Problemas resueltos de Teoría de Galois

Redactados por Lorena Vidal Blasco

Becaria de Colaboración del Departamento de Algebra
de la Universidad de Valencia

23.09.09

1.Sea $k = \mathbb{Z}/p\mathbb{Z}$, p primo y $p(x) \in k[x]$ un polinomio irreducible en $k[x]$ de grado n, $n \geq 1$. Razonar que el cuerpo $k[x]/(p(x))$ tiene exactamente p^n elementos.

Sabemos por teoría:
"*Si R es un anillo conmutativo y con unidad $1 \neq 0$, y M es un ideal de R, entonces*

$$M \text{ es ideal maximal de } R \Longleftrightarrow R/M \text{ es un cuerpo}"$$

"*Sea R un $D.I.P$ no cuerpo y $a \in R$, son equivalentes:*
i) a es irreducible.
ii) (a) es maximal de R((a)= ideal generado por a)"

Teniendo en cuenta estos dos resultados, podemos justificar que $k[x]/(p(x))$ es un cuerpo, ya que como $p(x)$ es irreducible en $k[x]$ y $k[x]$ es un $D.I.P$ no cuerpo $\Longrightarrow$ $(p(x))$ es un ideal maximal.

Todo elemento de $k[x]/(p(x))$ será de la forma

$$g(x) + (p(x))$$

Por el algoritmo de las división, $\exists q(x), r(x) \in k[x]$ tal que
$g(x) = p(x)q(x) + r(x)$ siendo $r(x) = 0$ ó $\delta(r(x)) < \delta(p(x)) = n \Longrightarrow$

$$g(x)+(p(x)) = p(x)g(x)+r(x)+(p(x)) = r(x)+(p(x)) = \underbrace{a_0 + a_1x + ... + a_{n-1}x^{n-1}}_{\text{representante canónico único}} + (p(x))$$

Como a_0,a_1,...,$a_{n-1} \in \mathbb{Z}/p\mathbb{Z}$, hay p^n representantes canónicos $\Longrightarrow$ $k[x]/(p(x))$ tiene p^n elementos, como queríamos demostrar.

2. Demostrar que $x^3 + x^2 + 1$ es irreducible en $(\mathbb{Z}/2\mathbb{Z})[x]$ y que $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3 + x^2 + 1)$ es un cuerpo de 8 elementos.

Para ver que $x^3 + x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ es irreducible, hay que ver que no se puede poner como producto de 2 polinomios de grado inferior a 3 (uno de grado 1 y el otro de grado 2), y como consecuencia, se reduce a comprobar que dicho polinomio no tiene raíces en $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$. Así

$$\left.\begin{array}{l} f(x) = x^3 + x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x] \\ f(\overline{0}) = \overline{1} \neq \overline{0} \\ f(\overline{1}) = \overline{1} \neq \overline{0} \end{array}\right\} \Longrightarrow f(x) \text{ no tiene raíces en } \mathbb{Z}/2\mathbb{Z}.$$

Por otra parte, por el ejercicio anterior, como $f(x)$ es irreducible, $\mathbb{Z}/2\mathbb{Z})[x]/(x^3 + x^2 + 1)$ es un cuerpo de $2^3 = 8$ elementos.

3. Determinar para que primos p es $x^2 + 1$ irreducible en $(\mathbb{Z}/p\mathbb{Z})[x]$.

Probaremos que

$$x^2 + 1 \text{ es irreducible en } (\mathbb{Z}/p\mathbb{Z})[x] \Longleftrightarrow p \neq 2 \text{ y } p \not\equiv 1(4)$$

($\Longrightarrow$)

Suponemos que $x^2 + 1$ es irreducible en $(\mathbb{Z}/p\mathbb{Z})[x]$. Como el polinomio es de grado 2, su irreducibilidad se reduce a que no tiene raíces en $\mathbb{Z}/p\mathbb{Z}$.

Si $p = 2 \Rightarrow x^2 + 1 = (x + 1)^2 \Rightarrow f(x)$ tendría raíces en $\mathbb{Z}/2\mathbb{Z}$ (el $\overline{1}$ es raíz), lo que no es posible.

Si $p \equiv 1(4) \Rightarrow 4 \mid (p - 1) = |(\mathbb{Z}/p\mathbb{Z})^*| \Rightarrow$ Como $(\mathbb{Z}/p\mathbb{Z})^*$ es un grupo cíclico, $\exists S \leq (\mathbb{Z}/p\mathbb{Z})^*$ tal que $|S| = 4$ y S es cíclico $\Rightarrow \exists a \in S$ tal que $S =< a >$ y $o(a) = 4 \Rightarrow a^4 = 1 \Rightarrow a^4 - 1 = 0 \Rightarrow (a^2 + 1)(a^2 - 1) = 0 \Rightarrow (a^2 + 1) = 0$ ó $(a^2 - 1) = 0$, ya que $\mathbb{Z}/p\mathbb{Z}$ es un $D.I.$
Si $a^2 - 1 = 0 \Rightarrow a^2 = 1$, lo que no es posible puesto que $o(a) = 4$. Por tanto, $a^2 + 1 = 0 \Rightarrow a \in \mathbb{Z}/p\mathbb{Z}$ sería raíz de $x^2 + 1$, que no puede ser porque hemos supuesto que $x^2 + 1$ es irreducible en $(\mathbb{Z}/p\mathbb{Z})[x]$.

Por tanto, si $x^2 + 1$ es irreducible en $(\mathbb{Z}/p\mathbb{Z})[x]$, se tiene que $p \neq 2$ y $p \not\equiv 1(4)$.

($\Longleftarrow$)

Supongamos que $p \neq 2$ y que $p \not\equiv 1(4)$. Veamos que $x^2 + 1$ es irreducible en $(\mathbb{Z}/p\mathbb{Z})[x]$ por reducción al absurdo.

Supongamos que $\exists a \in \mathbb{Z}/p\mathbb{Z}$ raíz de $x^2 + 1 \Rightarrow a^2 + 1 = 0$.

Por una parte, como $a^2 + 1 = 0 \Rightarrow a \neq 0$ y $a^2 = -1$, lo que conlleva que $o(a) = 4$ puesto que como $p \neq 2$ se tiene que $\overline{1} \neq \overline{-1}$ en $\mathbb{Z}/p\mathbb{Z}$ y por tanto, $a^4 = 1$.

Por otra parte, como $a \neq 0 \Rightarrow a \in (\mathbb{Z}/p\mathbb{Z})^* \Rightarrow a^{p-1} = a^{|(\mathbb{Z}/p\mathbb{Z})^*|} = 1 \Rightarrow$

$o(a) = 4 \mid (p-1) \Rightarrow p \equiv 1(4)$, lo cual no es posible.

Así que $x^2 + 1$ es irreducible en $(\mathbb{Z}/p\mathbb{Z})[x]$.

4. Describir los subcuerpos de $\mathbb{C}$ de la forma:
a) $\mathbb{Q}(\sqrt{2})$
b) $\mathbb{Q}(i)$
c) $\mathbb{Q}(\alpha)$ **donde** α **es la raíz cúbica real de 2**
d) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$
e) $\mathbb{Q}(i\sqrt{11})$

Antes de empezar con el ejercicio, recordemos el resultado teórico que se va a usar en su resolución:

"Si E/F es una extensión de cuerpos y $a \in E$ es algebraico sobre F, entonces, $F(a)/F$ es finita y $[F(a) : F] = \delta(Irr(a, F))$.
Además, en la demostración de este resultado se observa que si $\delta(Irr(a, F)) = n$, entonces 1, a,a^2,...,a^{n-1} es una F-base de $F(a)$".

a) $\mathbb{Q}(\sqrt{2})$

* Sabemos que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$.
* $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ ya que es raíz de $x^2 - 2$.
* $x^2 - 2$ es irreducible en $\mathbb{Q}$ porque sus únicas raíces son $\sqrt{2}$ y $-\sqrt{2}$, que no están en $\mathbb{Q}$. Además, $x^2 - 2$ es mónico. Entonces

$$x^2 - 2 \text{ mónico } + \text{ irreducible } + \sqrt{2} \text{ raíz } \Longrightarrow x^2 - 2 = Irr(\sqrt{2}, \mathbb{Q})$$

* Teniendo en cuenta el resultado de teoría, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \Longrightarrow \{1, \sqrt{2}\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$.
Por tanto,

$$\mathbb{Q}(\sqrt{2}) = \{t_0 + t_1\sqrt{2} : t_0, t_1 \in \mathbb{Q}\}$$

b) $\mathbb{Q}(i)$

* Sabemos que $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{C}$.
* i es algebraico sobre $\mathbb{Q}$ ya que es raíz de $x^2 + 1$.
* $x^2 + 1$ es irreducible en $\mathbb{Q}$ porque sus únicas raíces son i y $-i$, que no están en $\mathbb{Q}$. Además, $x^2 + 1$ es mónico. Entonces

$$x^2 + 1 \text{ mónico } + \text{ irreducible } + i \text{ raíz } \Longrightarrow x^2 + 1 = Irr(i, \mathbb{Q})$$

