

Álgebra 3
PRIMER PARCIAL
AXEL SIROTA

Ejercicio 1 ■ Primero recordemos el ejercicio 27 de la práctica 3 que dice:

$$\text{Gal}(K(t)/K) \simeq \text{PGL}_2(K)$$

Luego afirmo que en realidad $G = \langle \tau, \sigma, i \rangle = \text{Gal}(K(t)/K)$ de lo que el orden de G va a ser el orden de $\text{PGL}_2(K) = q^3 - q$.

En pos de eso, para un lado es claro que los tres generadores de G estan en $\text{Gal}(K(t)/K)$, luego $G \subseteq \text{Gal}(K(t)/K)$. Recíprocamente, notemos que si $f \in \text{Gal}(K(t)/K)$ entonces ya sabemos que $f(t) = \frac{at+b}{ct+d}$ donde $ac - bd \neq 0$; por lo tanto podemos representarlo como $f(t) = \frac{A}{Ct+D} + B$.

Luego, si notamos $\sigma_C(t) = Ct$, $t_B(t) = t + B$:

$$\begin{aligned} f(t) &= \sigma_C \left(\frac{A}{t+D} + B \right) \\ &= \sigma_C \circ \tau_D \left(\frac{A}{t} + B \right) \\ &= \sigma_C \circ \tau_D \circ -i (At + B) \\ &= \sigma_C \circ \tau_D \circ -i \circ \tau_B \circ \sigma_A(t) \end{aligned}$$

Para concluir, es claro que como $B \in K$ entonces $\tau_B = \tau^B$ y como $(8, 37) = 1$ y 37 es primo (acá usamos que $K = \mathbb{F}_{37}$) entonces existe $j_A, j_C \in \{1, \dots, 36\}$ tal que $A = 8^{j_A}$ y $C = 8^{j_C}$. Luego tenemos que para $f \in \text{Gal}(K(t)/K)$ existe $j_A, B, D, j_C \in \mathbb{F}_{37}$ tal que $f = \sigma^{j_C} \circ \tau^D \circ -i \circ \tau^B \circ \sigma^{j_A}$; concluimos que $G = \text{Gal}(K(t)/K)$ y como $|\text{Gal}(K(t)/K)| = q^3 - q$ ya sabemos el orden de G .

- Sean $p, q \in \mathbb{F}_{37}[t]$ coprimos y analicemos que tiene que pasar para que $\frac{f}{g} \in \mathbb{F}_{37}(t)^{\langle h \rangle}$ donde h van a ser σ, τ, i respectivamente.

Para σ notemos que si $u = t^{36}$ entonces para $f \in \mathbb{F}_{37}[t]$ vale:

$$\begin{aligned} \sigma(f(t^{36})) &= \sum_{i \in \text{sop}(f)} \sigma(a_i(t^{36})^i) \\ &= \sum_{i \in \text{sop}(f)} a_i(\sigma(t^{36}))^i \\ &= \sum_{i \in \text{sop}(f)} a_i \left(\underbrace{8^{36}}_{\cong 1 \pmod{37}} (t^{36}) \right)^i \\ &= f(t^{36}) \end{aligned}$$

Luego si $u = t^{36}$ vimos que $\mathbb{F}_{37}(t^{36}) \subset E^{\langle \sigma \rangle}$.

Por un lado, como $\text{ord}(\sigma) = 37$ pues $\text{mcd}(8, 37) = 1$ del teorema de Galois sabemos que $[E : E^{\langle \sigma \rangle}] = 36$; por el otro, como $f(x) = x^{36} - t^{36} \in \mathbb{F}_{37}(t^{36})[X]$ es mónico, irreducible (Einstein en t^{36} que es primo) y anula a t sabemos que $[\mathbb{F}_{37}(t^{36}) : \mathbb{F}_{37}(t)] = 36$. Luego, juntando todo, tenemos la torre $\mathbb{F}_{37}(t^{36}) \subseteq E^{\langle \sigma \rangle} \subseteq \mathbb{F}_{37}(t)$ donde:

$$[\mathbb{F}_{37}(t^{36}) : E^{\langle \sigma \rangle}] = \frac{[\mathbb{F}_{37}(t^{36}) : \mathbb{F}_{37}(t)]}{[\mathbb{F}_{37}(t) : E^{\langle \sigma \rangle}]} = 1$$

De lo que concluimos que $E^{\langle \sigma \rangle} = \mathbb{F}_{37}(t^{36})$.

Ahora vayamos a i ! Si $u = t^2 + t^{-2}$ entonces para $f \in \mathbb{F}_{37}[t]$ vale:

$$\begin{aligned}
i(f(t^2 + t^{-2})) &= \sum_{i \in \text{sop}(f)} i(a_i(t^2 + t^{-2})^i) \\
&= \sum_{i \in \text{sop}(f)} a_i(i(t^2 + t^{-2}))^i \\
&= \sum_{i \in \text{sop}(f)} a_i\left(i(t)^2 + \left(\frac{1}{i(t)}\right)^2\right)^i \\
&= \sum_{i \in \text{sop}(f)} a_i(t^{-2} + t^2)^i \\
&= f(t^2 + t^{-2})
\end{aligned}$$

Luego si $u = t^2 + t^{-2}$ vimos que $\mathbb{F}_{37}(u) \subset E^{(i)}$.

