Extensiones de morfismos y algunas aplicaciones

Mariano Negri

Proposición 1: Sea $\sigma : F_1/K \to F_2/K$ morfismo de extensiones. Entonces, si $f \in F_1[x]$ y $\alpha \in F_1$ raíz de f, entonces $\sigma(\alpha)$ es raíz de f^σ.
Dem: Recordemos que si $f(x) = \sum_{i=0}^n a_i x^i$, entonces $f^\sigma(x) = \sum_{i=0}^n \sigma(a_i)x^i$. Por lo tanto, $f^\sigma(\sigma(\alpha)) = \sum_{i=0}^n \sigma(a_i)\sigma(\alpha)^i = \sigma(\sum_{i=0}^n a_i\alpha^i) = \sigma(0) = 0$ □

Corolario: Sea $\sigma : F_1/K \to F_2/K$ morfismo de extensiones. Entonces, si $f \in K[x]$ y $\alpha \in F_1$ raíz de f, entonces $\sigma(\alpha)$ es raíz de f. En particular, si $\sigma : E/K \to E/K$ automorfismo de extensiones entonces $\sigma(\alpha)$ es raíz de $m(\alpha, K)$.
Dem: Es solo observar que en este caso $f = f^\sigma$ porque $\sigma|_K = Id$ y luego usar la proposición anterior. □

Proposición 2: *(¿Como extender morfismos?)* Sean F_1/K, F_2/K dos extensiones de K cuerpo, sean α y β algebraicos sobre F_1 y F_2 respectivamente tales que $[F_1[\alpha] : F_1] = [F_2[\alpha] : F_2]$. Si $\sigma : F_1/K \to F_2/K$ es un morfismo de extensiones, entonces: existe $\hat{\sigma} : F_1[\alpha]/K \to F_2[\beta]/K$ isomorfismo de extensiones tal que $\hat{\sigma}|_{F_1} = \sigma$ y $\hat{\sigma}(\alpha) = \beta$ si y solo si $m(\alpha, F_1)^\sigma = m(\beta, F_2)$
Dem: $\Rightarrow$) Notemos que β es raíz de $m(\alpha, F_1)^{\hat{\sigma}}$ porque α es raíz de $m(\alpha, F_1)$, luego la proposición 1 nos dice que $\hat{\sigma}(\alpha) = \beta$ es raíz de $m(\alpha, F_1)^{\hat{\sigma}}$. Pero además, notemos que $m(\alpha, F_1)^{\hat{\sigma}} = m(\alpha, F_1)^\sigma$ porque $\hat{\sigma}|_{F_1} = \sigma$. Esto nos dice que $m(\beta, F_2)|m(\alpha, F_1)^\sigma$. Pero aparte tienen el mismo grado (porque $[F_1(\alpha) : F_1] = [F_2(\beta) : F_2]$ y $gr(m(\alpha, F_1)) = gr(m(\alpha, F_1))^\sigma)$ y son mónicos, luego $m(\alpha, F_1)^\sigma = m(\beta, F_2)$.
$\Leftarrow$) Consideremos el siguiente morfismo de anillos $f : F_1[x] \to F_2[\beta]$:

$$\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \sigma(a_i)\beta^i.$$

Notemos que $m(\alpha, F_1) \in Ker(f)$, y como es irreducible resulta que el ideal $\langle m(\alpha, F_1)\rangle$ es maximal y por lo tanto $kerf = \langle m(\alpha, F_1)\rangle$. Por primer teo de iso, esto induce un isomorfismo de cuerpos $\overline{\sigma} : F_1[x]/\langle m(\alpha, F_1)\rangle \to F_2[\beta]$ pero $F_1[x]/\langle m(\alpha, F_1) \cong F_1[\alpha]$. Así que tenemos un isomorfismo de cuerpos $\overline{\sigma} : F_1[\alpha] \to F_2[\beta]$ y queda como ejercicio chequear que $\overline{\sigma}|_{F_1} = \sigma$ y $\overline{\sigma}(\alpha) = \beta$. □

Aplicación: Calcular los automorfismos de extensiones de $\mathbb{Q}[\sqrt[3]{2}, \xi_3]$ sobre $\mathbb{Q}$.
Solución: Pronto veremos que $\mathbb{Q}[\sqrt[3]{2}, \xi_3]$ es una extensión Galois sobre $\mathbb{Q}$. En esos casos hay exactamente $[\mathbb{Q}[\sqrt[3]{2}, \xi_3] : \mathbb{Q}] = 6$ automorfismos. Por el momento veamos a mano que a lo sumo hay seis.