* Igual que antes, $[\mathbb{Q}(i) : \mathbb{Q}] = 2 \Longrightarrow \{1, i\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(i)$.
Por tanto,

$$\mathbb{Q}(i) = \{t_0 + t_1 i : t_0, t_1 \in \mathbb{Q}\}$$

c) $\mathbb{Q}(\alpha)$ donde α es la raíz cúbica real de 2

* Sabemos que $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{C}$.
* α es algebraico sobre $\mathbb{Q}$ ya que es raíz de $x^3 - 2$.
* $x^3 - 2$ es irreducible en $\mathbb{Q}[x]$. Basta aplicar el criterio de Eisenstein con $p = 2$. Además, $x^3 - 2$ es mónico. Entonces

$$x^3 - 2 \text{ mónico } + \text{ irreducible } + \alpha \text{ raíz } \Longrightarrow x^3 - 2 = Irr(\alpha, \mathbb{Q})$$

* Consecuentemente, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \Longrightarrow \{1, \alpha, \alpha^2\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$. Por tanto,

$$\mathbb{Q}(\alpha) = \{t_0 + t_1\alpha + t_2\alpha^2 : t_0, t_1, t_2 \in \mathbb{Q}\}$$

d) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$

Sabemos que $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = (\mathbb{Q}(\sqrt{5}))(\sqrt{7})$, entonces, aparece la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq (\mathbb{Q}(\sqrt{5}))(\sqrt{7}) \subseteq \mathbb{C}$$

* Veamos en primer lugar $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$

$$\left.\begin{array}{l} \sqrt{5} \text{ es algebraico sobre } \mathbb{Q} \text{ porque es raíz de } x^2 - 5 \\ x^2 - 5 \text{ es irreducible en } \mathbb{Q}[x] \text{ y es mónico} \\ x^2 - 5 = Irr(\sqrt{5}, \mathbb{Q}) \end{array}\right\} \Longrightarrow [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$$

* Calculemos ahora $[(\mathbb{Q}(\sqrt{5}))(\sqrt{7}) : \mathbb{Q}(\sqrt{5})]$. Para ello, necesitamos saber $Irr(\sqrt{7}, \mathbb{Q}(\sqrt{5}))$.

Sabemos que $Irr(\sqrt{7}, \mathbb{Q}) = x^2 - 7$ con $x^2 - 7 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt{5})[x]$. Las únicas raíces de éste polinomio son $\sqrt{7}$ y $-\sqrt{7}$. Si dichas raíces no pertenecen a $\mathbb{Q}(\sqrt{5})$ $\Longrightarrow x^2 - 7$ seguirá siendo irreducible en $\mathbb{Q}(\sqrt{5})[x]$. Se trata pués de ver si $\sqrt{7}$ y $-\sqrt{7}$ pertenecen a $\mathbb{Q}(\sqrt{5})$ o no.

Sabemos, por el resultado de teoría recordado, que $\{1, \sqrt{5}\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{5})$, y por tanto,

$$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\} \qquad (*)$$

Si $\sqrt{7} \in \mathbb{Q}(\sqrt{5}) \Longrightarrow \exists a, b \in \mathbb{Q}$ tal que $\sqrt{7} = a + b\sqrt{5} \Longrightarrow 7 = a^2 + 5b^2 + 2ab\sqrt{5}$

Si $a = 0 \Longrightarrow b^2 = \dfrac{7}{5} \Longrightarrow b = \pm\dfrac{\sqrt{7}}{\sqrt{5}}$, lo que no es posible porque $b \in \mathbb{Q}$.

Si $b = 0 \Longrightarrow a = \pm\sqrt{7}$ que no puede suceder por el mismo motivo que antes.

Por tanto, $a, b \neq 0 \Longrightarrow \sqrt{5} = \dfrac{7 - a^2 - 5b^2}{2ab}$ lo cual es también imposible porque el primer miembro de la igualdad es irracional mientras que el segundo es racional.

As', $Irr(\sqrt{7}, \mathbb{Q}(\sqrt{5})) = x^2 - 7 \Longrightarrow [(\mathbb{Q}(\sqrt{5}))(\sqrt{7}) : \mathbb{Q}(\sqrt{5})] = 2$.

* Por transitividad de índices, sabemos que

$$[(\mathbb{Q}(\sqrt{5}))(\sqrt{7}) : \mathbb{Q}] = [(\mathbb{Q}(\sqrt{5}))(\sqrt{7}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

Por tanto, $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = 4$, con lo que $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ puede verse como un $\mathbb{Q}$-espacio vectorial de dimensión 4. Veamos cómo calcular una base.

Hemos visto que $[(\mathbb{Q}(\sqrt{5}))(\sqrt{7}) : \mathbb{Q}(\sqrt{5})] = 2 \Longrightarrow$ una $\mathbb{Q}(\sqrt{5})$-base de $(\mathbb{Q}(\sqrt{5}))(\sqrt{7})$ es $\{1, \sqrt{7}\}$ y así,

$$\begin{aligned}
\mathbb{Q}(\sqrt{5}, \sqrt{7}) &= (\mathbb{Q}(\sqrt{5}))(\sqrt{7}) \\
&= \{c + d\sqrt{7} : c, d \in \mathbb{Q}(\sqrt{5})\} \\
&\underbrace{=}_{(*)} \{(a_0 + b_0\sqrt{5}) + (a_1 + b_1\sqrt{5})\sqrt{7} : a_0, b_0, a_1, b_1 \in \mathbb{Q}\} \\
&= \{a_0 + b_0\sqrt{5} + a_1\sqrt{7} + b_1\sqrt{5}\sqrt{7} : a_0, b_0, a_1, b_1 \in \mathbb{Q}\}
\end{aligned}$$

En conclusión, $\left\{1, \sqrt{5}, \sqrt{7}, \sqrt{5}\sqrt{7}\right\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ y

$$\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \left\{t_0 + t_1\sqrt{5} + t_2\sqrt{7} + t_3\sqrt{5}\sqrt{7} : t_0, t_1, t_2, t_3 \in \mathbb{Q}\right\}$$

e) $\mathbb{Q}(i\sqrt{11})$

* Sabemos que $\mathbb{Q} \subseteq \mathbb{Q}(i\sqrt{11}) \subseteq \mathbb{C}$.
* $i\sqrt{11}$ es algebraico sobre $\mathbb{Q}$ ya que es raíz de $x^2 + 11$.
* $x^2 + 11$ es irreducible en $\mathbb{Q}$ porque sus únicas raíces son $i\sqrt{11}$ y $-i\sqrt{11}$, que no están en $\mathbb{Q}$. Además, $x^2 + 11$ es mónico. Entonces

$$x^2 + 11 \text{ mónico } + \text{ irreducible } + i\sqrt{11} \text{ raíz } \Longrightarrow x^2 + 11 = Irr(i\sqrt{11}, \mathbb{Q})$$

* Igual que en los casos anteriores, $[\mathbb{Q}(i\sqrt{11}) : \mathbb{Q}] = 2 \Longrightarrow \{1, i\sqrt{11}\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(i\sqrt{11})$.
Por tanto,

$$\mathbb{Q}(i\sqrt{11}) = \{t_0 + t_1 i\sqrt{11} : t_0, t_1 \in \mathbb{Q}\}$$

5.Si E/F es una extensión algebraica y D es un dominio de integridad tal que $F \subseteq D \subseteq E$, probar que D es un cuerpo.

Como D es un dominio de integridad, para ver que es un cuerpo, sólo hay que probar que todo elemento no nulo tiene inverso.

Sea $0 \neq a \in D \subseteq E$. Como E/F es una extensión algebraica $\Longrightarrow a$ es algebraico sobre F.

Consideremos el cuerpo $F(a)$. Como a es algebraico, sabemos que
$F(a) = F[a] = \{f(a) : f(x) \in F[x]\}$. Así, si $b \in F[a] \Longrightarrow$
$b = t_0 + t_1 a + ... + t_m a^m$ con $t_i \in F$.

Por otra parte, como $a \in D$ y D es un dominio de integridad $\Longrightarrow a^i \in D$.

Así $\left\{ \begin{array}{l} t_i \in F \subseteq D \\ a^i \in D \end{array} \right\} \Longrightarrow b \in D \Longrightarrow F(a) = F[a] \subseteq D$

Por último, como $F(a)$ es un cuerpo conteniendo a $a \Longrightarrow a^{-1} \in F(a) \Longrightarrow$ Como consecuencia, tras haber visto que $F(a) \subseteq D \Longrightarrow a^{-1} \in D$.

Concluimos que D es un cuerpo.

6. Sean $p_1, ..., p_n$ primos distintos entre sí y $F = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$. Sean $q_1, ..., q_r$ cualquier conjunto de primos distintos entre sí y distintos de $p_1, ..., p_n$. Probar que $\sqrt{q_1...q_r}$ no pertenece a F.

Haremos la demostración por inducción sobre n.

Si $n = 1 \Longrightarrow F = \mathbb{Q}(\sqrt{p_1})$.