A continuación notemos que en realidad $i = i_1 \circ i_2$ donde $i_1(t) = -t$ y $i_2(t) = \frac{1}{t}$ cumplen las relaciones $i_1^2 = i_2^2 = Id$ y $i_1 \circ i_2 = i_2 \circ i_1$; por lo tanto $\langle i_1, i_2 \rangle = \langle i \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Luego $4 = \left| \text{Gal}(\mathbb{F}_{37}(t)/E^{(i)}) \right| = [E : E^{(i)}]$ por el teorema de Galois.

Por otro lado, si $p(x) = x^4 - x^2(t^2 + t^{-2}) + 1$ entonces $p \in \mathbb{F}_{37}(t^2 + t^{-2})[X]$ es mónico y $p(t) = 0$, por lo que $f(t, \mathbb{F}_{37}(t^2 + t^{-2})) \mid p$ con lo que $[\mathbb{F}_{37}(u) : \mathbb{F}_{37}(t)] \leq 4$.

Luego, juntando todo, tenemos la torre $\mathbb{F}_{37}(u) \subseteq E^{(i)} \subseteq \mathbb{F}_{37}(t)$ donde:

$$[\mathbb{F}_{37}(u) : E^{(i)}] = \frac{[\mathbb{F}_{37}(u) : \mathbb{F}_{37}(t)]}{[\mathbb{F}_{37}(t) : E^{(i)}]} = 1$$

Pues $1 \leq [\mathbb{F}_{37}(u) : E^{(i)}] \leq 1$, de lo que concluimos que $E^{(i)} = \mathbb{F}_{37}(t^2 + t^{-2})$.

Finalmente analicemos a τ , si $u = t^{37} - t$ entonces para $f \in \mathbb{F}_{37}[t]$ vale:

$$\begin{aligned}
\tau(f(t^{37} - t)) &= \sum_{i \in \text{sop}(f)} \tau(a_i(t^{37} - t)^i) \\
&= \sum_{i \in \text{sop}(f)} a_i(\tau(t^{37} - t))^i \\
&= \sum_{i \in \text{sop}(f)} a_i((t+1)^{37} - t - 1)^i \\
&= \sum_{i \in \text{sop}(f)} a_i(t^{37} + 1^{37} - t - 1)^i \\
&= f(t^{37} - t)
\end{aligned}$$

Luego si $u = t^{37} - t$ vimos que $\mathbb{F}_{37}(u) \subset E^{(\tau)}$.

Por un lado, como $\text{ord}(\tau) = 37$ del teorema de Galois sabemos que $[E : E^{(\tau)}] = 37$; por el otro, como $f(x) = x^{37} - x - t^{37} + t \in \mathbb{F}_{37}(t^{37} - t)[X]$ es mónico, irreducible (Eisenstein en $t^{37} - t$ que es primo) y anula a t sabemos que $[\mathbb{F}_{37}(t^{37} - t) : \mathbb{F}_{37}(t)] = 37$. Luego, juntando todo, tenemos la torre $\mathbb{F}_{37}(t^{37} - t) \subseteq E^{(\tau)} \subseteq \mathbb{F}_{37}(t)$ donde:

$$[\mathbb{F}_{37}(t^{37} - t) : E^{(\tau)}] = \frac{[\mathbb{F}_{37}(t^{37} - t) : \mathbb{F}_{37}(t)]}{[\mathbb{F}_{37}(t) : E^{(\tau)}]} = 1$$

De lo que concluimos que $E^{(\tau)} = \mathbb{F}_{37}(t^{37} - t)$.

Para concluir el punto notemos que ahora simplemente tenemos que juntar lo que fuimos descubriendo! Es decir es claro que:

$$\begin{aligned}
E^{\langle \sigma \rangle} &= \mathbb{F}_{37}(t^{36}) \\
E^{\langle \sigma, i \rangle} &= \mathbb{F}_{37}\left((t^2 - t^{-2})^{36}\right) \\
E^{\langle \sigma, \tau \rangle} &= \mathbb{F}_{37}\left((t^{37} - t)^{36}\right) \\
E^{\langle \tau, i \rangle} &= \mathbb{F}_{37}\left((t^2 + t^{-2})^{37} - t^2 + t^{-2}\right)
\end{aligned}$$

- Afirimo que $f(t) = \frac{(t^{37^2} - t)^{38}}{(t^{37} - t)^{37^2+1}}$ cumple que $\mathbb{F}_{37}(t)^{\langle \sigma, i, \tau \rangle} = \mathbb{F}_{37}(t)^{Gal(\mathbb{F}_{37}(t))} = \mathbb{F}_{37}(f)$.

Por un lado recordemos que $q^3 - q = |Gal(\mathbb{F}_{37}(t)/E^G)| = [E : E^G]$ por el teorema de Galois y el primer punto; y por el otro del ejercicio 19 de la práctica 2 si $f = \frac{g}{h} \in E \setminus \mathbb{F}_{37}$ entonces $[E : E(f)] = \max\{gr(g), gr(h)\}$. Luego, si probamos que al reducir f a factores coprimos g, h vale que $\max\{gr(g), gr(h)\} = q^3 - q$ podemos concluir, ya que claramente $\mathbb{F}_{37}(f) \subseteq E^G$, que $E^G = \mathbb{F}_{37}(f)$.

