Algunos ejemplos de uso del teorema de Galois

Matías Saucedo

Consideraciones generales

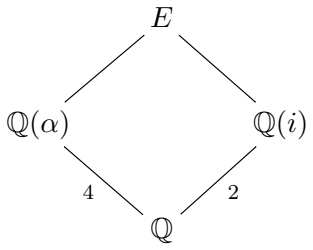
Sea $f \in \mathbb{Q}[X]$ y sea E un cuerpo de descomposición de f sobre $\mathbb{Q}$.
La extensión $E/\mathbb{Q}$ es galoisiana (es normal pues es un cuerpo de descomposición, y es separable pues $\text{char}(\mathbb{Q}) = 0$).
En esta situación, sabemos que vale la igualdad $\boxed{|\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]}$.
En los ejercicios que siguen, la idea siempre será obtener información sobre el grupo de Galois de $E/\mathbb{Q}$ (si es posible, caracterizarlo completamente, pero a veces nos será suficiente con menos que eso) y luego, usando el teorema de Galois, deducir cosas sobre los cuerpos intermedios de la extensión $E/\mathbb{Q}$.

Ejemplo 1.
Sea E un cuerpo de descomposición del polinomio $X^4 + 3$ sobre $\mathbb{Q}$.

a) Caracterizar $\text{Gal}(E/\mathbb{Q})$.

b) Hallar todas las subextensiones normales de grado 4 de $E/\mathbb{Q}$ (es decir, todos los cuerpos intermedios F tales que $F/\mathbb{Q}$ es normal y $[F : \mathbb{Q}] = 4$).

En primera instancia haremos lo que veníamos haciendo en las prácticas anteriores: obtener un sistema de generadores de $E/\mathbb{Q}$ y usarlo para calcular el grado de la extensión. Esto es útil porque así ya sabremos el orden del grupo de Galois que debemos caracterizar.
Sea $\alpha \in \mathbb{C}$ una raíz cuarta de -3. Es fácil probar que entonces $E = \mathbb{Q}(\alpha, i)$. Tenemos la siguiente situación (notar que f es irreducible sobre $\mathbb{Q}$ por el criterio de Eisenstein con el primo $p = 3$, y por eso $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$):



Para determinar $[E : \mathbb{Q}]$ podemos intentar calcular $[E : \mathbb{Q}(\alpha)]$ o bien $[E : \mathbb{Q}(i)]$.
Sabemos que $[E : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(i) : \mathbb{Q}] = 2$. Para decidir si es 1 o 2, bastará con saber si i está o no en $\mathbb{Q}(\alpha)$. Esto es lo mismo que ver si existen a, b, c, d racionales tales que

$$(a + b\alpha + c\alpha^2 + d\alpha^3)^2 = -1.$$

Si desarrollamos el cuadrado e igualamos coeficientes, nos queda un sistema de cuatro ecuaciones con cuatro incógnitas, que no es muy complicado ver que no tiene soluciones racionales, aunque no es para nada divertido.
Veamos en cambio la otra opción, que es calcular $[E : \mathbb{Q}(i)]$. Si pudiésemos probar que $X^4 + 3$ es irreducible sobre $\mathbb{Q}(i)$, entonces la extensión tiene grado 4, pues se obtiene agregándole a $\mathbb{Q}(i)$ una raíz de dicho polinomio. Como $\mathbb{Q}(i)$ es el cuerpo de fracciones del DFU $\mathbb{Z}[i]$, podemos intentar aplicar el criterio de Eisenstein. Y efectivamente funciona, pues el 3 es un primo de $\mathbb{Z}$ congruente a 3 módulo 4 y entonces sigue siendo primo en $\mathbb{Z}[i]$.
De este modo, sin hacer cuentas conseguimos probar que $[E : \mathbb{Q}] = 8$, y por lo tanto el grupo de Galois de la extensión también tiene orden 8.
El siguiente paso es entender cuáles son los morfismos de $\mathrm{Gal}(E/\mathbb{Q})$. Sabemos que todo morfismo $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ queda determinado por los valores que toma sobre los generadores α e i.
Para el valor de $\sigma(\alpha)$ hay 4 posibilidades (las 4 raíces de su minimal): $\alpha, -\alpha, \alpha i, -\alpha i$.
Para el valor de $\sigma(i)$ hay 2 posibilidades (las 2 raíces de su minimal): $i, -i$.
Esto nos indicaría que hay a lo sumo $4 \cdot 2 = 8$ posibles morfismos. Pero nosotros ya sabíamos que $|\mathrm{Gal}(E/\mathbb{Q})| = 8$. Por lo tanto, las 8 combinaciones posibles de los valores que mostramos antes son todas válidas (es decir, determinan morfismos bien definidos).
Ya tenemos caracterizados los 8 morfismos del grupo de Galois. Para lo que sigue, es conveniente tener una buena manera de nombrar a estos 8 morfismos, que nos permita escribir de manera compacta y cómoda las relaciones que existen entre ellos.
Usaremos la siguiente notación: dados $0 \leq j \leq 3$ y $0 \leq k \leq 1$, llamaremos σ_{jk} al morfismo definido por