Una base explicita de $\mathbb{Q}[\sqrt[3]{2}]$ es $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Una base explicita de $\mathbb{Q}[\xi_3]$ es $\{1, \xi_3\}$. Entonces como la extensión es de dimensión 6, una base de $\mathbb{Q}[\sqrt[3]{2}, \xi_3]$ será solo multiplicar los elementos de las dos bases: $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \xi_3, \sqrt[3]{2}\xi_3, \sqrt[3]{4}\xi_3\}$.

Notemos que si $\sigma : \mathbb{Q}[\sqrt[3]{2}, \xi_3]/\mathbb{Q} \to \mathbb{Q}[\sqrt[3]{2}, \xi_3]/\mathbb{Q}$ es automorfismo sabemos que manda raices de $m(\sqrt[3]{2}, \mathbb{Q})$ en raices de $m(\sqrt[3]{2}, \mathbb{Q})$. Por lo tanto solo hay tres posibilidades para asignarle a $\sqrt[3]{2}$ que son $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3^j$ con $0 \leq j \leq 2$. Por otro lado, lo mismo pasa con $m(\xi_3, \mathbb{Q})$ así que a priori hay tres posibilidades para $\sigma(\xi_3)$, que serían ξ_3, ξ_3^2. Ahora, notemos que al asignarle un valor a $\sigma(\xi_3)$ y un valor a $\sigma(\sqrt[3]{2})$, ya queda completamente determinado el morfismo en toda la base que dimos! y como en particular el morfismo es una t.l., ya queda univocamente determinado. Luego hay a lo sumo $3.2 = 6$ posibilidades.

Veamos que esas son todas posibilidades viables.

Caractericemos primero los automorfismos de $\mathbb{Q}[\xi_3]/\mathbb{Q}$, que son, como vimos de forma indirecta, a lo sumo 2. Tenemos a la identidad, que llamaremos f_0, y luego tenemos f_1 morfismo que extiende a la identidad de $\mathbb{Q}$ y manda $\xi_3 \mapsto \xi_3^2$ que es un isomorfismo bien definido por la proposición 2 (ya $m(\xi_3, \mathbb{Q})^{id|_{\mathbb{Q}}} = m(\xi_3^2, \mathbb{Q}) = x^3 - 1$). Ahora, gracias a la proposición 2 nuevamente podemos chequear fácilmente que las asignaciones $\sigma_{j,i}(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3^j$ $0 \leq j \leq 2$, $0 \leq i \leq 1$ nos dan isomorfismos de extensiones $\mathbb{Q}[\xi_3][\sqrt[3]{2}] \to \mathbb{Q}[\xi_3][\sqrt[3]{2}]$ tales que $\sigma_{j,i}|_{\mathbb{Q}[\xi_3]} = f_i$ y $\sigma_{j,i}(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3^j$ pues $m(\sqrt[3]{2}\xi_3^j, \mathbb{Q}[\xi_3]) = x^3 - 2$ y $m(\sqrt[3]{2}\xi_3^j, \mathbb{Q}[\xi_3])^{f_i} = x^3 - 2$.

O sea, acabamos de ver que los automorfismos son:

- $\sigma_{0,0}(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_{0,0}(\xi_3) = \xi_3$
- $\sigma_{1,0}(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3$, $\sigma_{1,0}(\xi_3) = \xi_3$
- $\sigma_{2,0}(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3^2$, $\sigma_{2,0}(\xi_3) = \xi_3$
- $\sigma_{0,1}(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_{0,1}(\xi_3) = \xi_3^2$
- $\sigma_{1,1}(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3$, $\sigma_{1,1}(\xi_3) = \xi_3^2$
- $\sigma_{2,1}(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3^2$, $\sigma_{2,1}(\xi_3) = \xi_3^2$

$\square$

Aplicación: Veamos que $[\mathbb{Q}[\sqrt[3]{3}, \sqrt[3]{2}] : \mathbb{Q}] = 9$.
Primera forma:
Paso 1: No hay dudas de que $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, la pregunta ahora es ¿Es verdad que $[\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{3}] : \mathbb{Q}[\sqrt[3]{2}]] = 3$?. Si esto es así, ya estamos. Tratemos de descartar que esta sea una extensión cuadrática. Sabemos que $x^3 - 3$ anula a $\sqrt[3]{3}$. Si la extensión fuese cuadrática entonces $f := m(\sqrt[3]{3}, \mathbb{Q}[\sqrt[3]{2}])$ tiene grado 2 y divide a $x^3 - 2$. O sea $x^3 - 2 = (x - a)f(x) \in \mathbb{Q}[\sqrt[3]{2}][x]$. Pero las raices de $x^3 - 3$ están en $\mathbb{C} \setminus \mathbb{R}$, salvo $\sqrt[3]{3}$, o sea que la raíz $a = \sqrt[3]{3}$. Pero entonces $\sqrt[3]{3} \in \mathbb{Q}[\sqrt[3]{2}]$, es decir $[\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{3}] : \mathbb{Q}[\sqrt[3]{2}]] = 1 \neq 2$. Concluimos que las únicas dos opciones son $[\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{3}] : \mathbb{Q}[\sqrt[3]{2}]] = 1$ ó 3.
Paso 2: Para llegar a un absurdo supongamos que $[\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{3}] : \mathbb{Q}[\sqrt[3]{2}]] = 1$. En cuyo caso $\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{3}] = \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{3}]$.
Paso 3: Consideremos $\mathbb{Q}[\sqrt[3]{2}, \xi_3]/\mathbb{Q}$ y miremos los automorfismos de la extensión. Nos concetraremos en uno de ellos:

