Álgebra 3

Primer Parcial

Axel Sirota

Ejercicio 1

- Primero recordemos el ejercicio 27 de la práctica 3 que dice:

$$Gal\left(K(t)/K\right) \simeq PGL_2(K)$$

Luego afirmo que en realidad $G = \langle \tau, \sigma, i\rangle = Gal\left(K(t)/K\right)$ de lo que el orden de G va a ser el orden de $PGL_2(K) = q^3 - q$.

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

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

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

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 $f \in Gal\left(K(t)/K\right)$ 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 $G = Gal\left(K(t)/K\right)$ y como $|Gal\left(K(t)/K\right)| = q^3 - q$ 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:

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

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

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

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

De lo que concuimos 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:

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

Luego si $u=t^2+t^{-2}$ vimos que $\mathbb{F}_{37}(u)\subset E^{\langle i\rangle}$.
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 $4=\left|Gal\left(\mathbb{F}_{37}(t)\,/_{E^{\langle i\rangle}}\right)\right|=\left[E:E^{\langle i\rangle}\right]$ por el teorema de Galois.
Por otro lado, si $p(x)=x^4-x^2\left(t^2+t^{-2}\right)+1$ entonces $p\in\mathbb{F}_{37}(t^2+t^{-2})[X]$ es mónico y $p(t)=0$, por lo que $f\left(t,\mathbb{F}_{37}(t^2+t^{-2})\right)|p$ con lo que $[\mathbb{F}_{37}(u):\mathbb{F}_{37}(t)]\le 4$.
Luego, juntando todo, tenemos la torre $\mathbb{F}_{37}(u)\subseteq E^{\langle i\rangle}\subseteq\mathbb{F}_{37}(t)$ donde:

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

Pues $1\le\left[\mathbb{F}_{37}(u):E^{\langle i\rangle}\right]\le 1$, de lo que concuimos que $E^{\langle i\rangle}=\mathbb{F}_{37}(t^2+t^{-2})$.
Finalmente analicemos a τ, si $u=t^{37}-t$ entonces para $f\in\mathbb{F}_{37}[t]$ vale:

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

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

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

De lo que concuimos que $E^{\langle\tau\rangle}=\mathbb{F}_{37}(t^{37}-t)$.
Para concluir el punto notemos que ahora simplemente tenemos que juntar lo que fuimos descubriendo! Es decir es claro que:

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

- Afirmo que $f(t)=\dfrac{\left(t^{37^2}-t\right)^{38}}{\left(t^{37}-t\right)^{37^2+1}}$ 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 $q^3-q=\left|Gal\left(\mathbb{F}_{37}(t)\,/E^G\right)\right|=\left[E:E^G\right]$ 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 $[E:E(f)]=\text{máx}\{gr(g),gr(h)\}$. Luego, si probamos que al reducir f a factores coprimos g,h vale que $\text{máx}\{gr(g),gr(h)\}=q^3-q$ podemos concluir, ya que claramente $\mathbb{F}_{37}(f)\subseteq E^G$, que $E^G=\mathbb{F}_{37}(f)$.

  Notemos que:

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

  Y finalmente $\text{máx}\{gr(g),gr(h)\}=\text{máx}\left\{\underbrace{q^2-q+(q-1)\left(q^2-q\right)}_{q^3-q^2},\underbrace{(q-1)q(q+1)}_{q^3-q}\right\}=q^3-q$, luego conlcuimos 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 $\beta^2\notin\mathbb{Q},\mathbb{Q}[\sqrt{2}],\mathbb{Q}[\sqrt{5}],\mathbb{Q}[\sqrt{10}]$ 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:

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

  Donde $\{\sigma_i(\alpha)\}_i$ son los valores diferentes que toma $\sigma(\alpha)$ con $\sigma\in Gal\left(\mathbb{Q}[\sqrt{2},\sqrt{5}]\,/\mathbb{Q}\right)$ y $N_\alpha=|\{\sigma_i(\alpha)\}_i|$ la cantidad de valores diferentes que toma α en los morfismos del grupo de Galois. En particular si $\alpha\in\mathbb{Q}$ entonces $\sigma(\alpha)=\alpha$ para todo $\sigma\in Gal\left(\mathbb{Q}[\sqrt{2},\sqrt{5}]\,/\mathbb{Q}\right)$ por lo que $N_\alpha=1$ y $\{\sigma_i(\alpha)\}_i=\{\alpha\}$ con lo que $f(\alpha,\mathbb{Q})=x-\alpha$.