Notemos que:

$$\begin{aligned}
\frac{(t^{37^2} - t)^{38}}{(t^{37} - t)^{37^2+1}} &= \frac{t^{q+1} (t^{q^2-1} - 1)^{q+1}}{t^{q^2+1} (t^{q-1} - 1)^{q^2+1}} \\
&= \frac{((t^{q-1})^{q+1} - 1)^{q+1}}{t^{q^2-q} (t^{q-1} - 1)^{q^2+1}} \\
&= \frac{((t^{q-1}) - 1)^{q+1} \left(\sum_{r=0}^q t^{(q-1)r}\right)^{q+1}}{t^{q^2-q} (t^{q-1} - 1)^{q^2+1}} \\
&= \frac{\left(\sum_{r=0}^q t^{(q-1)r}\right)^{q+1}}{t^{q^2-q} (t^{q-1} - 1)^{q^2-q}} \\
&= \frac{g}{h} \quad \text{pues } (g, h) = 1
\end{aligned}$$

$$\text{Y finalmente } \max\{gr(g), gr(h)\} = \max\left\{\underbrace{q^2 - q + (q-1)(q^2 - q)}_{q^3 - q^2}, \underbrace{(q-1)q(q+1)}_{q^3 - q}\right\} = q^3 - q,$$

luego concluimos que $E^G = \mathbb{F}_{37}(f)$. ■

Ejercicio 2

- Notemos primero que $\beta^2 = 10 + 5\sqrt{2} + 2\sqrt{5} + \sqrt{10} \in \mathbb{Q}[\sqrt{2}, \sqrt{5}]$; es más, notemos que de la misma cuenta $\beta^2 \notin \mathbb{Q}, \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{5}]$ que son (lo vimos en la práctica analizando $\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}]$) las únicas subextensiones propias de $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$. Luego como $\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}$ es separable, de la teórica sabemos que para todo $\alpha \in \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ vale:

$$f(\alpha, \mathbb{Q}) = \prod_{i=1}^4 (x - \sigma_i(\alpha))$$

Donde $\{\sigma_i(\alpha)\}_i$ son los valores diferentes que toma $\sigma(\alpha)$ con $\sigma \in Gal(\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q})$.

Por otro lado, ya de la práctica sabemos que $Gal(\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ y los 4 morfismos están generados por las restricciones de la conjugación en $\mathbb{Q}[\sqrt{5}]/\mathbb{Q}$ y $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$.

Como en nuestro caso $\beta^2 \notin \mathbb{Q}, \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{5}]$ no está en ninguna subextensión de $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ entonces por el teorema de correspondencia de Galois (es claramente normal) β^2 no esta en ningún cuerpo fijo, lo que es equivalente a que $\sigma(\beta) \neq \beta$ para ninguno de estos 4 morfismos. Luego podemos concluir que:

$$\{\sigma_i(\beta^2)\}_i = \left\{ \left(10 - 5\sqrt{2} + 2\sqrt{5} - \sqrt{10}\right), \left(10 + 5\sqrt{2} - 2\sqrt{5} - \sqrt{10}\right), \right. \\ \left. \left(10 + 5\sqrt{2} + 2\sqrt{5} + \sqrt{10}\right), \left(10 - 5\sqrt{2} - 2\sqrt{5} + \sqrt{10}\right) \right\}$$

Es decir, β^2 evaluado en cada uno de los 4 morfismos que generan el grupo de Galois; pues si alguno fijara β^2 esto sería equivalente a que β^2 este en algún cuerpo fijo, lo que sería equivalente a que β^2 pertenezca a alguna subextensión propia de $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$. Por lo tanto:

$$f(\beta^2, \mathbb{Q}) = \left(x - \left(10 - 5\sqrt{2} + 2\sqrt{5} - \sqrt{10}\right)\right) \left(x - \left(10 + 5\sqrt{2} - 2\sqrt{5} - \sqrt{10}\right)\right) \\ \left(x - \left(10 + 5\sqrt{2} + 2\sqrt{5} + \sqrt{10}\right)\right) \left(x - \left(10 - 5\sqrt{2} - 2\sqrt{5} + \sqrt{10}\right)\right) \\ = x^4 - 40x^3 + 440x^2 - 1600x + 1600 \quad \text{si hice bien las cuentas}$$

De yapa, como ya sabemos que f es el minimal y tiene grado 4, sacamos que $\mathbb{Q}[\sqrt{2}, \sqrt{5}] = \mathbb{Q}[\beta^2]$ pues ya habíamos visto una inclusión y sus grados sobre \mathbb{Q} son iguales.

Para continuar, entonces tenemos la torre $\mathbb{Q} \subsetneq \mathbb{Q}[\beta^2] \subset \mathbb{Q}[\beta]$, **veamos que las inclusiones son estrictas!**

En pos de esto supongamos que $\beta \in \mathbb{Q}[\beta^2] = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$, luego:

$$\beta = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}$$

Notemos que las matrices de multiplicar por $\beta, \sqrt{2}, \sqrt{5}, \sqrt{10}$ en la base $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ resultan respectivamente (esto es cuentitas):

$$m_\beta = \begin{pmatrix} a & b & c & d \\ 2b & a & 2d & c \\ 5c & 5d & a & b \\ 10 & 5c & 2b & a \end{pmatrix}$$

$$m_{\sqrt{2}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

$$m_{\sqrt{5}} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \end{pmatrix}$$

$$m_{\sqrt{10}} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 5 & 0 & 0 \\ 10 & 0 & 0 & 0 \end{pmatrix}$$

Luego debe valer:

$$Tr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\beta) = a + bTr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{2}) + cTr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{5}) + dTr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{10})$$

De lo que concluimos que $a = 0$. Apliquemos el mismo razonamiento para $\sqrt{2}\beta, \sqrt{5}\beta$ y $\sqrt{10}\beta$; no obstante, al solo interesarnos el término de la diagonal vamos a escribir el resto de los coeficientes

con * pues no afectan el cálculo de la traza. Continuando con $\sqrt{2}\beta$

$$m_{\sqrt{2}\beta} = \begin{pmatrix} 2b & * & * & * \\ * & 2b & * & * \\ * & * & 2b & * \\ * & * & * & 2b \end{pmatrix}$$