Sabemos que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1})$.
Además, $Irr(\sqrt{p_1}) = x^2 - p_1 \Longrightarrow [\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2 \Longrightarrow$ Una $\mathbb{Q}$-base de F sería $\{1, \sqrt{p_1}\} \Longrightarrow F = \left\{t_0 + t_1\sqrt{p_1} : t_0, t_1 \in \mathbb{Q}\right\}$.

Por reducción al absurdo, supongamos que $\sqrt{q_1...q_r} \in F \Longrightarrow \exists t_0, t_1 \in \mathbb{Q}$ tal que $\sqrt{q_1...q_r} = t_0 + t_1\sqrt{p_1}$

- Si $t_0 = 0 \Longrightarrow t_1 = \dfrac{\sqrt{q_1...q_r}}{\sqrt{p_1}}$ que no está en $\mathbb{Q}$, lo que no es posible .
- Si $t_1 = 0 \Longrightarrow t_0 = \sqrt{q_1...q_r}$ que no está en $\mathbb{Q}$, lo que no es posible. .
- Si $t_0, t_1 \neq 0 \Longrightarrow \sqrt{q_1...q_r} = t_0 + t_1\sqrt{p_1} \Longrightarrow q_1...q_r = t_0^2 + 2t_0t_1\sqrt{p_1} + t_1^2p_1$ $\Longrightarrow \sqrt{p_1} = \dfrac{q_1...q_r - t_0^2 - t_1^2p_1}{2t_0t_1} \in \mathbb{Q}$, lo que no es posible.

Por tanto, $\sqrt{q_1...q_r}$ no pertenece a F, con lo que para $n = 1$ se cumple la tesis.

Por inducción, supongamos que $\sqrt{q_1...q_r}$ no pertenece a $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}})$ para cualquier conjunto de primos distintos entre sí y distintos a $p_1, ..., p_{n-1}$.

Sea $L = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}})$ y consideremos $L(\sqrt{p_n})$.

Por reducción al absurdo, supongamos que $\sqrt{q_1...q_r} \in L(\sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) = F$.

Tenemos $\mathbb{Q} \subseteq L \subseteq L(\sqrt{p_n}) = F$

Veamos que $Irr(\sqrt{p_n}, L) = x^2 - p_n$ (lo sabemos sobre $\mathbb{Q}$, no sobre L).
Como $p_n \neq p_1, ..., p_{n-1}$ y primo, por hipótesis de inducción, $\sqrt{p_n}$ no pertenece a $L = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}}) \Longrightarrow Irr(\sqrt{p_n}, L) = x^2 - p_n$ (pués las únicas raíces de $x^2 - p_n$ no pertenecen a L) $\Longrightarrow [F : L] = [L(\sqrt{p_n}) : L] = 2 \Longrightarrow$ una L-base de $L(\sqrt{p_n}) = F$ será $\left\{1, \sqrt{p_n}\right\}$.

Como hemos supuesto que $\sqrt{q_1...q_r} \in L(\sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) = F \Longrightarrow$ $\exists\, t_0, t_1 \in L$ tal que $\sqrt{q_1...q_r} = t_0 + t_1\sqrt{p_n}$

- Si $t_1 = 0 \Longrightarrow t_0 = \sqrt{q_1...q_r}$ lo que no es posible porque $t_0 \in L$ y, sin embargo, por hipótesis de inducción, $\sqrt{q_1...q_r}$ no está en L.
- Si $t_0 = 0 \Longrightarrow \sqrt{q_1...q_r p_n} = t_1 p_n \in L$ lo que no es posible por la hipótesis de inducción.

.
Si $t_0, t_1 \neq 0 \Longrightarrow \sqrt{q_1...q_r} = t_0 + t_1\sqrt{p_n} \Longrightarrow q_1...q_r = t_0^2 + 2t_0t_1\sqrt{p_n} + t_1^2 p_n \Longrightarrow$ $\sqrt{p_n} = \dfrac{q_1...q_r - t_0^2 - t_1^2 p_n}{2t_0t_1} \in L$, que de nuevo es imposible.
Luego $\sqrt{q_1...q_r}$ no pertenece a $L(\sqrt{p_n}) = F$.

7. Continuando con el problema anterior probar:
a) $[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n$

b) Si $p_1, ..., p_i, ...$ es una sucesión infinita de primos distintos entre sí, entonces $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_i}, ...)$ es una extensión algebraica no finita de $\mathbb{Q}$.

a) Haremos la demostración por inducción sobre n.

Si $n = 1$, entonces, $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$ ya que $Irr(\sqrt{p_1}, \mathbb{Q}) = x^2 - p_1$.

Suponemos la hipótesis cierta para $n - 1$, es decir, suponemos que
$[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}}) : \mathbb{Q}] = 2^{n-1}$.

LLamamos $L = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}})$. Entonces, aparece la situación

$$\mathbb{Q} \subseteq L \subseteq L(\sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$$

Por transitividad de grados sabemos que

$$[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_n}):\mathbb{Q}] = [L(\sqrt{p_n}):\mathbb{Q}] = [L:\mathbb{Q}][L(\sqrt{p_n}):L] \underbrace{=}_{HI} 2^{n-1}[L(\sqrt{p_n}):L]$$

Por tanto, se trata de comprobar si $[L(\sqrt{p_n}):L] = 2$. Para ello, calculemos $Irr(\sqrt{p_n}, L)$.

Sabemos que $Irr(\sqrt{p_n},\mathbb{Q}) = x^2 - p_n$, pero, ¿sigue siéndolo sobre L?.
La respuesta será positiva $\iff \sqrt{p_n}$ no pertenece a L.

Como $p_n \neq p_i \ \forall i = 1,...,n-1$ y p_n es primo, por el ejercicio anterior, $\sqrt{p_n}$ no pertenece a $L \implies Irr(\sqrt{p_n}, L) = x^2 - p_n \implies [L(\sqrt{p_n}):L] = 2 \implies$
$[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_n}):\mathbb{Q}] = 2^n$.

b)Veamos en primer lugar que $\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_i},...)$ es una extensión no finita de $\mathbb{Q}$.

Por reducción al absurdo, supongamos que

$$[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_i},...):\mathbb{Q}] = m < \infty$$

Entonces, tenemos la situación

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1},...,\sqrt{p_m}) \subseteq \mathbb{Q}(\sqrt{p_1},...,\sqrt{p_i},...)$$

Por transitividad de grados sabemos

$$\begin{array}{lll} m & = & [\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_i},...):\mathbb{Q}] \\ & = & [\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_i},...):\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_m})][\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_m}):\mathbb{Q}] \\ & \underbrace{=}_{(b)} & a\cdot 2^m \quad (\text{ con } a>1) \\ & > & 2^m \implies m > 2^m \qquad \nexists \qquad \forall m \in \mathbb{N} \end{array}$$

Por tanto, la extensión no es finita.

Para ver que la extensión es algebraica necesitamos el resultado:

"Si E/F es una extensión de cuerpos y S es un subconjunto de elementos de E algebraicos sobre F, entonces, $F(S)/F$ es algebraica".

Teniendo en cuenta este resultado y que $\sqrt{p_i}$ son algebraicos sobre $\mathbb{Q}$ $\forall i$ $(Irr(\sqrt{p_i},\mathbb{Q}) = x^2 - p_i)$, se deduce que $\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_i},...)$ es una extensión algebraica no finita de $\mathbb{Q}$.

8. Sean p_1, p_2, p_3 y p_4 primos distintos entre sí. Hallar:
i) $[\mathbb{Q}(\sqrt{p_1p_2},\sqrt{p_1p_3}):\mathbb{Q}]$
ii) $[\mathbb{Q}(\sqrt{p_1p_2},\sqrt{p_3p_4}):\mathbb{Q}]$

i) Sabemos que $\mathbb{Q}(\sqrt{p_1p_2}, \sqrt{p_1p_3}) = \mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_1p_3})$, con lo que aparece la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1p_2}) \subseteq \mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_1p_3})$$

Por transitividad de grados se tiene

$$[\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_1p_3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_1p_3}) : \mathbb{Q}(\sqrt{p_1p_2})][\mathbb{Q}(\sqrt{p_1p_2}) : \mathbb{Q}]$$

Como $Irr(\sqrt{p_1p_2}, \mathbb{Q}) = x^2 - p_1p_2$, se tiene que $[\mathbb{Q}(\sqrt{p_1p_2}) : \mathbb{Q}] = 2$.

Por otra parte, calculemos $[\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_1p_3}) : \mathbb{Q}(\sqrt{p_1p_2})]$.
Para ello, necesitamos conocer $Irr(\sqrt{p_1p_3}, \mathbb{Q}(\sqrt{p_1p_2}))$. Sabemos que $Irr(\sqrt{p_1p_3}, \mathbb{Q}) = x^2 - p_1p_3$, pero, ¿sigue siendo el polinomio irreducible de $\sqrt{p_1p_3}$ sobre $\mathbb{Q}(\sqrt{p_1p_2})$?.
Esto pasará $\iff \sqrt{p_1p_3}$ no pertenece a $\mathbb{Q}(\sqrt{p_1p_2})$.

