K del polinomio $x^n - a$, la extensión $K\big(z_n, \sqrt[n]{a}\,\big)/K$ es normal.

Caso $r > 1$. Por hipótesis de inducción, existe una torre radical $K \le F_1 \le \cdots \le F_t$, tal que $K_{r-1} \le F_t$ y F_t/K es normal. Será F_t el cuerpo de descomposición sobre K de algún polinomio $f \in K[x]$, esto es, $F_t = K(\alpha_1, \ldots, \alpha_l)$ donde $\alpha_1, \ldots, \alpha_l$ son las diferentes raíces en $\mathbb{C}$ de ese f. Supongamos que su grupo de Galois es $G(F_t/K) = \{\sigma_1 = id, \sigma_2, \ldots, \sigma_m\}$.

Puesto que K_r/K_{r-1} es radical, será $K_r = K_{r-1}(\sqrt[n]{a}\, z_n^k)$, para algún $a \in K_{r-1}$, $n \ge 1$ y $1 \le k \le n$. Construimos entonces la torre radical

$$K \le F_1 \le \cdots \le F_t \le F_t(z_n) \le F_t\big(z_n, \sqrt[n]{a}\,\big) \le F_t\big(z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}\,\big) \le \cdots$$

$$\cdots \le F_t\big(z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}, \ldots, \sqrt[n]{\sigma_m(a)}\,\big) = E_s\,.$$

Manifiestamente se trata de una torre radical y $K_r \le E_s$. Bastará por tanto argumentar que E_s/K es normal:

Consideremos el polinomio $g = \prod_{i=1}^m \big(x^n - \sigma_i(a)\big) \in F_t[x]$. Para cualquier $\sigma \in G(F_t/K)$, la lista $(\sigma\sigma_1, \ldots, \sigma\sigma_m)$ es una permutación de la lista $(\sigma_1, \ldots, \sigma_m)$, y por consiguiente

$$g^\sigma = \prod_{i=1}^m (x^n - \sigma\sigma_i(a)) = \prod_{i=1}^m (x^n - \sigma_i(a)) = g;$$

esto es, los coeficientes de g están en el cuerpo fijo $F_t^{G(F_t/K)} = K$. Así que $g \in K[x]$. El cuerpo de descomposición sobre K del polinomio producto fg es justamente

$$K\big(\alpha_1, \ldots \alpha_k, z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}, \ldots, \sqrt[n]{\sigma_m(a)}\,\big) = F_t\big(z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}, \ldots, \sqrt[n]{\sigma_m(a)}\,\big) = E_s\,,$$

y concluimos que la extensión E_s/K es efectivamente normal. □

Proposición 3. *Si $f \in K[x]$ es resoluble, existe una torre radical $K = K_0 \le K_1 \le \cdots \le K_r$ tal que K_r/K es normal y $K(f) \le K_r$.*

Recordemos ahora que, si $f \in K[x]$, donde $K \le \mathbb{C}$ es un cuerpo de números, su **grupo de Galois sobre** K, denotado por $G(f/K)$, es el grupo de Galois sobre K de su cuerpo de descomposición. Esto es, $G(f/K) = G(K(f)/K)$.

Teorema 4 (Abel-Galois)**.** * *Un polinomio sobre un cuerpo de números es resoluble si y solo si su grupo de Galois es resoluble.*

DEMOSTRACIÓN. *Necesidad*: Por hipótesis, y aplicando el anterior lema, existe una torre radical $K = K_0 \leq K_1 \leq \cdots \leq K_r$, tal que f descompone totalmente en su extremo K_r y K_r/K es una extensión normal. Supongamos que cada $K_{i+1} = K_i(\alpha_i)$, donde $\alpha_i^{n_i} \in K_i$. Si tomamos $n = \prod n_i$ tendremos que $\alpha_i^n \in K_i$, para todo $i = 0, \ldots, r-1$, de manera que cada extensión K_{i+1}/K_i es una extensión radical generada por una raíz n-ésima de un elemento de K_i. Consideremos la raíz n-ésima primitiva de la unidad, $z = z_n$, y construimos la torre

$$K = K_0 \leq K_0(z) \leq K_1(z) \leq \cdots \leq K_r(z)\,.$$

Esta es también una torre radical, ya que $K_{i+1}(z) = K_i(\alpha_i, z) = K_i(z)(\alpha_i)$ y $\alpha_i^n \in K_i(z)$, y se verifica también que $K_r(z)/K$ es normal (ya que si K_r es el cuerpo de descomposición de un polinomio $g \in K[x]$, entonces $K_r(z)$ es el cuerpo de descomposición sobre K del polinomio producto $g(x^n - 1)$) y, obviamente, todas las raíces de f están en $K_r(z)$. Probaremos ahora sucesivamente los siguientes hechos:

(1) El grupo de Galois $G\big(K_r(z)/K(z)\big)$ es resoluble.
(2) El grupo de Galois $G\big(K_r(z)/K\big)$ es resoluble.
(3) El grupo de Galois $G\big(f/K\big) = G\big(K(f)/K\big)$ es resoluble.

(1): La extensión $K_r(z)/K$ es normal y la torre de subcuerpos

$$K(z) = K_0(z) \leq K_1(z) \leq \cdots \leq K_i(z) \leq K_{i+1}(z) \leq \cdots \leq K_r(z)\,,$$

corresponde por la conexión de Galois a la torre de subgrupos de su grupo de Galois

$$G\big(K_r(z)/K_0(z)\big) \geq \cdots \geq G\big(K_r(z)/K_i(z)\big) \geq G\big(K_r(z)/K_{i+1}(z)\big) \geq \cdots \geq G\big(K_r(z)/K_r(z)\big) = \{id\}.$$

Y resulta que esta es precisamente una serie del grupo $G\big(K_r(z)/K(z)\big)$ con factores cíclicos, de donde el grupo es resoluble. En efecto, puesto que cada $K_{i+1}(z)/K_i(z)$ es una extensión radical generada por una raíz n-ésima, y $z = z_n \in K_i(z)$, por el Teorema de Lagrange la extensión $K_{i+1}(z)/K_i(z)$ es cíclica, o sea, normal y con grupo de Galois $G\big(K_{i+1}(z)/K_i(z)\big)$ cíclico. Ahora, aplicando el Teorema Fundamental de la Teoría de Galois a la torre

$$K_i(z) \leq K_{i+1}(z) \leq K_r(z),$$

podemos asegurar que

$$G\big(K_r(z)/K_{i+1}(z)\big) \trianglelefteq G\big(K_r(z)/K_i(z)\big),$$

y que

$$G\big(K_{i+1}(z)/K_i(z)\big) \cong \frac{G\big(K_r(z)/K_i(z)\big)}{G\big(K_r(z)/K_{i+1}(z)\big)}.$$

(2): En la torre $K \leq K(z) \leq K_r(z)$, la extensión $K(z)/K$ es normal (es ciclotómica). Por tanto

$$G\big(K_r(z)/K(z)\big) \trianglelefteq G\big(K_r(z)/K)\big)\,, \quad \text{y} \quad G\big(K(z)/K\big) \cong \frac{G\big(K_r(z)/K\big)}{G\big(K_r(z)/K(z)\big)}\,.$$

Conocemos que el grupo de Galois de la extensión ciclotómica $K(z)/K$ es abeliano y, por tanto resoluble; luego el grupo $G\big(K_r(z)/K\big)$ contiene un subgrupo normal y resoluble (por (1)), cuyo cociente es también resoluble y podemos concluir que él mismo es resoluble.

(3): Puesto que en $K_r(z)$ están todas las raíces de f, el cuerpo de descomposición de este polinomio sobre K está contenido en él, así que $K \leq K(f) \leq K_r(z)$. Entonces,

$$G\big(K_r(z)/K(f)\big) \trianglelefteq G\big(K_r(z)/K)\big)\,, \quad \text{y} \quad G\big(K(f)/K\big) \cong \frac{G\big(K_r(z)/K\big)}{G\big(K_r(z)/K(f)\big)}\,.$$

Como todo grupo cociente de un resoluble es resoluble, concluimos que $G(f/K) = G\big(K(f)/K\big)$ es resoluble.

Suficiencia: Denotemos por $E = K(f)$ al cuerpo de descomposición de f sobre K. Por hipótesis el grupo $G\big(E/K\big)$ es resoluble. Supongamos que $[E : K] = n$. Llamemos $z = z_n$ y consideremos la torre $K \leq K(z) \leq E(z)$. Como $E(z) = K(f(x^n - 1))$, la extensión $E(z)/K$ es normal, y también entonces lo es la extensión $E(z)/K(z)$. Si $\sigma \in G\big(E(z)/K(z)\big)$, su restricción a E es una K-inmersión compleja del cuerpo E y, por tanto, ya que E una extensión normal de K, se verificará que $\sigma\big(E\big) = E$; así que $\sigma|_E \in G\big(E/K\big)$. La correspondencia

$$G\big(E(z)/K(z)\big) \longrightarrow G\big(E/K\big)\,, \quad \sigma \mapsto \sigma|_E\,,$$

es un homomorfismo de grupos que fácilmente se reconoce como un monomorfismo (si $\sigma|_E = id$, como $\sigma(z) = z$, entonces $\sigma \in G\big(E(z)/E(z)\big) = \{id\}$). Desde que todo subgrupo de un grupo resoluble lo es así mismo, concluimos que el grupo $G\big(E(z)/K(z)\big)$ es resoluble.

Existirá entonces una serie de ese grupo

$$G\big(E(z)/K(z)\big) = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{r-1} \trianglerighteq G_r = \{id\}\,,$$

cuyos factores G_i/G_{i+1} son cíclicos y de orden un divisor de $n = |G(E/K)|$ (el orden de cada G_i es un divisor del orden del grupo $G\big(E(z)/K(z)\big)$ que a su vez es un divisor del orden del grupo $G(E/K)$ que es $n = [E : K]$). Por la Conexión de Galois, tendremos asociada una torre de subcuerpos

$$K(z) = E(z)^{G_0} \leq E(z)^{G_1} \leq \cdots E(z)^{G_i} \leq E(z)^{G_{i+1}} \leq \cdots \leq E(z)^{G_r} = E(z)\,. \tag{1}$$

Como cada $G_i = G\big(E(z)/E(z)^{G_i}\big)$ y es $G_{i+1} \trianglelefteq G_i$, el Teorema Fundamental de la Teoría de Galois, aplicado a cada torre $E(z)^{G_i} \leq E(z)^{G_{i+1}} \leq E(z)$, nos garantiza que cada eslabón $E(z)^{G_{i+1}}/E(z)^{G_i}$ de la torre (1) es una extensión normal con grupo de Galois

$$G\Big(E(z)^{G_{i+1}}/E(z)^{G_i}\Big) \cong G_i/G_{i+1}\,,$$

que es cíclico de orden un divisor de n. Como $z = z_n \in E(z)^{G_i}$, por el Teorema de Lagrange podemos concluir que cada extensión $E(z)^{G_{i+1}}/E(z)^{G_i}$ de la torre (1) es una extensión radical. Así que (1) es una torre de extensiones radicales, de manera que también lo es la torre

$$K \leq K(z) = E(z)^{G_0} \leq E(z)^{G_1} \leq \cdots E(z)^{G_i} \leq E(z)^{G_{i+1}} \leq \cdots \leq E(z)^{G_r} = E(z)\,.$$

en cuyo extremo están todas las raíces de f. □

Corolario 5 (Teorema de Abel)**.** *Todo polinomio cuyo grupo de Galois es conmutativo es resoluble por radicales.*

Debido al anterior resultado, los grupos conmutativos se llaman **abelianos**.

5.1. **El grupo de Galois como grupo de permutaciones.**

Supongamos que un polinomio $f = \sum_i a_i x^i \in K[x]$, con coeficientes en un cuerpo de numeros $K \leq \mathbb{C}$, tiene n raíces complejas diferentes, y que numeramos estas en la forma $\alpha_1, \ldots, \alpha_n$.

Si $\sigma \in G(f/K) = G\big(K(\alpha_1, \ldots, \alpha_n)/K\big)$, entonces para cualquier raíz α_j de f se tiene que

$$f(\sigma(\alpha_j)) = \sum_i a_i \sigma(\alpha_j) = \sum_i \sigma(a_i)\sigma(\alpha_j) = \sigma\big(\sum_i a_i \alpha_j\big) = \sigma(0) = 0.$$

Esto es, $\sigma(\alpha_j)$ es de nuevo una raíz del polinomio f. Se sigue que cada $\sigma \in G(f/K)$ define, por restricción, una aplicación, a la que denotaremos igual,

$$\sigma : \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}\,, \qquad \alpha_j \mapsto \sigma(\alpha_j)\,,$$

que es inyectiva (σ lo es), y entonces biyectiva. Así que la restricción de σ al conjunto $\{\alpha_1, \ldots, \alpha_n\}$ de las raíces de f es una permutación en este conjunto. La aplicación

$$G(f/K) \to S_n, \quad \sigma \mapsto \sigma \mid \sigma(i) = j \text{ si } \sigma(\alpha_i) = \alpha_j,$$

es un homomorfismo de grupos que es de hecho un monomorfismo (si $\sigma, \sigma' \in\in G(f/K)$ definiesen la misma permutación de S_n, sería por que actúan igualmente sobre todos los generadores α_i de la extensión $K(\alpha_1, \cdots, \alpha_n)$ y sería $\sigma = \sigma'$; ver Lema 2.20 en Tema 2). Consecuentemente, esa aplicación establece un isomorfismo entre el grupo de Galois del polinomio y su imagen. De esta forma vemos que

"El grupo de Galois $G(f/K)$ es isomorfo a un subgrupo de S_n."

