Mariano Negri

Problemas para practicar

Enunciados

Ejercicio 1. *Demostrar que existe $F \subseteq \mathbb{R}$ tal que $F/\mathbb{Q}$ es cíclica de orden n.*
Sugerencia: *Recordar el teorema de Dirichlet que Nico probó en clase.*

Ejercicio 2. *Sean $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ las raíces del polinomio $f = X^4 - X - 1 \in \mathbb{Q}[X]$. Sea L la extensión de $\mathbb{Q}$ generada por todos los productos $\alpha_i\alpha_j$ con $i \neq j$. Calcular $[L : \mathbb{Q}]$.*

Ejercicio 3. *Sea $f = X^5 - bX - a$ un polinomio irreducible de $\mathbb{Q}[X]$. Sea β una raíz de f y sea $E = \mathbb{Q}(\beta)$. Si se Sabe que $N_{E/\mathbb{Q}}(\beta + 1) = -77$ y $N_{E/\mathbb{Q}}(\beta - 1) = 83$, decidir si f es resoluble por radicales.*

Ejercicio 4.

1. *Sea p primo impar, y sea $G = Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ donde ξ_p es una raíz p-ésima primitiva de la unidad. Sea $H \leq G$. Definimos $\alpha := \sum_{\sigma \in H} \sigma(\xi_p)$. Demuestre que $\mathbb{Q}(\xi_p)^H = \mathbb{Q}(\alpha)$.*
2. *Hallar $\alpha \in \mathbb{Q}[\xi_{19}]$ tal que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 6$*
3. *Calcular $m(\xi_{19}, \mathbb{Q}[\alpha])$.*

Ejercicio 5. *Decidir si Φ_n es irreducible en $\mathbb{Q}[\sqrt[p]{5}][X]$ para cada primo $p > 2$ y cada n natural.*

Ejercicio 6. *Decidir si toda extensión $E/\mathbb{Q}$ de grado 4 admite una subextensión de grado 2.*

Ejercicio 7. *Sea α una raíz de $f = X^3 - X + 1 \in \mathbb{Q}[X]$*

1. *Probar que $\mathbb{Q}[\alpha^k] = \mathbb{Q}[\alpha]$ para todo $k \geq 1$.*
2. *Hallar $m(\alpha^4, \mathbb{Q})$. **Nota:** Quizás este item pueda tener que ver un poco más con la primer mitad de la materia.*

Ejercicio 8. *Sea $f = (X - a)(X - b)(X - c) \in K[X]$ irreducible, K de caracteristica distinta de 2.*

1. *Demuestre que $Desc(f/K) = K[a, \sqrt{Disc(f)}]$*
2. *Demuestre que $K[a]/K$ es normal sii $\sqrt{Disc(f)} \in K$*

Ejercicio 9.

1. *Decida si el discriminante de una cúbica irreducible puede tomar cualquier valor entero.*

2. *Decida si toda extensión cuadrática de $\mathbb{Q}$ está contenida en el cuerpo de descomposición de la familia $F = \{f \in \mathbb{Q}[X] : f$ es irreducible de grado 3$\}$*

Ejercicio 10. *Sea $\alpha \in \mathbb{C}$ una raíz de $X^3 + X + 1$. Decidir si $X^3 - X + 1$ tiene alguna raíz en $\mathbb{Q}(\alpha)$.*

Ejercicio 11. *Sea $\xi \in \mathbb{C}$ tal que $\xi^9 = 1$ pero $\xi^3 \neq 1$. Muestre que $\sqrt[3]{3} \notin \mathbb{Q}(\xi)$.*

Ejercicio 12. *Sea $f \in \mathbb{Q}[X]$ y $\xi \in \mathbb{C}$ una raíz de la unidad. Muestre que $f(\xi) \neq \sqrt[4]{2}$.*

Ejercicio 13.
1. *Demuestre que si una extensión F/K es separable y finita, entonces $Tr_{F/K}$ no es exactamente cero.*
2. *Encuentre una extensión F/K tal que $Tr_{F/K}$ sea exactamente 0*

Ejercicio 14.
1. *Calcular Φ_{18} y Φ_{90}*
2. *Sean $n, m \in \mathbb{Z}$. Probar que el polinomio:*

$$X^6 - (5n+1)X^3 + (5m+1)$$

es irreducible en $\mathbb{Q}[X]$.

Ejercicio 15.
1. *Demuestre usando la traza que si p y q son primos distintos entonces $\sqrt{p} \notin \mathbb{Q}(\sqrt[4]{q})$.*
2. *Sea $E = \mathbb{Q}[\sqrt{p}, \sqrt[4]{q}]$. Calcular $Tr_{E/\mathbb{Q}}(\sqrt{p^i}\sqrt[4]{q^j})$ para todo $i, j \geq 0$*

Ejercicio 16. *Sea K un cuerpo de q elementos, n coprimo con su característica. Sea $\xi_n \in \overline{K}$ raíz n-esima primitiva de la unidad.*

1. *Pruebe que $\xi_n + \xi_n^{-1} \in K$ sii $q \equiv \pm 1 \mod n$*
2. *Sea $\xi_7 \in \overline{\mathbb{F}_2}$ una raíz primitiva de la unidad. Calcular el minimal de $\xi_7 + \xi_7^{-1}$ en $\mathbb{F}_2$*

Ejercicio 17. *Sea Φ_{28} el ciclotómico de orden 28.*

1. *Factorizar $\Phi_{28}(X^{10})$ como producto de irreducibles en $\mathbb{Q}[X]$.*

   Sugerencia: *Vale que $\Phi_{np}(X) = \Phi_n(X^p)$ donde p es un primo tal que $p \mid n$*
2. *Determinar la cantidad de factores irreducibles de $\Phi_{28}(X^{10})$ como producto de irreducibles en $\mathbb{F}_{13}[X]$.*

Ejercicio 18.
1. *Sea $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X]$, mónico tal que todas sus raíces tienen valor absoluto 1. Probar que si $0 \leq r \leq n$, se tiene que $|a_r| \leq \binom{n}{r}$*
2. *Dado $n \in \mathbb{N}$, probar que hay finitos enteros algebraicos de grado n, tales que todos sus conjugados (incluyendo él mismo) tienen valor absoluto 1.*
3. *Probar que un elemento como en el item anterior es una raíz de la unidad.*

Soluciones

Solución 1. Por el teorema de Dirichlet probado por Nico en clase, tenemos que existe un primo p tal que $2n \mid (p-1)$.