Si $\sqrt{p_1p_3} \in \mathbb{Q}(\sqrt{p_1p_2}) \subseteq \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) \implies \sqrt{p_1} \cdot \sqrt{p_1p_3} = p_1\sqrt{p_3} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ $\implies \sqrt{p_3} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ lo que no es posible por el ejercicio 6. Por lo tanto $Irr(\sqrt{p_1p_3}, \mathbb{Q}(\sqrt{p_1p_2}) = x^2 - p_1p_3 \implies [\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_1p_3}) : \mathbb{Q}(\sqrt{p_1p_2})]$=2.

Finalmente $[\mathbb{Q}(\sqrt{p_1p_2}, \sqrt{p_1p_3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

ii) Sabemos que $\mathbb{Q}(\sqrt{p_1p_2}, \sqrt{p_3p_4}) = \mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_3p_4})$, con lo que aparece la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1p_2}) \subseteq \mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_3p_4})$$

Por transitividad de grados se tiene

$$[\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_3p_4}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_3p_4}) : \mathbb{Q}(\sqrt{p_1p_2})][\mathbb{Q}(\sqrt{p_1p_2}) : \mathbb{Q}]$$

Como $Irr(\sqrt{p_1p_2}, \mathbb{Q}) = x^2 - p_1p_2$, se tiene que $[\mathbb{Q}(\sqrt{p_1p_2}) : \mathbb{Q}] = 2$.

Por otra parte, calculemos $[\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_3p_4}) : \mathbb{Q}(\sqrt{p_1p_2})]$.

De nuevo por el ejercicio 6, se deduce que $\sqrt{p_3p_4}$ no pertenece a $\mathbb{Q}(\sqrt{p_1p_2}) \subseteq \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ luego :
$Irr(\sqrt{p_3p_4}, \mathbb{Q}(\sqrt{p_1p_2})) = Irr(\sqrt{p_3p_4}, \mathbb{Q}) = x^2 - p_3p_4 \implies [\mathbb{Q}(\sqrt{p_1p_2})(\sqrt{p_3p_4}) :$ $\mathbb{Q}(\sqrt{p_1p_2})] = 2$.

Como consecuencia $[\mathbb{Q}(\sqrt{p_1p_2}, \sqrt{p_3p_4}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

9. Sean $p_1, ..., p_n$ primos distintos entre sí y $F = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$. Probar que para cada i existe $\sigma_i \in G(F/\mathbb{Q})$ tal que $\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$ y $\sigma_i(\sqrt{p_j}) = \sqrt{p_j}$ si $j \neq i$.
Usar este hecho para demostrar que $\sqrt{p_1}, ..., \sqrt{p_n}$ son $\mathbb{Q}$-linealmente independientes.

Para resolver la primera parte del ejercicio, recordemos el resultado:

Sean E_1/E y E_2/E extensiones, $a \in E_1$ y $b \in E_2$, ambos algebraicos sobre E. Entonces

a y b son E-conjugados $\iff \exists \sigma : E(a) \longrightarrow E(b)$ E-isomorfismo tal que $\sigma(a) = b$

Veamos en primer lugar que para cada i existe el $\mathbb{Q}$-automorfismo buscado.

Fijado i, queremos encontrar $\sigma_i \in G(F/\mathbb{Q})$ tal que $\begin{cases} \sigma_i(\sqrt{p_i}) = -\sqrt{p_i} \\ \sigma_i(\sqrt{p_j}) = \sqrt{p_j} \text{ si } j \neq i \end{cases}$

Sabemos por el ejercicio 6 que $\sqrt{p_i}$ no pertenece a $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{i-1}}, \sqrt{p_{i+1}}, ..., \sqrt{p_n}) = L \implies Irr(\sqrt{p_i}, L) = Irr(\sqrt{p_i}, \mathbb{Q}) = x^2 - p_i = Irr(-\sqrt{p_i}, L)$.

Como consecuencia, $\sqrt{p_i}$ y $-\sqrt{p_i}$ son L-conjugados, con lo que aplicando el resultado recordado para $E_1 = E_2 = F$, $E = L$, $a = \sqrt{p_i}$ y $b = -\sqrt{p_i}$, se deduce que

$$\exists \sigma_i : \underbrace{L(\sqrt{p_i})}_{F} \longrightarrow L(-\sqrt{p_i}) = L(\sqrt{p_i}) = F \quad L\text{-isomorfismo tal que } \sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$$

Notar que como σ_i es un L-isomorfismo, se verifica que $\sigma_i(\sqrt{p_j}) = \sqrt{p_j}$ para $j \neq i$. Además, como σ_i deja fijos a los elementos de L, en particular, también dejará fijos a los elementos de $\mathbb{Q}$, con lo que σ_i es también un $\mathbb{Q}$-automorfismo.

Por lo tanto, para cada i existe $\sigma_i \in G(F/\mathbb{Q})$ tal que $\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$ y $\sigma_i(\sqrt{p_j}) = \sqrt{p_j}$ si $j \neq i$.

Veamos ahora que $\sqrt{p_1}, ..., \sqrt{p_n}$ son $\mathbb{Q}$-linealmente independientes.

Supongamos que existen $a_1, ..., a_n \in \mathbb{Q}$ tales que $\underbrace{a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} = 0}_{(1)}$.

Aplicamos a (1) $\sigma_1 \in G(F/\mathbb{Q})$ ($\sigma_1(\sqrt{p_1}) = -\sqrt{p_1}$ y $\sigma_1(\sqrt{p_j}) = \sqrt{p_j}$ si $j \neq 1$):

$$0 = \sigma_1(0) = \sigma_1(a_1\sqrt{p_1} + \cdots a_n\sqrt{p_n}) = a_1\sigma_1(\sqrt{p_1}) + \cdots + a_n\sigma_1(\sqrt{p_n})$$

$$\Downarrow$$

$$\underbrace{-a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} = 0}_{(2)}$$

Restamos (1) − (2):

$$\begin{array}{c} a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} = 0 \\ \underline{- \ -a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} = 0} \\ 2a_1\sqrt{p_1} = 0 \quad \implies \quad a_1 = 0 \end{array}$$

Aplicamos ahora a (1) $\sigma_2 \in G(F/\mathbb{Q})$ ($\sigma_2(\sqrt{p_2}) = -\sqrt{p_2}$ y $\sigma_2(\sqrt{p_j}) = \sqrt{p_j}$ si $j \neq 2$):

$$0 = \sigma_2(0) = \sigma_2(a_1\sqrt{p_1}+a_2\sqrt{p_2}+\cdots a_n\sqrt{p_n}) = a_1\sigma_2(\sqrt{p_1})+a_2\sigma_2(\sqrt{p_2})+\cdots+a_n\sigma_2(\sqrt{p_n})$$

$$\Downarrow$$

$$\underbrace{a_1\sqrt{p_1} - a_2\sqrt{p_2} + \cdots + a_n\sqrt{p_n} = 0}_{(3)}$$

Restamos (1) − (3):

$$\begin{array}{r} a_1\sqrt{p_1} + a_2\sqrt{p_2} + \cdots + a_n\sqrt{p_n} = 0 \\ \underline{- a_1\sqrt{p_1} - a_2\sqrt{p_2} + \cdots + a_n\sqrt{p_n} = 0} \\ 2a_2\sqrt{p_2} = 0 \quad \Longrightarrow \quad a_2 = 0 \end{array}$$

Repitiendo el proceso reiteradamente, vamos obteniendo $a_3 = \ldots = a_n = 0$ al aplicar $\sigma_3, \ldots \sigma_n$, respectivamene. Por tanto, $\sqrt{p_1}, \ldots, \sqrt{p_n}$ son $\mathbb{Q}$-linealmente independientes.

10. Sean $p_1, ..., p_n$ primos distintos entre sí y $F = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$. Probar que $F = \mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n})$ y que $G(F/\mathbb{Q}) \cong C_2 \times ... \times C_2$.

Veamos en primer lugar que $F = \mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n})$.

Sabemos, por el ejercicio 7, que $[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) : \mathbb{Q}] = [F : \mathbb{Q}] = 2^n$.

Notar que $\mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n}) \subseteq \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$

Aparece entonces la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n}) \subseteq \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$$

Queremos ver que $[\mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n}) : \mathbb{Q}] = 2^n$, es decir, que $\delta(Irr(\sqrt{p_1}+...+\sqrt{p_n}, \mathbb{Q})) = 2^n$ ya que así, dado que $[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n$, por transitividad de grados, tendremos que $[F : \mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n})] = 1 \Longrightarrow \mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n}) = F = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$.

Notar que $F/\mathbb{Q}$ es una extensión finita de Galois ya que $\sqrt{p_1}, ..., \sqrt{p_n}$ son las raíces de

$$f(x) = (x^2 - p_1)(x^2 - p_2)\cdots(x^2 - p_n)$$

que es separable por ser $\mathbb{Q}$ de característica $0 \Longrightarrow F$ es cuerpo de escisión sobre $\mathbb{Q}$ de $f(x) \in \mathbb{Q}[x]$, polinomio separable sobre $\mathbb{Q}$. (Se ha usado la tercera condición del teorema de caracterización de las extensiones finitas de Galois).