Ejemplo 6. Consideremos el polinomio

$$f = x^3 - 7x^2 + 12x - 4 = (x-2)(x^2 - 5x + 2) \in \mathbb{Q}[x].$$

Sus raíces son $\alpha_1 = 2$, $\alpha_2 = \frac{5-\sqrt{17}}{2}$ y $\alpha_3 = \frac{5+\sqrt{17}}{2}$. Su cuerpo de descomposición es $\mathbb{Q}(\sqrt{17})$. Su grupo de Galois es

$$G(f/\mathbb{Q}) = G\big(\mathbb{Q}(\sqrt{17})/\mathbb{Q}\big) = \{id, \sigma\},$$

donde $\sigma : \mathbb{Q}(\sqrt{17}) \to \mathbb{Q}(\sqrt{17})$ es el automorfismo definido por $\sigma(a + b\sqrt{17}) = a - b\sqrt{17}$. Puesto que $\sigma(\alpha_1) = \alpha_1$, $\sigma(\alpha_2) = \alpha_3$ y $\sigma(\alpha_3) = \alpha_2$, vemos que $G(f/\mathbb{Q})$ es isomorfo al subgrupo de S_3 que consiste de la identidad y de la trasposición $(2, 3)$. Esto es, salvo isomorfismo,

$$G\big(x^3 - 7x^2 + 12x - 4\big) = \{id, (2,3)\} \leq S_3,$$

Por supuesto, que también concluimos que $G\big(x^3 - 7x^2 + 12x - 4\big) \cong C_2$ es un grupo cíclico de orden dos.

En varias ocasiones nos será de utilidad recurrir al polinomio reducido asociado a un polinomio. Un polinomio mónico $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$, donde K es un cuerpo de números, diremos que es **reducido** si $a_{n-1} = 0$. Puesto que, si $\alpha_1, \ldots, \alpha_n$ son sus raíces, es $f = \prod_{i=1}^{n}(x - \alpha_i)$ y, por tanto, $a_{n-1} = -(\alpha_1 + \cdots + \alpha_n)$. Resulta que f es reducido si y solo si sus raíces suman cero.

Para cualquier $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, mónico de grado n, se define su correspondiente **"reducido"** $\tilde{f}$ como el obtenido desde f al reemplazar la indeterminada x por $x - \frac{a_{n-1}}{n}$, esto es,

$$\tilde{f} = f\big(x - \tfrac{a_{n-1}}{n}\big)\,.$$

Si las raíces de $\tilde{f}$ son β_i, $i = 1, \ldots, n$, entonces las de f son $\alpha_i = \beta_i - \frac{a_{n-1}}{n}$, $i = 1, \ldots, n$. Como $\sum \beta_i = \sum(\alpha_i + \frac{a_{n-1}}{n}) = \sum \alpha_i + n\frac{a_{n-1}}{n} = -a_{n-1} + a_{n-1} = 0$, el polinomio $\tilde{f}$ es efectivamente reducido. Notemos también que f y $\tilde{f}$ tienen el mismo cuerpo de descomposición sobre K. Consecuentemente,

$$G(f/K) = G(\tilde{f}/K)\,.$$

Ejemplo 7. *Si $f = x^2 + 2x + 3$, su reducido es*

$$\tilde{f} = f(x-1) = (x-1)^2 + 2(x-1) + 3 = x^2 - 2x + 1 + 2x - 2 + 3 = x^2 + 2. \quad \square$$

5.2. **Ecuaciones cuadráticas.**

El grupo de Galois de un polinomio cuadrático sobre cualquier cuerpo de números es un subgrupo de S_1 o de S_2, según el número de raíces distintas que tenga, por tanto este siempre es resoluble por radicales. De hecho es bien familiar para todos la fórmula que permite el cálculo de sus raíces (y cuyo conocimiento histórico se remonta a la civilización babilónica):

Consideremos la ecuación cuadrática

$$x^2 + bx + c = 0\,,$$

cuyas soluciones son las raíces del polinomio cuadrático $f = x^2 + bx + c$. Reemplazando x por $x - \frac{b}{2}$, obtenemos su reducido

$$\tilde{f} = f\big(x - \frac{b}{2}\big) = x^2 - \frac{b^2 - 4c}{4},$$

cuyas raíces son claramente $\beta_1 = \frac{1}{2}\sqrt{b^2 - 4c}$ y $\beta_2 = -\frac{1}{2}\sqrt{b^2 - 4c}$. Entonces, las soluciones de la ecuación cuadrática original son $\alpha_i = \beta_i - \frac{b}{2}$, $i = 1, 2$; esto es,

$$\alpha_1 = \frac{-b - \sqrt{b^2 - 4c}}{2} \quad \text{y} \quad \alpha_2 = \frac{-b + \sqrt{b^2 - 4c}}{2}\,.$$

5.3. **Ecuaciones cúbicas.**

El grupo de Galois de un polinomio cúbico sobre cualquier cuerpo de números es un subgrupo de S_1, S_2 o S_3, según el número de raíces distintas que tenga, por tanto este siempre es resoluble. De hecho existen varios métodos para el cálculo de sus raíces. El primero es debido a Scipio del Ferro (1515: Martin Luther, La Reforma, El Renaciminento, ...), aunque una fórmula equivalente fue descubierta por Tartaglia sobre el mismo tiempo, y aparece impreso por primera vez en un libro de Cardano (1545), por lo que usualmente es conocida como el método de "Cardano".

Consideremos la ecuación cúbica

$$x^3 + bx^2 + cx + d = 0\,.$$

Obtengamos su reducida reemplazando x por $x - \frac{b}{3}$, que ser de la forma

$$x^3 + p\,x + q = 0\,,$$

cuyas soluciones $\beta_1, \beta_2, \beta_3$ nos darán las de la original por las igualdades $\alpha_i = \beta_i - \frac{b}{3}$, $i = 1, 2, 3$. La idea es obtener las soluciones x de la reducida como suma de dos números, digamos $x = y + z$, tales que $yz = \frac{-p}{3}$. Bajo esta última condición, obtener x es lo mismo que obtener y y z, pues dos números están totalmente determinados por quién sea su suma y su producto (si suman S y multiplica P, son las dos raíces del polinomio cuadrático $x^2 - Sx + P$). Ahora, $x = y + z$ es solución de la cúbica reducida si y solo si

$$\begin{aligned} 0 &= (y+z)^3 + p(y+z) + q = y^3 + z^3 + 3yz^2 + 3y^2 z + py + pz + q \\ &= y^3 + z^3 + 3z\frac{-p}{3} + 3y\frac{-p}{3} + py + pz + q = y^3 + z^3 - pz - py + py + pz + q \\ &= y^3 + z^3 + q. \end{aligned}$$

Esto es, si y solo si $y^3 + z^3 = -q$. Formamos entonces el sistema

$$\begin{cases} y^3 + z^3 = -q, \\ y^3 z^3 = \frac{-p^3}{27}, \end{cases}$$

que nos permite calcular y^3 y z^3 como las dos raíces del polinomio de segundo grado

$$x^2 + q\,x - \frac{p^3}{27} = 0,$$

obteniendo que (los valores de y y z son intercambiables sin que afecte al resultado de $x = y + z$)

$$y^3 = \frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}, \quad z^3 = \frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}\,.$$

Ahora, si $\omega = z_3 = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ es la raíz cúbica primitiva de la unidad, tenemos como posibles valores de y:

$$y_1 = \sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}}, \quad y_2 = \omega\sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}} \quad \text{e} \quad y_3 = \omega^2\sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}};$$

y de z:

$$z_1 = \sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}}, \quad z_2 = \omega\sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}} \quad \text{y} \quad z_3 = \omega^2\sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}}.$$

Para cualquiera de esas posibilidades se verifica que $y_j^3 + z_k^3 = -q$. Pero necesitamos que $y_j z_k = -p/3$ (para que $x = y_j + z_k$ sea solución de la cúbica reducida), y solo sabemos que $(y_j z_k)^3 = (-p/3)^3$ o, lo que es lo mismo, que $y_j z_k \in \{-p/3, -(p/3)\omega, -(p/3)\omega^2\}$. Entonces, cada y_j debe ser apareado con el z_k tal que su producto sea exactamente $-p/3$. Esto nos lleva a una breve discusión, que haríamos así:

- Si $y_1 z_1 = -p/3$, entonces $y_2 z_3 = -p/3 = y_3 z_2$, luego las soluciones de la reducida serían $\beta_1 = y_1 + z_1$, $\beta_2 = y_2 + z_3$ y $\beta_3 = y_3 + z_2$.
- Si fuese $y_1 z_1 = (-p/3)\omega$, entonces $y_1 z_3 = -p/3 = y_2 z_2 = y_3 z_1$, luego las soluciones serían $\beta_1 = y_1 + z_3$, $\beta_2 = y_2 + z_2$ y $\beta_3 = y_3 + z_1$.
- Si fuese $y_1 z_1 = (-p/3)\omega^2$, entonces $y_1 z_2 = -p/3 = y_2 z_1 = y_3 z_3$, y las soluciones $\beta_1 = y_1 + z_2$, $\beta_2 = y_2 + z_1$ y $\beta_3 = y_3 + z_3$.

Ejemplo 8. *Resolver la ecuación* $x^3 + 6x^2 + 9x + 4 = 0$

SOLUCIÓN: Sea $f = x^3 + 6x^2 + 9x + 4$. El reducido será

$$\tilde{f} = f(x-2) = (x-2)^3 + 6(x-2)^2 + 9(x-2) + 4 = \cdots = x^3 - 3x + 2.$$

Siguiendo el método de Cardano, buscamos sus raíces en la forma $x = y + z$ tal que $yz = 1$, y resulta que y^3 y z^3 han de ser soluciones al sistema

$$\begin{cases} y^3 + z^3 = -2, \\ y^3 z^3 = 1, \end{cases}$$

que nos permite calcular y^3 y z^3 como las dos soluciones de la ecuación $x^2 + 2x + 1 = 0$. Por tanto $y^3 = -1 = z^3$. Esto nos da tres posibles ys y zs:

$$\begin{cases} y_1 = e^{i\frac{\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \\ y_2 = \omega y_1 = e^{i\frac{2\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\pi} = -1, \\ y_3 = \omega^2 y_1 = e^{i\frac{4\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\frac{5\pi}{3}} = \frac{1}{2} - i\frac{\sqrt{3}}{2}, \end{cases}$$

$$\begin{cases} z_1 = e^{i\frac{\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \\ z_2 = \omega z_1 = e^{i\frac{2\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\pi} = -1, \\ z_3 = \omega^2 z_1 = e^{i\frac{4\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\frac{5\pi}{3}} = \frac{1}{2} - i\frac{\sqrt{3}}{2} \end{cases}$$

Estas han de emparejarse de manera que $y_j z_k = 1$. Vemos que $y_2 z_2 = (-1)(-1) = 1$, $y_1 z_3 = e^{i\frac{\pi}{3}} e^{i\frac{5\pi}{3}} = 1$ y que $y_3 z_1 = e^{i\frac{5\pi}{3}} e^{i\frac{\pi}{3}} = 1$, lo que nos da las raíces de la cúbica reducida

$$\begin{cases} \beta_1 = y_2 + z_2 = (-1) + (-1) = -2, \\ \beta_2 = y_1 + z_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2} + \frac{1}{2} - i\frac{\sqrt{3}}{2} = 1, \\ \beta_3 = y_3 + z_1 = \frac{1}{2} - i\frac{\sqrt{3}}{2} + \frac{1}{2} + i\frac{\sqrt{3}}{2} = 1. \end{cases}$$

Luego las soluciones de la ecuación $x^3+6x^2+9x+4=0$ son

$$\begin{cases} \alpha_1=\beta_1-2=-4, \\ \alpha_2=\beta_2-2=-1, \\ \alpha_3=\beta_3-2=-1. \end{cases}$$

5.4. **Ecuaciones cuárticas.**

El grupo de Galois de un polinomio de grado cuatro es un subgrupo de S_1, de S_2, de S_3, o de S_4, según el número de raíces diferentes que tenga, por tanto este siempre es resoluble. Y también en este caso hay fórmulas para la determinación de sus raíces. La primera fórmula cuártica fue encontrada por Luigi Ferrari (1545), pero nosotros aprenderemos el método de Descartes (1637) que comentamos a continuación.

Consideremos la ecuación cuártica

$$x^4+bx^3+cx^2+dx+e=0\,,$$

cuyas soluciones, es decir la raíces del polinomio $f=x^4+bx^3+cx^2+dx+e$, las denotaremos por $\alpha_1,\alpha_2,\alpha_3$ y α_4 respectivamente. Reemplazando x por $x-\frac{b}{4}$, obtenemos su reducido

$$\tilde{f}=x^4+p\,x^2+qx+r\,,$$

cuyas soluciones $\beta_1,\beta_2,\beta_3,\beta_4$ nos darán las de la original por las igualdades $\alpha_i=\beta_i-\frac{b}{4}$.