De lo que concluimos que:

$$Tr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{2}\beta) = 2b + cTr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{10}) + 2dTr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{5})$$

De lo que concluimos que $b = 0$. Continuando con $\sqrt{5}\beta$:

$$m_{\sqrt{5}\beta} = \begin{pmatrix} 5c & * & * & * \\ * & 5c & * & * \\ * & * & 5c & * \\ * & * & * & 5c \end{pmatrix}$$

De lo que concluimos que:

$$Tr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{5}\beta) = 5c + 5dTr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{2})$$

De lo que concluimos que $c = 0$. Finalizando con $\sqrt{10}\beta$:

$$m_{\sqrt{10}\beta} = \begin{pmatrix} 10d & * & * & * \\ * & 10d & * & * \\ * & * & 10d & * \\ * & * & * & 10d \end{pmatrix}$$

De lo que concluimos que:

$$Tr_{\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}}(\sqrt{10}\beta) = 10d$$

De lo que concluimos que $d = 0$. Probamos que $\beta \notin \mathbb{Q}[\beta^2]$ y las inclusiones eran estrictas. Como $f = x^2 - \beta^2$ es un polinomio mónico que anula a β y $f \in \mathbb{Q}[\beta^2][X]$ podemos concluir que $1 < [\mathbb{Q}[\beta] : \mathbb{Q}[\beta^2]] \leq 2$, o sea que la extensión es cuadrática. Por lo tanto por grados sabemos que $[\mathbb{Q}[\beta], \mathbb{Q}] = 8$.

Para concluir este punto, recordemos además que como \mathbb{Q} es de característica 0 todas nuestras extensiones son separables y eso implica que $Hom(\mathbb{Q}[\beta]/\mathbb{Q}) = Hom(\mathbb{Q}[\beta]/\mathbb{Q}[\beta^2]) \times Hom(\mathbb{Q}[\beta^2]/\mathbb{Q})$. Similarmente al punto anterior, ya probamos que β no se encuentra en ninguna subextensión de $\mathbb{Q}[\beta]/\mathbb{Q}$ (esto es consecuencia de la cuenta anterior) por lo que por el teorema de correspondencia de Galois no es fijado por ningún elemento de $Hom(\mathbb{Q}[\beta]/\mathbb{Q})$. En consecuencia, $\{\sigma_i(\beta)\}_i$ es exactamente $\sigma(\beta)$ para cada una de los 8 morfismos que son base de $Hom(\mathbb{Q}[\beta]/\mathbb{Q})$ y entonces de lo que dedujimos en la teórica:

$$f(\beta, \mathbb{Q}) = \prod_{\psi \in Hom(\mathbb{Q}[\beta^2]/\mathbb{Q})} \psi(f(\beta, \mathbb{Q}[\beta^2]))$$

Como habíamos visto que $f(\beta, \mathbb{Q}[\beta^2]) = x^2 - \beta^2 = p$ entonces:

$$\begin{aligned} \sigma_1(x^2 - (10 + 2\sqrt{5} + 5\sqrt{2} + \sqrt{10})) &= (x^2 - (10 - 5\sqrt{2} + 2\sqrt{5} - \sqrt{10})) \\ \sigma_2(x^2 - (10 + 2\sqrt{5} + 5\sqrt{2} + \sqrt{10})) &= (x^2 - (10 + 5\sqrt{2} - 2\sqrt{5} - \sqrt{10})) \\ \sigma_3(x^2 - (10 + 2\sqrt{5} + 5\sqrt{2} + \sqrt{10})) &= (x^2 - (10 + 5\sqrt{2} + 2\sqrt{5} + \sqrt{10})) \\ \sigma_4(x^2 - (10 + 2\sqrt{5} + 5\sqrt{2} + \sqrt{10})) &= (x^2 - (10 - 5\sqrt{2} - 2\sqrt{5} + \sqrt{10})) \end{aligned}$$

De lo que deducimos que:

$$\begin{aligned} f(\beta, \mathbb{Q}) &= \left(x^2 - \left(10 - 5\sqrt{2} + 2\sqrt{5} - \sqrt{10} \right) \right) \left(x^2 - \left(10 + 5\sqrt{2} - 2\sqrt{5} - \sqrt{10} \right) \right) \\ &\quad \left(x^2 - \left(10 + 5\sqrt{2} + 2\sqrt{5} + \sqrt{10} \right) \right) \left(x^2 - \left(10 - 5\sqrt{2} - 2\sqrt{5} + \sqrt{10} \right) \right) \\ &= x^8 - 40x^6 + 440x^4 - 1600x^2 + 1600 \quad \text{si hice bien las cuentas} \end{aligned}$$

Y sabemos que es el minimal (además de por todos los teoremas) porque es mónico, anula a β (se ve) y es del grado correcto.

- Si recopilamos un poco lo que fuimos calculando notemos que llegamos a la conclusión que las 8 raíces del minimal son $\pm \sqrt{(2 \pm \sqrt{2})(5 \pm \sqrt{5})}$, veamos que todas están en $\mathbb{Q}[\beta]$ y para eso es claro que basta verlo para $\sqrt{(2 \pm \sqrt{2})(5 \pm \sqrt{5})}$.

