Definiciones básicas de teoría de Galois

Facultad de Ciencias UNAM

Introducción

En esta sección empezamos nuestro estudio de la teoría de Galois con definiciones y resultados básicos.

Automorfismos

Definición

Supongamos que K es un campo.

- Si $\sigma : K \to K$ es un isomorfismo de campos, entonces decimos que σ es un **automorfismo** de K. En otras palabras, un isomorfismo de campos es un automorfismo si su dominio y codominio coinciden.
- El conjunto de todos los automorfismos de K es denotado por $\mathrm{Aut}(K)$. Específicamente,

$$\mathrm{Aut}(K) \coloneqq \left\{ \varphi : K \to K \mid \varphi \text{ es un isomorfismo de campos} \right\}.$$

Ejemplos básicos de automorfismos

Supongamos que K es un campo.

- Claramente, la función identidad es un automorfismo de K y en particular, $\mathrm{Aut}(K) \neq \emptyset$ para cualquier campo K.
- Sea $\sigma : \mathbb{C} \to \mathbb{C}$ tal que $a + ib \mapsto a - ib$. Es fácil verificar que σ es un automorfismo de $\mathbb{C}$.
- En la proposición 1.6.8 demostramos que si $X = \mathbb{Q}, \mathbb{R}$ y $\varphi : X \to X$ es un homomorfismo de anillos no trivial, entonces $\varphi = \mathrm{id}_X$. Como todo isomorfismo de campos es también un isomorfismo de anillos, lo anterior implica que

$$\mathrm{Aut}(\mathbb{Q}) = \left\{\mathrm{id}_{\mathbb{Q}}\right\} \quad \text{y} \quad \mathrm{Aut}(\mathbb{R}) = \left\{\mathrm{id}_{\mathbb{R}}\right\}.$$

Conjuntos/elementos fijos bajo un automorfismo

Definición

Supongamos que K es un campo y que $\sigma \in \mathrm{Aut}(K)$.

- Sea $x \in K$. Decimos que σ **fija a** x si $\sigma(x) = x$.
- Sea $S \subset K$ un subconjunto arbitrario de K. Decimos que σ **fija a** S si σ fija a todo $s \in S$.

Automorfismos y el campo primo

Supongamos que K es un campo. Como los isomorfismos de campos respetan las unidades, entonces $\sigma(1_K) = 1_K$ para todo $\sigma \in \mathrm{Aut}(K)$. En particular,

$$\sigma(n \cdot 1_K) = n \cdot 1_K \text{ para toda } n \in \mathbb{Z}. \tag{1}$$

Usando esto, veamos que σ fija a K_{pri}, el campo primo de K (recuerda que el campo primo de K es el subcampo de K generado por la unidad).
En la proposición 2.1.5 demostramos que

$$K_{\mathrm{pri}} = \begin{cases} \left\{ (n \cdot 1_K)\,(m \cdot 1_K)^{-1} \mid n, m \in \mathbb{Z} \right\} & \text{si } \mathrm{ch}(K) = 0 \\ \left\{ 1_K, 2 \cdot 1_K, \ldots, (p-1) \cdot 1_K \right\} & \text{si } \mathrm{ch}(K) = p \end{cases} \tag{2}$$

Juntando (1) y (2), obtenemos lo deseado.

Mas aun, como $\mathbb{Q} = \mathbb{Q}_{\mathrm{pri}}$, entonces lo anterior implica que todo automorfismo de $\mathbb{Q}$ fija a $\mathbb{Q}$ y en particular, $\mathrm{Aut}(\mathbb{Q}) = \left\{ \mathrm{id}_{\mathbb{Q}} \right\}$. Análogamente, como $\mathbb{Z}_p$ coincide con su campo primo, $\mathrm{Aut}(\mathbb{Z}_p) = \left\{ \mathrm{id}_{\mathbb{Z}_p} \right\}$.