Supuesto $q\neq 0$ (en otro caso estamos en presencia de una bicuadrática, fácil de resolver), el procedimiento de Descartes consiste en determinar números complejos k,ℓ y m, de tal manera que se de la igualdad

$$x^4+p\,x^2+qx+r=(x^2+kx+\ell)(x^2-kx+m)\,, \tag{2}$$

y, entonces, calcular las raíces de $\tilde{f}$ por la fórmula cuadrática para cada factor. Notemos que el término de grado uno en el segundo factor cuadrático ha de ser $-k$ puesto que la cuártica no tiene término cúbico.

Al desarrollar el miembro de la derecha e igualar coeficientes de términos del mismo grado, nos encontramos con el sistema

$$\begin{cases} -k^2+\ell+m &= p\,, \\ k(m-\ell) &= q\,, \\ \ell m &= r\,. \end{cases}$$

las primeras dos ecuaciones pueden expresarse como $m+\ell=p+k^2$ y $m-\ell=\frac{q}{k}$ ($k\neq 0$, pues $q\neq 0$), lo que nos lleva a que

$$\begin{aligned} m &= \tfrac{1}{2}(k^2+p+\tfrac{q}{k})=\tfrac{k^3+pk+q}{2k}\,, \\ \ell &= \tfrac{1}{2}(k^2+p-\tfrac{q}{k})=\tfrac{k^3+pk-q}{2k}, \end{aligned}$$

y sustituyendo en la tercera, obtenemos la ecuación para k

$$\tfrac{k^3+pk+q}{2k}\,\tfrac{k^3+pk-q}{2k}=r\Leftrightarrow (k^3+pk+q)(k^3+pk-q)=4k^2r\Leftrightarrow$$

$$k^6+2p\,k^4+(p^2-4r)k^2-q^2=0.$$

De manera que k^2 ha de solución de la ecuación cúbica

$$x^3+2p\,x^2+(p^2-4r)x-q^2=0\,, \tag{3}$$

(que es llamada la "resolvente cúbica" de la cuártica) y uno puede entonces determinar un valor de k^2 usando el método de Cardano. Desde ahí, es ahora fácil determinar valores de k, ℓ y m, de manera que se tenga la factorización (2), y entonces determinar las raíces de $\tilde{f}$.

Ejemplo 9. *Resolver la ecuación* $x^4-8x^3+24x^2-28x+11=0$

SOLUCIÓN: Si $f = x^4 - 8x^3 + 24x^2 - 28x + 11$, su reducido es

$$\tilde{f} = f(x+2) = (x+2)^4 - 8(x+2)^3 + 24(x+2)^2 - 28(x+2) + 11 = \cdots = x^4 + 4x + 3.$$

Siguiendo el método de Descartes, buscamos la factorización en $\mathbb{C}[x]$

$$x^4 + 4x + 3 = (x^2 + kx + l)(x^2 - kx + m),$$

donde los posibles valores de k, l, m habrán de satisfacer las ecuaciones

$$\begin{array}{rcl} l + m - k^2 & = & 0 \\ k(m-l) & = & 4 \\ lm & = & 3 \end{array}$$

Las dos primeras nos dicen que $m + l = k^2$ y $m - l = 4/k$ (por la ecuación 2^{a}, $k \neq 0$). Equivalentemente,

$$m = \frac{k^2 + \frac{4}{k}}{2} = \frac{k^3 + 4}{2k}, \qquad l = \frac{k^2 - \frac{4}{k}}{2} = \frac{k^3 - 4}{2k}.$$

Llevando esto a la última, obtenemos que $(k^3 + 4)(k^3 - 4) = 12k^2$, esto es, $k^6 - 16 = 12k^2$. En definitiva, k^2 es cualquier raíz de la ecuación cúbica ("resolvente cúbica de la cuártica")

$$x^3 - 12x - 16 = 0$$

Y procedemos a buscar una de sus soluciones, siguiendo el método de Cardano. Buscamos sus soluciones en la forma $x = y + z$ de manera que $yz = 4$, y resulta que y^3 y z^3 son las soluciones de la ecuación $x^2 - 16x + 64$:

$$\frac{16 \pm \sqrt{16^2 - 4 \cdot 64}}{2} = 8 \qquad \text{(solución doble)}.$$

Una de las soluciones de la resolvente cúbica es entonces $y_1 + z_1 = \sqrt[3]{8} + \sqrt[3]{8} = 2 + 2 = 4$. Entonces podemos tomar k cualquiera tal que $k^2 = 4$.

Tomemos $k = 2$, en cuyo caso $l = (8-4)/4 = 1$ y $m = (8+4)/4 = 3$. Así que

$$x^4 + 4x + 3 = (x^2 + 2x + 1)(x^2 - 2x + 3).$$

Y ya es fácil ver que las soluciones de la cuártica propuesta son

$$1 \ (doble), 3 + i\sqrt{2},\ 3 - i\sqrt{2}.$$

5.5. **Irresolubilidad en grado superior. Teorema de Abel-Ruffini.**

El resultado fundamental aquí es la existencia de ecuaciones quínticas irresolubles (y entonces de cualquier grado mayor o igual que cinco). Este resultado fue esencialmente probado por Ruffini (1799) y Abel (1824), aunque sus demostraciones no fueron correctas en todos los detalles (si bien la de Abel fue aceptada, al contrario de la de Ruffini).

Lema 10. *Si $f \in \mathbb{Q}[x]$ es irreducible, entonces el orden del grupo $G(f/\mathbb{Q})$ es un múltiplo del grado de f.*

DEMOSTRACIÓN. Podemos asumir que f es mónico, y supongamos que grado n. Sea α cualquier raíz de f en $\mathbb{C}$. Entonces $f = Irr(\alpha, \mathbb{Q})$ y tenemos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Por la fórmula multiplicativa del grado para la torre $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(f)$, tenemos que

$$[\mathbb{Q}(f) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(f) : \mathbb{Q}(\alpha)] = n\,[\mathbb{Q}(f) : \mathbb{Q}(\alpha)].$$

Así que el grado de la extensión $\mathbb{Q}(f)/\mathbb{Q}$ es un múltiplo de n. Como el grupo $G(f/\mathbb{Q}) = G(\mathbb{Q}(f)/\mathbb{Q})$ es de orden igual al grado de la extensión $\mathbb{Q}(f)/\mathbb{Q}$, se deduce el resultado. □

Lema 11. *Sea p un número primo. Si $G \leq S_p$ es un subgrupo cuyo orden es múltiplo de p y contiene una trasposición, entonces $G = S_p$.*

DEMOSTRACIÓN.: Supongamos que G contiene a la trasposición (a_1, a_2). Como p divide a su orden, G contendrá una permutación de orden p. Como p es primo y el orden de una permutación es igual al mínimo común múltiplo de las longitudes de los ciclos disjuntos en que descompone, esa permutación de orden p será necesariamente un ciclo de longitud p, digamos σ, que podremos escribir en la forma $\sigma = (b_1, \ldots, b_p)$ con $b_1 = a_1$. Si $a_2 = b_{r+1}$, entonces $\sigma^r(a_1) = \sigma^r(b_1) = b_{r+1} = a_2$. Como σ^r es también de orden p (pues p es primo), será también un p-ciclo, que se escribirá de la forma $(a_1, a_2, \ldots, a_p)$. Así que tenemos que el subgrupo G de S_p contiene a la trasposición (a_1, a_2) y al p-ciclo $(a_1, a_2, \ldots, a_p)$.

Por las igualdades

$$(a_1, a_2, \ldots, a_p)(a_i, a_{i+1})(a_1, a_2, \ldots, a_p)^{-1} = (a_{i+1}, a_{i+2})$$

y una fácil inducción, deducimos que todas las trasposiciones de la forma (a_i, a_{i+1}) están en el subgrupo G. Entonces, por las igualdades

$$(a_1, a_i)(a_i, a_{i+1})(a_1, a_i) = (a_1, a_{i+1})$$

deducimos que todas las trasposiciones de la forma (a_1, a_i) están en el subgrupo G. Finalmente, or las igualdades

$$(a_1, a_i)(a_1, a_j)(a_1, a_i) = (a_i, a_j)$$

concluimos que todas las trasposiciones (a_i, a_j) de S_p están en el subgrupo G. Puesto que toda permutación es producto de trasposiciones, $G = S_p$. □

Proposición 12. *Sea $f \in \mathbb{Q}[x]$ un polinomio irreducible de grado un número primo p y que tiene exactamente dos raíces complejas no reales. Entonces $G(f/\mathbb{Q}) \cong S_p$.*

DEMOSTRACIÓN. Sean $\alpha_1, \alpha_2, \ldots, \alpha_p \in \mathbb{C}$ las raíces del polinomio, donde $\alpha_1, \alpha_2 \in \mathbb{C}$, $\alpha_1, \alpha_2 \notin \mathbb{R}$ y $\alpha_3, \ldots, \alpha_p \in \mathbb{R}$. Recordemos el monomorfismo de grupos

$$G(f/K) \to S_p, \quad \sigma \mapsto \sigma \mid \sigma(i) = j \text{ si } \sigma(\alpha_i) = \alpha_j.$$

Así que, si $G \leq S_p$ es el subgrupo imagen, será $G(f/\mathbb{Q}) \cong G$. Probamos ahora que $G = S_p$:

Por el Lema 10, sabemos que el orden del grupo $G(f/\mathbb{Q})$ es múltiplo de p, por tanto también lo será el orden de G. Por el Lema 11 anterior, bastara probar que G contiene una trasposición. Para ello, observemos que la aplicación que asocia a cada complejo su conjugado, $z \mapsto \bar{z}$, restringe dando una $\mathbb{Q}$-inmersión compleja $\mathbb{Q}(f) \to \mathbb{C}$ que, por la normalidad, define un elemento del grupo $G(f/\mathbb{Q}) = G(\mathbb{Q}(f)/\mathbb{Q})$. Es evidente que este deja fijas todas las raíces reales y altera las complejas no reales. Por tanto, la permutación que define en S_p es precisamente la permutación $(1, 2)$. Esto es, $(1, 2) \in G$. □

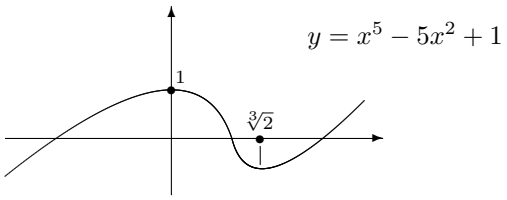
Teorema 13 (Abel-Ruffini)**.** *Para todo $n \geq 5$ existe un polinomio de grado n, $f \in \mathbb{Q}[x]$, que no es resoluble por radicales.*

DEMOSTRACIÓN. Sea $f = x^5 - 5x^2 + 1$. Al reducirlo módulo 2, obtenemos el polinomio $x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$, que no tiene raíces ni es divisible por $x^2 + x + 1$ en $\mathbb{Z}_2[x]$. Luego el reducido es irreducible en $\mathbb{Z}_2[x]$ y el propio f lo es en $\mathbb{Q}[x]$.

Usamos ahora cálculo diferencial elemental para analizar la gráfica de la función $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto f(x)$. Puesto que $f' = 5x^4 - 10x = 5x(x^3 - 2)$, esta tiene tiene exactamente dos puntos críticos, en $x_1 = 0$ y en $x_2 = \sqrt[3]{2}$. Ahora, $f'' = 20x^3 - 10$. Como $f''(0) = -10 < 0$, el punto de la gráfica $(0, f(0)) = (0, 1)$ es un máximo. Como $f''(\sqrt[3]{2}) = 40 - 10 > 0$, el punto de la gráfica

$$(\sqrt[3]{2}, f(\sqrt[3]{2})) = (\sqrt[3]{2}, 2\sqrt[3]{4} - 5\sqrt[3]{4} + 1) = (\sqrt[3]{2}, 1 - 3\sqrt[3]{4})$$

es un mínimo. La gráfica es entonces de la forma



y se sigue fácilmente que f tiene exactamente 3 raíces reales (y, entonces, exactamente dos complejas no reales). Por la proposición anterior,

$$G(x^5 - 5x^2 + 1) = S_5\,,$$

que, sabemos, no es resoluble. Luego el polinomio no es resoluble.

Puesto que $G(x^m(x^5 - 5x^2 + 1)) = G(x^5 - 20x^2 + 2) = S_5$, para todo $m = 0, 1, \ldots$, tenemos un polinomio de grado $m + 5$ en $\mathbb{Q}[x]$ que no es resoluble. □

ALGEBRA III (Doble grado Informática-Matemáticas)

6. Construcciones con Regla y Compás

En esta sección vamos a abordar diversos problemas clásicos de matemática griega.

6.1. **Planteamiento del problema.**

Sea Π un plano Euclídeo dado (nuestro folio). Una **regla** es una herramienta nos permite trazar la linea recta que pasa por dos puntos dados del plano y un **compás** es una herramienta que nos permite trazar la circunferencia de centro un punto dado y de radio el segmento de extremos otros dos puntos dados.

Si $S = \{P_0, \dots, P_n\} \leq \Pi$ es un conjunto finito de puntos del plano, se nos define una sucesión de subconjuntos

$$S = C_1(S) \subseteq C_2(S) \subseteq \cdots \subseteq C_m(S) \subseteq \cdots$$

donde $C_1(S) = S$ y, recursivamente, $C_{m+1}(S)$ es la unión de $C_m(S)$ y el conjunto de todos los puntos tales que

(1) son intersecciones de rectas que pasan por dos puntos de $C_m(S)$,
(2) son intersecciones de rectas que pasan por puntos de $C_m(S)$ con circunferencias de centro un punto de $C_m(S)$ y radio el segmento con extremos dos puntos de $C_m(S)$,
(3) son intersecciones de dos circunferencias cuyos centros son puntos de $C_m(S)$ y radios segmentos con extremos puntos de $C_m(S)$.