Sea $G = G(F/\mathbb{Q})$ el grupo de Galois de $F/\mathbb{Q}$. Sabemos que $|G| = [F : \mathbb{Q}]=2^n$.

Sea $a = \sqrt{p_1} + \ldots + \sqrt{p_n}$ y $p(x) = Irr(a, \mathbb{Q})$.

Como $\left\{ \begin{array}{l} \sqrt{p_i} \in F \\ \sqrt{p_i} \text{ es algebraico} \\ \sigma \in G \end{array} \right\} \Longrightarrow \sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$ ya que $\sigma(\sqrt{p_i})$ es también raíz de $Irr(\sqrt{p_i}, \mathbb{Q}) = x^2 - p_i$ (lo veremos después en $(*)$).

Teniendo en cuenta esto, es claro que los 2^n $\mathbb{Q}$-automorfismos de F están perfectamente determinados. Ahora bien:
i) $\delta(Irr(a, \mathbb{Q}) \leq 2^n$
ii)todo elemento $\sigma(a)$, con $\sigma \in G$, es raíz de $p(x)$
iii) $|\{\sigma(a)|\sigma \in G\}| = 2^n$ por el ejercicio 9
luego $\delta(Irr(a, \mathbb{Q}) = 2^n$.

$(*)$ *Sea E/F una extensión de cuerpos y $a \in E$ un elemento algebraico. Sea $p(x) = Irr(a, F)$ y sea $\sigma \in G(E/F)$, entonces $\sigma(a)$ es también raíz de $p(x)$ y $p(x) = Irr(\sigma(a), F)$.*
En efecto, supongamos que $p(x) = s_0 + s_1x + s_2x^2 + \cdots + s_{n-1}x^{n-1} + x^n \in F[x]$ $\Longrightarrow s_0 + s_1a + s_2a^2 + \cdots + s_{n-1}a^{n-1} + a^n = 0$.
Aplicando σ se obtiene que:

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(s_0 + s_1a + s_2a^2 + \cdots + s_{n-1}a^{n-1} + a^n) \\ &= \sigma(s_0) + \sigma(s_1)\sigma(a) + \cdots + \sigma(s_{n-1})\sigma(a^{n-1}) + \sigma(a^n) \\ &= s_0 + s_1\sigma(a) + \cdots + s_{n-1}(\sigma(a))^{n-1} + (\sigma(a))^n \end{aligned}$$

Luego, $\sigma(a)$ es raíz de $p(x)$ y $p(x) = Irr(\sigma(a), F)$.

Veamos ahora que $G(F/\mathbb{Q}) \cong C_2 \times ... \times C_2$.

Sabemos hasta ahora:

1. $F/\mathbb{Q}$ es una extensión finita de Galois con $|G(F/\mathbb{Q})| = [F : \mathbb{Q}] = 2^n$.
2. Hemos visto que $\forall\ 1 \neq \sigma \in G(F/\mathbb{Q})$ se cumple que $\sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$ para cualquier $i \Longrightarrow o(\sigma) = 2$ (ya que como $F = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) = \mathbb{Q}[\sqrt{p_1}, ..., \sqrt{p_n}]$, σ queda determinado por las imágenes de $\sqrt{p_1}, ..., \sqrt{p_n}$) $\Longrightarrow G(F/\mathbb{Q})$ es abeliano.

Para demostrar que $G(F/\mathbb{Q}) \cong C_2 \times ... \times C_2$ lo haremos por indución sobre n.

Si $n = 1$, $F = \mathbb{Q}(\sqrt{p_1}) \Longrightarrow [\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2 = |G(F/\mathbb{Q})| \Longrightarrow G(F/\mathbb{Q}) \cong C_2$

Establecemos la aplicación

$$\begin{aligned} \varphi : G(F/\mathbb{Q}) &\longrightarrow G(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}})/\mathbb{Q}) \times G(\mathbb{Q}(\sqrt{p_n})/\mathbb{Q}) \\ \sigma &\longmapsto (\sigma_{|_{\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})}}, \sigma_{|_{\mathbb{Q}(\sqrt{p_n})}}) \end{aligned}$$

Notar que como la extensión $F/\mathbb{Q}$ es abeliana, las extensiones $\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_{n-1}})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt{p_n})/\mathbb{Q}$ son de Galois y φ está bien definida.

Llamemos $L = \mathbb{Q}(\sqrt{p_1},...,\sqrt{p_{n-1}}) = \mathbb{Q}[\sqrt{p_1},...,\sqrt{p_{n-1}}]$.

φ es un homomorfismo de grupos

Demostración obvia teniendo en cuenta que la restricción del producto de automorfismos es el producto de las restricciones respectivas.

φ es inyectiva

Si $\varphi(\sigma) = (1_L, 1_{\mathbb{Q}(\sqrt{p_n})})$ debe ser $\sigma = 1_F$. Por lo tanto φ es un monomorfismo entre dos grupos del mismo orden, luego es un isomorfismo.

Por hipótesis de inducción se sigue que:

$$G(F/\mathbb{Q}) \cong G(L/\mathbb{Q}) \times G(\mathbb{Q}(\sqrt{p_n})/\mathbb{Q}) \cong \underbrace{C_2 \times \ldots \times C_2}_{n}$$

11. Hallar $Irr(a,\mathbb{Q})$ para $a = 2+\sqrt{2}$, $\sqrt{2+\sqrt{2}}$, $\sqrt{2+\sqrt{2+\sqrt{2}}}$.

$a = 2+\sqrt{2}$

$$a = 2+\sqrt{2} \implies (a-2)^2 = 2 \implies a^2 - 4a + 2 = 0$$

Luego a es raíz del polinomio $p(x) = x^2 - 4x + 2$.

Además, $p(x)$ es irreducible en $\mathbb{Q}[x]$ por el criterio de Eisenstein para $p = 2$.

Por último, como $p(x)$ es mónico, se deduce que $Irr(a,\mathbb{Q}) = x^2 - 4x + 2$.

$a = \sqrt{2+\sqrt{2}}$

$$a = \sqrt{2+\sqrt{2}} \implies a^2 = 2+\sqrt{2} \implies (a^2-2)^2 = 2 \implies a^4 - 4a^2 + 2 = 0$$

Luego , a es raíz del polinomio $p(x) = x^4 - 4x^2 + 2$.

Además, $p(x)$ es irreducible en $\mathbb{Q}[x]$ por el criterio de Eisenstein para $p = 2$.

Por último, como $p(x)$ es mónico, se deduce que $Irr(a,\mathbb{Q}) = x^4 - 4x^2 + 2$.

$a = \sqrt{2+\sqrt{2+\sqrt{2}}}$

$$a = \sqrt{2+\sqrt{2+\sqrt{2}}} \implies a^2 = 2+\sqrt{2+\sqrt{2}} \implies (a^2-2)^2 = 2+\sqrt{2} \implies$$

$$a^4-4a^2+4 = 2+\sqrt{2} \implies ((a^4+2)-4a^2)^2 = 2 \implies a^8-8a^6+20a^4-16a^2+2 = 0$$

Luego a es raíz del polinomio $p(x) = x^8 - 8x^6 + 20x^4 - 16x^2 + 2$.

Además, $p(x)$ es irreducible en $\mathbb{Q}[x]$ por el criterio de Eisenstein para $p = 2$.

Por último, como $p(x)$ es mónico, se deduce que
$Irr(a, \mathbb{Q}) = x^8 - 8x^6 + 20x^4 - 16x^2 + 2$.

12. Sea $a \in \mathbb{C}$ raíz de $x^3 + x + 1$. Probar que $\mathbb{Q}(a, \sqrt{2}) = \mathbb{Q}(a\sqrt{2})$.

Veamos que $\mathbb{Q}(a, \sqrt{2}) = \mathbb{Q}(a\sqrt{2})$.

$\boxed{\supseteq}$ Esta inclusión es inmediata, ya que como a y $\sqrt{2} \in \mathbb{Q}(a, \sqrt{2})$ y $\mathbb{Q}(a, \sqrt{2})$ es un cuerpo $\Longrightarrow a\sqrt{2} \in \mathbb{Q}(a, \sqrt{2})$, y dado que $\mathbb{Q}(a\sqrt{2})$ es el menor cuerpo conteniendo a $\mathbb{Q}$ y a $a\sqrt{2}$, se concluye que

$$\mathbb{Q}(a\sqrt{2}) \subseteq \mathbb{Q}(a, \sqrt{2})$$

$\boxed{\subseteq}$ Para demostrar esta inclusión, basta con ver que a (y por tanto $\sqrt{2}$) $\in \mathbb{Q}(a\sqrt{2})$, ya que como $\mathbb{Q}(a, \sqrt{2})$ es el menor cuerpo conteniendo a ambos elementos, se tendrá

$$\mathbb{Q}(a, \sqrt{2}) \subseteq \mathbb{Q}(a\sqrt{2})$$

Como $x^3 + x + 1$ es irreducible en $\mathbb{Q}[x]$ se tiene que $Irr(a, \mathbb{Q}) = x^3 + x + 1$ y $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.