Sea ξ_p una raíz p-ésima primitiva de la unidad. Consideremos $K = \mathbb{Q}[\xi_p]$, cuyo grupo de Galois es isomorfismo a C_{p-1}.

Notemos que la conjugación compleja restringida a K es un automorfismo no trivial de $Gal(K/\mathbb{Q})$, sea H el subgrupo de orden 2 generado por este elemento y consideremos $L := K^H$ el cuerpo fijo por H. Este cuerpo está contenido en $\mathbb{R}$ porque obviamente ningún elemento que no esté en $\mathbb{R}$ queda fijo por H. Notemos además que L es una subextensión de grado $(p-1)/2$ (pues este es el índice de H en el grupo de Galois de K), es Galois (pues $Gal(K/\mathbb{Q})$ es abeliano) y además el grupo de Galois de L es $Gal(L/\mathbb{Q}) = Gal(K/\mathbb{Q})/H$ que es cíclico por ser cociente de un cíclico.

Como n divide a $(p-1)/2$ y L es cíclico de este orden, existe un grupo H' de L' de índice n. Finalmente sea $L^{H'}$, es una subextensión de orden n con grupo de galois $Gal(L^{H'}/\mathbb{Q}) = Gal(L/\mathbb{Q})/H' \cong C_n$ ya que, nuevamente, cociente de un cíclico es cíclico.

□

Solución 2. *Gracias Agus Marchionna por la solución más sencilla!*

Consideremos $F = Q(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, es decir el cuerpo de descomposición de $X^4 - X - 1$. Veamos que su grupo de Galois es $\mathbb{S}_4$.

Primero observemos que se trata de un polinomio irreducible porque mirandolo modulo 2 queda x^4+x+1 (no tiene raíces en $\mathbb{F}_2$, el único polinomio de grado 2 irreducible módulo 2 es x^2+x+1, pero $(x^2+x+1)^2 = x^4+x^2+1$).

Recordemos que Nico en clase mostró que la resolvente cúbica de un polinomio cuártico $X^4 + AX^3 + BX^2 + CX^3 + D$ es $X^3 - BX^2 + (AC - 4D)X - (A^2D + C^2 - 4BD)$.

En el caso especial de $A = B = 0$, o sea $f = X^4 + CX + D$, obtenemos que la resolvente cúbica es $X^3 - 4DX - C^2$. En nuestro caso tenemos que la cúbica resolvente es $X^3 + 4X - 1$ que es irreducible porque 1 y -1 no son raíces. Por el ejercicio 1.c de la práctica 7 podemos calcular el discriminante del polinomio f, ya que coincide con el discriminante de su resolvente cúbica. Es -283 y claramente no es un cuadrado en $\mathbb{Q}$.

Recordemos que si f es cuartica irreducible, separable, su cúbica resolvente es irreducible y su discriminante no es un cuadrado entonces el grupo de Galois de su cuerpo de descomposición es $\mathbb{S}_4$ (probado por Nico en la práctica). Esto es lo que queriamos probar.

Notemos ahora que en L tenemos a $\frac{(\alpha_1\alpha_2)(\alpha_1\alpha_3)}{\alpha_2\alpha_3}$ que es $\alpha_1^2 \in L$. Entonces tenemos a $\alpha_1^4 = \alpha_1 + 1$ de donde $\alpha_1 \in L$. Ya con esto tenemos que α_2, α_3 y α_4 están en L, lo que nos dice que $L = F$, o sea $[L : \mathbb{Q}] = 24$.

Otra forma mas terrenal: Sea $E = \mathbb{Q}[\alpha_1\alpha_2 + \alpha_2\alpha_3, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3]$ que es una subextensión de L y es el cuerpo de descomposición de la cúbica resolvente. Ya sabemos que este cuerpo tiene grupo de Galois isomorfo a S_6 porque es irreducible y su discriminante no es un cuadrado. Además, es el cuerpo fijo por $H = \{Id, (12)(34), (13)(24), (14)(23)\}$ como probó Nico. Notemos que $[F : L] = 1$ ó 4 ya que si $[F : L] = 2$ entonces $[F : \mathbb{Q}] = 12$ luego F sería el cuerpo fijo por un elemento de orden 2 en S_4. Recordemos que toda permutación se escribe como producto de ciclos disjuntos, y más aún el orden de un producto de ciclos disjuntos es igual al mínino común multiplo del orden de los ciclos. Entonces todos los elementos generadores de L deberían quedar fijos por alguno de las siguientes permutaciones:

$(12)(34), (13)(24), (14)(23), (12), (34), (13), (24), (14), (23)$ (que son todas las permutaciones de orden 2). Es claro que algún $\alpha_i\alpha_j$ siempre se mueve por alguna de estas permutaciones, así que concluimos que $[F : L] = 4$ ó 1. Pero entonces $[L : E] = 4$ ó 1, pero si fuese 1 los generadores de L quedarían fijos por los elementos de H y esto no pasa! concluimos que $[L : F] = 4$, y luego $[L : \mathbb{Q}] = 24$

□

Solución 3. Recordemos que probamos en clase que si K es un cuerpo, $f \in K[X]$ irreducible de grado n y $\beta \in K$ una raíz de f, entonces para todo $c \in K$ se tiene que $N_{K[\beta]/K}(\beta - c) = (-1)^n f(c)$. En este caso, $-77 = N_{\mathbb{Q}[\beta]/\mathbb{Q}}(\beta - (-1)) = (-1)^5 f(-1) = -(-1+b-a) = 1-b+a$ y por otro lado $83 = N_{\mathbb{Q}[\beta]/\mathbb{Q}}(\beta-1) = (-1)^5 f(1) = -(1-b-a) = -1+b+a$. Esto nos da un sistema de ecuaciones sencillo:

$$\begin{cases} 84 = b + a \\ -78 = -b + a \end{cases}$$

La solución de este sistema es $a = 3$, $b = 81$, o sea el polinomio es $X^5 - 81X - 3$. Veamos que el grupo de Galois del cuerpo de descomposición de este polinomio es $\mathbb{S}_5$. Notemos que el grado del polinomio es primo, luego sabemos que hay un 5-ciclo. Por un ejercicio de la práctica 7, sabemos que si encontramos un 2-ciclo entonces el grupo de Galois será $\mathbb{S}_5$.