Por otro lado, ya de la práctica sabemos que $Gal\left(\mathbb{Q}[\sqrt{2},\sqrt{5}]\,/_{\mathbb{Q}}\right)\simeq\mathbb{Z}_2\times\mathbb{Z}_2$ 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 $\beta^2\notin\mathbb{Q},\mathbb{Q}[\sqrt{2}],\mathbb{Q}[\sqrt{5}],\mathbb{Q}[\sqrt{10}]$ 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:

$$\begin{aligned}\left\{\sigma_i(\beta^2)\right\}_i=\Big\{&\left(10-5\sqrt{2}+2\sqrt{5}-\sqrt{10}\right),\left(10+5\sqrt{2}-2\sqrt{5}-\sqrt{10}\right),\\&\left(10+5\sqrt{2}+2\sqrt{5}+\sqrt{10}\right),\left(10-5\sqrt{2}-2\sqrt{5}+\sqrt{10}\right)\Big\}\end{aligned}$$

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:

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

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 inclusón 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!
Sea $\xi\in Gal\left(\mathbb{Q}[\sqrt{2},\sqrt{5}]\,/_{\mathbb{Q}}\right)$ el morfismo que deja fijo a $\mathbb{Q}[\sqrt{2}]$, es decir, el generador de $Gal\left(\mathbb{Q}[\sqrt{2},\sqrt{5}]\,/_{\mathbb{Q}[\sqrt{2}]}\right)$ y supongamos que $\beta\in\mathbb{Q}[\sqrt{2},\sqrt{5}]$. Luego de la teórica sabemos que $N_{\mathbb{Q}[\sqrt{2},\sqrt{5}]/\mathbb{Q}[\sqrt{2}]}(\beta)=\beta\xi(\beta)\in\mathbb{Q}[\sqrt{2}]$ y por el otro lado sabemos que:

$$\begin{aligned}\left(\beta\xi\left(\beta\right)\right)^2=&\beta^2\xi\left(\beta^2\right)\\=&\left(2+\sqrt{2}\right)^2\left(5+\sqrt{5}\right)\left(5-\sqrt{5}\right)\\=&20\left(2+\sqrt{2}\right)^2\end{aligned}$$

Luego tenemos que $\sqrt{20\left(2+\sqrt{2}\right)^2}=\sqrt{20}\left(2+\sqrt{2}\right)\in\mathbb{Q}[\sqrt{2}]$. Si dividimos por $2\left(2+\sqrt{2}\right)$ concluimos que $\sqrt{5}\in\mathbb{Q}[\sqrt{2}]$ lo que es absurdo. Luego, probamos que β^2 no es un cuadrado en $\mathbb{Q}[\sqrt{2},\sqrt{5}]$ por lo 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 separabales y eso implica que $Hom(\mathbb{Q}[\beta]\,/_{\mathbb{Q}})=Hom\left(\mathbb{Q}[\beta]\,/_{\mathbb{Q}[\beta^2]}\right)\times Hom\left(\mathbb{Q}[\beta^2]\,/_{\mathbb{Q}}\right)$. 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:

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

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

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

De lo que deducimos que:

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

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 $\pm\sqrt{\left(2 \pm \sqrt{2}\right)\left(5 \pm \sqrt{5}\right)}$, veamos que todas están en $\mathbb{Q}[\beta]$ y para eso es claro que basta verlo para $\sqrt{\left(2 \pm \sqrt{2}\right)\left(5 \pm \sqrt{5}\right)}$.