Definimos entonces el conjunto

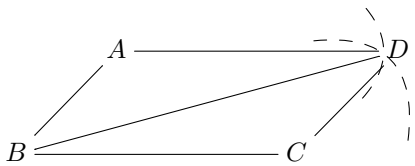
$$C(S) = \bigcup_{m \geq 1} C_m(S) \ ,$$

al que nos referimos como **el conjunto de puntos construibles (con regla y compás) desde los puntos** $S = \{P_0, \dots, P_n\}$.

Los llamados *problemas clásicos de construcciones con regla y compás* son aquellos que se traducen en conocer si un determinado punto P es construible desde un conjunto dado de puntos $\{P_0, \dots, P_n\}$, esto es, saber si $P \in C(P_0, \dots, P_n)$.

Ejemplo 1. *Dados tres puntos A, B, C, no alineados, ¿es construible el punto D, de tal manera los que A, B, C y D son los vértices de un paralelogramo uno de cuyos lados es el segmento de vértices A y B y el otro el de vértices B y C?*

Solución: En efecto, podemos construir el punto D como el punto de intersección de la circunferencia de centro A y radio el segmento de extremos B y C con la circunferencia de centro C y radio el segmento de extremos A y B.

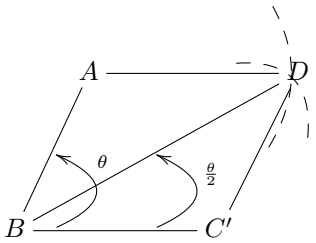


Observemos que la anterior simple construcción nos permite dar respuesta positiva a los siguientes dos problemas

Ejemplo 2. *Dados tres puntos distintos A, B, C, no alineados, ¿es construible un punto D tal que la recta que pasa por A y D es paralela a la que pasa por los puntos B y C?*

Ejemplo 3 (Bisección de ángulos)**.** *Dados tres puntos A, B, C, no alineados, ¿es construible un punto D tal que la recta que pasa por A y D es la bisectriz del ángulo $\widehat{ABC}$?*

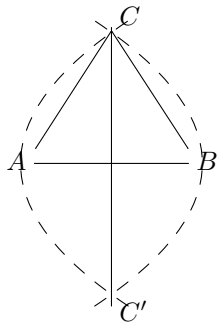
SOLUCIÓN: Construimos primero el punto C' intersección de la recta que pasa por B y C con la circunferencia centrada en B y de radio el segmento que une B con A, de manera que el segmento que une B con C' es de igual distancia que el que une B con A. Construimos entonces, como antes, el vértice D del paralelogramo, que nos resulta un rombo, que resuelve el problema:



Otros ejemplos elementales de respuesta positiva son los siguientes

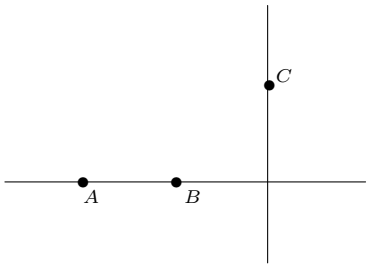
Ejemplo 4. *Dados dos puntos A, B, ¿Es posible construir un punto C tal que el triángulo de vertices A, B y C sea equilátero?, ¿Es posible construir puntos C y C' tal que la recta que pasa por ellos es la mediatriz del segmento de extremos A y B?, ¿es posible construir el punto medio del segmento AB?*

SOLUCIÓN: Para el primer problema encontramos dos soluciones, C y C', que son las intersecciones de las circunferencias de radio el segmento de extremos A y B y cuyos centros respectivos son estos mismos puntos.



Combinando las anteriores es claro que podemos dar respuesta positiva al siguiente problema

Ejemplo 5. *Dados tres puntos no alineados A, B, C ¿es construible un punto D tal que la recta que pasa por C y D es perpendicular a la que pasa por A y B?*

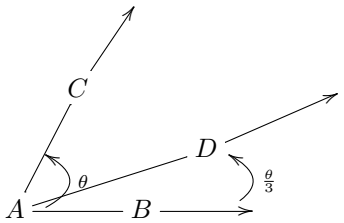


Otro ejemplo sería este

Ejemplo 6. *Dados dos puntos A y B, ¿podemos construir los vértices C y D del cuadrado del que el segmento que une A y B es uno de los lados?*

Otros problemas tienen dificultades, por ejemplo

Ejemplo 7 (Trisección de ángulos)**.** *Consideremos el problema de trisecar un ángulo θ. Aquí tenemos tres puntos, el vértice A y dos puntos B y C de forma que las rectas que determinan con A forman un ángulo θ, entonces ¿es posible construir un punto D tal que la rectas que pasan por A y B y por A yD respectivamente formen el ángulo $\theta/3$?*



Ejemplo 8 (Cuadratura del círculo)**.** *Dados dos puntos A y B ¿es posible construir puntos A' y B' tal que el cuadrado de lado el segmento de extremos A' y B' tenga igual area que el círculo de centro A y radio el segmento de extremos A y B?*

Ejemplo 9 (Duplicación de cubo)**.** *Dados dos puntos A y B ¿es posible construir puntos A' y B' tal que el cubo de lado el segmento de extremos A' y B' tenga doble volumen que el cubo de lado el segmento de extremos A y B?.*

6.2. **Algebraización del problema.**

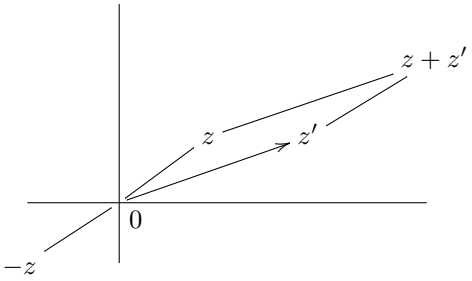
A continuación, en orden a algebraizar el problema, vamos a manejar coordenadas cartesianas para los puntos del plano. Notemos que, dado el conjunto de puntos datos $S = \{P_0, P_1, \ldots, P_n\} \subset \Pi$, es evidente que si $S = \emptyset$ entonces $C(S) = \emptyset$, y si $S = \{P_0\}$, entonces $C(S) = S = \{P_0\}$. Por tanto, para que haya un problema de construcción con regla y compás significativo el conjunto de puntos datos tendrá al menos dos puntos, P_0 y P_1, que nosotros utilizaremos para introducir coordenadas cartesianas: tomaremos P_0 como centro del sistema de ejes cartesianos, por tanto $P_0 = O = (0, 0)$; la recta $\overline{P_0P_1}$ como uno de los ejes, digamos el *eje de abscisas (las $x's$)*, y su perpendicular que pasa por P_0 (que podemos construir) como el otro eje, el *eje de las ordenadas (las $y's$)*; finalmente, tomaremos la distancia $|P_0P_1|$ como unidad de medida, así que será $P_1 = (1, 0)$.

Vamos también a pensar en los puntos del plano como representación geométrica de los números complejos, así que vamos a asociar cada punto P del plano de coordenadas

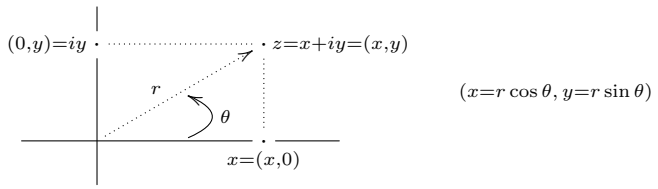
cartesianas (x, y) con el número complejo $z = x + iy$ y, de esta forma, identificamos los puntos del plano con los números complejos. El conjunto de puntos dados $S = \{P_0, \ldots, P_n\}$ lo tendremos identificado con el correspondiente conjunto de complejos $S = \{z_0, \ldots, z_n\}$, donde $z_0 = 0$ y $z_1 = 1$, y el conjunto $C(S) = C(P_0, \ldots, P_n)$ de puntos construibles con un correspondiente conjunto de números complejos, que denotaremos $C(S) = C(z_0, z_1, \ldots, z_n)$ y al que nos referiremos como **el conjunto de números complejos construibles (con regla y compás) desde** $z_0, \ldots, z_n$. De manera que el punto $(x, y) \in \Pi$ es construible desde $P_0, \ldots, P_n$ si y solo si el complejo $x + iy$ es construible desde $z_0, \ldots, z_n$. Queremos ahora probar la siguiente caracterización de $C(S) = C(z_0, z_1, \ldots, z_n)$:

Teorema 10. *$C(S)$ es el menor subcuerpo de $\mathbb{C}$ conteniendo a $z_0, z_1, \ldots, z_n$ y cerrado para raíces cuadradas y conjugación.*

Demostración: Vemos primero que $C(S)$ es un subcuerpo de $\mathbb{C}$ cerrado para raíces cuadradas y conjugación. Supongamos que $z = x + iy$ y $z' = x' + iy' \in C(S)$. Entonces $z + z' = (x + x') + i(y + y')$ puede ser construido por el ya mencionado método del paralelogramo



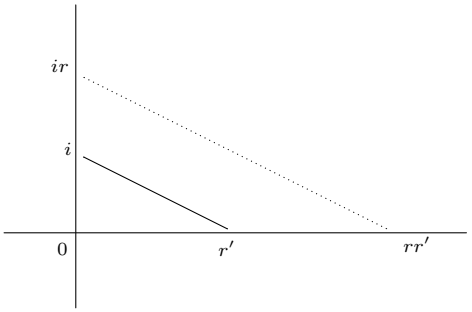
También es claro que $-z = -x + i(-y)$ es construible (es el otro punto de intersección de la recta que pasa por 0 y z con la circunferencia de centro 0 y radio $|z|$ = longitud del segmento de extremos 0 y z. De esta manera concluimos que $C(z_0, z_1, \ldots, z_n)$ es un subgrupo del grupo aditivo del cuerpo $\mathbb{C}$ de los números complejos. Para ver que $C(S)$ es cerrado para multiplicación, inversos, y raíces cuadradas es cómodo usar la expresión de los complejos en su forma polar $z = re^{i\theta}$, donde, si $z = x + iy$, entonces $r = |z| = \sqrt{x^2 + y^2}$ es la longitud del segmento de extremos 0 y z, $\theta \in \mathbb{R}$ es la amplitud en radianes del ángulo desde el eje de abscisas a la recta que pasa por 0 y z, y $e^{i\theta} = \cos\theta + i\sin\theta$.



y es fácil ver que z es construible si y solo si r y $e^{i\theta}$ son construibles: Si z lo es, entonces r es la intersección de la circunferencia de centro el origen de coordenadas 0 y radio $r = |z|$ con el semieje positivo de abscisas y $e^{i\theta}$ la intersección de la circunferencia centrada en el origen y radio 1 con la semirecta que pasa por 0 y z. Si r y $e^{i\theta}$ son construibles, entonces

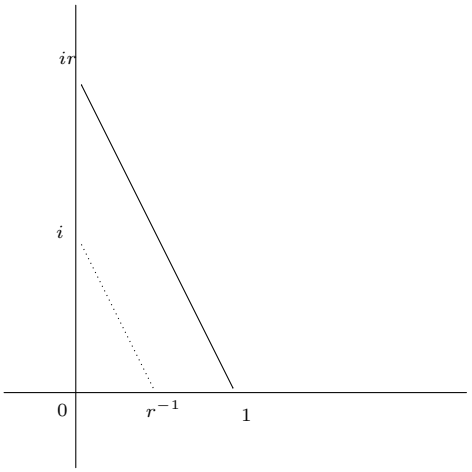
z es la intersección de la semirecta que pasa por 0 y $e^{i\theta}$ con la circunferencia de centro 0 y radio r.

Si $z = re^{i\theta}$ y $z' = r'e^{i\theta'}$ son construibles, entonces $zz' = rr'e^{i(\theta+\theta')}$ tiene valor absoluto rr' igual al producto de los valores absolutos de z y z', y su amplitud es la suma de las dos amplitudes dadas. La construcción de rr' es indicada en la figura



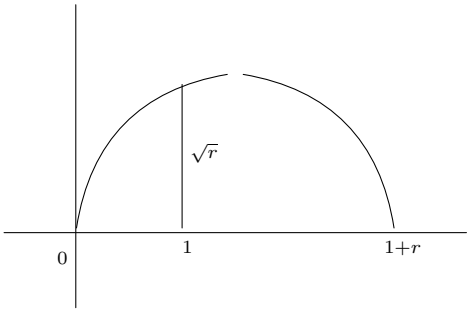
Aquí, la recta que pasa por ir y rr' es paralela a la recta que pasa por i y r' (Usar el Teorema de Thales). Por otra parte, la construcción de $e^{i(\theta+\theta')}$ es fácil: es el nuevo punto de intersección de la circunferencia de centro 0 y radio 1 con la circunferencia de centro $e^{i\theta}$ y radio el segmento que une 1 con $e^{i\theta'}$.