Para ello, vamos a demostrar que la conjugación compleja es una trasposición. Primero que nada, debemos ver que el polinomio tiene raíces complejas. En efecto, podemos calcular el discriminante del polinomio via el ejercicio 2.*b* de la práctica 7:

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2}(n^n a^{n-1} + (1-n)^{n-1} b^n) = 5^5 3^4 - 4^4 81^5 < 0$$

Si todas las raíces fueran reales, como el discriminante es $\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2$ tendriamos que sería positivo, pero en este caso es negativo lo cual demuestra que este polinomio tiene raíces complejas.

Ahora, si demostramos que f tiene al menos dos raíces reales, terminamos porque esto demostraría que f tiene solo dos raíces complejas luego la conjugación es una transposición.

Hay varias maneras de hacer esto, podemos derivar y queda $f' = 5X^4 - 81$, esto nos ayuda a hacer un análisis de función facilmente (notemos que esto también nos habría ayudado a descubrir que hay exactamente 2 raíces complejas), sin embargo un análisis a ojo alcanza. Notemos que $f(-1) > 0$, $f(0) < 0$ y $\lim_{x\to\infty} f = +\infty$, luego por Bolzano sabemos que hay al menos dos ceros reales.

Otra forma es notar que en una quíntica irreducible, si el discriminante es negativo entonces tiene exactamente 2 raíces complejas y 3 raíces reales.

Por lo tanto el grupo de Galois del cuerpo de descomposición de f es $\mathbb{S}_5$ que es un grupo no soluble.

□

Solución 4.

1. Ver Dummit & Foote pág. 597
2. Nos gustaria encontrar un subgrupo de índice 6 en $Gal(\mathbb{Q}(\xi_{19})/\mathbb{Q})$ ya que el cuerpo fijo de este subgrupo sería de grado 6 y podriamos encontrar un elemento primitivo con el inciso anterior.

$\mathbb{Z}/19\mathbb{Z}$ es un cuerpo, al ser 19 primo, así que $(\mathbb{Z}/19\mathbb{Z})^\times$ es cíclico de orden 18. Podemos chequear a mano que 2 es de orden 18 (o sea chequear que 2^2, 2^3, 2^6, 2^9 no dan 1). Por lo tanto, $2^6 = 7$ es un elemento de orden 3 en $(\mathbb{Z}/19\mathbb{Z})^\times$ (o sea el grupo que genera es de índice 6).

Tenemos que el automorfismo ψ_7 que manda $\xi_{19} \mapsto \xi_{19}^7$, genera $H =: \langle \psi_7 \rangle$ grupo de índice 6. Es decir, $\mathbb{Q}(\xi_{19})^H$ es un cuerpo de grado 6 sobre $\mathbb{Q}$. Queremos encontrar un generador de este cuerpo. Por el inciso anterior $\alpha = \xi_{19} + \sigma_7(\xi_{19}) + \sigma_7^2(\xi_{19})$ es invariante por σ_7, o sea está en el cuerpo fijo que hallamos y más aún $\alpha = \xi_{19} + \xi_{19}^7 + \xi_{19}^{11}$ genera a este cuerpo.

3. Nos piden calcular el $m(\xi_{19}, \mathbb{Q}[\alpha])$. Como $Gal(\mathbb{Q}(\xi_{19}), \mathbb{Q}) = H = \langle \psi_7 \rangle$ entonces el minimal es $(x - \xi_{19})(x - \psi_7(\xi_{19}))(x - \psi_7^2(\xi_{19})) = (x - \xi_{19})(x - \xi_{19}^7)(x - \xi_{19}^{11}) = x^3 - \alpha x^2 + \overline{\alpha} x - 1$.

□

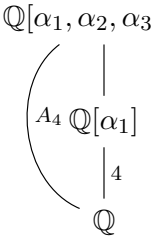
Solución 5. Supongamos que Φ_n es reducible en $\mathbb{Q}[\sqrt[p]{5}]$. Como Φ_n es irreducible en $\mathbb{Q}$, algún coeficiente de algún factor de la descomposición en irreducibles de Φ_n sobre $\mathbb{Q}[\sqrt[p]{5}]$ debe estar en $\mathbb{Q}[\sqrt[p]{5}] \setminus \mathbb{Q}$. Pero como los coeficientes de un polinomio no son más que sumas y productos de las raíces, resulta que un elemento de la forma $a_0 + a_1 \sqrt[p]{5} + ... + a_{p-1} \sqrt[p]{5^{p-1}}$ con al menos un $a_i \neq 0$, donde $i > 0$, está en $\mathbb{Q}[\xi_n]$.

Llamemos $\alpha = a_0 + a_1 \sqrt[p]{5} + ... + a_{p-1} \sqrt[p]{5^{p-1}}$. Resulta entonces que $\mathbb{Q}[\alpha]$ es una subextensión de $\mathbb{Q}[\xi_n]$. Pero además $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt[p]{5}]$, pues es también una subextensión de $\mathbb{Q}[\sqrt[p]{5}]$ y como $[\mathbb{Q}[\sqrt[p]{5}] : \mathbb{Q}] = p$, la unica posibilidad es que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 1$ ó p. Que el grado sea 1 no puede ser pues ya dijimos que $\alpha \notin \mathbb{Q}$ así que concluimos que el grado de la extensión es p, con lo cual $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt[p]{5}]$

Finalmente, como $Gal(\mathbb{Q}[\xi_n]/\mathbb{Q})$ es abeliano y por tanto todo subgrupo es normal, resulta que toda subextensión es también normal. Esto nos diria que $\mathbb{Q}[\sqrt[p]{5}]$ es normal, lo cual es obviamente falso si $p > 2$. Concluimos que Φ_n es irreducible para todo n y $p > 2$.