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

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

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

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:

$$\beta \to \alpha \to -\beta \to -\alpha \to \beta$$

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

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

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:

$$\beta \to \omega \to -\beta \to -\omega \to \beta$$

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

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

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

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

Luego si vemos como actuan las composiciones en β:

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

Por lo que concluímos que una presentación de $Gal\left(\mathbb{Q}[\beta]/\mathbb{Q}\right)$ es $\left\{\sigma, \tau \ : \ \sigma^4 = \tau^4 = Id \ , \ \sigma^2 = \tau^2 \ , \ \sigma\tau = \tau\sigma\right\} \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$

- Este punto es muy parecido a la práctica asi 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 $\left\{1, \sqrt{10}\right\}$ 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 $p_2 = x^2 - \left(10+\sqrt{10}\right) \in \mathbb{Q}[\sqrt{10}]$ 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 $\eta \in Gal\left(\mathbb{Q}[\sqrt{10+\sqrt{10}}]\, /_{\mathbb{Q}}\right)$ tal que $\eta(\sqrt{10+\sqrt{10}}) = \sqrt{10-\sqrt{10}}$, luego:

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

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

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

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

- Ya vimos del punto anterior que la extensión $\mathbb{Q}[\gamma]\, /_{\mathbb{Q}}$ era Galois finita, luego si recordamos la teórica y lo juntamos con el hecho que $Gal\left(\mathbb{Q}[\gamma]\, /_{\mathbb{Q}}\right) = \langle \eta \rangle$ obtenemos que:

$$Tr_{\mathbb{Q}[\gamma]/_{\mathbb{Q}}}(\gamma) = \gamma + \eta(\gamma) + \eta^2(\gamma) + \eta^3(\gamma) \in \mathbb{Q} \subset \mathbb{Q}[\beta]$$

Ahora notemos que:

$$\left(\frac{\eta(\gamma)}{\gamma}\right)^2 = \frac{\eta(\gamma)^2}{\gamma^2} = \frac{10-\sqrt{10}}{10+\sqrt{10}} = \frac{(10-\sqrt{10})^2}{3\sqrt{10}} = \left(\frac{\sqrt{10}-1}{3}\right)^2$$

Por lo que concluimos que:

$$\eta(\gamma) = \gamma\left(\frac{\sqrt{10}-1}{3}\right)$$

De la misma manera:

$$\begin{aligned}
\eta^2(\gamma) =& \eta(\gamma)\left(\frac{\eta(\gamma)^2 - 10 - 1}{3}\right) \\
=& -\gamma\left(\frac{\sqrt{10}-1}{3}\right)\left(\frac{\sqrt{10}+1}{3}\right) \\
=& -3\gamma \\
\eta^3(\gamma) =& -3\eta(\gamma) \\
=& -3\gamma\left(\frac{\sqrt{10}-1}{3}\right) \\
=& -\gamma(\sqrt{10}-1) \qquad \text{si las cuentas no me fallan}
\end{aligned}$$

De lo que concluimos que:

$$Tr_{\mathbb{Q}[\gamma]/\mathbb{Q}}(\gamma) = \gamma\left(1 + \left(\frac{\sqrt{10}-1}{3}\right) - 3 - (\sqrt{10}-1)\right) \in \mathbb{Q}[\beta]$$

Como $\sqrt{10} \in \mathbb{Q}[\beta^2] \subset \mathbb{Q}[\beta]$ entonces $\left(1 + \left(\frac{\sqrt{10}-1}{3}\right) - 3 - (\sqrt{10}-1)\right) \in \mathbb{Q}[\beta]$ por lo que entonces dividiendolo obtenemos que $\gamma \in \mathbb{Q}[\beta]$. ∎

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 $\widetilde{p}(x) = \frac{p(x-\frac{b}{4a})}{a}$ cumple que no tiene término cúbico y que si $\widetilde{p}$ es irreducible entonces p lo es (esto lo vimos tanto en la práctica como la teórica).
Luego:

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

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 asi que f lo es.
Ahora si $char(K) = 2$ entonces notemos que $\Phi_{12}(x) = x^4 - x^2 + 1 = \left(x^2 - x + 1\right)^2$ por lo que f no seria irreducible
Si $char(K) = 3$ notemos que $\Phi_{12}(x) = x^4 - x^2 + 1 = \left(x^2+1\right)^2$ 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:*