$\mathrm{Gal}(K/F)$

Definición

Supongamos que K/F es una extensión de campos. Definimos $\mathrm{Gal}(K/F)$ como el conjunto de automorfismos de K que fijan a F. En otras palabras,

$$\mathrm{Gal}(K/F) \coloneqq \left\{\sigma \in \mathrm{Aut}(K) \mid \sigma \text{ fija a } F\right\}.$$

Usando esta notación, tenemos el siguiente resultado: Si K es un campo y K_{pri} es su campo primo, entonces

$$\mathrm{Gal}(K/K_{\mathrm{pri}}) = \left\{\sigma \in \mathrm{Aut}(K) \mid \sigma \text{ fija a } K_{\mathrm{pri}}\right\} = \mathrm{Aut}(K).$$

Donde la segunda igualdad se cumple porque para todo $\sigma \in \mathrm{Aut}(K)$, σ fija a K_{pri}.

Notación

Supongamos que K es un campo.

- Si $\sigma \in \mathrm{Aut}(K)$ y $x \in K$, usualmente escribimos σx en vez de $\sigma(x)$.
- Si $\sigma, \tau \in \mathrm{Aut}(K)$, entonces la composición $\sigma \circ \tau$ tiene sentido y por brevedad, usualmente escribimos $\sigma\tau$ en vez de $\sigma \circ \tau$.

$\mathrm{Aut}(K)$ es un grupo bajo la composición y $\mathrm{Gal}(K/F) \leq \mathrm{Aut}(K)$

Proposición 1

Supongamos que K es un campo y F es un subcampo de K. Entonces

1. $\mathrm{Aut}(K)$ es un grupo con la operación dada por la composición usual de funciones.
2. $\mathrm{Gal}(K/F)$ es un subgrupo de $\mathrm{Aut}(K)$.

La demostración es muy sencilla y por eso se la dejamos al lector. Por eso, también decimos que

- $\mathrm{Aut}(K)$ es el **grupo de automorfismos de** K y que
- $\mathrm{Gal}(K/F)$ es el **grupo de Galois de** K/F.

Extensiones isomorfas producen grupos de Galois isomorfos

Proposición 2

Supongamos que K/F y L/F son extensiones de campo. Si $K \cong L$, entonces

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L/F).$$

Demostración. Supongamos que $\phi : K \to L$ es un isomorfismo de campos. El lector podrá fácilmente verificar que

$$\begin{aligned} \mathrm{Gal}(L/F) &\to \mathrm{Gal}(K/F) \\ \sigma &\mapsto \phi^{-1} \circ \sigma \circ \phi \end{aligned}$$

es un isomorfismo de grupos. □

$\mathrm{Gal}(L/K) \leq \mathrm{Gal}(L/F)$ si $F \subset K \subset L$

Proposición 3

Supongamos que F, L, K son campos tales que $F \subset K \subset L$. Entonces $\mathrm{Gal}(L/K)$ es un subgrupo de $\mathrm{Gal}(L/F)$.

La demostración es muy sencilla y por eso se la dejamos al lector.

$\sigma \in \mathrm{Gal}(K/F)$ y $\alpha \in K$ algebraico sobre $F \implies$ $\sigma\alpha$ raíz de $m_{\alpha,F}(x)$

Proposición 4

Supongamos que K/F es una extensión de campos y que $\sigma \in \mathrm{Gal}(K/F)$. Si $p(x) \in F[x]$ y $\alpha \in K$ es raíz de $p(x)$, entonces $\sigma\alpha$ también es raíz de $p(x)$.

En particular, si $\alpha \in K$ es algebraico sobre F, entonces $\sigma\alpha$ es una raíz de $m_{\alpha,F}(x) \in F[x]$, el polinomio mínimo de α en F.

Mas aun, lo anterior implica que $m_{\alpha,F}(x) = m_{\sigma\alpha,F}(x)$.