□

Solución 6. La respuesta es no. Recordemos que Nico probó en clase que si un polinomio $f \in K[x]$ cuártico es irreducible, separable, su cúbica resolvente es irreducible y su discriminante es un cuadrado en K, entonces el grupo de Galois de su cuerpo de descomposición es A_4. Entonces, si $\alpha_1, \alpha_2, \alpha_3$ y α_4 son las raíces de f estariamos en la situación siguiente:



Si $\mathbb{Q}[\alpha_1]$ admitiese una subextensión cuadrática entonces también lo haría $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ pero esto diría que A_4 tiene un subgrupo de índice 2, pero A_4 no tiene ningun subgrupo de orden 6.

Otra forma de pensar este problema es con el ejercicio de la práctica 7 que nos dice que un número real α es construible sii α es algebraico sobre $\mathbb{Q}$ y el grado de la clausura

normal de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$ es una potencia de 2. Entonces con encontrar un polinomio de grado 4 irreducible tal que el grupo de Galois de su cuerpo de descomposición sea S_4 o A_4 ya estamos porque sus grados sobre $\mathbb{Q}$ no son potencias de 2, luego las raíces de este polinomio no son construibles. Como $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$, si $\mathbb{Q}(\alpha)$ tuviera una subextensión de grado 2, entonces sería construible lo cual contradice lo que dijimos.

Para dar un ejemplo concreto, recordemos el ejercicio $1.c$ de la práctica 7 nos dice que si $f=X^4+bX^2+c$, entonces $Disc(f)=16c(4c-b^2)^2$. Tomamos entonces por ejemplo $f=X^4+X^2+1$ es irreducible en $\mathbb{Q}[x]$ y tiene resolvente cúbica X^3-X^2-4X+4 que también es irreducible en $\mathbb{Q}[X]$. Finalmente, su discriminante es 16.3^2, que es un cuadrado.

□

Solución 7. 1. Notemos que f es irreducible porque ± 1 no son raíces. Entonces $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$. Como $\mathbb{Q}(\alpha^k)\subseteq\mathbb{Q}(\alpha)$, solo nos resta ver que $[\mathbb{Q}(\alpha^k):\mathbb{Q}]=3$. Notemos que $[\mathbb{Q}(\alpha^k):\mathbb{Q}]\leq 3$ así que vamos a descartar los casos en donde el grado sea 2 ó 1.

Descartemos el caso $[\mathbb{Q}(\alpha^k):\mathbb{Q}]=2$. Si así fuera, tendriamos que $[\mathbb{Q}(\alpha,\alpha^k):\mathbb{Q}]=6$, pero $\mathbb{Q}(\alpha,\alpha^k)=\mathbb{Q}(\alpha)$ que es de grado 3 sobre $\mathbb{Q}$ absurdo.

Descartemos el caso de que $[\mathbb{Q}(\alpha^k):\mathbb{Q}]=1$. Si así fuera, tendriamos que $\alpha^k\in\mathbb{Q}$. Por un lado $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)=-1$ (es el coeficiente independiente de su minimal por $(-1)^3$) y por otro lado como $\alpha^k\in\mathbb{Q}$ tendriamos que $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^k)=\alpha^{3k}$. Ahora, por la multiplicatividad de la norma, tenemos que $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^k)=N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^k=(-1)^k$, por lo tanto $\alpha^{3k}=(-1)^k$ de donde elevando al cuadrado obtenemos que $\alpha^{6k}=1$, es decir α es una raíz primitiva de la unidad para algún n. Sin embargo, no existe n tal que $\phi(n)=3$, de hecho es una función par excepto para 1 y 2 que da 1. Esto es absurdo.

Concluimos que $[\mathbb{Q}(\alpha^k):\mathbb{Q}]=3$ como queriamos.

2. Ahora, ya sabemos que $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha^4)$, entonces una base como $\mathbb{Q}$-E.V de $\mathbb{Q}(\alpha^4)$ es $B=\{1,\alpha,\alpha^3\}$. Podemos calcular el polinomio caractestíco de L_{α^4} que anula a α^4.

$1\mapsto\alpha^4=\alpha^3.\alpha=(\alpha-1)\alpha=\alpha^2-\alpha$

$\alpha\mapsto\alpha^5=\alpha^3.\alpha^2=(\alpha-1)\alpha^2=-\alpha^2-1+\alpha$

$\alpha\mapsto\alpha^6=\alpha^3.\alpha^3=(\alpha-1)(\alpha-1)=x^2-2\alpha+1$

Entonces la matriz en la base B de esta T.L. es

$$M=\begin{pmatrix}0&-1&1\\-1&1&-2\\1&-1&1\end{pmatrix}$$

Calculamos el polinomio característico $det(M-xI)=-x^3+2x^2+3x+1$. Es un polinomio de grado 3 y $m(\alpha^k,\mathbb{Q})$ lo divide así que este debe ser el polinomio minimal.

□

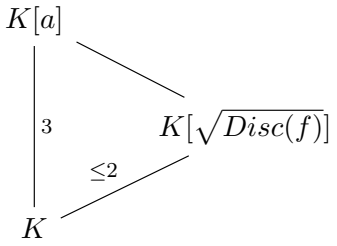
Solución 8. 1. Notemos que $\sqrt{Disc(f)}=(a-b)(a-c)(b-c)$ por lo tanto $K[a,b,c]$ obviamente contiene a $K[a,(a-b)(a-c)(b-c)]$ asi que debemos ver que $K[a,b,c]\subseteq K[a,\sqrt{Disc(f)}]$.

Notemos que como $(x-a)|f$ en $K[a][X]$, entonces $(X-b)(X-c) \in K[a][X]$. Por lo tanto evaluando en a obtenemos que $(a-b)(a-c) \in K[a]$. Por lo tanto, $(b-c) = \frac{\sqrt{Disc(f)}}{(a-b)(a-c)} \in K[a, \sqrt{Disc(f)}]$. Como $a+b+c$ es un coeficiente de f, luego está en K, por lo tanto tenemos que $b+c \in K[a, \sqrt{Disc(f)}]$.