Sea $\alpha_1 = \sqrt{(2 - \sqrt{2})(5 + \sqrt{5})}$, luego $\alpha_1\beta = \sqrt{(2^2 - 2)(5 + \sqrt{5})^2} = \sqrt{2}(5 + \sqrt{5}) \in \mathbb{Q}[\sqrt{2}, \sqrt{5}] = \mathbb{Q}[\beta]$. Similarmente sea $\alpha_2 = \sqrt{(2 + \sqrt{2})(5 - \sqrt{5})}$ y vemos que $\alpha_2\beta = 2\sqrt{5}(2 + \sqrt{2}) \in \mathbb{Q}[\beta]$; y $\alpha_3 = \sqrt{(2 - \sqrt{2})(5 - \sqrt{5})}$ que se ve que $\alpha_3\beta = 2\sqrt{2}\sqrt{5} \in \mathbb{Q}[\beta]$. Luego concluimos que $\pm\alpha_1, \pm\alpha_2, \pm\alpha_3 \in \mathbb{Q}[\beta]$ de lo que deducimos que las 8 raíces de $f(\beta, \mathbb{Q})$ están en $\mathbb{Q}[\beta]$, lo que dice que $\mathbb{Q}[\beta]$ es el cuerpo de descomposición de f y por ende es Galois.

- Sea $\sigma \in \text{Gal}(\mathbb{Q}[\beta]/\mathbb{Q})$ un automorfismo que mande β a $\alpha_1 := \alpha$, luego por ser automorfismo sabemos que:

$$(2 + \sigma(\sqrt{2}))(5 + \sigma(\sqrt{5})) = \sigma((2 + \sqrt{2})(5 + \sqrt{5})) = \sigma(\beta^2) = \sigma(\beta)^2 = \alpha^2 = (2 - \sqrt{2})(5 + \sqrt{5})$$

Y concluimos que $\sigma(\sqrt{2}) = -\sqrt{2}$ y $\sigma(\sqrt{5}) = \sqrt{5}$. Luego:

$$\sigma(\alpha)\alpha = \sigma(\alpha)\sigma(\beta) = \sigma(\alpha\beta) = \sigma(\sqrt{2})(5 + \sigma(\sqrt{5})) = -\sqrt{2}(5 + \sqrt{5}) = -\alpha\beta$$

Por lo que $\sigma(\alpha) = -\beta$ y tenemos el siguiente diagrama de la acción de σ :

$$\beta \rightarrow \alpha \rightarrow -\beta \rightarrow -\alpha \rightarrow \beta$$

Y σ es un elemento de orden 4. Similarmente vamos a analizar $\tau \in \text{Gal}(\mathbb{Q}[\beta]/\mathbb{Q})$ tal que $\tau(\beta) = \alpha_2 := \omega = \sqrt{(2 + \sqrt{2})(5 - \sqrt{5})}$.

$$(2 + \tau(\sqrt{2}))(5 + \tau(\sqrt{5})) = \tau((2 + \sqrt{2})(5 + \sqrt{5})) = \tau(\beta^2) = \sigma(\beta)^2 = \omega^2 = (2 + \sqrt{2})(5 - \sqrt{5})$$

Y concluimos que $\tau(\sqrt{2}) = \sqrt{2}$ y $\tau(\sqrt{5}) = -\sqrt{5}$. Luego:

$$\tau(\omega)\omega = \tau(\omega)\tau(\beta) = \tau(\omega\beta) = 2\tau(\sqrt{5})(2 + \tau(\sqrt{2})) = -2\sqrt{5}(2 + \sqrt{2}) = -\omega\beta$$

Por lo que $\tau(\omega) = -\beta$ y tenemos el siguiente diagrama de la acción de τ :

$$\beta \rightarrow \omega \rightarrow -\beta \rightarrow -\omega \rightarrow \beta$$

Y τ es un elemento de orden 4. A su vez notamos que σ, τ generan y que $\sigma^2 = \tau^2$ con lo que nos faltaría ver si conmutan; en pos de eso

$$\frac{\sigma(\beta)^2}{\beta^2} = \frac{2 - \sqrt{2}}{2 + \sqrt{2}} = \left(\frac{2 - \sqrt{2}}{\sqrt{2}} \right)^2 = (\sqrt{2} - 1)^2$$

$$\frac{\tau(\beta)^2}{\beta^2} = \frac{5 - \sqrt{5}}{5 + \sqrt{5}} = \left(\frac{5 - \sqrt{5}}{2\sqrt{5}} \right)^2 = \left(\frac{\sqrt{5} - 1}{2} \right)^2$$

Lo que podemos deducir que (si notamos de igual manera a la extension):

$$\sigma(\beta) = (\sqrt{2} - 1) \beta$$

$$\tau(\beta) = \frac{\sqrt{5} - 1}{2} \beta$$

Luego si vemos como actuan las composiciones en β :

$$\beta \xrightarrow{\tau} \frac{\sqrt{5} - 1}{2} \beta \xrightarrow{\sigma} \frac{\sqrt{5} - 1}{2} (\sqrt{2} - 1) \beta$$

$$\beta \xrightarrow{\sigma} (\sqrt{2} - 1) \beta \xrightarrow{\tau} \frac{\sqrt{5} - 1}{2} (\sqrt{2} - 1) \beta$$

Por lo que concluimos que una presentación de $Gal(\mathbb{Q}[\beta]/\mathbb{Q})$ es

$$\{\sigma, \tau : \sigma^4 = \tau^4 = Id, \sigma^2 = \tau^2, \sigma\tau = \tau\sigma\} \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$$

- Este punto es muy parecido a la práctica así que notemos que tenemos la torre de extensiones $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{10}] \subseteq \mathbb{Q}[\sqrt{10 + \sqrt{10}}]$ y veamos que son inclusiones estrictas.