Demostración. Supongamos que

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Como α es raíz de $p(x)$, entonces

$$0 = a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1 \alpha + a_0.$$

Aplicando σ a la ecuación anterior obtenemos

$$\begin{aligned}
0 = \sigma(0) &= \sigma\left(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right) \\
&= \sigma(a_n)\sigma(\alpha^n) + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\
&\qquad\qquad (\sigma \text{ es homomorfismo de campos}) \\
&= a_n\sigma(\alpha^n) + a_{n-1}\sigma(\alpha^{n-1}) + \cdots + a_1\sigma(\alpha) + a_0 \\
&\qquad\qquad (\sigma(a) = a \text{ para toda } a \in F \text{ pues } \sigma \in \mathrm{Gal}(K/F)) \\
&= a_n(\sigma\alpha)^n + a_{n-1}(\sigma\alpha)^{n-1} + \cdots + a_1(\sigma\alpha) + a_0 \\
&\qquad\qquad (\sigma \text{ es homomorfismo de campos}) \\
&= p(\sigma\alpha).
\end{aligned}$$

Por lo tanto, $\sigma\alpha$ es raíz de $p(x)$. $\square$

Los elementos de $\mathrm{Gal}(K/F)$ permutan a las raíces de los polinomios con coeficientes en F

Corolario 5

Supongamos que K/F es una extensión de campos, que $\sigma \in \mathrm{Gal}(K/F)$, y que $p(x) \in F[x]$. Si S es el conjunto de todas las raíces de $p(x) \in F[x]$, entonces $\sigma(S) = S$ y por lo tanto,

$$\sigma \restriction_S : S \to S$$

esta bien definida y es una biyeccion.

En particular, si $S = \{\alpha_1, \ldots, \alpha_n\}$ con $\alpha_i \neq \alpha_j$ para $i \neq j$, entonces $S = \{\sigma\alpha_1, \ldots, \sigma\alpha_n\}$.

Usando la proposición anterior, la demostración de este resultado es muy sencilla y por eso se la dejamos al lector.

$\text{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right)$

Supongamos que $\sigma \in \text{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right)$. Si $a, b \in \mathbb{Q}$, entonces

$$\sigma\left(a + b\sqrt{2}\right) = \sigma(a) + \sigma\left(b\sqrt{2}\right) = \sigma(a) + \sigma(b)\sigma\left(\sqrt{2}\right) = a + b\sigma(\sqrt{2})$$

donde la ultima igualdad se cumple porque σ fija a $\mathbb{Q}$.

Como todo elemento de $\mathbb{Q}(\sqrt{2})$ es de la forma $a + b\sqrt{2}$ (con $a, b \in \mathbb{Q}$), entonces lo anterior implica que σ esta completamente determinado por su valor en $\sqrt{2}$.

En lo que sigue, usaremos la proposición anterior para encontrar *todos* los posibles valores de $\sigma(\sqrt{2})$. Para esto, primero recordemos que $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$ y por lo tanto,

$$\sigma(\sqrt{2}) = \sqrt{2} \quad \text{ó} \quad \sigma(\sqrt{2}) = -\sqrt{2}.$$

En el primer caso, $\sigma = \text{id}_{\mathbb{Q}(\sqrt{2})}$ y en el segundo caso $a + b\sqrt{2} \overset{\sigma}{\mapsto} a - b\sqrt{2}$.

Usando esto, es facil ver que $\text{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) \cong \mathbb{Z}_2$.

$\mathrm{Gal}(K/F)$ con $[K : F] = 2$ y $\mathrm{ch}(F) \neq 2$

Recordemos que en la proposición 2.6.8 vimos que si K/F es una extensión de campos con $[K : F] = 2$ y $\mathrm{ch}(F) \neq 2$, entonces $K = F(\sqrt{D})$ donde $\sqrt{D}$ es una solución a la ecuación

$$x^2 - D = 0$$

y D es tal que $a^2 \neq D$ para toda $a \in F$.