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

Demostración En efecto, como ξ es una raíz de Φ_n entonces $f(\xi, F) = \Phi_n$ pues es irreducible, mónico y anula; luego $[F[\xi] : F] = \varphi(n) = gr(\Phi_n)$ y la vuelta es por definición. Como ${F[\xi]}/{F}$ es Galois ($p \nmid n$), sabemos que $\varphi(n) = \left|Gal\left({F[\xi]}/{F}\right)\right| = \left|({\mathbb{Z}}/{n\mathbb{Z}}\right| = \varphi(n)$, luego la inyección $Gal\left({F[\xi]}/{F}\right) \hookrightarrow \left({\mathbb{Z}}/{n\mathbb{Z}}\right)^*$ 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, y la vuelta es trivial. Finalmente de la teoría de cuerpos finitos sabemos que siempre:

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

donde $k = [\mathbb{F}_p[\xi] : \mathbb{F}_p]$. Luego sabemos que $f(\xi, \mathbb{F}_p) | \Phi_n$ y van a ser iguales si y sólo si sus raíces son iguales. Como las raíces de Φ_n son de la forma ξ^a para todo $a \leq n$ tal que $(a, n) = 1$ entonces las raíces son iguales si para todo $a \leq n$ tal que $(a, n) = 1$ existe un único $\widetilde{i} \leq k$ tal que $\xi^a = \xi^{p^{\widetilde{i}}}$ .Esto vimos que pasa si y sólo si $a = p^{\widetilde{i}} \mod (n)$. Luego esto pasa si y sólo si para cada elemento $a \in \left({\mathbb{Z}}/{n\mathbb{Z}}\right)^*$ se puede escribir de la forma p^i para un único $i \leq k$ lo que pasa si y sólo si p es generador de $\left({\mathbb{Z}}/{n\mathbb{Z}}\right)^*$. ∎

Luego, Φ_n es irreducible en $\mathbb{F}_p$ con $p \nmid n$ si y sólo si $\left({\mathbb{Z}}/{n\mathbb{Z}}\right)^*$ 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:

$$\begin{tikzcd}
 & \mathbb{Q}[\sqrt[p]{5},\xi_n] & \\
\mathbb{Q}[\sqrt[p]{5}] \arrow[ur, "\varphi(n)?"] & & \mathbb{Q}[\xi_n] \arrow[ul] \\
 & \mathbb{Q} \arrow[ul, "p"] \arrow[ur, "\varphi(n)"'] &
\end{tikzcd}$$

Pues Φ_n es irreducible en $\mathbb{Q}[\sqrt[p]{5}]$ si y sólo si el polinomio minimal de ξ_n en $\mathbb{Q}[\sqrt[p]{5}]$ es Φ_n si y sólo si $[\mathbb{Q}[\sqrt[p]{5},\xi_n] : \mathbb{Q}[\sqrt[p]{5}]] = \varphi(n)$.
Luego, sabemos que si $p \not| \varphi(n)$ entonces como los grados inferiores del diamante son coprimos $[\mathbb{Q}[\sqrt[p]{5},\xi_n] : \mathbb{Q}[\sqrt[p]{5}]] = \varphi(n)$ y Φ_n resulta irreducible en $\mathbb{Q}[\sqrt[p]{5}]$.
Supongamos ahora que $p|\varphi(n)$, veamos que $\mathbb{Q}[\sqrt[p]{5}] \cap \mathbb{Q}[\xi] = \mathbb{Q}$.
Supongamos que $\sqrt[p]{5} \in \mathbb{Q}[\xi_n]$, luego existe la torre de extensiones $\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt[p]{5}] \subsetneq \mathbb{Q}[\xi_n]$ y por el teorema de correspondencia de Galois $Gal\left(\mathbb{Q}[\sqrt[p]{5}]/\mathbb{Q}\right)$ resulta un subgrupo de $Gal(\mathbb{Q}[\xi_n]/\mathbb{Q})$.
Recordemos que vale:

