Teorema Fundamental de la Teoría de Galois aplicado a nuestro ejemplo del 29/10/19

1. Sea $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

a) Calcula $E = \mathbb{Q}(f)$.

b) Calcula el grado de $E/\mathbb{Q}$.

c) Calcula la clase de isomorfía de $G = \mathrm{Gal}(E/\mathbb{Q})$.

d) Describe explícitamente los elementos de G, indicando sus órdenes.

e) Escribe G como un producto semidirecto $\mathsf{C}_3 \rtimes \mathsf{C}_2$ donde $\mathsf{C}_2 = \mathrm{Aut}(\mathsf{C}_3)$.

f) Describe todas las subextensiones de $E/\mathbb{Q}$ indicando cuáles de ellas definen extensiones normales sobre $\mathbb{Q}$.

Solución.

(a) Las raíces de $x^3 - 2$ en $\mathbb{C}$ son $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega\}$, donde ω es una raíz primitiva cúbica de la unidad. Por tanto, el cuerpo de escisión de x^3-2 sobre $\mathbb{Q}$ es es $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Como $\omega = \frac{1}{2}(-1+\sqrt{3}i)$, también tenemos que $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$.

(b) Notamos que $\mathrm{Irr}(\mathbb{Q}, \sqrt[3]{2}) = x^3 - 2$ por Einsestein para $p = 2$ y que $\mathrm{Irr}(\mathbb{Q}, \omega) = x^2 + x + 1$ es el polinomio ciclotómico cúbico. Entonces $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ y $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$ por el Teorema del Elemento Algebraico. Por el ejercicio 12.b) de la Hoja 2, tenemos que $|E : \mathbb{Q}| = 6$. También podríamos haber notado que $x^2 + x + 1$ es irreducible sobre $\mathbb{Q}(\sqrt[3]{2})$ por no tener raíces, y haber aplicado el Teorema de Transitividad de Grados para hallar el grado de la extensión. En particular, obtenemos que $\mathrm{Irr}(\mathbb{Q}(\omega), \sqrt[3]{2}) = x^3 - 2$.

(c) Como $E/\mathbb{Q}$ es de Galois (normal en característica 0), por el Corolario 3.4.6 tenemos que $|G| = |E : \mathbb{Q}| = 6$. Sea $M = \mathbb{Q}(\sqrt[3]{2}) \subseteq E$, la extensión $M/\mathbb{Q}$ no es normal, por el Teorema Fundamenta de la Teoría de Galois, se corresponde con un subgrupo no normal de G. Podemos concluir, por tanto, que G no es abeliano. Ahora, G es un grupo de orden 6 no abeliano, por tanto, $G \cong \mathsf{S}_3$. Recordemos en este punto que, como consecuencia del Teorema 3.11.(d) también sabíamos que G es isomorfo a algún subgrupo de S_3, y la igualdad de órdenes en este caso, también nos permite concluir $G \cong \mathsf{S}_3$.

(d) Sea $L = \mathbb{Q}(\omega)$, tenemos que $L/\mathbb{Q}$ es normal por ser L el cuerpo de escisión de $x^2 + x + 1$. Podemos empezar calculando $H = \mathrm{Gal}(L/\mathbb{Q})$ ya que por el Corolario 3.12 todo elemento de G restringe a un elemento de H, y por el Teorema 3.4.5 todo $\sigma \in H$ se extiende de exactamente $|E : L| = 3$ formas distintas a G. Como $L/\mathbb{Q}$ es de Galois $|H| = |L : \mathbb{Q}| = 2$, así pues, $H \cong \mathsf{C}_2$, de hecho, $H = \langle \sigma \rangle$, donde $\sigma(\omega) = \omega^2$, pues σ debe permutar las raíces de $x^2 + x + 1$. Ahora usamos que $x^3 - 2$ es irreducible en $L[x]$ y el Teorema 2.5 con respecto a los dos $\mathbb{Q}$-automorfismos de H, la identidad y σ y obtenemos que cada uno de ellos se puede extender de 3 maneras distintas a G, pues podemos enviar $\sqrt[3]{2}$ a cualquiera de las tres raíces de $x^3 - 2$ en E. (La clave es que los elementos de H fijan el polinomio $x^3 - 2$.) Denotamos por τ_i con $i = 1, 2, 3$ a las tres extensiones de la identidad de L y por τ_i con $i = 4, 5, 6$ a las tres extensiones de σ a E. Como cada τ_i queda determinado por las imgenes de $\sqrt[3]{2}$ y ω podemos recoger toda la información de los automorfismos de G en la siguiente tabla. También, como comentamos en clase, siguiendo la prueba del Teorema 3.5, vemos que para cada elemento H y cada raíz α de $x^3 - 2$, existe una extensión del elemento de H a G que lleva $\sqrt[3]{2}$ en α.