Como

$$F(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in F\},$$

podemos usar un argumento análogo al de la diapositiva anterior para concluir que $\mathrm{Gal}(K/F) = \{\mathrm{id}, \sigma\}$ donde σ esta dada por

$$\sigma\left(a + b\sqrt{D}\right) = a - b\sqrt{D} \text{ para toda } a, b \in F.$$

Por lo tanto, $\mathrm{Gal}(K/F) \cong \mathbb{Z}_2$ y en particular, como $\mathbb{C} = \mathbb{R}(\sqrt{-1})$, entonces $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$.

Los elementos de Gal $\left(F(\alpha_1, \ldots, \alpha_n)/F\right)$ con $\alpha_1, \ldots, \alpha_n \in K$ algebraicos sobre F

Proposición 6

Supongamos que $\alpha_1, \ldots, \alpha_n \in K$ son algebraicos sobre F. Entonces todo $\sigma \in \text{Gal}\left(F(\alpha_1, \ldots, \alpha_n)/F\right)$ esta completamente determinado por su valor en los α_i. Específicamente, si $\sigma, \tau \in \text{Gal}\left(F(\alpha_1, \ldots, \alpha_n)/F\right)$ son tales que $\sigma(\alpha_i) = \tau(\alpha_i)$ para toda i, entonces $\sigma = \tau$.

Demostración. Es consecuencia inmediata de la proposición 2.7.6: recordemos que ahí vimos que para cada α_i existe[1] un $n_i \in \mathbb{Z}_{\geq 0}$ tal que

$$\left\{\alpha_1^{j_1}\alpha_2^{j_2}\cdots\alpha_m^{j_m} \mid j_i \in \{0, 1 \ldots, n_i - 1\} \text{ para cada } i \in \{0, 1, \ldots, k-1\}\right\}$$

es una F-base de $F(\alpha_1, \ldots, \alpha_n)$. □

[1] En la proposición 2.7.6 describimos explícitamente a n_i pero en este momento basta con saber que $n_i \in \mathbb{Z}_{\geq 0}$

$\mathrm{Gal}\left(F(\alpha_1, \ldots, \alpha_n)/F\right)$ es un grupo finito

Proposición 7

Si $\alpha_1, \ldots, \alpha_n \in K$ son algebraicos sobre F, entonces $\mathrm{Gal}\left(F(\alpha_1, \ldots, \alpha_n)/F\right)$ es un grupo finito.

Demostración. Para cada $i \in \{1, \ldots, n_i\}$ sea S_i el conjunto de todas las raíces en $F(\alpha_1, \ldots, \alpha_n)$ de $m_{\alpha_i, F}$, el polinomio de α_i en F. Como

- $\sigma\alpha_i \in S_i$ para cada i,
- $|S_i| < \infty$ para cada i, y
- todo $\sigma \in \mathrm{Gal}\left(F(\alpha_1, \ldots, \alpha_n)/F\right)$ esta completamente determinado por su valor en los α_i,

entonces existe a lo mas una cantidad finita de elementos en $\mathrm{Gal}(K/F)$. $\square$

$\text{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$

Supongamos que $\rho \in \text{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$. Por la proposición 6, ρ esta completamente determinado por su valor en $\sqrt{2}$ y $\sqrt{3}$. Como

$$m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2 \quad \text{y} \quad m_{\sqrt{3},\mathbb{Q}}(x) = x^2 - 3,$$

entonces la proposición 4 implica que $\rho(\sqrt{2}) = \pm\sqrt{2}$ y $\rho(\sqrt{3}) = \pm\sqrt{3}$.

Por lo tanto, cada elemento de $\text{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$ debe satisfacer (y quedara determinado por) alguna de las siguientes posibilidades

$$\begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \qquad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Es fácil verificar que cada una de estas posibilidades define un automorfismo y por lo tanto, estos son *todos* los automorfismos.

En lo que sigue, veremos que podemos describir a $\text{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$ de una forma mas sencilla (y posiblemente familiar).