Como $b+c \in K[a, \sqrt{Disc(f)}]$ y $b-c \in K[a, \sqrt{Disc(f)}]$, obtenemos que b y c están en $K[a, \sqrt{Disc(f)}]$ (notemos que aquí usamos que la característica no es 2, pues sino $2b$ y $2c$ serían 0).

2. $\Leftarrow$) Si $\sqrt{Disc(f)} \in K$ entonces $Desc(f/K) = K[a, \sqrt{Disc(f)}] = K[a]$, por ser cuerpo de descomposición es normal.

   $\Rightarrow$) Como $K[a]$ es normal, entonces $K[a] = K[a, b, c]$. Entonces $K[\sqrt{Disc(f)}]$ es un subcuerpo de $K[a]$, o sea tenemos una torre así:



   Pero $[K[\sqrt{Disc(f)} : K]$ no puede ser 2 porque $2 \nmid 3$. Luego $\sqrt{Disc(f)} \in K$

□

Solución 9. 1. La respuesta es no.

Por el ejercicio anterior, sabemos que el cuerpo de descomposición de un polinomio cúbico irreducible f es $\mathbb{Q}[\alpha, \sqrt{Disc(f)}]$ con α raíz de f. El discriminante de una cúbica es igual al de su cuadrática resolvente, y notemos que el discriminante de una cuadratica es $b^2 - 4ac$, que nunca puede ser un número de la forma $4k+3$ pues $b^2 \equiv 1$ ó $0 \mod 4$.

2. Según el profesor que me lo tomó, es verdad. La proto-idea es armar polinomios de la forma $X^3 + p.aX + p.a$ y similares (para que queden irreducible por Eisenstein) y mirar la raíz del discriminante de estos polinomios (lo cual tiene sentido por el ejercicio anterior) y tratar de encontrar todos las raíces cuadradas de los números primos y a i combinando convenientemente. Queda vacante la solución!. Un desafio...

□

Solución 10. La respuesta es que no.

Primero que nada, notemos que ambos polinomios son irreducibles pues ± 1 no son raíces. Supongamos que $X^3 - X + 1$ tiene alguna raíz en $\mathbb{Q}(\alpha)$ con α raíz de $X^3 + X + 1$. Sea K el cuerpo de descomposición $X^3 + X + 1$ sobre $\mathbb{Q}$. Supongamos que α,β y γ son las raíces de $X^3 + X + 1$. Entonces $K = \mathbb{Q}[\alpha, \beta, \gamma]$

Veamos que ambos polinomios se descomponen linealmente en K. Obviamente $X^3 + X + 1$ se descompone linealmente en K. Veamos que pasa con $X^3 - X + 1$. Tenemos que $X^3 - X + 1 = (X - f(\alpha))g(X)$ donde $f(X)$ es un polinomio de grado a lo sumo 2 en $\mathbb{Q}[X]$ (pues $\mathbb{Q}(a)$ es extesión de grado 3 sobre $\mathbb{Q}$, luego 1,α,α^2 es una base) y $g(X)$ un

polinomio en $K[X]$. Como $Gal(K/\mathbb{Q})$ actua transitivamente sobre las raíces de X^3+X+1 por ser este irreducible, tenemos que existen $\sigma_1 : \alpha \mapsto \beta$ y $\sigma_2 : \alpha \mapsto \gamma \in Gal(K/\mathbb{Q})$ tales que $\sigma_1(X^3 - X + 1) = X^3 - X + 1 = (X - f(\beta))\sigma_1(g(X))$ y también $\sigma_2(X^3 - X + 1) = X^3 - X + 1 = (X - f(\gamma))\sigma_2(g(X))$. Pero entonces tenemos que en K, $X^3 - X + 1$ tiene a $f(\alpha)$, $f(\beta)$ y $f(\gamma)$ como raíces, y no puede ocurrir que las 3 sean iguales, porque un polinomio de grado 2 que coincide en 3 puntos distintos debe ser constante. Luego hay dos raíces distintas de $X^3 - X + 1$ en K y luego se descompone linealmente allí como habiamos anticipado, o sea K sería el cuerpo de descomposición tanto de $X^3 + X + 1$ y $X^3 - X + 1$.

Por último, notemos que esto nos diría que $\mathbb{Q}[Disc(X^3 + X + 1), Disc(X^3 - X + 1)] = \mathbb{Q}(\sqrt{-31}, \sqrt{-23})$ es un subcuerpo de K, pero $[\mathbb{Q}(\sqrt{-31}, \sqrt{-23}) : \mathbb{Q}] = 4$, y $[F : K] = 6$ (porque el discriminante no es un cuadrado) lo cual es absurdo porque $4 \nmid 6$.

□

Solución 11.

Notemos que ξ es una raíz primitiva novena de la unidad, porque las raíces novenas de la unidad las podemos escribir como $G_9 = G_1^* \sqcup G_3^* \sqcup G_9^* = G_3 \sqcup G_9^*$.

Por tanto $\mathbb{Q}(\xi)$ es en verdad la extensión ciclotómica generada por una raíz primitiva novena de la unidad. Si $\sqrt[3]{3} \in \mathbb{Q}(\xi)$ entonces $\mathbb{Q}(\sqrt[3]{3})$ sería una subextensión, pero esta no es normal lo cual no puede ser porque el grupo de Galois de una extensión ciclotómica es abeliano.

□

Solución 12. Si existiera $f \in \mathbb{Q}[X]$ y $\xi \in \mathbb{C}$ una raíz de la unidad tal que $f(\xi) = \sqrt[4]{2}$, entonces tendríamos que $\mathbb{Q}(\sqrt[4]{2})$ es una subextensión de $\mathbb{Q}(\xi_n)$ donde ξ_n es una raíz primitiva n-ésima de la unidad (pues ξ es raíz primitiva de la unidad para algún n) .

Ahora, sabemos que el grupo de Galois de $\mathbb{Q}(\xi_n)$ es abeliano, luego todas sus subextensiones deben ser normales. Sin embargo $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es normal.