$$\sigma_{jk} : \begin{cases} \alpha \mapsto \alpha \cdot i^j \\ i \mapsto (-1)^k \cdot i \end{cases}$$

Con esta notación, tenemos por ejemplo que σ_{00} es la identidad y que $\{\sigma_{j0}\}_j$ y $\{\sigma_{0k}\}_k$ son los subgrupos de $\mathrm{Gal}(E/\mathbb{Q})$ que dejan fijos a i y a α respectivamente.
A continuación, para resolver la parte a), deberíamos ver si $\mathrm{Gal}(E/\mathbb{Q})$ es isomorfo a algún grupo que conozcamos. Para hacer esto, suele ser útil encontrar primero un sistema de generadores del grupo que sea pequeño, pues entonces, viendo qué relaciones hay entre estos generadores posiblemente podamos terminar de caracterizar al grupo.
En nuestro caso, vamos a considerar $\sigma := \sigma_{10}$ y $\tau := \sigma_{01}$. Estos dos elementos generan todo el grupo pues vale la igualdad $\sigma_{jk} = \sigma^j \tau^k$ (verificar!).
Veamos qué orden tiene σ aplicándolo repetidas veces sobre los generadores:

$$\alpha \xrightarrow{\sigma} \alpha \cdot i \xrightarrow{\sigma} \sigma(\alpha) \cdot \sigma(i) = \alpha \cdot i^2 \xrightarrow{\sigma} \alpha \cdot i^3 \xrightarrow{\sigma} \alpha$$

$$i \xrightarrow{\sigma} i \xrightarrow{\sigma} i \xrightarrow{\sigma} i \xrightarrow{\sigma} i$$

Entonces $\mathrm{ord}(\sigma) = 4$. Análogamente se ve que $\mathrm{ord}(\tau) = 2$.
Recordemos que el grupo diedral $\mathbb{D}_4$ se puede presentar como $\langle r, s \mid r^4 = s^2 = (rs)^2 = 1 \rangle$. Si probamos que nuestros elementos σ y τ satisfacen además que $(\sigma\tau)^2 = \mathrm{id}_E$, podremos concluir que $\mathrm{Gal}(E/\mathbb{Q})$ recibe un epimorfismo de $\mathbb{D}_4$ (que manda r a σ y s a τ), y como ambos grupos tienen orden 8, resultarán ser isomorfos.
En efecto:

$$\alpha \xrightarrow{\tau} \alpha \xrightarrow{\sigma} \alpha \cdot i \xrightarrow{\tau} -\alpha \cdot i \xrightarrow{\sigma} -\alpha i^2 = \alpha$$

$$i \xrightarrow{\tau} -i \xrightarrow{\sigma} i \xrightarrow{\tau} -i \xrightarrow{\sigma} i$$

Queda así demostrado que $\boxed{\mathrm{Gal}(E/\mathbb{Q}) \simeq \mathbb{D}_4}$.