Si $z \neq 0$, entonces $z^{-1} = \frac{1}{r}e^{-i\theta}$. La construcción de $\frac{1}{r}$ es indicada en la figura



y $e^{-i\theta}$ lo construimos como el nuevo punto de intersección de la circunferencia de centro 0 y radio 1 con la circunferencia de centro 1 y radio el segmento que une 1 con $e^{i\theta}$. Puesto que el conjugado es $\bar{z} = re^{-i\theta}$, es claro ya que este es construible. Por otro lado, $\sqrt{z} = \sqrt{r}e^{i\theta/2}$. Ya conocemos como bisecar ángulos, por tanto como construir $e^{i\theta/2}$. La construcción de $\sqrt{r}$

es indicada en la siguiente figura



donde el punto $(1, \sqrt{r})$ es obtenido intersectando la circunferencia centrada en $(\frac{1+r}{2}, 0)$ y radio $\frac{1+r}{2}$ con la recta paralela al eje de ordenadas que pasa por el $(1, 0)$. En efecto, si llamamos $(1, x)$ a ese punto, a a la longitud del segmento que une $(0, 0)$ con $(1, x)$ y b a la del segmento que une $(1, x)$ con $(1 + r, 0)$, por el Teorema de Pitágoras, tenemos las igualdades $a^2 = x^2 + 1$, $b^2 = x^2 + r^2$ y $(1+r)^2 = a^2 + b^2$. De donde $r^2 + 2r + 1 = 2x^2 + r^2 + 1$ y $x^2 = r$; o sea que $x = \sqrt{r}$.

Supongamos ahora que $F \leq \mathbb{C}$ es cualquier subcuerpo conteniendo a los z_i, $1 \leq i \leq n$, y cerrado bajo raíces cuadradas y conjugación. Si tenemos en cuenta la definición de $C(S)$ como $\bigcup C_m(S)$ vemos que, en orden a probar que $F \supseteq C(z_0, z_1, \ldots, z_n)$, es suficiente probar F es cerrado para las construcciones con regla y compás. Esto es, que la intersección de dos rectas determinadas por complejos de F, o de tal una recta con una circunferencia de centro un complejo de F y radio la distancia entre complejos de F, o de dos tales circunferencias, están todos en F. Notamos primero que el hecho de que F es cerrado para conjugación y contiene a $i = \sqrt{-1}$ implica que si $z = x + iy \in F$, x, y reales, entonces $x, y \in F$ (y recíprocamente). Se sigue de este hecho que la ecuación de cualquier recta que pasa por dos puntos distintos de F tiene la forma $ax + by + c = 0$, donde a, b, c son números reales en F: un punto $x + iy$ pertenece a la recta que pasa por $x_0 + iy_0$ y $x_1 + iy_1$ si y solo si se satisface la ecuación

$$(y_1 - y_0)(x - x_0) + (x_0 - x_1)(y - y_0) = 0$$

o, equivalentemente,

$$(y_1 - y_0)x + (x_0 - x_1)y + (y_0 - y_1)x_0 + (x_1 - x_0)y_0 = 0.$$

Similármente, la ecuación de la circunferencia con centro un punto F y radio igual a la longitud de un segmento con extremos puntos de F es de la forma $x^2 + y^2 + dx + ey + f = 0$ donde d, e, f son números reales en F: un punto $x+iy$ pertenece a la circunferencia de centro $x_0 + iy_0$ y radio la distancia entre $x_1 + iy_1$ y $x_2 + iy_2$ si y solo si se satisface la ecuación

$$(x - x_0)^2 + (y - y_0)^2 - (x_2 - x_1)^2 + (y_2 - y_1)^2 = 0.$$

Ahora, las coordenadas de un punto $x + iy$ que sea intersección de dos rectas no paralelas $ax + by + c = 0$ y $a'x + b'y + c' = 0$, donde $a, b, c, a', b', c' \in F$, pueden ser determinadas por la regla de Cramer como

$$x = \frac{\begin{vmatrix} -c & b \\ -c' & b' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} = \frac{-cb' + c'b'}{ab' - a'b}, \quad y = \frac{\begin{vmatrix} -c & a \\ -c' & a' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} = \frac{-ca' + ca'}{ab' - a'b},$$

y vemos así que $x+iy \in F$. Las abscisas de los puntos de intersección de los de una recta de ecuación $y = ax + b$ con los de la circunferencia $x^2 + y^2 + dx + ey + f = 0$ se obtienen resolviendo la ecuación de 2^o grado $x^2 + (ax + b)^2 + dx + e(ax + b) + f = 0$. Usando la conocida fórmula cuadrática, vemos que las soluciones están en F si a, b, d, e, f están en F. Manejamos similármente el caso de la intersección de una recta $x = c$ con una circunferencia $x^2+y^2+dx+ey+f = 0$. Finalmente, el caso restante se sigue de que los puntos de intersección de dos circunferencia $x^2 + y^2 + dx + ey + f = 0$ y $x^2 + y^2 + d'x + e'y + f' = 0$ son los mismos que los puntos de intersección de los puntos de la circunferencia $x^2 + y^2 + dx + ey + f = 0$ con la recta $(d - d')x + (e - e')x + f - f' = 0$. □

Nota 11. *Observar que $C(S)$ contiene a todos los números complejos $a + bi$ donde a, b son racionales, y que este es un subconjunto denso en $\mathbb{C}$.*

Para el siguiente criterio, digamos que por una **extensión radical cuadrática** de un cuerpo de números $K \leq \mathbb{C}$ se entiende una extensión simple de este cuerpo que es generada por la raíz cuadrada de algún número $a \in K$, esto es, una extensión E/K tal que $E = K(\sqrt{a})$, para algún $a \in K$. Una torre de extensiones de cuerpos numéricos $K_0 \leq K_1 \leq \cdots \leq K_r$ es llamada una tal torre se llama una **torre radical cuadrática** si cada extensión K_{i+1}/K_i es radical cuadrática.

Lema 12. *Si $K = F_0 \leq F_1 \leq \ \cdots \ \leq F_r$ es una torre radical cuadrática que comienza en un cuerpo K, entonces existe una otra torre radical cuadrática que también comienza en K, $K = E_0 \leq E_1 \leq \ \cdots \ \leq E_s$, tal que $F_r \leq E_s$ y E_s/K es normal.*

Demostración. Procedemos inductivamente en r.

Caso $r = 1$. Tenemos $K \leq F_1$, donde $F_1 = K(\sqrt{a})$, para algún $a \in K$. Pero esta extensión es siempre normal, pues F_1 es el cuerpo de descomposición sobre K del polinomio $x^2 - a$ (sus raíces son $\pm\sqrt{a}$).

Caso $r > 1$. Por hipótesis de inducción, existe una torre radical $K = E_0 \leq E_1 \leq \ \cdots \ \leq E_t$, tal que $F_{r-1} \leq E_t$ y E_t/K es normal. Supongamos que su grupo de Galois es $G(E_t/K) = \{\sigma_1 = id, \sigma_2, \ldots, \sigma_m\}$.

Puesto que F_r/F_{r-1} es radical, será $F_r = F_{r-1}(\sqrt{a})$, para algún $a \in F_{r-1}$. Construimos entonces la torre radical cuadrática

$$K = E_0 \leq E_1 \leq \ \cdots \ \leq E_t \leq E_t(\sqrt{\sigma_1(a)}) \leq E_t(\sqrt{\sigma_1(a)}, \sqrt{\sigma_2(a)}) \leq \cdots$$
$$\leq \ldots \leq E_t\big(\sqrt{\sigma_1(a)}, \sqrt{\sigma_2(a)}, \ldots, \sqrt{\sigma_n(a)}\big) = E_s\,.$$

puesto que cada $\sigma_i(a) \in E_t$, es claro que se trata efectivamente de una torre radical cuadrática y, claramente, $F_r \leq E_s$. Bastará por tanto argumentar que E_s/K es normal:

Supongamos que E_t el cuerpo de descomposición sobre K de un polinomio $f \in K[x]$; esto es, $E_t = K(\alpha_1, \ldots, \alpha_k)$ donde $\alpha_1, \ldots, \alpha_k$ son las diferentes raíces de ese f. Consideremos el polinomio $g = \prod_{i=1}^{n}(x^2 - \sigma_i(a)) \in E_t[x]$. Para cualquier $\sigma \in G(E_t/K)$, la lista $\sigma\sigma_1, \ldots, \sigma\sigma_n$ es una permutación de la lista $\sigma_1, \ldots, \sigma_n$, y por consiguiente

$$g^\sigma(x) = \prod_{i=1}^{n}(x^2 - \sigma\sigma_i(a)) = \prod_{i=1}^{n}(x^2 - \sigma_i(a)) = g(x);$$

esto es, los coeficientes de g están en el cuerpo fijo $E_t^{G(E_t/K)} = K$. Así que $g \in K[x]$. El cuerpo de descomposición sobre K del polinomio producto fg es justamente

$$K\big(\alpha_1, \ldots \alpha_k, \sqrt{\sigma_1(a)}, \ldots, \sqrt{\sigma_n(a)}\,\big) = E_t(\sqrt{\sigma_1(a)}, \ldots, \sqrt{\sigma_n(a)}\,) = E_s\,,$$

y concluimos que la extensión E_s/K es normal. □

Teorema 13. *Sea $\{z_0 = 0, z_1 = 1, \ldots, z_n\} \subseteq \mathbb{C}$ el conjunto de números asociado a un conjunto de puntos dato $S = \{P_0, P_1, \ldots, P_n\}$. Pongamos*

$$\mathbb{Q}_S = \mathbb{Q}(z_0, z_1, \ldots, z_n, \overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1).$$

Entonces, un complejo $z \in C(S)$ si y solo si existe una torre radical cuadrática

$$\mathbb{Q}_S = K_0 \leq K_1 \leq \cdots \leq K_r$$

tal que $z \in K_r$.

Demostración. Si $\mathbb{Q}_S = K_0 \leq K_1 \leq \cdots \leq K_r$ es una torre radical cuadrática, vemos, por inducción, que $K_r \leq C(S)$: Puesto que $C(S)$ es cerrado para conjugación y cada $z_i \in C(S)$, también cada $\bar{z}_i \in C(S)$, y resulta claro que $K_0 = \mathbb{Q}_S \leq C(S)$. Supongamos demostrado que que $K_{r-1} \leq C(S)$. Como $K_r = K_{r-1}(\sqrt{d})$, para algún $d \in K_{r-1}$, y $C(S)$ es cerrado para raíces cuadradas, se sigue que $\sqrt{d} \in C(S)$ y, entonces, que $K_r \leq C(S)$.

Sea $F \leq \mathbb{C}$ el conjunto de todos los números complejos que pertenecen al extremo de una torre radical cuadrática que comienza en $\mathbb{Q}_s$. F es un subcuerpo: Sean $z, z' \in F$. Existirán torres radicales cuadráticas $\mathbb{Q}_s = K_0 \leq K_1 \leq \cdots \leq K_r$ y $\mathbb{Q}_S = K'_0 \leq K'_1 \leq \cdots \leq K'_s$ tal que $z \in K_r$ y $z' \in K'_s$. Supongamos que $K'_{i+1} = K'_i(\sqrt{d_{i+1}})$, $i = 0, \ldots, r' - 1$, con $d_{i+1} \in K'_i$. Construyamos la torre de extensiones

$$(1) \quad \mathbb{Q}_S = K_0 \leq \cdots \leq K_r \leq K_r(\sqrt{d_1}) \leq K_r(\sqrt{d_1}, \sqrt{d_2}) \leq \cdots \leq K_r(\sqrt{d_1}, \ldots, \sqrt{d_s}).$$

Por inducción, vemos fácilmente que $K'_i \subseteq K_r(\sqrt{d_1}, \ldots, \sqrt{d_i})$:
- $K'_1 = K'_0(\sqrt{d_1}) \leq K_r(\sqrt{d_1})$
- $K'_{i+1} = K'_i(\sqrt{d_{i+1}}) \leq K_r(\sqrt{d_1}, \ldots, \sqrt{d_{i+1}})$.

y, entonces, cada $d_{i+1} \in K_r(\sqrt{d_1}, \ldots, \sqrt{d_i})$. Así que (1) es una torre radical cuadrática. Puesto que $z, z' \in K_r(\sqrt{d_1}, \ldots, \sqrt{d_s})$, entonces también $-z$, $z + z'$, zz', y z^{-1} si $z \neq 0$, están en el extremo de la torre. Luego también en F. Así que F es un subcuerpo.

Claramente F es cerrado para raíces cuadradas.

Para ver que F es cerrado por conjugación, notemos primero que si calculamos la imagen de $\mathbb{Q}_S$ por el automorfismo de conjugación obtenemos que

$$\overline{\mathbb{Q}_S} = \overline{\mathbb{Q}(z_0, z_1, \ldots, z_n, \overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1)} = \mathbb{Q}(\overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1, z_0, z_1, \ldots, z_n) = \mathbb{Q}_S$$

Además, si E/F es una extensión radical cuadrática, entonces la extensión de los cuerpos conjugados $\bar{E}/\bar{F}$ es también radical cuadrática: Si $E = F(\sqrt{a})$ con $a \in F$, entonces

$$\bar{E} = \bar{F}(\overline{\sqrt{a}}) = \bar{F}(\sqrt{\bar{a}}),$$

pues $(\overline{\sqrt{a}})^2 = \bar{a}$ y, por tanto, $\overline{\sqrt{a}} = \pm\sqrt{\bar{a}}$, donde $\bar{a} \in \bar{F}$. Entonces, si $z \in F$ y pertenece al extremo de la torre de extensiones cuadráticas $\mathbb{Q}_S = K_0 \leq K_1 \leq \cdots \leq K_r$, entonces su conjugado $\bar{z}$ pertenece al extremo de la torre de extensiones cuadráticas $\mathbb{Q}_S = \bar{K}_0 \leq \bar{K}_1 \leq \cdots \leq \bar{K}_r$, y concluimos que $\bar{z} \in F$.