□

Solución 13. 1. Es una aplicación de la independencia de caracteres. Recordemos que

$$Tr_{F/K}(\alpha) = [F : K]_{ins} \sum_{\sigma \in Hom(F/K, \overline{K}/K)} \sigma(\alpha)$$

Como la extensión es separable tenemos que $[F : K]_{ins} = 1$, luego

$$Tr_{F/K}(\alpha) = \sum_{\sigma \in Hom(F/K, \overline{K}/K)} \sigma(\alpha)$$

Luego, si fuera la traza fuera 0 para todo α tendriamos

$$\sum_{\sigma \in Hom(F/K, \overline{K}/K)} \sigma = 0$$

lo cual no puede ser por el teorema de la independencia de caracteres.

2. Recordemos que que si F/K no es extensión separable entonces $Tr_{F/K} = 0$ porque $[F : K]_{ins} = p^s$ para $s \in \mathbb{N}$ con p primo la característica de K.

   Podemos tomar entonces $F = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^p)$ con p primo y t trascendente sobre $\mathbb{F}_p$. Su grado de inseparabilidad es p pues $m(t, K)(X) = X^p - t^p$ es irreducible en K, pero en F es $(X - t)^p$.

   Concluimos que la traza de esta extensión es identicamente cero.

□

Solución 14. 1. Recordemos de la guía 6 que $\Phi_{p_1.p_2^2} = \Phi_{p_1.p_2}(X^{p_2})$. En nuestro caso $\Phi_{18}(X) = \Phi_6(X^3)$.

   Por otro lado, recordemos de la guía 6 que si n impar entonces $\Phi_{2n}(X) = \Phi_n(-X)$. Luego, $\Phi_6(X) = \Phi_3(-X)$. Por lo tanto $\Phi_{18}(X) = \Phi_6(X^3) = \Phi_3(-X^3)$, como $\Phi_3 = X^2 + X + 1$, tenemos que $\Phi_{18} = X^6 - X^3 + 1$.

   Por otro lado $90 = 18.5$, luego también por ejercicio de la guía 6 tenemos $\Phi_{90}(X) = \frac{\Phi_{18}(X^5)}{\Phi_{18}(X)} = \frac{X^{30}-X^{15}+1}{X^6-X^3+1}$. Si hacemos la división queda $x^{24}+x^{21}-x^{15}-x^{12}-x^9+x^3+1$.

2. Miremos $X^6 - (5n + 1)X^3 + (5m + 1)$ en $\mathbb{F}_5$. Queda $X^6 - X^3 + 1 = \Phi_{18}$. Luego si probamos que Φ_{18} es irreducible en $\mathbb{F}_5$ ya está, por ejercicio de la guía 0.

   Por un ejercicio de la práctica 6, esto es lo mismo que ver que 5 tiene orden $\phi(18) = 6$ en $(\mathbb{Z}/18\mathbb{Z})^\times$. Chequeemos que esto es así. $5^2 \equiv 7 \mod 18$, $5^3 \equiv 17 \mod 18$, $5^4 \equiv 13 \mod 18$, $5^5 \equiv 11 \mod 18$, $5^6 \equiv 1 \mod 18$. Así que concluimos lo que queriamos.

□

Solución 15. 1. Primero sea $K = \mathbb{Q}(\sqrt[4]{q})$. Una base de este espacio es $B = \{1, \sqrt[4]{q}, \sqrt[4]{q^2}, \sqrt[4]{q^3}\}$.

   Notemos que $Tr_{K/\mathbb{Q}}(\sqrt[4]{q}) = 0$ pues el minimal sobre $\mathbb{Q}$ de $\sqrt[4]{q}$ es $X^4 - q$.

   También $Tr_{K/\mathbb{Q}}(\sqrt[4]{q^2}) = 0$ pues el minimal sobre $\mathbb{Q}$ es $x^2 - q$.

   Por último, veamos que $Tr_{K/\mathbb{Q}}(\sqrt[4]{q^3}) = 0$. Para esto calculemos la matriz de $L_{\sqrt[4]{q^3}}$ en la base B.

   $1 \mapsto \sqrt[4]{q^3}$

   $\sqrt[4]{q} \mapsto \sqrt[4]{q^4} = q$

   $\sqrt[4]{q^2} \mapsto \sqrt[4]{q^5} = q\sqrt[4]{q}$

   $\sqrt[4]{q^3} \mapsto \sqrt[4]{q^6} = q\sqrt[4]{q^2}$

   Entonces la matriz en la base B de esta T.L. es

$$[L]_B = \begin{pmatrix} 0 & q & 0 & 0 \\ 0 & 0 & q & 0 \\ 0 & 0 & 0 & q \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

   cuya traza es 0.

   Ahora, supongamos que $\sqrt{p} = a + b\sqrt[4]{q} + c\sqrt[4]{q^2} + d\sqrt[4]{q^3}$ para llegar a un absurdo.

Tomando traza a ambos lados obtenemos

$Tr_{K/\mathbb{Q}}(\sqrt{p}) = aTr_{K/\mathbb{Q}}(1) + bTr_{K/\mathbb{Q}}(\sqrt[4]{q}) + cTr_{K/\mathbb{Q}}(\sqrt[4]{q^2}) + dTr_{K/\mathbb{Q}}(\sqrt[4]{q^3})$

Como el minimal de $\sqrt{p}$ es $x^2 - p$ por Eisenstein, entonces $Tr_{K/\mathbb{Q}}(\sqrt{p}) = 0$. Por ende, nos queda $0 = a[K : \mathbb{Q}]$, con lo cual $a = 0$.

De esta forma tenemos que $\sqrt{p} = b\sqrt[4]{q} + c\sqrt[4]{q^2} + d\sqrt[4]{q^3}$.

Ahora veamos que $d = 0$. Si multiplicamos a ambos lados por $\sqrt[4]{q}$ obtenemos que $\sqrt{p}\sqrt[4]{q} = b\sqrt[4]{q^2} + c\sqrt[4]{q^3} + d.q$. Tomando traza otra vez, y viendo que el minimal de $\sqrt{p}\sqrt[4]{q}$ sobre $\mathbb{Q}$ es $X^4 - p^2q$ (irreducible por Eisenstein con q), tenemos que todo se anula salvo $d.q.Tr_{K/\mathbb{Q}}(1)$, queda $0 = d.q.[K : \mathbb{Q}]$ luego $d = 0$.