Otra manera útil de pensar estos ejercicios es usando que el grupo de Galois de un polinomio de grado n siempre se puede pensar como un subgrupo de $\mathbb{S}_n$ etiquetando las n raíces del polinomio con los números del 1 al n y viendo cómo cada uno de los morfismos permuta estas raíces. En nuestro caso, si etiquetamos $1, 2, 3, 4$ a las raíces $\alpha, \alpha \cdot i, -\alpha, -\alpha \cdot i$, respectivamente, podemos observar que el morfismo que llamamos σ se corresponde con el 4-ciclo (1234) y el morfismo que llamamos τ se corresponde con la trasposición (24). Representando esto gráficamente, se vuelve evidente que el grupo que buscamos tiene que ser $\mathbb{D}_4$.
Pasamos ahora a la parte b). El teorema de correspondencia de Galois nos dice que las subextensiones normales de $E/\mathbb{Q}$ de grado 4 están en correspondencia con los subgrupos normales de $\mathrm{Gal}(E/\mathbb{Q})$ de orden $\frac{8}{4} = 2$. Nos preguntamos entonces: ¿cuántos subgrupos normales de orden 2 tiene $\mathbb{D}_4$?
Un subgrupo de orden 2 es de la forma $\{1, x\}$ con $\mathrm{ord}(x) = 2$. Como para cualquier $y \in \mathbb{D}_4$ es $y \cdot 1 \cdot y^{-1} = 1$, el subgrupo será normal si y sólo si $y \cdot x \cdot y^{-1} = x$ para todo $y \in \mathbb{D}_4$; en otras palabras, si x *conmuta* con todos los elementos del grupo. Usando que un elemento conmuta con todos los elementos del grupo si y sólo si conmuta con los generadores r y s, es fácil ver que el centro de $\mathbb{D}_4$ es $H = \{1, r^2\}$. Luego existe un único subgrupo normal de orden 2 en $\mathbb{D}_4$, que es H; y por lo tanto, existe una única subextensión normal de grado 4 en $E/\mathbb{Q}$, que es E^H.
Ahora deberíamos determinar explícitamente quién es esta subextensión. Una posibilidad (que no puede fallar!) es ver qué morfismos de $\mathrm{Gal}(E/\mathbb{Q})$ se corresponden con el subgrupo H de $\mathbb{D}_4$, y calcular el subcuerpo fijo por estos morfismos, lo cual es, en última instancia, un problema de cálculo de autovectores.
Pero podemos hacer algo más inteligente. Como ya sabemos que hay una única subextensión normal de grado 4, si encontramos alguna «a ojo», esa tiene que ser la que estábamos buscando. Y en este caso es fácil hacer eso: basta notar que α^2 es una raíz cuadrada de -3, y por lo tanto $F = \mathbb{Q}(\sqrt{-3}, i) = \mathbb{Q}(\sqrt{3}, i) \subseteq E$. Esta subextensión efectivamente tiene grado 4, y es normal por estar generada por elementos de grado 2.
Esto completa la resolución del ejercicio. ■

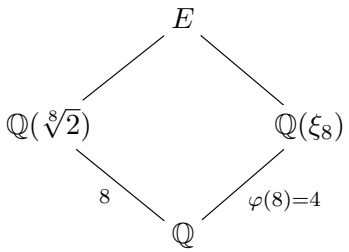
Ejemplo 2.

Sea E un cuerpo de descomposición del polinomio $X^8 - 2$ sobre $\mathbb{Q}$.

a) Calcular la cantidad de subextensiones de grado 8 de $E/\mathbb{Q}$.

b) Hallar un cuerpo F con $\mathbb{Q} \subseteq F \subseteq E$ tal que $\mathrm{Gal}(E/F) \simeq \mathbb{Z}_8$.