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

Y este grupo resulta abeliano, luego todo subgrupo de un grupo abeliano resulta normal al menos. Por lo tanto, eso implicaría que $Gal\left(\mathbb{Q}[\sqrt[p]{5}]/\mathbb{Q}\right)$ es un subgrupo normal, lo que implicaría, por el teorema de correspondencia de Galois nuevamente, que la extensión $(\mathbb{Q}[\sqrt[p]{5}]/\mathbb{Q}$ es normal. Esto es absurdo pues $p > 2$ y ya lo vimos varias veces en la materia.
Ya vimos entonces que $\mathbb{Q}[\sqrt[p]{5}] \not\subset \mathbb{Q}[\xi]$, supongamos que existe $\mathbb{Q} \subsetneq E = \mathbb{Q}[\sqrt[p]{5}] \cap \mathbb{Q}[\xi]$, luego tenemos la torre de subextensiones $\mathbb{Q} \subsetneq E \subset \mathbb{Q}[\sqrt[p]{5}]$ y por grados:

$$p = \left[\mathbb{Q}[\sqrt[p]{5}] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt[p]{5}] : E\right][E : \mathbb{Q}]$$

Como p es primo entonces concluimos que o $E = \mathbb{Q}[\sqrt[p]{5}]$ o $E = \mathbb{Q}$, pero ya vimos que $E \neq \mathbb{Q}[\sqrt[p]{5}]$ pues la extension $\mathbb{Q}[\sqrt[p]{5}]/\mathbb{Q}$ no es normal; concluimos que $\mathbb{Q}[\sqrt[p]{5}] \cap \mathbb{Q}[\xi] = \mathbb{Q}$. 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 $Gal(EL/L) \simeq Gal(E/F)$*

Luego entonces como $Q[\xi]/\mathbb{Q}$ es Galois y $\mathbb{Q}[\sqrt[p]{5}] \cap \mathbb{Q}[\xi] = \mathbb{Q}$, usando el teorema sabemos que $\mathbb{Q}[\xi,\sqrt[p]{5}]\Big/\mathbb{Q}[\sqrt[p]{5}]$ es Galois y que $\varphi(n) = \left|Gal(Q[\xi]/\mathbb{Q})\right| = \left|Gal(\mathbb{Q}[\xi,\sqrt[p]{5}]\Big/\mathbb{Q}[\sqrt[p]{5}])\right| = [\mathbb{Q}[\sqrt[p]{5},\xi_n] : \mathbb{Q}[\sqrt[p]{5}]]$ pues además es Galois.
Luego, $[\mathbb{Q}[\sqrt[p]{5},\xi_n] : \mathbb{Q}[\sqrt[p]{5}]] = \varphi(n)$ para este caso también y entonces concluímos que Φ_n resulta irreducible en $Q[\sqrt[p]{5}]$ para todo $p > 2$. ∎

Ejercicio 4

- Sea $S = \left\{K \text{ subextensiones de } \mathbb{C}/\mathbb{Q} \ : \ \alpha \notin K\right\}$ y notemos que es no vacío pues $\mathbb{Q} \in S$; sea entonces $\mathcal{F}$ una cadena totalmente ordenada ee 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 sobre K, lo esto implica que tenemos la torre de extesiones $\mathbb{Q} \subsetneq K \subsetneq K(x) \subset \mathbb{C}$ y $K(x)$ es una subextensión de ${}^{\mathbb{C}}/_{\mathbb{Q}}$. Afirmo que no tiene a α.

  En efecto, supongamos que $\alpha = \dfrac{f(x)}{g(x)}$ con $f, g \in K[X]$ coprimos, luego por ser algebraico sobre $\mathbb{Q}$ sabemos que existe $h \in \mathbb{Q}[X]$ no nulo tal que $h(\alpha) = 0$. En particular, si notamos $h_0, \ldots, h_n \in \mathbb{Q}$ a los coeficientes de h esto es equivalente a:

  $$h_0 + h_1 \frac{f(x)}{g(x)} + \cdots + h_n \frac{f^n(x)}{g^n(x)} = 0 \qquad h_0, \ldots, h_n \text{ no todos nulos}$$

  Luego:

  $$\begin{aligned} 0 =& h_0 g^n(x) + h_1 g^{n-1}(x) f(x) + \cdots + h_n f^n(x) \\ =& \left(h_0 g^n + h_1 g^{n-1} f + \cdots + h_n f^n\right)(x) \end{aligned}$$