Luego, por el anterior teorema, $F \supseteq C(S)$. □

Lema 14. *Toda extension de cuerpos de números E/K con $[E : K] = 2$ es radical cuadrática.*

Demostración. Escojamos un $\alpha \in E$ tal que $\alpha \notin K$. Tenemos la torre $K \leq K(\alpha) \leq E$, y la igualdad $2 = [E : K] = [E : K(\alpha)][K(\alpha) : K]$ obliga a que $[E : K(\alpha)] = 1$ y $[K(\alpha) : K] = 2$, ya que $K \neq K(\alpha)$ y no puede ser $[K(\alpha) : K] = 1$. Entonces $E = K(\alpha)$ y $Irr(\alpha, K)$ es de grado 2. Supongamos $Irr(\alpha, K) = x^2 + bx + c$. Entonces $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$ y $E = K(\alpha) = K(\sqrt{b^2 - 4c})$ es una extensión radical cuadrática de K. □

Teorema 15. * *Sea $S = \{z_0 = 0, z_1 = 1, \ldots, z_n\} \subseteq \mathbb{C}$ un conjunto de números. Pongamos*

$$\mathbb{Q}_S = \mathbb{Q}(z_0, z_1, \ldots, z_n, \overline{z}_0, \overline{z}_1, \ldots, \overline{z}_1).$$

Las siguientes propiedades, para un complejo $z \in C$, son equivalentes:

(1) $z \in C(S)$.
(2) *z es algebraico sobre $\mathbb{Q}_S$ y si $f = Irr(z, \mathbb{Q}_S)$ entonces $[\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$, para algún entero $m \geq 2$.*
(3) *z es algebraico sobre $\mathbb{Q}_S$ y si $f = Irr(z, \mathbb{Q}_S)$ entonces $G(f/\mathbb{Q}_S)$ es un 2-grupo.*

Demostración. Las propiedades (2) y (3) son equivalentes, pues

$$[\mathbb{Q}_S(f) : \mathbb{Q}_S] = |G(\mathbb{Q}_S(f)/\mathbb{Q}_S) = |G(f/\mathbb{Q}_S)|.$$

Supongamos $z \in C(S)$. Existirá una torre radical cuadrática $\mathbb{Q}_S = K_0 \leq \cdots \leq K_r$ con $z \in K_r$ y $K_r/\mathbb{Q}_S$ normal. Puesto que cada extensión K_i/K_{i-1} es radical cuadrática, será $K_i = K_{i-1}(\sqrt{a_i})$ para algún $a_i \in K_{i-1}$. Si $\sqrt{a_i} \in K_{i-1}$, entonces $K_i = K_{i-1}$ y $[K_i : K_{i-1}] = 1$. Si $\sqrt{a_i} \notin K_{i-1}$, entonces $Irr(\sqrt{a_i}, K_{i-1}) = x^2 - a_i$ y $[K_i : K_{i-1}] = 2$. Entonces $[K_r : \mathbb{Q}_S] = \prod_1^r [K_i : K_{i-1}] = 2^k$ para algún entero $k \geq 0$.

Puesto que la extension $K_r/\mathbb{Q}_S$ es finita, por tanto algebraica, y $z \in K_r$, resulta que z es algebraico sobre $\mathbb{Q}_S$. Sea $f = Irr(z, \mathbb{Q}_S)$. Como $K_r/\mathbb{Q}_S$ es normal, todas las raíces f estarán en K_r y será $\mathbb{Q}_S(f) \leq K_r$. Considerando la torre $\mathbb{Q}_S \leq \mathbb{Q}_S(f) \leq K_r$, tendremos que $2^k = [K_r : \mathbb{Q}_S] = [K_r : \mathbb{Q}_S(f)]\,[\mathbb{Q}_S(f) : \mathbb{Q}_S]$, de donde concluimos que $[\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$ para algún $m \leq k$.

Recíprocamente, supongamos estamos en las hipótesis (2) = (3). Como $G(\mathbb{Q}_S(f)/\mathbb{Q}_S) = G(f/\mathbb{Q}_S)$ es un 2-grupo (y todo p-grupo es resoluble) tendrá una serie con factores cíclicos de orden 2, esto es, de la forma

$$G(\mathbb{Q}_S(f)/\mathbb{Q}_S) = G_0 \geq G_1 \geq \cdots G_i \geq G_{i+1} \geq \cdots \geq G_k = 1,$$

donde cada G_{i+1} es normal en el G_i y cada cociente G_i/G_{i+1} es cíclico de orden 2. Por la correspondencia de Galois, tendremos una correspondiente torre de subextensiones

$$\mathbb{Q}_S = \mathbb{Q}_S(f)^{G_0} \leq \cdots \mathbb{Q}_S(f)^{G_i} \leq \mathbb{Q}_S(f)^{G_{i+1}} \leq \cdots \mathbb{Q}_S(f)^{G_1} \leq \mathbb{Q}_S(f)^{G_k} = \mathbb{Q}_S(f). \tag{2}$$

Como cada $G_i = G(\mathbb{Q}_S(f)/\mathbb{Q}_S(f)^{G_i})$ y es $G_{i+1} \trianglelefteq G_i$, el Teorema Fundamental de la Teoría de Galois, aplicado a la torre $\mathbb{Q}_S(f)^{G_i} \leq \mathbb{Q}_S(f)^{G_i+1} \leq \mathbb{Q}_S(f)$, nos garantiza que cada extensión $\mathbb{Q}_S(f)^{G_{i+1}}/\mathbb{Q}_S(f)^{G_i}$ es normal con grupo de Galois

$$G\big(\mathbb{Q}_S(f)^{G_{i+1}}/\mathbb{Q}_S(f)^{G_i}\big) \cong G_i/G_{i+1},$$

que cíclico de orden 2. En particular, $[\mathbb{Q}_S(f)^{G_{i+1}} : \mathbb{Q}_S(f)^{G_i}] = 2$ y, por el lema anterior la torre de extensiones (2) es radical cuadrática. Como en su extremo $\mathbb{Q}_S(f)$ está obviamente z, el anterior teorema nos garantiza que $z \in C(S)$. □

Corolario 16. *Sea $S = \{z_0 = 0, z_1 = 1, \ldots, z_n\} \subseteq \mathbb{C}$ un conjunto de números. Si un complejo $z \in C(S)$ entonces z es algebraico sobre $\mathbb{Q}_S$ y su polinomio irreducible $Irr(z, \mathbb{Q}_S)$ es de grado 2^k, para algún entero $k \geq 0$.*

Demostración. Si $z \in C(S)$, ya sabemos que z es algebraico sobre $\mathbb{Q}_S$ y que, si $f = Irr(z, \mathbb{Q}_S)$ entonces $[\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$ para un cierto entero $m \geq 0$. Puesto que $\mathbb{Q}_S \leq \mathbb{Q}_S(z) \leq \mathbb{Q}_S(f)$, de la igualdad $[\mathbb{Q}_S(z) : \mathbb{Q}_S][\mathbb{Q}_S(f) : \mathbb{Q}_S(z)] = [\mathbb{Q}_S(f) : \mathbb{Q}_S] = 2^m$ se deduce que $[\mathbb{Q}_S(z) : \mathbb{Q}_S] = gr(Irr(z, \mathbb{Q}_S))$ es también una potencia de 2. □

Ejemplo 17 (*Trisección de ángulos).* No todo ángulo se puede trisecar con regla y compás. En particular el de 60° ($=\frac{\pi}{3}$ radianes) no se puede trisecar. En este caso, tenemos tres puntos datos: el vértice $P_0 = (0,0)$, el punto $P_1 = (1,0)$ y el punto $P_2 = (\cos 60^\circ, \sin 60^\circ) = (\frac{1}{2}, \frac{\sqrt{3}}{2})$. La cuestión es saber si el punto $P = (\cos 20^\circ, \sin 20^\circ)$ es construible con regla y compás desde esos puntos. Claramente esto es equivalente a que lo sea el punto $(\cos 20^\circ, 0)$.

Vamos a aplicar el criterio del teorema anterior. En el caso presente, tenemos el conjunto complejos dato

$$S = \{z_0 = 0, z_1 = 1, z_2 = e^{i\pi/3} = \tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\},$$

y el cuerpo $\mathbb{Q}_S = \mathbb{Q}(z_0, z_1, z_2, \bar{z}_0, \bar{z}_1, \bar{z}_2) = \mathbb{Q}(i\sqrt{3})$. Por el teorema anterior, la trisección del ángulo de 60° requiere que $\cos 20^\circ$ sea algebraico y su irreducible sobre $\mathbb{Q}(i\sqrt{3})$ sea de grado una potencia de 2, o sea que $[\mathbb{Q}(i\sqrt{3}, \cos 20^o) : \mathbb{Q}(i\sqrt{3})]$ ha de ser una potencia de dos. Como $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$, por la torre $\mathbb{Q} \leq \mathbb{Q}(i\sqrt{3}) \leq \mathbb{Q}(i\sqrt{3}, \cos 20^o)$, deducimos que sería también $[\mathbb{Q}(i\sqrt{3}, \cos 20^o) : \mathbb{Q}]$ una potencia de dos. Y por la torre $\mathbb{Q} \leq \mathbb{Q}(\cos 20^o) \leq \mathbb{Q}(i\sqrt{3}, \cos 20^o)$ también lo sería $[\mathbb{Q}(\cos 20^o) : \mathbb{Q}]$. Esto es, sería $Irr(\cos 20, \mathbb{Q})$ un polinomio de grado una potencia de dos.

Ahora, tenemos la identidad trigonométrica

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

que nos da la igualdad

$$4(\cos 20^\circ)^3 - 3\cos 20^\circ - \frac{1}{2} = 0.$$

Así que $\cos 20^\circ$ es raíz del polinomio $x^3 - \frac{3}{4}x - \frac{1}{8}$. Pero ocurre que este polinomio es irreducible sobre $\mathbb{Q}$, ya que es de grado 3 y no tiene raíces (sus posibles raíces es $\mathbb{Q}$ son las mismas que las del polinomio $8x^3 - 6x - 1 \in \mathbb{Z}[x]$, cuyas únicas posibles raíces son $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$, y comprobamos directamente que ninguno de estos racionales lo es). Entonces $Irr(\cos 20^\circ, \mathbb{Q}) = x^3 - \frac{3}{4}x - \frac{1}{8}$, que es de grado 3, y no una potencia de 2.

Alternativamente: Si $z = e^{\frac{\pi i}{9}}$, entonces $z + \bar{z} = 2\cos 20^o$ es raíz de $x^3 - 3x - 1$, pues

$$(z+\bar{z})^3 - 3(z+\bar{z}) - 1 = z^3 + \bar{z}^3 + 3z + 3\bar{z} - 3z - 3\bar{z} - 1 = 2\cos\frac{\pi}{3} - 1 = 1 - 1 = 0.$$

Como $x^3 - 3x - 1$ no tiene raíces en $\mathbb{Q}$, es irreducible, así que $Irr(2\cos 20^o, \mathbb{Q}) = x^3 - 3x - 1$ y $[[\mathbb{Q}(\cos 20^o) : \mathbb{Q}] = [\mathbb{Q}(2\cos 20^o) : \mathbb{Q}] = 3$. □

Ejemplo 18 (*Duplicación del cubo).* En este caso, tenemos dos puntos datos, $P_0 = (0,0)$ y $P_1 = (1,0)$, que son una de las aristas de un cubo, y la cuestión es saber si es construible con regla y compás desde esos puntos el punto $P = (a, 0)$ tal que el cubo del cual el segmento de extremos P_0 y P es una de sus aristas tenga volumen doble. Claramente esto es equivalente a que lo sea el punto $(\sqrt[3]{2}, 0)$, y por el teorema anterior, habría de ser $Irr(\sqrt[3]{2}, \mathbb{Q})$ de grado una potencia de 2 (en este caso $\mathbb{Q}_S = \mathbb{Q}$). Pero $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ que es de grado 3.

Ejemplo 19 (*Cuadratura del círculo).* En este caso, tenemos dos puntos datos, $P_0 = (0,0)$ y $P_1 = (1,0)$, que determinan un círculo de centro P_0 y radio 1, y la cuestión es saber si es construible el punto $P = (a, 0)$ tal que el cuadrado del cual el segmento de extremos P_0 y P es uno de sus lados tenga igual area que el círculo dado. Claramente esto requiere que $a = \sqrt{\pi}$ y que a sea algebraico sobre $\mathbb{Q}$. Pero esto implicaría que π es algebraico sobre $\mathbb{Q}$, lo que contradice el Teorema de Lindemann, que nos asegura que π, y entonces también $\sqrt{\pi}$, es trascendente.

6.3. **Poligonos regulares.**

En este caso, tenemos dos puntos datos, P_0 y P_1, que determinan un círculo de centro P_0 y radio la amplitud del segmento que los une, y la cuestión es saber si son construibles los n vértices de un polígono regular inscrito en la circunferencia de centro P_0 y radio el segmento de extremos P_0 y P_1, uno de los cuales es P_1. Tomando $P_0 = (0.0)$ y $P_1 = (1, 0)$, la cuestión reduce claramente a saber si el punto $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ es, o no, construible desde P_0 y P_1.