$\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\xi_3 \quad \sigma : \xi_3 \mapsto \xi_3$

Paso 4: Como $\sqrt[3]{3}$ es obviamente raíz de $m(\sqrt[3]{3}, \mathbb{Q})$, resulta que $\sigma(\sqrt[3]{3})$ también es raíz de $m(\sqrt[3]{3}, \mathbb{Q})$. Como $\sqrt[3]{3} \in \mathbb{Q}[\sqrt[3]{2}]$ Tenemos que $\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ con $a, b, c \in \mathbb{Q}$, luego se tiene que $\sigma(\sqrt[3]{3}) = a + b\sqrt[3]{2}\xi_3 + c\sqrt[3]{4}\xi_3^2$, y debe ser raíz del minimal.

Paso 5: Notemos que las raices de x^3-3 son $\sqrt[3]{3}$, $\sqrt[3]{3}\xi_3$ y $\sqrt[3]{3}\xi_3^2$.

Queremos ver que $a+b\sqrt[3]{2}\xi_3+c\sqrt[3]{4}\xi_3^2$ no puede ser ninguna de ellas para llegar a un absurdo.

- Si $a+b\sqrt[3]{2}\xi_3+c\sqrt[3]{4}\xi_3^2=\sqrt[3]{3}$ entonces reordenando un poco la igualdad obtenemos $b\sqrt[3]{2}\xi_3+c\sqrt[3]{4}\xi_3^2=\sqrt[3]{3}-a$, pero del lado izquierdo tenemos que la parte imaginaria es $\frac{\sqrt{3}}{2}(b\sqrt[3]{2}-c\sqrt[3]{4})=\frac{\sqrt{3}}{2}\sqrt[3]{2}(b-c\sqrt[3]{2})$ que solo puede ser 0 si $b=c=0$. Pero entonces $a=\sqrt[3]{3}$, absurdo!

- Si $a+b\sqrt[3]{2}\xi_3+c\sqrt[3]{4}\xi_3^2=\sqrt[3]{3}\xi_3$ multiplicamos por ξ_3^2 obtenemos

$$a\xi_3^2+b\sqrt[3]{2}+c\sqrt[3]{4}\xi_3=\sqrt[3]{3}$$

  O sea $a\xi_3^2+c\sqrt[3]{4}\xi_3=\sqrt[3]{3}+b\sqrt[3]{2}$. Pero el lado izquierdo de la igualdad tiene parte imaginaria $\frac{\sqrt{3}}{2}(-a+c\sqrt[3]{4})$ que solo puede ser 0 si $a=c=0$ pero esto rapidamente nos da un absurdo porque diria que $b=-\sqrt[3]{3/2}$.

- si $a+b\sqrt[3]{2}\xi_3+c\sqrt[3]{4}\xi_3^2=\sqrt[3]{3}\xi_3^2$ multiplicamos por ξ_3 y obtenemos

$$a\xi_3+b\sqrt[3]{2}\xi_3^2+c\sqrt[3]{4}=\sqrt[3]{3}$$

  O sea $a\xi_3+b\sqrt[3]{2}\xi_3^2=\sqrt[3]{3}-c\sqrt[3]{4}$. Pero el lado izquierdo de la igualdad tiene parte imaginaria $\frac{\sqrt{3}}{2}(a-b\sqrt[3]{2})$ que solo puede ser 0 si $a=b=0$, lo que nos daria que $c=-\sqrt[3]{3/4}$, absurdo.

Concluimos que $a+b\sqrt[3]{2}\xi_3+c\sqrt[3]{4}\xi_3^2$ no es raíz de $m(\sqrt[3]{2},\mathbb{Q})$, absurdo!