  Y como $p = h_0 g^n + h_1 g^{n-1} f + \cdots + h_n f^n \in K[X]$ y x es trascendente sobre K concluimos que $p = 0$, veamos que esto deriva un absurdo. Notemos que $g | h_i g^{n-i} f^i$ para todo $0 \leq i < n$, luego como $g|0$ podemos afirmar que $g | h_n f^n$. Como $(g, f) = 1$ entonces concluimos que $g | h_n$ y luego por grados $\deg(g) \leq \deg(h_n) = 0$ ($h_n \in \mathbb{Q}$) de lo que concluimos que $\deg(g) = 0$ y $g \in K$. Similarmente sea j el menor índice tal que $h_j \neq 0$ y notemos que por definición $j \leq n$. Luego $f^{j+1} | h_k f^k g^{n-k}$ para todo $j+1 \leq k \leq n$, luego como $f^{j+1} | 0$ podemos afirmar que $f^{j+1} | h_j f^j g^{n-j}$ y cancelando obtenemos $f | h_j g^{n-j}$. Como $(g, f) = 1$ entonces concluimos que $f | h_j$ y luego por grados $\deg(f) \leq \deg(h_j) = 0$ ($h_j \in \mathbb{Q}$) de lo que concluimos que $\deg(f) = 0$ y $f \in K$. Luego, $\alpha \in K$ lo que resulta absurdo.Con esto demostramos que $\alpha \notin K(x)$

  Como K es maximal respecto a no tener a α uno obtiene que $K = K(x)$ lo que es absurdo que provino de suponer que x era trascendente. Concluimos que ${}^{\mathbb{C}}/_{K}$ es algebraico.

- Sea ${}^{M}/_{K}$ una subextension finita de ${}^{\mathbb{C}}/_{K}$ luego, por un lado, sabemos que $\alpha \in M$ por la maximalidad de K.

  Consideremos ${}^{\widetilde{M}}/_{K}$ la clasura normal de ${}^{M}/_{K}$, como ${}^{\mathbb{C}}/_{K}$ es separable y $\mathbb{C}$ es algebraicamente cerrado sabemos que ${}^{\widetilde{M}}/_{K}$ es una subextensión normal y separable de ${}^{\mathbb{C}}/_{K}$, luego Galois. Por ser Galois y $\alpha \notin K$ existe $\sigma \in Gal\left({}^{\widetilde{M}}/_{K}\right)$ tal que $\sigma(\alpha) \neq \alpha$. Luego ${}^{\widetilde{M}^{\langle\sigma\rangle}}/_{K}$ es una extensión tal que $\alpha \notin \widetilde{M}^{\langle\sigma\rangle}$. Por la maximalidad de K concluimos que $K = \widetilde{M}^{\langle\sigma\rangle}$ y entonces por el teorema de correspondencia de Galois esto es si y sólo si $\langle\sigma\rangle = Gal\left({}^{\widetilde{M}}/_{K}\right)$. Concluimos que ${}^{M}/_{K}$ es cíclico al ser subextensión de ${}^{\widetilde{M}}/_{K}$ que lo es.

- Dijimos que no habia que probarlo ∎

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 Einsenstein con $p = 2$ y su resolvente pues $\widehat{g} = x^3 + 2x + 4$ es irreducible en $\mathbb{F}_5$.

  Como el discriminante de g es $-4864 \notin \mathbb{Q}^2$ entonces concluimos que $Gal(g) \simeq Gal({}^{L}\big/_{\mathbb{Q}[\alpha]}) \simeq S_3$ con α raíz de f y $Gal(f) = Gal({}^{L}/_{\mathbb{Q}}) \simeq S_4$.

  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 $S_3 \simeq Gal({}^{L}\big/_{\mathbb{Q}[\alpha]}) \leq Gal({}^{L}/_{M}) \leq Gal({}^{L}/_{\mathbb{Q}}) \simeq S_4$ (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 $H \simeq S_4$.

  Concluímos que tal subextensión cuadrática M no puede existir. ∎