	$\sqrt[3]{2}$	ω
τ_1	$\sqrt[3]{2}$	ω
τ_2	$\sqrt[3]{2}\omega$	ω
τ_3	$\sqrt[3]{2}\omega^2$	ω
τ_4	$\sqrt[3]{2}$	ω^2
τ_5	$\sqrt[3]{2}\omega$	ω^2
τ_6	$\sqrt[3]{2}\omega$	ω^2

¿Cómo calculamos lo órdenes en G? La identidad de G es la identidad $1\colon E \to E$. Notamos que $\tau_1 = 1 \in G$. Ahora $\tau_2^2(\sqrt[3]{2}) = \tau_2(\sqrt[3]{2}\omega) = \tau_2(\sqrt[3]{2})\tau_2(\omega) = \sqrt[3]{2}\omega^2$, además τ_2^2 fija a ω porque τ_2 lo fija. Como cualquier elemento $\tau \in G$ queda determinado por las imágenes en $\sqrt[3]{2}$ y ω (esto se puede ver escribiendo una $\mathbb{Q}$-base de E, como vimos en clase, o simplemente por la forma de los elementos de $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$), tenemos que $\tau_2^2 = \tau_3$. Se puede comprobar que $\tau_2^3 = \tau_1 = 1$, así que tenemos que $o(\tau_2) = 3$ en G. Es conveniente calcular los órdenes (como ejercicio para el lector) de todos los elementos, que podemos incluir en la tabla anterior.

	$\sqrt[3]{2}$	ω	orden
τ_1	$\sqrt[3]{2}$	ω	1
τ_2	$\sqrt[3]{2}\omega$	ω	3
τ_3	$\sqrt[3]{2}\omega^2$	ω	3
τ_4	$\sqrt[3]{2}$	ω^2	2
τ_5	$\sqrt[3]{2}\omega$	ω^2	2
τ_6	$\sqrt[3]{2}\omega$	ω^2	2

(e) Sabemos que $\mathsf{S}_3 = \langle (123), (23) \rangle = \langle (123) \rangle \rtimes \langle (23) \rangle$ es un producto semidirecto de modo que $(123)^{(23)} = (132) = (123)^{-1}$. Como $G \cong \mathsf{S}_3$, se tiene que G es el producto semidirecto de un automorfismo de E de orden 3 y uno de orden 2, además, el conjugado del elemento de orden 3 por el elemento de orden 2 resulta el inverso del elemento de orden 3. (La única acción posible sobre un grupo cíclico de orden 3 es enviar cada elemento a su inverso.) Sabemos que $\tau_4^2 = 1$. En particular, $\tau_4^{-1} = \tau_4$. Ahora $\tau_2^{\tau_4} = \tau_4\tau_2\tau_4$ fija ω y $\tau_2^{\tau_4}(\sqrt[3]{2}) = \tau_4(\tau_2(\sqrt[3]{2})) = \tau_4(\sqrt[3]{2}\omega) = \sqrt[3]{2}\omega^2$. Es decir, $\tau_2^{\tau_4} = \tau_3 = \tau_2^{-1}$. Por tanto, $G = \mathrm{Gal}(E/\mathbb{Q}) = \langle \tau_2 \rangle \rtimes \langle \tau_4 \rangle$. Por el Teorema Fundamental de la Teoría de Galois, esta expresión tiene sentido porque $\langle \tau_2 \rangle = \{\tau_1, \tau_2, \tau_3\} = \mathrm{Gal}(E/L) \triangleleft G$ pues $L/\mathbb{Q}$ es una extensión normal. Si escribimos $N = \mathrm{Gal}(E/L)$, por el Teorema 3.11(c) (o por el Corolario 3.12(b) o por el TFTG) se tiene que $G/N \cong H = \mathrm{Gal}(L/\mathbb{Q})$ y el isomorfismo está dado por la restricción de automorfismos a L. Vemos que esto tiene sentido pues $G/N = \{1N, \tau_4 N\}$ y $\tau_4|_L = \sigma$ con $H = \{1, \sigma\}$.

También es interesante entender un isomorfismo $G \cong \mathsf{S}_3$. Basta numerar el conjunto $\Omega = \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\overline{\omega}\}$ de raíces de $x^3 - 2$, escribimos $a_1 = \sqrt[3]{2}$, $a_2 = \sqrt[3]{2}\omega$ y $a_3 = \sqrt[3]{2}\overline{\omega}$. Notamos que τ_2 se corresponde con la permutación $(a_1, a_2, a_3) = (123)$ y τ_4 se corresponde con la permutación $(a_2, a_3) = (23)$.