Por otra parte, $(a\sqrt{2})^2 = 2a^2 \in \mathbb{Q}(a\sqrt{2})$. Como $\mathbb{Q} \subseteq \mathbb{Q}(a^2) \subseteq \mathbb{Q}(a)$ y $\mathbb{Q} \neq \mathbb{Q}(a^2)$ pues $a^2 \notin \mathbb{Q}$, se sigue que $\mathbb{Q}(a^2) = \mathbb{Q}(a) \Longrightarrow a \in \mathbb{Q}(a^2) \subseteq \mathbb{Q}(a\sqrt{2})$.

Por lo tanto $\mathbb{Q}(a, \sqrt{2}) \subseteq \mathbb{Q}(a\sqrt{2}) \Longrightarrow \boxed{\mathbb{Q}(a, \sqrt{2}) = \mathbb{Q}(a\sqrt{2})}$

13. Comprobar que $\mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\sqrt[3]{2} + i)$ y obtener $Irr(\sqrt[3]{2} + i, \mathbb{Q})$.

Veamos primero que $\mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\sqrt[3]{2} + i)$.

$\boxed{\supseteq}$ Se cumple ya que $\sqrt[3]{2}$ y $i \in \mathbb{Q}(\sqrt[3]{2}, i) \Longrightarrow \sqrt[3]{2} + i \in \mathbb{Q}(\sqrt[3]{2}, i) \Longrightarrow$
$\mathbb{Q}(\sqrt[3]{2} + i) \subseteq \mathbb{Q}(\sqrt[3]{2}, i)$.

$\boxed{=}$ Tenemos la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2} + i) \subseteq \mathbb{Q}(\sqrt[3]{2}, i)$$

Veamos que el grado de $\mathbb{Q}(\sqrt[3]{2}, i)$ es 6, ya que entonces, por trasitividad de grados podremos deducir los grados $[\mathbb{Q}(\sqrt[3]{2} + i) : \mathbb{Q}]$ y $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2} + i)]$,

respectívamente.

Dado que $\mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\sqrt[3]{2})(i)$ aparece la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})(i)$$

Entonces,

$$[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

Como $\sqrt[3]{2}$ es algebraico y $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2 \Longrightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Como i no pertenece a $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R} \Longrightarrow Irr(i, \mathbb{Q}(\sqrt[3]{2})) = Irr(i, \mathbb{Q}) = x^2 + 1$ $\Longrightarrow [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})] = 2$ luego $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = 2 \cdot 3 = 6$

Sea $L = \mathbb{Q}(\sqrt[3]{2} + i)$. Supongamos que $i \notin L$, entonces $L \subset L(i) = \mathbb{Q}(\sqrt[3]{2}, i) \Longrightarrow$ $[L : \mathbb{Q}] = 3 = \delta(Irr(\sqrt[3]{2} + i, \mathbb{Q})$.
Si $Irr(\sqrt[3]{2} + i, \mathbb{Q}) = a + bx + cx^2 + x^3 \Longrightarrow a + b(\sqrt[3]{2}) + bi + c(\sqrt[3]{4} - 1 + 2i\sqrt[3]{2}) +$ $(\sqrt[3]{2} + i)^3 = a + b\sqrt[3]{2} + bi + c\sqrt[3]{4} - c + 2ic\sqrt[3]{2} + 2 + i\sqrt[3]{4} - \sqrt[3]{2} - i + 2i\sqrt[3]{4} - 2\sqrt[3]{2} =$ $0 \Longrightarrow b + 2c\sqrt[3]{2} + 3\sqrt[3]{4} - 1 = 0$, lo que no es posible pues 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[3]{2})$.

Por lo tanto $i \in L \Longrightarrow \sqrt[3]{2} \in L$ y finalmente $L = \mathbb{Q}(\sqrt[3]{2} + i) = \mathbb{Q}(\sqrt[3]{2}, i)$.

Vamos ahora a calcular $Irr(\sqrt[3]{2} + i, \mathbb{Q})$. Para ello, necesitamos tener en cuenta una serie de resultados:

Sea E/F una extensión y sea $a \in E$, $a \neq 0$, algebraico sobre F.
Consideremos la aplicación

$$h : E \longrightarrow E$$

$$y \longmapsto ay$$

Notar que $Irr(a, F) =$ polinomio mínimo de a respecto de h.
Sea $S_{h,a}$ el F-subespacio generado por a y todas sus imágenes respecto de h

$$S_{h,a} =< \{a, h(a), h^2(a), ...\} >=< \{a, a^2, a^3, ...\} >$$

Entonces, $S_{h,a} \subseteq F(a) = F[a]$.
Por otra parte, como $dim S_{h,a} =$grado del polinomio mínimo de $a = \delta(Irr(a, F)) =$ $dim_F F(a) \Longrightarrow S_{h,a} = F(a)$.
Consideremos la restricción

$$h_{|_{F(a)}} : F(a) \longrightarrow F(a)$$

Entonces, como polmin $a \mid$ polmin $h_{|_{F(a)}} \mid$ polcar $h_{|_{F(a)}}$ y
$\delta($polcar $h_{|_{F(a)}}) =$ $dim_F(F(a)) = \delta($polmin $a) \Longrightarrow$ polcar $h_{|_{F(a)}} =$ polmin $a =$ $Irr(a, F)$.
Por tanto, para obtener el $Irr(a, F)$ basta con calcular el polinomio característico de la aplicación

$$h_{|_{F(a)}} : F(a) \longrightarrow F(a)$$

$$y \longmapsto ay$$

Una vez hechos los incisos necesarios vamos a seguir con el ejercicio.

Hemos visto antes que $[\mathbb{Q}(\sqrt[3]{2}+i):\mathbb{Q}]=6$, con lo que una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[3]{2}+i)$ es $\beta=\left\{1,\sqrt[3]{2},\sqrt[3]{4},i,\sqrt[3]{2}i,\sqrt[3]{4}i\right\}$.

LLamemos $a=\sqrt[3]{2}+i$.

Por los resultados recordados, para obtener $Irr(a,\mathbb{Q})$, basta con calcular el polinomio característico de la aplicación

$$h:\mathbb{Q}(a)\longrightarrow\mathbb{Q}(a)$$

$$y\longmapsto ay$$

es decir, basta con calcular la matriz coordenada A de h en la base β y obtener $|xI-A|$.

Por tanto, calculemos A (por columnas):

$$\left.\begin{array}{l} h(1)=a\cdot 1=a=\sqrt[3]{2}+i \\ h(\sqrt[3]{2})=a\cdot\sqrt[3]{2}=\sqrt[3]{4}+\sqrt[3]{2}i \\ h(\sqrt[3]{4})=a\cdot\sqrt[3]{4}=2+\sqrt[3]{4}i \\ h(i)=a\cdot i=\sqrt[3]{2}i-1 \\ h(\sqrt[3]{2}i)=a\cdot\sqrt[3]{2}i=\sqrt[3]{4}i-\sqrt[3]{2} \\ h(\sqrt[3]{4}i)=a\cdot\sqrt[3]{4}i=2i-\sqrt[3]{4} \end{array}\right\}\Longrightarrow A=\begin{pmatrix} 0 & 0 & 2 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Entonces basta obtener

$$|xI-A|$$

.

.

14. Hallar:
a) $Irr(1+\sqrt[3]{2}+\sqrt[3]{4},\mathbb{Q})$
b) $Irr\left(\sqrt{3+2\sqrt{2}},\mathbb{Q}\right)$

a) $Irr(1+\sqrt[3]{2}+\sqrt[3]{4},\mathbb{Q})$

Sea $a=1+\sqrt[3]{2}+\sqrt[3]{4}$
Siguiendo el mismo razonamiento que en el ejercio 13, para obtener $Irr(a,\mathbb{Q})$, basta con calcular el polinomio característico de la aplicación

$$h:\mathbb{Q}(a)\longrightarrow\mathbb{Q}(a)$$

.

$$y \longmapsto ay$$

es decir, basta con calcular la matriz coordenada A de h en una cierta base de $\mathbb{Q}(a)$ y obtener $|xI - A|$.

Busquemos una $\mathbb{Q}$-base de $\mathbb{Q}(a)$ Sabemos que

$$\mathbb{Q} \subseteq \mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) \subseteq \mathbb{Q}(\sqrt[3]{2})$$

Además, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, pués $\sqrt[3]{2}$ es algebraico y $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$.

Por tanto, por transitividad de grados se verifica, $\begin{cases} \mathbb{Q} = \mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{2}) \\ \text{ó} \\ \mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}) \end{cases}$

Como $1 + \sqrt[3]{2} + \sqrt[3]{2}$ no pertenece a $\mathbb{Q}$, se tiene que $\mathbb{Q} \neq \mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{2})$ $\Longrightarrow \mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})$.