Veamos ahora que $c = 0$. Tenemos que $\sqrt{p} = b\sqrt[4]{q} + c\sqrt[4]{q^2}$. Multiplicamos a ambos lados por $\sqrt[4]{q^2}$, obtenemos que $\sqrt{p.q} = b\sqrt[4]{q^3} + c.q$. Tomando norma otra vez, como el minimal de $\sqrt{p.q}$ es $X^2 - \sqrt{p.q}$ tenemos que la traza de ese elemento es 0, de la misma forma que antes entonces obtenemos que $c = 0$.

De esta forma llegamos a que $\sqrt{p} = b\sqrt[4]{q}$. Esto es absurdo porque elevando al cuadrado obtenemos que $p = b\sqrt{q}$.

2. Sea $\alpha = \sqrt{p^i}\sqrt[4]{q^j}$. Consideramos la misma extensión intermedia K del item anterior. Veamos que si $i \equiv 1 \mod 2$, entonces $Tr_{E/K}(\alpha) = 0$. Notemos que $X^2 - p^i\sqrt{j} \in K[X]$ anula a α. Ahora, las raíces de este polinomio son $\pm\sqrt{p^i}\sqrt[4]{j}$, que no están en $K[X]$ sii $i \equiv 1 \mod 2$ por lo que probamos en el item 1 de este ejercicio. Luego este polinomio es irreducible y por tanto $Tr_{E/K}(\alpha) = 0$. Por la transitividad de la traza, esto significa que $Tr_{E/\mathbb{Q}}(\alpha) = 0$.

Veamos que pasa si $i \equiv 0 \mod 2$. En este caso, tenemos que $Tr_{E/\mathbb{Q}}(\alpha) = p^{i/2}Tr_{E/\mathbb{Q}}(\sqrt[4]{q^j})$

Nos falta ver que pasa con $Tr_{E/\mathbb{Q}}(\sqrt[4]{q^j})$. Digo que si $j \equiv 1, 2, 3 \mod 4$ entonces $Tr_{E/\mathbb{Q}}(\sqrt[4]{q^j}) = 0$. Pero esto es equivalente a ver que $Tr_{K/\mathbb{Q}}(\sqrt[4]{q^j}) = 0$, porque por transitividad de nuevo, si $Tr_{K/\mathbb{Q}}(\sqrt[4]{q^j}) = 0$, entonces

$$Tr_{E/\mathbb{Q}}(\sqrt[4]{q^j}) = Tr_{K/\mathbb{Q}}(Tr_{E/K}(\sqrt[4]{q^j})) = [E : K]Tr_{K/\mathbb{Q}}(\sqrt[4]{q^j})$$

Pero notemos que si $j \equiv 1 \mod 4$ esto es lo mismo que calcular $q^k.Tr_{K/\mathbb{Q}}(\sqrt[4]{q})$ y ya vimos $Tr_{K/\mathbb{Q}}(\sqrt[4]{q}) = 0$.

De manera análoga se prueba que si $j \equiv 2$ ó $3 \mod 4$ entonces $Tr_{K/\mathbb{Q}}(\sqrt[4]{q^j}) = 0$.

En resumen, si $i \equiv 1 \mod 2$ entonces la $Tr_{E/\mathbb{Q}}(\alpha) = 0$.

Si $i \equiv 0 \mod 2$ y $j \equiv 1, 2, 3 \mod 4$, entonces $Tr_{E/\mathbb{Q}}(\alpha) = 0$.

Si $i \equiv 0 \mod 2$ y $j \equiv 0 \mod 4$, entonces tenemos que $Tr_{E/\mathbb{Q}}(\alpha) = p^{i/2}q^{j/4}Tr_{E/\mathbb{Q}}(1) = p^{i/2}q^{j/4}[E : \mathbb{Q}] = 8p^{i/2}q^{j/4}$.

□

Solución 16. 1. *Gracias Juan Piombo por la idea de la ida!* $\Rightarrow$) Veamos que ξ_n está en $\mathbb{F}_{q^2}$. En efecto, tenemos que $f := (X - \xi_n)(X + \xi_n^{-1}) = X^2 - (\xi_n + \xi_n^{-1})X + 1 \in \mathbb{F}_q[X]$. Este polinomio puede ser el minimal de ξ_n sobre $\mathbb{F}_q$, o no serlo (es decir puede ser irreducible o no). Supongamos que es irreducible. Tenemos que

$f = (X - \xi_n)(X - Frob_q(\xi_n))$ Entonces $\xi_n^{-1} = \xi_n^q$ lo que nos dice que $1 = \xi_n^{q+1}$ y como n es por definición el orden de ξ_n, tenemos que $n \mid q+1$.

Por otro lado, si este no fuera el minimal entonces $\xi_n \in \mathbb{F}_q$, luego $\xi_n^{q-1} = 1$ y por lo tanto $n \mid q-1$. Concluimos lo que queriamos.

$\Leftarrow$) Si $q \equiv \pm 1 \mod n$ entonces Al ser $\mathbb{F}_{q^2}^\times$ cíclico de orden q^2-1, y $n|q^2-1$, tenemos que existe un elemento de orden n en $\mathbb{F}_{q^2}$. Es decir, existe una raíz n-ésima primitiva de la unidad en $\mathbb{F}_{q^2}$, que llamamos ξ_n. Ahora veamos que $\xi_n + \xi_n^{-1} \in \mathbb{F}_q$. Notemos que, $n \mid q+1$ ó $n \mid q-1$. Si $n \mid q+1$ entonces $1 = \xi_n^{q+1} = \xi_n^q.\xi_n$ con lo cual $\xi_n^q = \xi_n^{-1}$, de esta forma $(\xi_n + \xi_n^{-1})^q = \xi_n^q + \xi_n^{-q} = \xi_n^{-1} + \xi_n$, o sea $\xi_n + \xi_n^{-1} \in \mathbb{F}_q$.