Definición 20. *Un primo $p \geq 2$ de $\mathbb{Z}$ se dice que p* **de Fermat** *si es de la forma $p = 2^k + 1$ para algún entero $k \geq 1$.*

Por ejemplo, los primos 3, 5, 17, 257 y 65537 son primos de Fermat.

Teorema 21. * *El polígono regular de n lados es construible si y solo si n factoriza en la forma*

$$n = 2^m p_1 p_2 \cdots p_r,$$

donde $m \geq 0$, cada p_i es un primo de Fermat, y $p_i \neq p_j$ si $i \neq j$.

Demostración. Algebraizando el problema, tenemos $S = \{0, 1\}$ y $\mathbb{Q}_S = \mathbb{Q}$. Puesto que ya sabemos que $z_n = e^{\frac{2\pi i}{n}}$ es algebraico sobre $\mathbb{Q}$, que $Irr(z_n, \mathbb{Q}) = \Phi_n$, y que $\mathbb{Q}(\Phi_n) = \mathbb{Q}(z_n)$. El teorema nos asegura que z_n es construible si y solo si $gr(\Phi_n)$ es una potencia de dos, esto es , si y solo si $\varphi(n)$ es una potencia de dos.

Supongamos que la factorización en primos distintos de n es

$$n = 2^m p_1^{m_1} \cdots p_r^{m_r},$$

donde $m \geq 0$, cada $m_i \geq 1$, y cada $p_i \geq 3$. Entonces

$$\varphi(n) = 2^{e-1}(p_1 - 1)p_1^{m_1 - 1} \cdots (p_r - 1)p_r^{m_r - 1}.$$

Es claro que, $\varphi(n)$ es una potencia de 2 si y solo si cada $m_i = 1$ y cada $p_i = 1 + 2^{k_i}$ para algún $k_i \geq 2$. □

ALGEBRA III (Doble grado Informática-Matemáticas)

Cuerpos Finitos

Sobre cuerpos de característica positiva.

Si F es un cuerpo cualquiera, como en cualquier anillo conmutativo, tenemos definido el producto na de enteros $n \geq 0$ por elementos $a \in F$: Si $n = 0$, entonces $0a = 0$, y si $n > 0$, entonces $na = \sum_{i=1}^{n} a = a + \overset{n}{\cdots} + a$ es la suma reiterada de ese elemento a consigo mismo n veces. Recordemos también que, para cualesquiera $m, n \geq 0$ y $a, b \in F$, se verifican (entre otras) las igualdades

(1) $1a = a$,
(2) $(m+n)a = ma + na$,
(3) $m(na) = (mn)a$,
(4) $(ma)(nb) = (mn)(ab)$.
(5) $(ma)b = m(ab) = a(mb)$.

Fijándonos en el caso en $a = 1 \in F$, los diferentes productos $n1 = 1 + \overset{n}{\cdots} + 1$, para $n \geq 0$, no tienen por qué ser todos distintos (por ejemplo, si F es finito no podrán serlo). En ese caso, existirán enteros $m > n \geq 0$ tales que $m1 = n1$. Pero entonces, si $m = n + k$, será $n1 + k1 = n1$ y $k1 = 0$. Luego existe un $k \geq 1$ tal que $k1 = 0$. Sea

$$p = \min\{k \geq 1 \mid k1 = 0\}.$$

Notemos que ha de ser $p \geq 2$, pues si fuese $p = 1$ sería $1 = 0$ en F, y en un cuerpo esto no se puede dar. Este número p **es primo**: Supongamos por el contrario que no es primo o, equivalentemente, que no es irreducible. Será $p = mn$, con $m, n < p$. Pero entonces $(m1)(n1) = (mn)1 = p1 = 0$. Como F es un cuerpo, será $m1_F = 0$ o $n1_F = 0$. Pero ninguna de estas igualdades puede darse al ser $m, n < p$. A este número primo p se le llama la **característica del cuerpo** F.

Por ejemplo, para cualquier número primo $p \geq 2$, $\mathbb{Z}_p$ es un cuerpo de característica p. Recordemos las operaciones de suma y producto en $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$: Si, para cualquier entero $n \in \mathbb{Z}$ denotamos por $\overline{n}$ al resto de dividir n entre p, entonces, $\overline{n} = n$ si $0 \leq n \leq p-1$ y la suma y producto en $\mathbb{Z}_p$ está determinada por que para cualesquiera $m, n \in \mathbb{Z}$

$$\overline{m} + \overline{n} = \overline{m+n}, \qquad \overline{m}\ \overline{n} = \overline{mn}.$$

En particular, si $1 \leq k < p$, en $\mathbb{Z}_p$, $k1 = \overline{k} = k \neq 0$, mientras que $p1 = \overline{p} = 0$. Así que la característica de $\mathbb{Z}_p$ es, en efecto, p. Si $F/\mathbb{Z}_p$ es cualquier extensión, entonces la característica de F es también p (tienen el mismo 1 y se suma consigo mismo en F como en $\mathbb{Z}_p$).

Lema 1. *Sea F un cuerpo de característica p. Para cualesquiera $m, n \geq 0$, se verifica que*

$$m1 = n1 \Leftrightarrow m \equiv n \mod (p) \Leftrightarrow \overline{m} = \overline{n}.$$

En particular,

(1) $m1 = \overline{m}\,1$.
(2) $m1 = 0 \Leftrightarrow p/n$.

Demostración. Supongamos $m \geq n$, $m = n + k$. Si $m \equiv n \mod (p)$, será $k = qp$. Entonces $m1 = n1 + q(p1) = n1$, pues $p1 = 0$. Y, recíprocamente, si $m1 = n1$, será $n1 + k1 = n1$ y $k1 = 0$. Pongamos $k = pq + r$, con $0 \leq r < p$. Entonces $r1 = 0$ y, como $r < p$, ha de ser $r = 0$. Así que $p \mid k$ y $m \equiv n \mod (p)$. □

Las conclusiones del lema anterior son válidas para cualquier elemento $0 \neq a \in F$:

Lema 2. *Sea F un cuerpo de característica p. Para cualesquiera $m, n \geq 0$ y $0 \neq a \in F$, se verifica que*

$$ma = na \Leftrightarrow m \equiv n \mod (p) \Leftrightarrow \overline{m} = \overline{n}.$$

En particular,

(1) $ma = \overline{m}\, a$.
(2) $ma = 0 \Leftrightarrow p/n$.

Demostración. $ma = na \Leftrightarrow (ma)a^{-1} = (na)a^{-1} \Leftrightarrow m(aa^{-1}) = n(aa^{-1}) \Leftrightarrow m1 = n1$, y basta aplicar el lema anterior. □

Teorema 3. *Sea F un cuerpo de característica p. La aplicación $\sigma : \mathbb{Z}_p \to F$ definida por*

$$\sigma(n) = n1, \qquad n = 0, 1, \ldots, p-1,$$

es una inmersión, y es la única que hay de $\mathbb{Z}_p$ en F.

Demostración. Claramente $\sigma(0) = 0$ y $\sigma(1) = 1$. Además, para cualesquiera $m, n \in \mathbb{Z}_p$,

$$\sigma(m) + \sigma(n) = (m1) + (n1) = (m+n)1 = \overline{m+n}\,1 = \sigma(\overline{m+n}),$$
$$\sigma(m)\,\sigma(n) = (m1)\,(n1) = (mn)1 = \overline{m\,n}\,1 = \sigma(\overline{m\,n}).$$

Si $\sigma' : \mathbb{Z}_p \to F$ es cualquier otra supuesta inmersión, para todo $0 \leq n \leq q-1$, será $\sigma'(n) = \sigma'(n1) = n\sigma'(1) = n1 = \sigma(n)$, luego $\sigma' = \sigma$. □

La inmersión $\sigma : \mathbb{Z}_p \to F$ es estándar, y la consideramos siempre como una inclusión. Con esta identificación en mente, tenemos demostrado la primera afirmación del siguiente

Teorema 4. (*i*) *Un cuerpo es de característica p si y solo si es una extensión de $\mathbb{Z}_p$.*

(*ii*) *Si F es un cuerpo de característica p, E es un cuerpo de característica q, y $p \neq q$, entonces no existe ninguna inmersión $F \to E$.*

(*iii*) *Si E, F son cuerpos de característica p, toda inmersión $\sigma : F \to E$ es una $\mathbb{Z}_p$-inmersión, esto es, $\sigma|_{\mathbb{Z}_p} = id$.*

Demostración. (*ii*) Si $\sigma : F \to E$ fuese un homomorfismo, tendríamos que $0 = \sigma(0) = \sigma(p1) = p\sigma(1) = p1 \in E$. Pero entonces $q \mid p$, lo que no es posible al ser primos positivos distintos.

(*iii*) Sea $\sigma : F \to E$ un homomorfismo, entonces, para cualquier $m \in \mathbb{Z}_p$,

$$\sigma(m) = \sigma(m1) = m\sigma(1) = m1 = m.$$

□

Existencia y unicidad de cuerpos finitos.

Un cuerpo finito necesariamente será de característica p, para p un primo positivo de $\mathbb{Z}$, y entonces una extensión, también necesariamente finita, de $\mathbb{Z}_p$. Esto nos limita las posibilidades del tamaño del cuerpo F a ser una potencia del primo p.

Teorema 5. *Si F un cuerpo finito, entonces $|F| = p^n$, donde p es su característica y $n = [F : \mathbb{Z}_p]$.*

Demostración. Sea $\{a_1, ..., a_n\}$ una base de F como espacio vectorial sobre $\mathbb{Z}_p$. Cada elemento $a \in F$ se escribe de forma única como $a = m_1 a_1 + ... + m_n a_n$, con $m_i \in \mathbb{Z}_p$. Consecuentemente, el número total de elementos de F es p^n. □

Lema 6. *Sea E un cuerpo de característica p donde el polinomio $x^{p^n} - x$ descompone totalmente. Entonces el subconjunto de E formado por todas las raíces de ese polinomio es un subcuerpo con p^n elementos.*

Demostración. Sea $F \subseteq E$ el subconjunto de todas las raíces de ese polinomio. Esto es, $F = \{\alpha \in E \mid \alpha^{p^n} = \alpha\}$. Notemos que el polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ tiene exactamente p^n raíces distintas en E, ya que no tiene raíces múltiples al ser su derivado $(x^{p^n} - x)' = -1$ primo relativo con él (notar que $px = 0$, pues $px = \sum_1^p x = (\sum_1^p 1)x = (p1)x = 0x = 0$). Veamos que F es un subcuerpo de E: Claramente $0, 1 \in F$. Puesto que E es de característica p, para cualesquiera $\alpha, \beta \in E$

$$(\alpha + \beta)^p = \sum_{i=0}^{p} \binom{p}{i} \alpha^i \beta^{p-i} = \sum_{i=0}^{p} \overline{\binom{p}{i}} \alpha^i \beta^{p-i} = \alpha^p + \beta^p,$$

de donde se deduce que $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$. Entonces, si $\alpha, \beta \in F$, es $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ y, por tanto $\alpha + \beta \in F$. Vemos también que $\alpha\beta \in F$, pues $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$. Además, si $0 \neq \alpha \in F$ entonces $-\alpha, \alpha^{-1} \in F$, pues $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = (-1)\alpha = -\alpha$ y $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. □

Puesto que siempre existe una extensión $E/\mathbb{Z}_p$ donde el polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ descompone totalmente, obtenemos el siguiente importante resultado.

Teorema 7. *Para cada primo p y cada entero $n \geq 1$ existe un cuerpo con p^n elementos.*

La obtención anterior de un cuerpo con p^n elementos cuyos elementos son todas las raíces del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ no es fruto de especial ingenio. Esa propiedad la tienen todos los cuerpos con p^n elementos.

Lema 8. *Si F es un cuerpo finito con p^n elementos, todos los elementos de F son raíces del polinomio $x^{p^n} - x$ y este polinomio tiene todas sus raíces en F, así que en $F[x]$ se tiene que $x^{p^n} - x = \prod_{\alpha \in F}(x - \alpha)$.*

Demostración. Puesto que $|F^\times| = p^n - 1$, y en un grupo finito el orden de cualquier elemento divide al orden del grupo, para todo $\alpha \in F^\times$, será $\alpha^{p^n-1} = 1$ y, por tanto, $\alpha^{p^n} = \alpha$ para todo $\alpha \in F$. □

El saber que los elementos de un cuerpo finito con p^n elementos son necesariamente las diferentes raíces del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ no nos dice mucho sobre la estructura de ese cuerpo, esto es, sobre como se representan sus elementos y sobre como se suman o multiplican estos entre si. Para poder precisar esto, nos ayuda el siguiente lema.