Como consecuencia, una $\mathbb{Q}$-base de $\mathbb{Q}(a) = \mathbb{Q}(\sqrt[3]{2})$ es $\beta = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, y la matriz coordenada A de h en dicha base es

$$\left.\begin{array}{l} h(1) = a \cdot 1 = 1 + \sqrt[3]{2} + \sqrt[3]{4} \\ h(\sqrt[3]{2}) = a \cdot \sqrt[3]{2} = \sqrt[3]{2} + \sqrt[3]{4} + 2 \\ h(\sqrt[3]{4}) = a \cdot \sqrt[3]{4} = \sqrt[3]{4} + 2 + 2\sqrt[3]{2} \end{array}\right\} \Longrightarrow A = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

Por tanto,

$$Irr(a, \mathbb{Q}) = |xI - A| = \begin{vmatrix} x-1 & -2 & -2 \\ -1 & x-1 & -2 \\ -1 & -1 & x-1 \end{vmatrix} \underbrace{=}_{\text{operando}} x^3 - 3x^2 - 3x - 1$$

. Por lo tanto, $Irr(a, \mathbb{Q}) = x^3 - 3x^2 - 3x - 1$.

b) $Irr\left(\sqrt{3 + 2\sqrt{2}}, \mathbb{Q}\right)$

Sea a= $\sqrt{3 + 2\sqrt{2}}$.

$a^2 = 3 + 2\sqrt{2} \Longrightarrow (a^2 - 3) = 2\sqrt{2} \Longrightarrow a^4 - 6a^2 + 9 = 4 \cdot 2 \Longrightarrow a^4 - 6a^2 + 1 = 0$ $\Longrightarrow$ a es raíz del polinomio $x^4 - 6x^2 + 1 = p(x)$, pero $p(x)$ no es irreducible.

Sin embargo,

$$x^4 - 6x^2 + 1 = (x^2 + 2x - 1)(x^2 - 2x - 1)$$

siendo ambos polinomios irreducibles.

Como a es raíz de $p(x)$, necesariamente a es raíz de uno de los polinomios, siendo éste su irreducible.

Notar que $\sqrt{3 + 2\sqrt{2}} = \sqrt{(1 + \sqrt{2})^2} = (1 + \sqrt{2})$. Entonces, teniendo en cuenta esto, se comprueba que

$$(1 + \sqrt{2})^2 - 2(1 + \sqrt{2}) - 1 = 0 \quad \Longrightarrow \quad Irr(a, \mathbb{Q}) = x^2 - 2x - 1$$

15. Sea $f(x) = x^3 - x + 1 \in \mathbb{Z}_3[x]$. Probar:
i) **$f(x)$ es irreducible en $\mathbb{Z}_3[x]$.**
ii) **Si E es cuerpo de escisión sobre $\mathbb{Z}_3$ de $f(x)$ se tiene que $[E : \mathbb{Z}_3] = 3$, luego E es un cuerpo de 27 elementos.**

i) Para ver que $f(x)$ es irreducible en $\mathbb{Z}_3[x]$, bastará con probar que $f(x)$ no tiene raíces en $\mathbb{Z}_3$:

$$\left.\begin{array}{l} f(\overline{0}) = \overline{1} \neq \overline{0} \\ f(\overline{1}) = \overline{1} \neq \overline{0} \\ f(\overline{2}) = \overline{1} \neq \overline{0} \end{array}\right\} \Longrightarrow f(x) \text{ no tiene raíces en } \mathbb{Z}_3 \Longrightarrow f(x) \text{ es irreducible en } \mathbb{Z}_3[\text{x}].$$

ii) Calculemos el cuepo de escisión E de $f(x)$ sobre $\mathbb{Z}_3$, y veamos que su grado es 3.

Sabemos por teoría que $\exists\ a$ raíz de $f(x)$ en una cierta extensión de $\mathbb{Z}_3$. Además:

∘ Consideremos $a + 1$.
$(a+1)^3 = a^3+1$ (porque $car\mathbb{Z}_3 = 3) \Longrightarrow (a+1)^3-(a+1)+1 = a^3+1-a-1+1 = a^3 - a + 1 \underbrace{=}_{\text{a es raíz}} 0 \Longrightarrow a + 1$ también es raíz de $f(x)$.

∘ Consideremos ahora $a + 2$.
$(a+2)^3 = a^3+2 \Longrightarrow (a+2)^3-(a+2)+1 = a^3+2-a-2+1 = a^3-a+1 \underbrace{=}_{\text{a es raíz}} 0$
$\Longrightarrow a + 2$ también es raíz de $f(x)$.

Luego, $E = \text{Z}_3\text{(a,a+1,a+2)} \underbrace{=}_{\text{como E es un cuerpo}} \text{Z}_3\text{(a)} \Longrightarrow$

$$[E : \mathbb{Z}_3] = [\mathbb{Z}_3(a) : \mathbb{Z}_3] = \delta(f(x)) = 3$$

Veamos ahora que E es un cuerpo de 27 elementos.

Sabemos que E puede verse como un $\mathbb{Z}_3$-espacio vectorial de
$dim_{\mathbb{Z}_3} E = [E : \mathbb{Z}_3] = 3$, con lo que si $\{b_1, b_2, b_3\}$ es una $\mathbb{Z}_3$-base de E, todo elemento $e \in E$ podrá escribirse como

$$e = a_1b_1 + a_2b_2 + a_3b_3$$

con $a_1, a_2, a_3 \in = \mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

Así, $|E| = |\mathbb{Z}_3|^3 = 3^3 = 27$.

16. Hallar dos polinomios distintos entre sí con el mismo cuerpo de escisión.

Consideremos los polinomios $p(x) = x^2 + 3$ y $q(x) = x^2 + x + 1$ sobre $\mathbb{Q}[x]$. Obviamente, son polinomios distintos. Veamos que tienen el mismo cuerpo de escisión.

Cuerpo de escisión de $p(x)$

Las raíces de $p(x) = x^2 + 3$ son $\sqrt{3}i$ y $-\sqrt{3}i$, con lo que el cuerpo de escisión de $p(x)$ sobre $\mathbb{Q}$ vendrá dado, en principio, por

$$E_1 = \mathbb{Q}(\sqrt{3}i, -\sqrt{3}i)$$

No obstante, como E_1 es un cuerpo, si aparece $\sqrt{3}i$, también lo hará su opuesto, y por tanto, podemos evitar la adjunción de tal elemento, así que

$$E_1 = \mathbb{Q}(\sqrt{3}i)$$

Cuerpo de escisión de $q(x)$

Las raíces de $q(x) = x^2 + x + 1$ son $-\frac{1}{2}(1 + \sqrt{3}i)$ y $-\frac{1}{2}(1 - \sqrt{3}i)$, y por tanto, el cuerpo de escisión de $q(x)$ es

$$E_2 = \mathbb{Q}\left(-\frac{1}{2}(1 + \sqrt{3}i), -\frac{1}{2}(1 - \sqrt{3}i)\right)$$

Igual que antes, dado que E_2 es un cuerpo se tiene:

- Como -2 y $-\frac{1}{2}(1 + \sqrt{3}i)$ pertenecen a $E_2 \Longrightarrow$ $-2 \cdot -\frac{1}{2}(1 + \sqrt{3}i) = (1 + \sqrt{3}i) \in E_2$. Y análogo para $-\frac{1}{2}(1 - \sqrt{3}i) \Longrightarrow$ $E_2 = \mathbb{Q}(1 + \sqrt{3}i, 1 - \sqrt{3}i)$.
- Como $-1 \in E_2$ y $1 + \sqrt{3}i \in E_2 \Longrightarrow -1 + 1 + \sqrt{3}i = \sqrt{3}i \in E_2$. Y análogo para $1 - \sqrt{3}i \Longrightarrow E_2 = \mathbb{Q}(\sqrt{3}i, -\sqrt{3}i)$
- Por último, siguiendo el mismo razonamiento que en caso anterior, si $\sqrt{3}i \in E_2$, también lo estará su opuesto, con lo que $E_2 = \mathbb{Q}(\sqrt{3}i)$

Por lo tanto $E_1 = E_2$.

17. Sea $E = GF(p^n)$. Si $m \geq 1$ es entero, probar que son equivalentes:

i) E **tiene un subcuerpo de** p^m **elementos**
ii) $m \mid n$
iii) $p^m - 1$ **divide a** $p^n - 1$

Veamos primero que $i) \Rightarrow ii)$

Dado que E es un cuerpo de p^n elementos , sabemos que su cuerpo primo es isomorfo a $\mathbb{Z}/p\mathbb{Z}$, con lo que, por definición, $carE = p$.

Suponemos que E contiene un subcuerpo F de p^m elementos. Es decir, E es una extensión de F.

Consideremos a E como F-espacio vectorial (Se puede hacer porque $(E, +)$ es un grupo abeliano y $\exists\ F \times E \longrightarrow E$ definida como $(t, a) \longrightarrow ta$ cumpliendo las condiciones necesarias). Como E es finito como cuerpo, considerado como F-espacio vectorial también lo es, es decir, $dim_F(E) = d < \infty$.

Recordar que $dim_F(E)$ coincide con el grado de la extensión E/F ($[E : F]$)
$\Rightarrow$
$[E : F] = d < \infty$.