Claramente, $E = \mathbb{Q}(\sqrt[8]{2}, \xi_8)$, donde ξ_8 es una raíz octava primitiva de la unidad. Si queremos calcular el grado de la extensión manteniendo estos generadores, nos topamos con la situación



en la que los grados de las extensiones inferiores no son coprimos, y si bien $[E : \mathbb{Q}(\sqrt[8]{2})]$ no puede ser 1 porque $\mathbb{Q}(\sqrt[8]{2})$ está contenida en $\mathbb{R}$ y E no lo está, no está claro que el grado no pueda dar 2 o 3.

Aquí, el truco estará en notar que podemos tomar $\xi_8 = e^{\frac{2\pi i}{8}} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$. Con esta igualdad se puede probar fácilmente que $E = \mathbb{Q}(\sqrt[8]{2}, i)$, y por lo tanto que $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 16$ (**ejercicio**).
Ahora, caractericemos los morfismos de $\mathrm{Gal}(E/\mathbb{Q})$. De manera similar a lo hecho en el ejemplo anterior, dados $0 \leq j \leq 7$ y $0 \leq k \leq 1$, llamaremos σ_{jk} al morfismo definido por

$$\sigma_{jk} : \begin{cases} \sqrt[8]{2} & \mapsto \sqrt[8]{2} \cdot \xi_8^j \\ i & \mapsto (-1)^k \cdot i \end{cases}$$

Observemos que esta vez el ejercicio no nos pide caracterizar completamente al grupo, así que existe la posibilidad de que no sea necesario hacerlo. (Al que lo quiera intentar le advierto que esta vez no da un grupo tan conocido como en el caso anterior, aunque sí se puede escribir como un producto semidirecto entre $\mathbb{Z}_8$ y $\mathbb{Z}_2$.)
La parte a) nos pide contar la cantidad de subextensiones de grado 8, lo cual, por el teorema de Galois, equivale a contar la cantidad de subgrupos de orden $\frac{16}{8} = 2$ de $\mathrm{Gal}(E/\mathbb{Q})$. Como todo subgrupo de orden 2 es cíclico, bastará con contar cuántos ***elementos*** de orden 2 hay en $\mathrm{Gal}(E/\mathbb{Q})$. Y como conocemos cuáles son los 16 morfismos de $\mathrm{Gal}(E/\mathbb{Q})$, esta cuenta la vamos a poder hacer aunque no sepamos exactamente quién es el grupo.
Hay un obstáculo, y es que cuando queramos calcular $\sigma_{jk}^2(\sqrt[8]{2})$ (que es algo que vamos a necesitar hacer, para saber si σ_{jk}^2 es la identidad o no) vamos a necesitar saber cuánto es $\sigma_{jk}(\xi_8)$. Hagamos primero esta cuenta, usando que $\xi_8 = \frac{\sqrt{2}}{2}(1+i) = \frac{\sqrt[8]{2}^4}{2}(1+i)$:

$$\sigma_{jk}(\xi_8) = \frac{\sigma_{jk}(\sqrt[8]{2})^4}{2}(1 + \sigma_{jk}(i)) = \begin{cases} \frac{\sqrt{2}}{2}(1+i) = \xi_8 & \text{si } j \text{ es par y } k = 0 \\ \frac{-\sqrt{2}}{2}(1+i) = \xi_8^5 & \text{si } j \text{ es impar y } k = 0 \\ \frac{\sqrt{2}}{2}(1-i) = \xi_8^7 & \text{si } j \text{ es par y } k = 1 \\ \frac{-\sqrt{2}}{2}(1-i) = \xi_8^3 & \text{si } j \text{ es impar y } k = 1 \end{cases}$$

