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 $[K(\alpha) : K] = n$. □

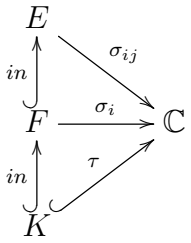
Para "construir" las diferentes τ-inmersiones de una extensión finita no simple, digamos $E = K(\alpha_1, \ldots, \alpha_r)/K$, lo más útil suele ser el mirar a una tal extensión como el extremos de una torre de extensiones simples

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

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

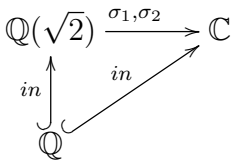
Teorema 6. *Sea E/K es una extensión finita de cuerpos de numeros y $\tau : K \to \mathbb{C}$ una inmersión. Si $[E : K] = n$, existen exactamente n diferentes τ-inmersiones $\sigma : E \to \mathbb{C}$.*

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

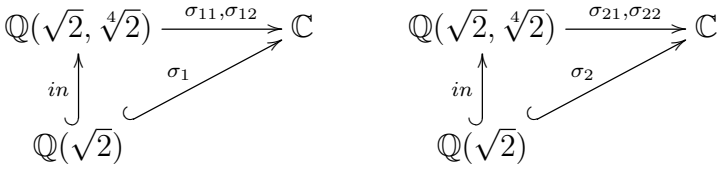
$$\begin{cases} \sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}, \\ \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}. \end{cases}$$

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}
$\sqrt[4]{2}\mapsto$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$

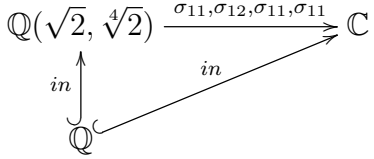
Para conocer las σ_2-inmersiones, debemos determinar las raíces del polinomio

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

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

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

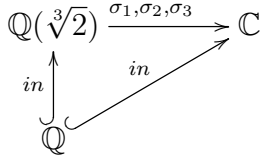
concluimos que $G(\mathbb{C}/\mathbb{R})$ es un grupo de orden dos con $G(\mathbb{C}/\mathbb{R}) = \{\sigma_1, \sigma_2\}$ donde, explícitamente,

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

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

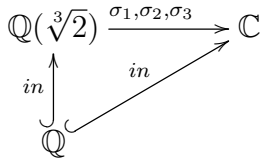
$$G=G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}).$$

(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

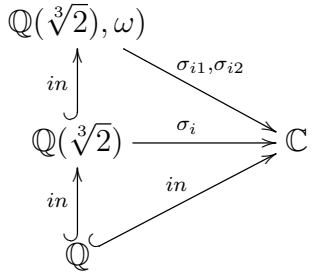


que están determinadas por que su respectiva imagen del generador es cada una de las raíces en $\mathbb{C}$ del polinomio x^3-2, esto es, según se índica en el cuadro

	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

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

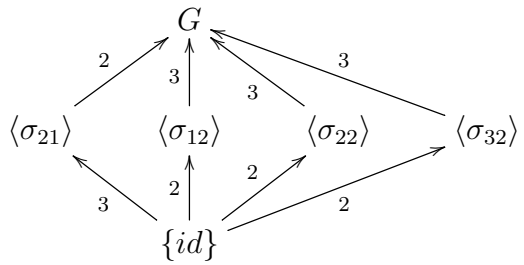
(1) *Descripción del retículo de subgrupos del grupo de Galois.* Puesto que $|G| = 6$, Los subgrupos propios serán de orden 3 y de orden 2. Puesto que 3 es la máxima potencia de 3 que divide al orden del grupo, los subgrupos de orden 3 serán los 3-subgrupos de Sylow de G y, por los Teoremas de Sylow, 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

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

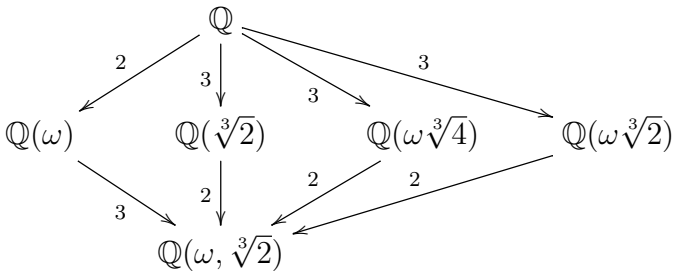
Conocemos que $[\mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{22}} : \mathbb{Q}] = 3$. Puesto que $\sigma_{22}(\omega\sqrt[3]{4}) = \omega^2\omega^2\sqrt[3]{4} = \omega\sqrt[3]{4}$, tenemos que $\mathbb{Q}(\omega\sqrt[3]{4}) \leq \mathbb{Q}(\sqrt[3]{2},\omega)^{\sigma_{22}}$. Como $[\mathbb{Q}(\omega\sqrt[3]{4})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