Si $n \mid q-1$, ya está porque esto ya significa que $\xi_n^{q-1} = 1$, o sea $\xi_n \in \mathbb{F}_q^\times$, y luego trivialmente ocurre que $\xi_n + \xi_n^{-1} \in \mathbb{F}_q$

2. Notemos que $2^3 \equiv 1 \mod 7$, y esta es la primer potencia que hace que esto suceda, por el item anterior sabemos que $\xi_7 + \xi_7^{-1} \in \mathbb{F}_8$, o sea es raíz de $x^8 - x \in \mathbb{F}_2[X]$. Recordemos que en la factorización en irreducibles solo apareceran polinomios de grado 1 y 3 (o sea que dividen a 3) En este caso $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

   Debemos decidir cual de estos dos polinomios cúbicos que aparecieron es el minimal de $\xi_7 + \xi_7^{-1}$. Digo que es $x^3 + x^2 + 1$. Veamos que $\xi_7 + \xi_7^{-1}$ es raíz.

   primero, $(\xi_7 + \xi_7^{-1})^2 = \xi_7^2 + \xi_7^{-2}$

   Por otro lado, $(\xi_7 + \xi_7^{-1})^3 = (\xi_7^2 + \xi_7^{-2})(\xi_7 + \xi_7^{-1}) = \xi_7^3 + \xi_7^{-1} + \xi_7 + \xi_7^{-3}$

   Luego:

   $$(\xi_7+\xi_7^{-1})^3+(\xi_7+\xi_7^{-1})^2 = \xi_7^3+\xi_7^{-1}+\xi_7+\xi_7^{-3}+\xi_7^2+\xi_7^{-2} = \xi_7+\xi_7^2+\xi_7^3+\xi_7^4+\xi_7^5+\xi_7^6 = -1$$

   Lo cual demuestra lo que queriamos.

□

Solución 17. 1. Vamos a usar dos identidades:

- $\Phi_{np}(X) = \Phi_n(X^p)$ donde p es un primo tal que $p \mid n$
- $\Phi_n p(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$ donde p es un primo que no divide a n (esta identidad está en la práctica 6)

   De la segunda identidad, despejamos que $\Phi_{5.28}(X)\Phi_{28}(X) = \Phi_{28}(X^5)$

   Ahora evaluamos en X^2 y obtenemos que $\Phi_{5.28}(X^2)\Phi_{28}(X^2) = \Phi_{28}(X^{10})$. Por la primera identidad esto es lo mismo que $\Phi_{2.5.28}(X)\Phi_{2.28}(X) = \Phi_{28}(X^{10})$.

   Es decir, obtuvimos que $\Phi_{28}(X^{10}) = \Phi_{280}(X)\Phi_{56}(X)$. Como los polinomios ciclotómicos son irreducibles en $\mathbb{Q}[X]$, esta es la factorización pedida.

2. Para este item vamos usar el ejercicio 9 de la práctica 6.

   Recordemos que dice que si K es un cuerpo y $n \in \mathbb{N}$ coprimo con la característica de K, si ξ_n una raíz n-ésima primitiva de la unidad $\overline{K}$, entonces si $f \in K[X]$ es irreducible y f dividide a Φ_n entonces el grado de f es $[K(\xi_n) : K]$. Más aún Φ_n se factoriza como producto de polinomios irreducibles de grado $[K(\xi_n) : K]$.

Del item 1, sabemos que tenemos que aplicar esto a Φ_{280} y Φ_{56}. Entonces debemos averiguar $[\mathbb{F}_{13}(\xi_{56}) : \mathbb{F}_{13}]$. Debemos encontrar el menor m tal que $56 \mid 13^m - 1$. Haciendo la cuenta resulta que $m = 2$, luego $[\mathbb{F}_{13}(\xi_{56}) : \mathbb{F}_{13}] = 2$.

De manera similar, resulta que el menor m tal que $280 \mid 13^m - 1$ es 4. Luego $[\mathbb{F}_{13}(\xi_{280}) : \mathbb{F}_{13}] = 4$.

Ahora, Φ_{56} tiene grado $\phi(56) = \phi(8)\phi(7) = 4.6 = 24$. Luego en $\mathbb{F}_{13}[X]$ se descompone en 12 polinomios irreducibles de grado 2. Finalmente Φ_{280} es de grado $\phi(280) = \phi(8)\phi(5)\phi(7) = 4.4.6 = 96$. Entonces en $\mathbb{F}_{13}[X]$ este polinomio se descompone en 24 polinomios irreducibles de grado 4. Así que en total, se descompone en 36 polinomios irreducibles

Solución 18. 1. Simplemente usamos los polinomios simétricos elementales en las raíces $r_1, \ldots, r_n$.

$$\begin{cases} r_1 + r_2 + \cdots + r_{n-1} + r_n = -a_{n-1} \\ (r_1r_2 + r_1r_3 + \cdots + r_1r_n) + (r_2r_3 + r_2r_4 + \cdots + r_2r_n) + \cdots + r_{n-1}r_n = a_{n-2} \\ \quad \vdots \\ r_1r_2 \ldots r_n = (-1)^n a_0. \end{cases}$$

Tomando módulo y usando desigualdad triangular en cada sumando obtenemos que como en a_{n-1} hay $\binom{n}{n-1}$ de norma 1, entonces $|a_{n-1}| \leq \binom{n}{n-1}$. En a_{n-2} tenemos $\binom{n}{n-2}$ sumandos de norma 1, luego $|a_{n-1}| \leq \binom{n}{n-2}$, etc.

2. El item anterior muestra que los coeficientes están acotados, y en este caso son enteros, luego hay solo finitos polinomios en $\mathbb{Z}[X]$ de grado n que cumplen que todas sus raíces tienen valor absoluto 1.

3. Sea α entero algebraico y sea $f = \prod_{i=0}^{n}(X - \alpha_i) \in \mathbb{Z}[X]$ su minimal, donde los α_i son los conjugados de α.

   Ahora, consideramos $f_n = \prod_{i=0}^{n}(X - \alpha_i^n) \in \mathbb{Z}[X]$. Este polinomio de grado n tiene a α^n como raíz, es mónico y todas sus raíces tienen valor absoluto 1.

   Como solo puede haber una cantidad finita de polinomios f_n (por el item anterior), las potencias de α son un conjunto finito, por lo tanto deben existir $n < m$ tal que $\alpha^n = \alpha^m$, de donde se concluye que $\alpha^{m-n} = 1$.

□