Es simple y ya sabemos que $\sqrt{10} \notin \mathbb{Q}$, luego asumamos que $\sqrt{10 + \sqrt{10}} \in \mathbb{Q}[\sqrt{10}]$; entonces existen $a, b \in \mathbb{Q}$ tal que $\sqrt{10 + \sqrt{10}} = a + b\sqrt{10}$. Elevando al cuadrado e igualando término a término de la base $\{1, \sqrt{10}\}$ de $\mathbb{Q}[\sqrt{10}]$ tenemos el sistema:

$$2ab = 1$$

$$a^2 + 10b^2 = 10$$

Lo que lleva a que $b = \frac{1}{2a}$ y a cumpla $a^4 + \frac{10}{4} - 10a^2 = 0$ que podemos verificar que no tiene soluciones racionales; luego las inclusiones son estrictas.

Pero como $p_1 = x^2 - 10 \in \mathbb{Q}[X]$ y $p_2 = x^2 - (10 + \sqrt{10}) \in \mathbb{Q}[\sqrt{10}]$ son polinomios mónicos y anulan a $\sqrt{10}, \sqrt{10 + \sqrt{10}}$ respectivamente podemos concluir que ambas extensiones son cuadráticas y esos son los polinomios minimales; es más, tenemos en conclusión que el grado de la extensión $\mathbb{Q}[\sqrt{10 + \sqrt{10}}]/\mathbb{Q}$ es 4.

Si hacemos lo mismo que en el primer punto, podemos verificar entonces que las 4 raíces del polinomio minimal resultan $\pm\sqrt{10 \pm \sqrt{10}}$ y todas se encuentran en $\mathbb{Q}[\sqrt{10 + \sqrt{10}}]$ pues:

$$\sqrt{10 + \sqrt{10}}\sqrt{10 - \sqrt{10}} = 3\sqrt{10} = 3 \left[\left(\sqrt{10 + \sqrt{10}} \right)^2 - 10 \right] \in \mathbb{Q}[\sqrt{10 + \sqrt{10}}]$$

Por lo que $\mathbb{Q}[\sqrt{10 + \sqrt{10}}]/\mathbb{Q}$ es Galois!

Sea $\sigma \in Gal(\mathbb{Q}[\sqrt{10 + \sqrt{10}}]/\mathbb{Q})$ tal que $\sigma(\sqrt{10 + \sqrt{10}}) = \sqrt{10 - \sqrt{10}}$, luego:

$$\begin{aligned}
\sigma\left(\sqrt{10-\sqrt{10}}\right) &= \frac{3\left[\left(\sigma\left(\sqrt{10+\sqrt{10}}\right)\right)^2-10\right]}{\sigma\left(\sqrt{10+\sqrt{10}}\right)} \\
&= \frac{3\left[\left(\sqrt{10-\sqrt{10}}\right)^2-10\right]}{\sqrt{10-\sqrt{10}}} \\
&= \frac{-3\sqrt{10}}{3\sqrt{10}} \\
&= \frac{-1}{\sqrt{10+\sqrt{10}}} \\
&= -\sqrt{10+\sqrt{10}}
\end{aligned}$$

Luego tenemos la siguiente acción de σ sobre $\sqrt{10+\sqrt{10}}$

$$\gamma \rightarrow \sqrt{10-\sqrt{10}} \rightarrow -\gamma \rightarrow -\sqrt{10-\sqrt{10}} \rightarrow \gamma$$

Y σ resulta un generador de orden 4 de $\text{Gal}\left(\mathbb{Q}[\sqrt{10+\sqrt{10}}]/\mathbb{Q}\right)$; luego $\text{Gal}\left(\mathbb{Q}[\sqrt{10+\sqrt{10}}]/\mathbb{Q}\right) \simeq \mathbb{Z}_4$

- Notemos que si tomamos ahora $\sigma \circ \tau$ entonces $\mathbb{Q}[\beta]^{\langle \sigma \circ \tau \rangle} = \mathbb{Q}[\gamma]$. Como $(\sigma \circ \tau)^2 = \sigma^2 \circ \tau^2 = \sigma^4 = \text{Id}$ entonces sabemos que $\langle \sigma \circ \tau \rangle < \mathbb{Z}_4 \times \mathbb{Z}_2$ tiene índice 4; luego por el teorema de correspondencia de Galois sabemos que una subextensión de $\mathbb{Q}[\beta]/\mathbb{Q}$ de orden 4 es $\mathbb{Q}[\gamma]$. ■

Ejercicio 3

- Primero veamos si podemos reducir a f a una forma más tratable. Para eso recordemos que si $p = ax^4 + bx^3 + cx^2 + dx + e$ entonces $\tilde{p}(x) = \frac{p(x-\frac{b}{4a})}{a}$ cumple que no tiene término cúbico y que si \tilde{p} es irreducible entonces p lo es (esto lo vimos tanto en la práctica como la teórica).

Luego:

$$\tilde{f} = f(x+1) = x^4 - x^2 + 1 \quad \text{si hice bien las cuentas}$$

Con lo que llegamos a la hermosa conclusión que f es irreducible en K si y sólo si Φ_{12} es irreducible en $K[X]$.

Para el caso $K = \mathbb{Q}$ ya sabemos que todos los polinomios ciclotómicos son irreducibles así que f lo es.

Ahora si $\text{char}(K) = 2$ entonces notemos que $\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 - x + 1)^2$ por lo que f no sería irreducible

Si $\text{char}(K) = 3$ notemos que $\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 1)^2$ por lo que f no sería irreducible.