Ahora que tenemos esto, podemos determinar para cuáles pares (j, k) se tiene que el morfismo σ_{jk} tiene orden 2. Algo bueno y que es fácil de ver es que cualesquiera sean j y k se tiene $\sigma_{jk}^2(i) = (-1)^{2k} i = i$, de modo que sólo tenemos que preocuparnos por calcular $\sigma_{jk}^2(\sqrt[8]{2})$.
Tenemos $\sigma_{jk}^2(\sqrt[8]{2}) = \sigma_{jk}(\sigma_{jk}(\sqrt[8]{2})) = \sigma_{jk}(\sqrt[8]{2} \cdot \xi_8^j) = \sigma_{jk}(\sqrt[8]{2}) \cdot \sigma_{jk}(\xi_8)^j = \sqrt[8]{2} \cdot \xi_8^j \cdot \sigma_{jk}(\xi_8)^j$. Entonces:

$$\sigma_{jk}^2(\sqrt[8]{2}) = \begin{cases} \sqrt[8]{2} \cdot \xi_8^{2j} & \text{si } j \text{ es par y } k = 0 \\ \sqrt[8]{2} \cdot \xi_8^{6j} & \text{si } j \text{ es impar y } k = 0 \\ \sqrt[8]{2} \cdot \xi_8^{8j} = \sqrt[8]{2} & \text{si } j \text{ es par y } k = 1 \\ \sqrt[8]{2} \cdot \xi_8^{4j} & \text{si } j \text{ es impar y } k = 1 \end{cases}$$

Nosotros queremos que sea $\sigma_{jk}^2(\sqrt[8]{2}) = \sqrt[8]{2}$. En la primera rama, esto pasa si y sólo si $j = 0$ o $j = 4$; en la segunda rama, esto no pasa nunca porque $6j$ no puede ser múltiplo de 8 si j es impar; en la tercera rama, esto se cumple en todos los casos; y en la cuarta rama, no hay ningún caso que sirva porque $4j$ no es múltiplo de 8 si j es impar.
Hemos encontrado así que hay seis parejas (j, k) tales que $\sigma_{jk}^2 = \mathrm{id}_E$; de estas, debemos quitar la pareja $(0, 0)$ pues corresponde al morfismo identidad, que tiene orden 1 en vez de orden 2. Concluimos que $E/\mathbb{Q}$ tiene 5 subextensiones de grado 8.
Pasamos a la parte b). El teorema de correspondencia de Galois nos dice que un tal cuerpo F debe ser de la forma E^H con $H \leq \mathrm{Gal}(E/\mathbb{Q})$, y de hecho, es $\mathrm{Gal}(E/F) = H$ (a esto también se lo llama teorema de Artin). Entonces, lo que podríamos hacer es encontrar un subgrupo de $\mathrm{Gal}(E/\mathbb{Q})$ que sea isomorfo a $\mathbb{Z}_8$ (o lo que es lo mismo, encontrar un elemento de $\mathrm{Gal}(E/\mathbb{Q})$ que tenga orden 8) y luego calcular el cuerpo fijo por este subgrupo.

El candidato natural parecería ser $\sigma := \sigma_{10}$. De las cuentas que ya hicimos se deduce que $\sigma^2 = \sigma_{60}$, $\sigma^4 = \sigma_{60}^2 = \sigma_{40}$ y $\sigma^8 = \sigma_{40}^2 = \mathrm{id}_E$. Luego efectivamente $\mathrm{ord}(\sigma) = 8$.
Ahora, si $H = \langle\sigma\rangle$, es $H \simeq \mathbb{Z}_8$, y además vale que $\alpha \in E^H \iff \sigma(\alpha) = \alpha$. Así que alcanzará con ver los elementos que quedan fijos por σ. Una vez más, esto es hacer una cuenta de álgebra lineal o bien ser más astuto y notar que por definición es $\sigma(i) = i$. Como $[E : E^H][E^H : \mathbb{Q}] = [E : \mathbb{Q}] = 16$ y el primer factor sabemos que da 8 pues tiene grupo de Galois $\mathbb{Z}_8$, resulta $[E^H : \mathbb{Q}] = 2$, y como ya sabíamos que $\mathbb{Q}(i) \subseteq E^H$, vale la igualdad.
En definitiva, podemos tomar $\boxed{F = \mathbb{Q}(i)}$. ■

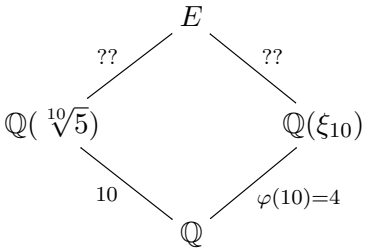
Ejemplo 3.