(e) Por el Teorema Fundamental de la Teoría de Galois

$$\{\mathbb{Q} \subseteq M \subseteq E\} \overset{1:1}{\longleftrightarrow} \{H \leq G\}$$

correspondencia bajo la cual $\mathbb{Q} \leftrightarrow G$ y $E \leftrightarrow 1$ (ya que las subextensiones de $E/\mathbb{Q}$ se corresponden con los cuerpos fijados por los distintos subgrupos de G). Como $|G| = 6$, los únicos subgrupos propios de G tienen orden 2 o 3. Si $P \leq G$ con $|P| = 3$, entonces $|G : P| = 2$ y esto implica que $Q \triangleleft G$. Además P es un 3-subgrupo de Sylow de G, y por Teoría de Sylow sabemos que los subgrupos de

G de orden 3 son todos conjugados de P. Como $P \triangleleft G$, tenemos que G tiene un único subgrupo de orden 3 que es $P = N = \langle \tau_2 \rangle$. Ahora, si $Q \leq G$ con $|Q| = 2$, entonces es un 2-subgrupo de Sylow de G. Tenemos que $P \cap Q = 1$, luego $PQ = G$. Si Q fuera normal, entonces $G = P \times Q$ sería abeliano. Por tanto, Q no es normal. Como $|G : Q| = 3$ y $Q \subseteq \mathbf{N}_G(Q) < G$, concluimos que $\mathbf{N}_G(Q) = Q$ (pues $|\mathbf{N}_G(Q) : Q|$ divide $|G : Q| = 3$ y es escrictamente menor que 3). Por Teoría de Sylow, Q tiene 3 conjugados, que son todos los subgrupos de orden 2 de G. Podemos tomar $Q = \langle \tau_4 \rangle$. Entonces 3 los conjugados distintos de Q son concretamente Q, Q^{τ_2} y Q^{τ_3}. ¿Por qué? Como $\tau_2, \tau_3 \notin \mathbf{N}_G(Q) = Q$ (pues tiene orden 3), entonces $Q^{\tau_2} \neq Q \neq Q^{\tau_3}$. Además, si $Q^{\tau_2} = Q^{\tau_3}$ obtendríamos que $Q = Q^{\tau_2 \tau_3^{-1}} = Q^{\tau_2^2} = Q^{\tau_3} \neq Q$, lo que es absurdo.

Además, $\mathbb{Q} \subseteq L \subseteq E$ con $L/\mathbb{Q}$ normal si, y solo si, $\mathrm{Gal}(L/\mathbb{Q})$ es un subgrupo normal de G. Como $L/\mathbb{Q}$ es normal de grado 2, y por el Teorema Fundamental Teoría de Galois $E/\mathbb{Q}$ tiene una única subextensión normal de grado 2 sobre $\mathbb{Q}$ necesariamente $L = E^P = E^N = E^{\tau_2}$. (El lector puede hacer las comprobaciones a mano.) Las subextensiones de grado 3 se van a corresponder con subcuerpos fijados por los 3-subgrupos de Sylow, así que podemos usar el Lema de conjugación 4.5 para calcularlas. Es decir, si calculamos $M_1 = E^Q = E^{\langle \tau_4 \rangle} = E^{\tau_4}$, tendremos que $M_2 = E^{Q^{\tau_2}} = \tau_2(L_1)$ y $M_3 = E^{Q^{\tau_3}} = \tau_3(L_2)$.

Vamos a calcular $M_1 = E^{\tau_4}$. Para ello, primero calculamos una $\mathbb{Q}$-base de E. Por lo dicho en el apartado (b) y el Teorema de Transitividad de Grados tenemos que $\mathcal{B} = \{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega\}$ es una $\mathbb{Q}$-base de E. Podemos escribir $\alpha = \sqrt[3]{2}$, entonces $\mathcal{B} = \{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\}$. Queremos calcular la forma de los elementos de E fijados por τ_4. Un elemento genérico de E tiene la forma $x = a + b\alpha + c\alpha^2 + d\omega + e\alpha\omega + f\alpha^2\omega$. Ahora, $\tau_4(x) = x$ si, y solo si,

$$a + b\alpha + c\alpha^2 + d\omega + e\alpha\omega + f\alpha^2\omega = a + b\alpha + c\alpha^2 + d\omega^2 + e\alpha\omega^2 + f\alpha^2\omega^2 \,.$$

Usando que $\omega^2 = -\omega - 1$, la igualdad arriba ocurre si y solo si,

$$d\omega + e\alpha\omega + f\alpha^2\omega = d(-\omega - 1) + e\alpha(-\omega - 1) + f\alpha^2(-\omega - 1) \,,$$

de donde

$$d + 2d\omega + e\alpha + 2e\alpha\omega + f\alpha^2 + 2f\alpha^2\omega = 0 \,.$$

Usando que $\mathcal{B}$ es base (independencia lineal), la igualdad arriba ocurre, si y solo, si $d = e = f = 0$. Por tanto, $x \in E^{\tau_4} = M_1$ si, y solo si, $x = a + b\alpha + c\alpha^2 \in \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$. Hemos probado que $M_1 = \mathbb{Q}(\sqrt[3]{2})$. Usando el Lema 4.5, tenemos que $M_2 = \tau_2(M_1) = \mathbb{Q}(\sqrt[3]{2}\omega)$ y $M_3 = \tau_3(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2}\omega^2)$. También podríais haber calculado M_2 y M_3 como lo hemos hecho con M_1 (y es un buen ejercicio para familiarizarse con este tipo de ejercicios y aprender a no cometer errores de cálculo).