Para finalizar, veamos el siguiente lema:

Lema 0.0.1 Sobre F finito con característica p con $p \nmid n$ son equivalentes:

- Φ_n es irreducible
- $[F[\xi] : F] = \phi(n)$
- $\text{Gal}\left(F[\xi]/F\right) \simeq (\mathbb{Z}/n\mathbb{Z})^*$
- p es un generador de $(\mathbb{Z}/n\mathbb{Z})^*$

Demostración En efecto, como ξ es una raíz de Φ_n entonces $f(\xi, F) = \Phi_n$ pues es irreducible, mónico y anula; luego $[F[\xi] : F] = \varphi(n) = \text{gr}(\Phi_n)$. Como $F[\xi]/F$ es Galois ($p \nmid n$), sabemos que $\varphi(n) = \left| \text{Gal}\left(F[\xi]/F\right) \right| = \left| (\mathbb{Z}/n\mathbb{Z})^* \right| = \varphi(n)$, luego la inyección $\text{Gal}\left(F[\xi]/F\right) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ es un isomorfismo de grupos pues de Álgebra 2 sabemos que un homomorfismo inyectivo (esto

lo sabemos de la teórica) entre grupos de igual orden es isomorfismo. Finalmente de la teoría de cuerpos finitos sabemos que siempre:

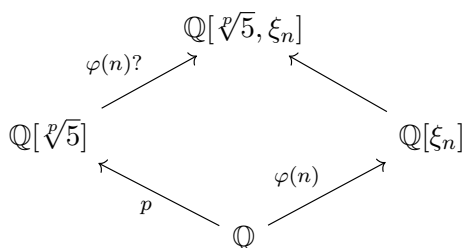
$$p = f(\xi, F) = \prod_{i=1}^k x - \xi^{p^i}$$

donde $k = [F[\xi] : F]$. Luego sabemos que $p|\Phi_n$ y van a ser iguales si y sólo si sus raíces son iguales, es decir cuando $\xi^a \cong \xi^{p^i}$ para todo $a \leq n$ tal que $(a, n) = 1$. Esto vimos que pasa si y sólo si $a \cong p^i \pmod{n}$ para algún i , lo que pasa si y sólo si p es generador de $(\mathbb{Z}/n\mathbb{Z})^*$. ■

Luego, Φ_n es irreducible en \mathbb{F}_p con $p \nmid n$ si y sólo si $(\mathbb{Z}/n\mathbb{Z})^*$ es cíclico, que de Álgebra 2 sabemos que pasa si y sólo si $n \in \{2, 4, l^s, 2l^s\}$ con l primo impar o $s \geq 1$; como 12 no entra en ninguna de esas posibilidades sabemos que Φ_{12} es reducible en \mathbb{F}_p para $p \neq 2, 3$.

Resumiendo vimos que f es irreducible solo si $K = \mathbb{Q}$. ■

- Notemos que podemos representar este problema con el siguiente diamante:



Pues Φ_n es irreducible en $\mathbb{Q}[\sqrt[n]{5}]$ si y sólo si el polinomio minimal de ξ_n en $\mathbb{Q}[\sqrt[n]{5}]$ es Φ_n si y sólo si $[\mathbb{Q}[\sqrt[n]{5}, \xi_n] : \mathbb{Q}[\sqrt[n]{5}]] = \varphi(n)$.

Luego, sabemos que si $p \nmid \varphi(n)$ entonces como los grados inferiores del diamante son coprimos $[\mathbb{Q}[\sqrt[n]{5}, \xi_n] : \mathbb{Q}[\sqrt[n]{5}]] = \varphi(n)$ y Φ_n resulta irreducible en $\mathbb{Q}[\sqrt[n]{5}]$.

Supongamos ahora que $p|\varphi(n)$, veamos que $\mathbb{Q}[\sqrt[n]{5}] \cap \mathbb{Q}[\xi] = \mathbb{Q}$.

Supongamos que $\sqrt[n]{5} \in \mathbb{Q}[\xi_n]$, luego existe la torre de extensiones $\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt[n]{5}] \subsetneq \mathbb{Q}[\xi_n]$ y por el teorema de correspondencia de Galois $\text{Gal}(\mathbb{Q}[\sqrt[n]{5}]/\mathbb{Q})$ resulta un subgrupo de $\text{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q})$. Recordemos que vale:

$$\text{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$$

Y este grupo resulta abeliano, luego todo subgrupo de un grupo abeliano resulta normal al menos. Por lo tanto, eso implicaría que $\text{Gal}(\mathbb{Q}[\sqrt[n]{5}]/\mathbb{Q})$ es un subgrupo normal, lo que implicaría, por el teorema de correspondencia de Galois nuevamente, que la extensión $(\mathbb{Q}[\sqrt[n]{5}]/\mathbb{Q})$ es normal. Esto es absurdo pues $p > 2$ y ya lo vimos varias veces en la materia.

Luego, como claramente además $\xi \notin \mathbb{Q}[\sqrt[n]{5}] \subset \mathbb{R}$ entonces concluimos que $\mathbb{Q}[\sqrt[n]{5}] \cap \mathbb{Q}[\xi] = \mathbb{Q}$. Recordemos el siguiente teorema:

Teorema 0.0.2 Sean E, L extensiones de $F = E \cap L$ tal que E/F es Galois, luego EL/L es Galois y además $\text{Gal}(EL/L) \simeq \text{Gal}(E/F)$

Luego entonces como $\mathbb{Q}[\xi]/\mathbb{Q}$ es Galois y $\mathbb{Q}[\sqrt[n]{5}] \cap \mathbb{Q}[\xi] = \mathbb{Q}$, usando el teorema sabemos que $\mathbb{Q}[\xi, \sqrt[n]{5}]/\mathbb{Q}[\sqrt[n]{5}]$ es Galois y que $\varphi(n) = |\text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})| = |\text{Gal}(\mathbb{Q}[\xi, \sqrt[n]{5}]/\mathbb{Q}[\sqrt[n]{5}])| = [\mathbb{Q}[\sqrt[n]{5}, \xi_n] : \mathbb{Q}[\sqrt[n]{5}]]$ pues además es Galois.