Sea E un cuerpo de descomposición del polinomio $X^{10} - 5$ sobre $\mathbb{Q}$.

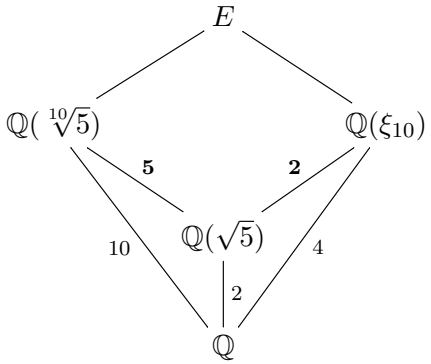
a) Calcular $[E : \mathbb{Q}]$. (*Sugerencia*: puede ser útil el hecho de que $\sqrt{5} \in \mathbb{Q}(\xi_5)$, que suele aparecer en un ejercicio de la primera guía.)

b) Calcular la cantidad de subextensiones de grado 5 de $E/\mathbb{Q}$.

Como siempre, va a ser $E = \mathbb{Q}(\sqrt[10]{5}, \xi_{10})$. Le hacemos caso a la sugerencia y vemos que $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\xi_5) \subseteq \mathbb{Q}(\xi_{10})$. Así que en vez de dibujar este diagrama



dibujamos este otro



y como 5 y 2 son coprimos, deducimos que $\boxed{[E : \mathbb{Q}] = 20}$, lo cual resuelve la parte a). Esto nos dice además que $|\mathrm{Gal}(E/\mathbb{Q})| = 20$.
Para resolver la parte b), por el teorema de correspondencia de Galois basta contar la cantidad de subgrupos de orden $\frac{20}{5} = 4$ de $\mathrm{Gal}(E/\mathbb{Q})$. A diferencia de lo que pasaba en el ejemplo anterior, no podemos traducir muy rápidamente esto a un problema de contar elementos, pues un subgrupo de orden 4 puede ser isomorfo a $\mathbb{Z}_4$ o a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Podríamos intentar ver si $\mathrm{Gal}(E/\mathbb{Q})$ es un grupo conocido, pero otra vez el hecho de que el ejercicio no nos pida hacerlo puede hacernos sospechar que quizás no sea tan fácil.
Otra opción es empezar a recordar teoremas de teoría de grupos que vimos en Álgebra 2 hasta que encontremos alguno que nos ayude. En este caso, nos resultará muy útil recordar el

Teorema de Sylow, pues los subgrupos de orden 4 de un grupo de orden 20 son precisamente sus 2-Sylows.
Si n_2 es la cantidad de 2-Sylows de $\mathrm{Gal}(E/\mathbb{Q})$, sabemos que $n_2 \mid 5$ y $n_2 \equiv 1 \pmod 2$, de modo que n_2 sólo puede ser 1 o 5.
El teorema de Sylow nos dice además que el grupo actúa transitivamente por conjugación en la familia de sus 2-Sylows (en otras palabras, dos 2-Sylows cualesquiera son conjugados). De esto se deduce que, si existe algún 2-Sylow que no sea normal, entonces necesariamente $n_2 > 1$. Usamos teoría de Galois para traducir esto a nuestro problema: si encontramos una subextensión de grado 5 que no sea normal, entonces necesariamente $n_2 > 1$ (y por lo tanto $n_2 = 5$, que era la única otra posibilidad). Pero es muy fácil probar que $\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}$ es una subextensión de grado 5 que no es normal (por ejemplo porque $X^5 - 5$, que es el minimal de $\sqrt[5]{5}$, tiene raíces no reales). Concluimos entonces que hay exactamente 5 subextensiones de grado 5. La solución está completa. ■