Denotemos

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Entonces

$$\sigma\tau = \tau\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

y por lo tanto, si denotamos $\mathrm{id} = 1$, entonces

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right) = \{1, \sigma, \tau, \sigma\tau\}.$$

Usando esto, el lector puede verificar que el homomorfismo de grupos que de $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right)$ en $\mathbb{Z}_2 \times \mathbb{Z}_2$ que satisface

$$\sigma \mapsto (1, 0) \quad \text{y} \quad \tau \mapsto (0, 1)$$

es un isomorfismo y por lo tanto,

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Antes de acabar con este ejemplo, es importante observar que si

$$\rho : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\sqrt{2} \mapsto \pm\sqrt{3}$$

entonces $\rho \notin \text{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})\right)$ porque $\rho(\sqrt{2}) = \pm\sqrt{3}$ no es raíz de $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$.
En lo anterior nos dimos la libertad de usar esto implícitamente porque (i) es mas o menos obvio y (ii) es consecuencia inmediata de que

$$\sigma \in \text{Gal}(K/F) \text{ y } \alpha \in K \text{ algebraico sobre } F \implies \sigma\alpha \text{ raíz de } m_{\alpha,F}(x).$$

A pesar de la "trivialidad" de esta observacion, en el siguiente corolario escribimos el caso general de esta situación con el objetivo de (i) evitar errores en el futuro, (ii) facilitar un poquito mas las cuentas, y (iii) entender un poquito mejor la forma en la que actúan los elementos de $\text{Gal}(K/F)$.

Los elementos de $\mathrm{Gal}(K/F)$ respetan a los factores irreducibles de los polinomios con coeficientes en F

Corolario 8

Supongamos que K/F es una extensión de campos, que $\sigma \in \mathrm{Gal}(K/F)$, que $p(x) \in F[x]$, y que $p(x) = p_1(x) \cdots p_m(x)$ es su factorización en irreducibles. Si $\alpha \in K$ es raíz de $p_i(x)$, entonces $\sigma\alpha \in K$ también es raíz de $p_i(x)$.

En particular, si S es el conjunto de las raíces de $p(x)$, S_i es el conjunto de las raíces de $p_i(x)$ y $f : S \to S$ es tal que $f(\alpha) = \sigma\alpha$, entonces

- f es una biyeccion.
- $f(S_i) = S_i$ y $f\restriction_{S_i} : S_i \to S_i$ esta bien definida y también es una biyeccion.

Claramente, esto es consecuencia inmediata de que

$$\sigma \in \mathrm{Gal}(K/F) \text{ y } \alpha \in K \text{ algebraico sobre } F \implies \sigma\alpha \text{ raíz de } m_{\alpha,F}(x).$$

$\text{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)$

Supongamos que $\rho \in \text{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)$. De nuevo, ρ esta determinado por su valor en $\sqrt[3]{2}$. De la misma manera que en los ejemplos anteriores, empezamos por encontrar las raíces de $m_{\sqrt[3]{2},\mathbb{Q}}(x)$. Como $m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2$, entonces las raíces de $m_{\sqrt[3]{2},\mathbb{Q}}(x)$ son

$$\sqrt[3]{2}, \quad \zeta\sqrt[3]{2}, \quad \zeta^2\sqrt[3]{2}$$

donde $\zeta = \frac{-1+i\sqrt{3}}{2}$ (es una 3-esima raíz primitiva de la unidad).

Aquí hay que tener cuidado: como $\zeta \notin \mathbb{Q}(\sqrt[3]{2})$, entonces la *única* raíz de $m_{\sqrt[3]{2},\mathbb{Q}}(x)$ que pertenece a $\mathbb{Q}(\sqrt[3]{2})$ es $\sqrt[3]{2}$.