$\square$

Segunda forma: *(mirar raices del minimal de $\sqrt[3]{3}+\sqrt[3]{2}$)*

Suponiendo como antes que $\mathbb{Q}[\sqrt[3]{2}]=\mathbb{Q}[\sqrt[3]{3}]$, ya caracterizamos a todos los automorfismos de $\mathbb{Q}[\sqrt[3]{2},\xi_3]$, pero además al ser morfismo de cuerpos, como tenemos que $\sigma_{i,j}(\sqrt[3]{3})^3=3$, debemos tener que $\sigma_{i,j}(\sqrt[3]{3})=\sqrt[3]{3}\xi_3^{\chi(i)}$, donde χ es solo una permutación de $\{0,1,2\}$

De esta manera, tenemos:

$$\sigma_{i,j}(\sqrt[3]{2}+\sqrt[3]{3})=\sigma_{i,j}(\sqrt[3]{2})+\sigma_{i,j}(\sqrt[3]{3})=\sqrt[3]{2}\xi_3^i+\sqrt[3]{3}\xi_3^{\chi(i)}$$

Entonces $\{\sqrt[3]{2}+\sqrt[3]{3}\xi_3^{\chi(0)},\sqrt[3]{2}\xi_3+\sqrt[3]{3}\xi_3^{\chi(1)},\sqrt[3]{2}\xi_3^2+\sqrt[3]{3}\xi_3^{\chi(2)}\}$ son 3 raices *distintas* del polinomio minimal $m(\sqrt[3]{3}+\sqrt[3]{2},\mathbb{Q})$. O sea, estas deben ser todas las raices del minimal porque a lo sumo podría tener grado 3 según nuestra suposición. Ahora, si las multiplicamos a las tres, por el corolario de la proposición 1 deberiamos obtener un número en $\mathbb{Q}$ (sería el coeficiente independiente del minimal módulo el signo). Veamos que no es así. Primero que nada, como $\sqrt[3]{3}+\sqrt[3]{2}$ es raíz de $m(\sqrt[3]{3}+\sqrt[3]{2},\mathbb{Q})$ las raices son $\{\sqrt[3]{2}+\sqrt[3]{3},\sqrt[3]{2}\xi_3+\sqrt[3]{3}\xi_3^{\chi(1)},\sqrt[3]{2}\xi_3^2+\sqrt[3]{3}\xi_3^{\chi(2)}\}$ donde ahora miramos $\chi:\{1,2\}\to\{0,1,2\}$ función inyectiva , luego:

$$(\sqrt[3]{2}+\sqrt[3]{3})(\sqrt[3]{2}\xi_3+\sqrt[3]{3}\xi_3^{\chi(1)})(\sqrt[3]{2}\xi_3^2+\sqrt[3]{3}\xi_3^{\chi(2)})=$$
$$=(\sqrt[3]{4}\xi_3+(\xi_3+\xi_3^{\chi(1)})\sqrt[3]{6}+\sqrt[3]{9}\xi_3^{\chi(1)})(\sqrt[3]{2}\xi_3^2+\sqrt[3]{3}\xi_3^{\chi(2)})=$$

$$= 2 + (\xi_3^{\chi(2)+1} + \xi_3^2 + \xi_3^{\chi(1)+2})\sqrt[3]{12} + (\xi_3^{\chi(2)+1} + \xi_3^{\chi(1)+\chi(2)} + \xi_3^{\chi(1)+2})\sqrt[3]{18} + 3 =$$
$$= 5 + (\xi_3^{\chi(2)+1} + \xi_3^2 + \xi_3^{\chi(1)+2})\sqrt[3]{12} + (\xi_3^{\chi(2)+1} + \xi_3^{\chi(1)+2})\sqrt[3]{18}$$

Tenemos seis opciones, son todas muy parecidas. Ilustramos dos de ellas, el caso $\chi(1) = 1$, $\chi(2) = 2$ y el caso $\chi(1) = 2$, $\chi(2) = 1$.

- Si $\chi(1) = 1$, $\chi(2) = 2$ la expresión queda $5 + 2\sqrt[3]{18}$ que es claramente irracional.
- Si $\chi(1) = 2$, $\chi(2) = 1$ la expresión queda $5 + (\xi_3^2 + \xi_3^2 + \xi_3)\sqrt[3]{12} + (\xi_3^2 + \xi_3)\sqrt[3]{18}$ o lo que es lo mismo, $5 + (\xi_3^2 - 1)\sqrt[3]{12} - \sqrt[3]{18}$ y mirando solo la parte imaginaria de este número vemos que es distinta de 0 así que tampoco está en $\mathbb{Q}$.

Completar las restantes con argumentos análogos.
Llegamos a un absurdo, luego $[\mathbb{Q}[\sqrt[3]{3}, \sqrt[3]{2}] : \mathbb{Q}] = 9$

$\square$