Lema 9. *Si K es un cuerpo, cualquier subgrupo finito del grupo multiplicativo $K^\times$ es cíclico.*

Demostración. Supongamos, por el contrario que $G \leq K^\times$ es un subgrupo finito que no es cíclico. Por el Teorema de Estructura de grupos abeliano finitos, sería $G \cong C_{d_1} \times \cdots \times C_{d_r}$, isomorfo a un producto de cíclicos de ordenes $d_1, \ldots, d_r$, donde cada $d_i \geq 2$, $d_i \mid d_{i+1}$ y $r > 1$. Pero entonces, para todo $\alpha \in G$, se tendría que $\alpha^{d_r} = 1$, y todo elemento de G sería una raíz del polinomio $x^{d_r} - 1$. Entonces $|G| \leq d_r$. Pero de la igualdad $d_1 \cdots d_r = |G|$, donde $d_1 \geq 2$ y $r > 1$, se deduce que $d_r < |G|$, lo que es una contradicción. □

Teorema 10. *Todo cuerpo finito de característica p es una extensión simple de $\mathbb{Z}_p$*

DEMOSTRACIÓN. El grupo $F^\times$ es cíclico. Supongamos que α es un generador de $F^\times$ y consideremos el subcuerpo $\mathbb{Z}_p(\alpha) \leq F$. Puesto que todo elemento no nulo de F es una potencia de α y pertenece a $\mathbb{Z}_p(\alpha)$, concluimos que $F = \mathbb{Z}_p(\alpha)$. □

Corolario 11. *Para todo número primo p y todo $n \geq 1$, existe un polinomio en $\mathbb{Z}_p[x]$ que es irreducible de grado n.*

DEMOSTRACIÓN. Sea F un cuerpo con p^n elementos. Será $F = \mathbb{Z}_p(\alpha)$ para algún $\alpha \in F$. Como $[F : \mathbb{Z}_p] = n$, el polinomio $Irr(\alpha, \mathbb{Z}_p)$ será de grado n. □

La anterior propiedad es cierta para $\mathbb{Q}$ (considerar los polinomios $(x^n - 2)$, pero claramente no es cierta para todos los cuerpos, por ejemplo en $\mathbb{C}[x]$ o en $\mathbb{R}[x]$. En este segundo caso no hay irreducibles de grado ≥ 3: Si f fuese un tal polinomio, que podemos suponer mónico, este tendría una raíz α en $\mathbb{C}$, sería $f = Irr(\alpha, \mathbb{R})$ y $[\mathbb{R}(\alpha) : \mathbb{R}] \geq 3$. Pero desde la torre $\mathbb{R} \leq \mathbb{R}(\alpha) \leq \mathbb{C}$, vemos que $[\mathbb{R}(\alpha) : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2$.

La siguientes observaciones ya nos prepara para precisar como describir los cuerpos finitos.

Lema 12. *Sea $p \geq 2$ un primo. Cualquier polinomio $f \in \mathbb{Z}_p[x]$ irreducible de grado n es un divisor de $x^{p^n} - x$.*

DEMOSTRACIÓN. Podemos suponer que f es mónico. Sea $E/\mathbb{Z}_p$ una extensión donde f descompone totalmente. Sea $\beta \in E$ una raíz de f, y sea $F = \mathbb{Z}_p(\beta) \leq E$. Puesto que $f = Irr(\beta, \mathbb{Z}_p)$, será $[F : \mathbb{Z}_p] = n$ y, por tanto, F es un cuerpo con p^n-elementos. Entonces β es una raíz de $x^{p^n} - x$ en F, y ha de ser $f \mid x^{p^n} - x$ en $\mathbb{Z}_p[x]$. □

Corolario 13. *Sea F un cuerpo con $|F| = p^n$. Cualquier polinomio $f \in \mathbb{Z}_p[x]$ irreducible de grado n descompone totalmente en F.*

DEMOSTRACIÓN. Sabemos que $x^{p^n} - x$ tiene todas sus raíces F. Como f es un divisor suyo, f también las tiene. □

Teorema 14. *Sea F un cuerpo con $|F| = p^n$ y $f \in \mathbb{Z}_p[x]$ cualquier polinomio mónico e irreducible de grado n. Si designamos por α cualquier raíz de f en F, entonces*

(1) $F = \mathbb{Z}_p(\alpha)$.
(2) *Los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, forman una base de $F/\mathbb{Z}_p$. Por tanto,*
$$F = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Z}_p\},$$
donde la expresión de cada elemento de F de tal forma es única.
(3) *Todo elemento de F es expresable como $g(\alpha)$, para algún polinomio $g \in \mathbb{Z}_p[x]$. Si $g \in K[x]$ es cualquier polinomio tal que $g(\alpha) = \beta$, entonces la expresión de β en función de la base es*
$$\beta = r(\alpha) = \textstyle\sum_{i=0}^{n-1} c_i\alpha^i,$$
donde $r = \sum_{i=0}^{n-1} c_i x^i$ es el resto de dividir g entre f.
(4) *Si $g, h \in K[x]$ son polinomios tal que $g(\alpha) = \beta$ y $h(\alpha) = \gamma$, entonces*
$$\begin{cases} \beta + \gamma = (g + h)(\alpha), \\ \beta\gamma = (gh)(\alpha). \end{cases}$$
Además, si $0 \neq \beta = g(\alpha)$, existen polinomios $u, v \in K[x]$ tal que $1 = gu + fv$ y se verifica que
$$\beta^{-1} = u(\alpha).$$

*La descripción anterior del cuerpo F solo depende del polinomio f y del símbolo α usado para referirnos a una de sus raíces en F. Nos referimos a esta como "***La descripción de F en la clave (α, f)***"*

Demostración. Puesto que será $f = Irr(\alpha, \mathbb{Z}_p)$. Tendremos entonces que $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n = [F : \mathbb{Z}_p]$, de donde se deduce que $F = \mathbb{Z}_p(\alpha)$, y todo lo anunciado ya nos es conocido. □

Corolario 15. *Sean F y F' dos cuerpos con p^n elementos. Supongamos que F está descrito por la clave (α, f). Entonces, para cualquier raíz α' de f en F' hay un isomorfismo $\varphi : F \cong F'$ tal que $\varphi(\alpha) = \alpha'$.*

Demostración. Si describimos F' en la clave (α', f), resulta obvio que la aplicación $\psi : F \to F'$ definida por

$$\psi(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = (a_0 + a_1\alpha' + \cdots + a_{n-1}\alpha'^{n-1})$$

es un isomorfismo (el único que hay tal que $\psi(\alpha) = \alpha'$). □

Teorema 16. *Dos cuerpos finitos con el mismo cardinal son isomorfos.*

Demostración. Sean F y F' cuerpos con p^n elementos. Sea $f \in \mathbb{Z}_p[x]$ cualquier mónico irreducible de grado n. Por el teorema anterior existen raíces $\alpha \in F$ y $\alpha' \in F'$ de f. Entonces, por el corolario anterior, hay un isomorfismo $\varphi : F \cong F'$ tal que $\varphi(\alpha) = \alpha'$ □.

Usualmente, se denota por

$$\mathbb{F}_{p^n}$$

al único (salvo isomorfismo) cuerpo con p^n elementos. En particular $\mathbb{F}_p = \mathbb{Z}_p$.

El retículo de subcuerpos de $\mathbb{F}_{p^n}$.

Para describir el retículo de subcuerpos $Sub(\mathbb{F}_{p^n}) = Sub(\mathbb{F}_{p^n}/\mathbb{F}_p)$, usaremos el siguiente lema:

Lema 17. *(i) Para cualesquiera enteros $m \geq 2$ y $\ell \geq k \geq 1$, se verifica que*

$$m^k - 1 \mid m^\ell - 1 \Leftrightarrow k \mid \ell.$$

(ii) Sea K es un cuerpo. Para cualesquiera enteros $\ell \geq k \geq 1$, se verifica que

$$x^k - 1 \mid x^\ell - 1 \text{ en } K[x] \Leftrightarrow k \mid \ell$$

y para $m \geq 2$ se verifica que

$$x^{m^k} - x \mid x^{m^\ell} - x \text{ en } K[x] \Leftrightarrow k \mid \ell.$$

Demostración.

(i) Notemos que, obviamente, $m^k \equiv 1 \mod (m^k - 1)$. Si $k \mid \ell$, poniendo $\ell = qk$, tenemos que $m^\ell - 1 = (m^k)^q - 1 \equiv 1^q - 1 = 0 \mod (m^k - 1)$. Por tanto $m^k - 1 \mid m^\ell - 1$. Recíprocamente, supongamos que $m^k - 1 \mid m^\ell - 1$, o sea que $m^\ell - 1 \equiv 0 \mod (m^k - 1)$, y que $k \nmid \ell$. Poniendo $\ell = qk + r$, con $0 < r < k$, tenemos que

$$m^\ell - 1 = (m^k)^q m^r - 1 \equiv m^r - 1 \mod (m^k - 1),$$

luego ha de ser $m^r - 1 \equiv 0 \mod (m^k - 1)$, o sea que $m^k - 1 \mid m^r - 1$. Pero esto implica que $m^k - 1 \leq m^r - 1$, o sea que $m^k \leq m^r$, lo que no es posible pues $0 < r < k$ y $m \geq 2$.

(ii) Es similar: Pongamos $\ell = qk + r$ con $0 \leq r < k$. Como, obviamente, $x^k \equiv 1 \mod (x^k - 1)$, tenemos que $x^\ell - 1 = (x^k)^q x^r - 1 \equiv x^r - 1 \mod (x^k - 1)$. Entonces

$$x^k - 1 \mid x^\ell - 1 \Leftrightarrow x^\ell - 1 \equiv 0 \mod (x^k - 1) \Leftrightarrow x^r - 1 \equiv 0 \mod (x^k - 1)$$
$$\Leftrightarrow x^k - 1 \mid x^r - 1 \Leftrightarrow r = 0 \Leftrightarrow k \mid \ell.$$

La tercera afirmación es consecuencia de las partes anteriores: Tenemos que

$$x^{m^k} - x \mid x^{m^\ell} - x \Leftrightarrow x^{m^k-1} - 1 \mid x^{m^\ell-1} - 1 \Leftrightarrow m^k - 1 \mid m^\ell - 1 \Leftrightarrow k \mid \ell.$$

□

Teorema 18. *Sea p un primo.*

(1) *Para cada divisor positivo d de n, el cuerpo $\mathbb{F}_{p^n}$ contiene exactamente un subcuerpo con p^d elementos, $\mathbb{F}_{p^d}$, y estos son sus únicos subcuerpos. Esto es,*

$$\mathrm{Sub}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{\mathbb{F}_{p^d},\ \textit{donde } d \geq 1,\ \textit{y } d \mid n\}.$$

(2) *Para cada $d \mid n$, $[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] = \frac{n}{d}$.*

(3) *Si $d_1, d_2 \mid n$, se tiene que $\mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p^{d_2}} \Leftrightarrow d_1 \mid d_2$.*

Demostración. (1) Si $F \leq \mathbb{F}_{p^n}$, será $|F| = p^d$, para un cierto $d \geq 1$. La torre de extensiones $\mathbb{F}_p \leq F \leq \mathbb{F}_{p^n}$, nos asegura que $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : F][F : \mathbb{F}_p] = [\mathbb{F}_{p^n} : F]\, d$, de donde necesariamente $d \mid n$.

Supongamos que $d \mid n$. Entonces $x^{p^d} - x \mid x^{p^n} - x$ en $\mathbb{Z}_p[x]$. Como $x^{p^n} - x$ descompone totalmente en $\mathbb{F}_{p^n}$, $x^{p^d} - x$ también lo hace. Sabemos entonces que las diferentes raíces de este polinomio en $\mathbb{F}_{p^n}$ forman un subcuerpo con p^d elementos. Podemos denotar a este por $\mathbb{F}_{p^d}$, ya que es el único subcuerpo de $\mathbb{F}_{p^n}$ de tal orden: si $F \leq \mathbb{F}_{p^n}$ es cualquier supuesto subcuerpo con $|F| = p^d$, sabemos que todo elemento de F es raíz del polinomio $x^{p^d} - x$ y, por tanto, $F \subseteq \mathbb{F}_{p^d}$, de donde concluimos que $F = \mathbb{F}_{p^d}$ por cardinalidad.

(2) La torre $\mathbb{F}_p \leq \mathbb{F}_{p^d} \leq \mathbb{F}_{p^n}$ nos dice que

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]\,[\mathbb{F}_{p^d} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]\, d$$

de donde la conclusión es clara.

(3) Sean $d_1, d_2 | n$. Si $\mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p_2^d}$, tomando grados en la torre $\mathbb{F}_p \leq \mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p^{d_2}}$, deducimos que $d_1 | d_2$. Y recíprocamente, si $d_1 | d_2$ entonces $\mathbb{F}_{p^{d_1}} \leq \mathbb{F}_{p^{d_2}}$ pues $x^{p^{d_1}} - x \mid x^{p^{d_1}} - x$. □

Una interesante consecuencia es la siguiente:

Proposición 19. (1) *Si $m \mid n$, entonces todo polinomio irreducible de grado m en $\mathbb{F}_p[x]$ descompone totalmente en $\mathbb{F}_{p^n}$.*

(2) *Si $m \nmid n$, entonces un polinomio irreducible de grado m en $\mathbb{F}_p[x]$ no tiene ninguna raíz en $\mathbb{F}_{p^n}$.*

Indicación de solución: (1) Sabemos que todo polinomio irreducible de grado m en $\mathbb{F}_p[x]$ descompone totalmente en $\mathbb{F}_{p^m}$. Si $m \mid n$, entonces $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$ y la conclusión es clara.

(2) Si $f \in \mathbb{F}_p[x]$ es irreducible de grado m y tiene una raíz α en $\mathbb{F}_{p^n}$, entonces $\mathbb{F}_p(\alpha) \leq \mathbb{F}_{p^n}$ es un subcuerpo. Pero como $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = m$, sería $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$. Luego tendríamos que $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$, lo que no puede ser ya que $m \nmid n$.