En particular, la única posibilidad es $\rho(\sqrt[3]{2}) = \sqrt[3]{2}$ y como ρ esta completamente determinado por su valor en $\sqrt[3]{2}$, lo anterior implica que $\rho = \text{id}$. Como ρ es un elemento arbitrario de $\text{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)$, entonces lo anterior implica que

$$\text{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right) = \{\text{id}\}.$$

$\mathrm{Gal}\left(K/\mathbb{Q}\right)$ con $K =$ el campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$

Supongamos que K es el campo de descomposición de $x^3 - 2$. Recordemos que las raíces de $x^2 - 3$ son

$$\sqrt[3]{2}, \quad \zeta\sqrt[3]{2}, \quad \zeta^2\sqrt[3]{2}$$

donde $\zeta = \frac{-1+i\sqrt{3}}{2}$ (es una 3-esima raíz primitiva de la unidad). Entonces (por la proposición 2.9.2),

$$\mathbb{Q}\left(\sqrt[3]{2},\ \zeta\sqrt[3]{2},\ \zeta^2\sqrt[3]{2}\right)$$

es un campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$. Por otro lado, el lector podra fácilmente verificar que

$$\mathbb{Q}\left(\sqrt[3]{2},\ \zeta\sqrt[3]{2},\ \zeta^2\sqrt[3]{2}\right) = \mathbb{Q}\left(\zeta, \sqrt[3]{2}\right)$$

y por lo tanto, vamos a describir a $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})\right)$. Para esto, supongamos que $\rho \in \mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})\right)$. Claramente, ρ esta determinado por su valor en ζ y $\sqrt[3]{2}$. Continuemos como en los ejemplos anteriores.

Evaluando directamente, es fácil ver que $\zeta = \frac{-1+i\sqrt{3}}{2}$ es raíz del polinomio irreducible $x^2 + x + 1$. Mas aun, como ζ no puede ser raíz de un polinomio de grado 1 con coeficientes en $\mathbb{Q}$ (de lo contrario, $\zeta \in \mathbb{Q}$), entonces lo anterior implica que

$$m_{\zeta,\mathbb{Q}}(x) = x^2 + x + 1.$$

De nuevo, evaluando directamente, es fácil ver que $\zeta^2 = -1 - \zeta\frac{-1-i\sqrt{3}}{2}$ es raiz de $x^2 + x + 1$. En resumen,

$$\rho(\zeta) \in \{\zeta,\ \zeta^2\} \quad \text{y} \quad \rho(\sqrt[3]{2}) \in \{\sqrt[3]{2},\ \zeta\sqrt[3]{2},\ \zeta^2\sqrt[3]{2}\}.$$

Notemos que como hay 2 posibles valores para $\rho(\zeta)$ y hay 3 posibles valores para $\rho(\sqrt[3]{2})$, entonces hay a lo mas 6 elementos en $\text{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right)$. Usando el hecho de que

$$\left\{1,\ \sqrt[3]{2},\ \left(\sqrt[3]{2}\right)^2,\ \zeta,\ \zeta\sqrt[3]{2},\ \zeta\left(\sqrt[3]{2}\right)^2\right\}$$

es una $\mathbb{Q}$-base de $\mathbb{Q}\left(\zeta, \sqrt[3]{2}\right)$ es fácil ver que cada una de las 6 posibilidades define un automorfismo.

De la misma manera que en el ejemplo anterior, veamos que podemos describir a $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right)$ de una forma mas sencilla (y posiblemente familiar). Para esto, denotemos

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \zeta\sqrt[3]{2} \\ \zeta \mapsto \zeta \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta \mapsto \zeta^2 \end{cases}$$

Evaluando directamente, uno puede verificar que

$$\sigma^3 = 1, \quad \tau^2 = 1, \quad \sigma\tau = \tau\sigma^2,$$

y por lo tanto,

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right) = \left\{1, \sigma, \sigma^2, \tau, \sigma\tau, \tau\sigma\right\}.$$

En la siguiente sección veremos (usando teoría de Galois) que $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right) \cong S_3$ (el grupo simétrico en 3 elementos), pero invitamos al lector a verificar que el homomorfismo de $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right)$ en S_3 que satisface $\sigma \mapsto (123)$ y $\tau \mapsto (23)$ es un isomorfismo.