Luego, $[\mathbb{Q}[\sqrt[n]{5}, \xi_n] : \mathbb{Q}[\sqrt[n]{5}]] = \varphi(n)$ para este caso también y entonces concluimos que Φ_n resulta irreducible en $\mathbb{Q}[\sqrt[n]{5}]$ para todo $p > 2$. ■

Ejercicio 4

- Sea $S = \{K \text{ subextensiones de } \mathbb{C}/\mathbb{Q} : \alpha \notin K\}$ y notemos que es no vacío pues $\mathbb{Q} \in S$; sea entonces \mathcal{F} una cadena totalmente ordenada en S y tomemos $L = \bigcup_{K \in \mathcal{F}} K$, afirmo que L es cota superior de S .

En efecto, si $K \in \mathcal{F}$ entonces $K \subset L$ por definición, L es subextensión de \mathbb{C}/\mathbb{Q} pues todos los $K \in \mathcal{F}$ lo son y $\alpha \notin L$ pues si lo estuviese, entonces $\alpha \in K_{\mathcal{F}}$ para algún $K_{\mathcal{F}} \in \mathcal{F}$ lo que es absurdo pues $K_{\mathcal{F}} \in S$.

Luego, por el lema de Zorn, existe un elemento maximal $K \in S$ que resulta la subextensión buscada.

- Sea $x \in \mathbb{C} - K$ y supongamos que es trascendente, lo esto implica que tenemos la torre de extensiones $\mathbb{Q} \subsetneq K \subsetneq K[x] \subset \mathbb{C}$ y $K[x]$ es una subextensión de \mathbb{C}/\mathbb{Q} tal que no tiene a α . Esto es claro pues $\alpha \notin K$ y $\alpha \neq x$ pues x es trascendente y α algebraico. Como K era maximal uno concluiría que $K = K[x]$ lo que es absurdo, luego \mathbb{C}/K es algebraico.
- Sea M/K una subextensión finita de \mathbb{C}/K luego, por un lado, sabemos que $\alpha \in M$ por la maximalidad de K y, por el otro, existe $\sigma \in \text{Gal}(M/K)$ tal que $\sigma(\alpha) \neq \alpha$ pues es Galois. Luego $M^{(\sigma)}/K$ es una extensión tal que $\alpha \notin M^{(\sigma)}$, por la maximalidad de K concluimos que $K = M^{(\sigma)}$ y entonces por el teorema de correspondencia de Galois esto es si y sólo si $\langle \sigma \rangle = \text{Gal}(M/K)$. Concluimos que M/K es cíclico.
- Sea $G = \text{Gal}(M/K)$ y sabemos porque $\alpha^2 = 3 \in \mathbb{Q} \subset K$ que $[K[\alpha] : K] = 2$. Sea q un primo que divida a $n = |G|$, luego como G es cíclico sabemos que existe una subextensión F/K de grado q . Finalmente, como $\alpha \in F$ (pues sino por la maximalidad de K respecto a la propiedad de $\alpha \notin K$ eso implicaría que $K = F$ lo que diría que $q = 1$ es primo) entonces sabemos que $2|q$ por lo que $q = 2$; luego $|G| = [M : K] = 2^r$.
Notemos que por lo visto anteriormente $\sqrt[n]{\alpha} \notin K$ para todo n (pues sino $\sqrt[n]{\alpha}^{n-1} = \pm \alpha \in K$) por lo que deducimos que $[\mathbb{C} : K] \geq [K[\sqrt[n]{\alpha}] : K] = n$ para todo n y entonces $[\mathbb{C} : K] = \infty$. ■

Ejercicio 5

- No se aun
- Veamos que es falso! Sea $f = x^4 - 4x + 2$ y su resolvente $g(x) = x^3 - 8x - 16$. Ambos resultan irreducibles pues f es Eisenstein con $p = 2$ y su resolvente pues $\hat{g} = x^3 + 2x + 4$ es irreducible en \mathbb{F}_5 .
Como el discriminante de g es $-4864 \notin \mathbb{Q}^2$ entonces concluimos que $\text{Gal}(g) \simeq \text{Gal}(L/\mathbb{Q}[\alpha]) \simeq S_3$ con α raíz de f y $\text{Gal}(f) = \text{Gal}(L/\mathbb{Q}) \simeq S_4$.
Supongamos que existe M subextensión de grado 2, luego tendríamos la torre $\mathbb{Q} \subseteq M \subseteq \mathbb{Q}[\alpha] \subseteq L$ (pues $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$ pues f irreducible) lo que implica que $S_3 \simeq \text{Gal}(L/\mathbb{Q}[\alpha]) \leq \text{Gal}(L/M) \leq \text{Gal}(L/\mathbb{Q}) \simeq S_4$ (donde \leq implica ser subgrupo) y veamos que eso no puede ser.
En efecto, sea H un subgrupo entre S_3 y S_4 con esas características, entonces H es transitivo (por ser un grupo de Galois), tiene un $n - 1$ ciclo y una transposición lo que implica que $H \simeq S_4$. Concluimos que tal subextensión cuadrática M no puede existir. ■