Sea $a \in E$ y sean $a_1, a_2, ..., a_d$ una F-base de E. Entonces

$$a = t_1a_1 + t_2a_2 + ... + t_da_d \text{ con } t_i \in F$$

Teniendo en cuenta esto, dado que cada t_i recorre p^m elementos distintos, se podrán formar $(p^m)^d$ términos distintos de E, es decir, $\mid E \mid = (p^m)^d$.

Por otro lado, sabemos que $\mid E \mid = p^n$. Así que

$$\mid E \mid = (p^m)^d = p^{md} = p^n \Rightarrow n = md \Rightarrow m \mid n$$

Veamos ahora que $ii) \Rightarrow iii)$

Para resolver este apartado, recordemos primero el teorema de EVALUACIÓN visto en temas anteriores de teoría:

"Sean R y S anillos conmutativos y con unidad y $\varphi : R \longrightarrow S$ homomorfismo de anillos tal que $\varphi(1_R) = 1_S$, entonces, $\exists$ un único homomorfismo de anillos $\tilde{\varphi} : R[x] \longrightarrow S$ tal que $\tilde{\varphi}_{|_R} = \varphi$ y $\tilde{\varphi}(x) = s$, siendo s un elemento de S previamente fijado".
Además, $\tilde{\varphi}$ viene dado por

$$\tilde{\varphi} : R[x] \longrightarrow S$$
$$a_0 + a_1x + ... + a_mx^m \longmapsto \varphi(a_0) + \varphi(a_1)s + ... + \varphi(a_m)s^m$$

Sigamos con el ejercicio. Supongamos que $m \mid n$, es decir, supongamos que $\exists d$ tal que $n = md$.
Sabemos que

$$x^d - 1 = (x - 1)(x^{d-1} + x^{d-2} + ... + x + 1)$$

Si se pudiera sustituir x por p^m, se tendría

$$p^n - 1 = p^{md} - 1 = (p^m)^d - 1 = (p^m - 1)(p^{m(d-1)} + p^{m(d-2)} + ... + p^m + 1) \Rightarrow$$
$$\Rightarrow (p^m - 1)|(p^n - 1)$$

como queremos, con lo que este apartado se reduce a comprobar si se puede realizar la sustitución, y ahí, es cuando entra el teorema de evaluación recordado.

Consideremos el homomorfismo $1_{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Z}$ y $p^m \in \mathbb{Z}$ ($\varphi : R \longrightarrow S$, y s del teorema de evaluación). El teorema garantiza que ese homomorfismo se extiende al homomorfismo único

$$\tilde{1}_{\mathbb{Z}} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$$

$$t_0 + t_1 x + ... + t_r x^r \longmapsto t_0 + t_1 p^m + ... + t_r p^{mr}$$

lo que justifica que se pueda realizar la sustitución, ya que simplemente sería aplicar $\tilde{1}_{\mathbb{Z}}$ al polinomio $x^d - 1$.

Por último, veamos que $iii) \Rightarrow i)$

Suponemos, por hipótesis, que $(p^m - 1) \mid (p^n - 1)$.

Sabemos que E es un cuerpo finito de p^n elementos $\Rightarrow E^* \cong C_{p^n-1}$ (C_{p^n-1} = grupo cíclico de $p^n - 1$ elementos).

Por ser E^* cíclico, sabemos que $\exists \mid H \leq E^*$ tal que $|H| = p^m - 1$ (Ya que en un grupo cíclico finito existe un único subgrupo para cada divisor del orden del grupo).

Notar que si $a \in H \Longrightarrow a^{p^m-1} = 1$ (porque dado un grupo finito G, $\forall g \in G$ se verifica que $g^{|G|} = 1) \Longrightarrow a^{p^m} = a \Longrightarrow$ todos los elementos de H son raíces del polinomio $x^{p^m} - x$.

Consideremos $H \cup \{0\}$. Los elementos de $H \cup \{0\}$ son raíces de $x^{p^m} - x$ (los de H lo acabamos de ver y el 0 es claro), y además, no hay más, pues $|H \cup \{0\}| = p^m = \ grado(x^{p^m} - x)$.

Como consecuencia, sabemos, por la demostración de un resultado visto en teoría, que $H \cup \{0\}$ es un subcuerpo de E de p^m elementos (se trata del resultado que hace referencia a la existencia de cuerpos finitos de p^n elementos para cada primo p y $n > 1$).

18.Sea $p(x)$ mónico irreducible en $GF(p)[x]$ de grado m. Dado un entero $n \geq 1$ probar que son equivalentes:

i) $p(x) \mid (x^{p^n} - x)$
ii) $p(x)$ **tiene alguna raíz en un cuerpo de** p^n **elementos**
iii) $m \mid n$

Veamos primero que $i) \Rightarrow ii)$

$\circ$ Como ya hemos recordado en el ejercicio anterior, las raíces de $x^{p^n} - x$ forman un cuerpo de p^n elementos.

∘ También sabemos, que salvo isomorfismos, $\exists$ un único cuerpo finito de p^n elementos ($GF(p^n)$).
∘ Además, las raíces de $x^{p^n} - x$ son raíces de sus factores irreducibles y al revés.

Teniendo en cuenta estos tres puntos, como podemos considerar que $GF(p^n)$ está formado por las raíces de $x^{p^n} - x$, si $p(x) \mid (x^{p^n} - x)$, $\exists a \in GF(p^n)$ tal que a es raíz de $p(x)$.

Veamos ahora que $ii) \Rightarrow iii)$

Supongamos que existe un cuerpo E de p^n elementos tal que $a \in E$ y a es raíz de $p(x)$. Notar, que entonces, $GF(p) \subseteq E$ ya que $carE = p$ y su cuerpo primo $\triangle = \mathbb{Z}/p\mathbb{Z} = GF(p)$.

Tenemos

$$\left.\begin{array}{l} a \text{ raíz de } p(x) \\ p(x) \text{ polinomio mónico irreducible en } GF(p)[x] \end{array}\right\} \Rightarrow p(x) = Irr(a, GF(p)) \Rightarrow [GF(p)(a) : GF(p)] = m.$$

Como consecuencia, $dim_{GF(p)} GF(p)(a) = m \Longrightarrow |GF(p)(a)| = p^m$, pues si $\{a_1, a_2, ..., a_m\}$ es una $GF(p)$-base de $GF(p)(a)$, todo elemento de $GF(p)(a)$ se puede poner como $t_1a_1 + t_2a_2 + ... + t_ma_m$ con $t_i \in GF(p)$.

Así

$$\left.\begin{array}{l} |E| = p^n \\ |GF(p)(a)| = p^m \\ GF(p)(a) \subseteq E \end{array}\right\} \Rightarrow m \mid n \text{ (por el ejercicio 17).}$$

Por último, veamos que $iii) \Rightarrow i)$

Supongamos que $m \mid n$.

Sea a raíz de $p(x)$ en una cierta extensión de $GF(p)$(existencia garantizada por un resultado de teoría). Entonces, $p(x) = Irr(a, GF(p))$.
Consideremos $GF(p)(a)$. Tal y como se ha visto en el apartado anterior, $[GF(p)(a) : GF(p)] = m$ y $|GF(p)(a)| = p^m$.

Si comprobáramos que a es raíz de $x^{p^n} - x$ se tendría que $p(x) \mid x^{p^n} - x$.

Dado que $a \in GF(p)(a)$ y que $|GF(p)(a)| = p^m$, sabemos que a es raíz del polinomio $x^{p^m} - x \Rightarrow a^{p^m} = a$.

Por otra parte, como $m \mid n \Rightarrow \exists r$ tal que $n = mr$, con lo que

$$a^{p^n} = a^{p^{mr}} = \left[\left[\left[\underbrace{a^{p^m}}_{a}\right]^{p^m}\right]^{\cdots}\right]^{p^m} = \left[\left[a^{p^m}\right]^{\cdots}\right]^{p^m} = ... = a$$

Por lo tanto a es raíz de $x^{p^n} - x$, y como consecuencia, $p(x) \mid x^{p^n} - x$.

19. Demostrar que x^4+1 no es irreducible sobre cualquier cuerpo finito.

Sea K un cuerpo finito ($K = GF(p^n) = GF(q)$).

Si $carK = 2 \Longrightarrow x^4+1 = (x+1)^4 \Longrightarrow x^4+1$ no es irreducible sobre K.

Suponemos que $carK = p$ con p primo distinto de 2.

Como q es impar, existe $r \geq 1$ tal que $q = 2r+1 \Longrightarrow q^2-1 = 4r(r+1) \Longrightarrow 8 \mid (q^2-1)$.

Considerar $E = GF(q^2) \Longrightarrow E^* \cong C_{q^2-1}$ y como $8|q^2-1$, sabemos que existe $a \in E^*$ tal que $o(a) = 8$. Por lo tanto $0 = a^8-1 = (a^4-1)(a^4+1)$ y necesariamente $a^4+1 = 0$. Si $p(x) = Irr(a, GF(q))$ entonces $p(x)|x^4+1$.Como $GF(q) \subseteq GF(q)(a) \subseteq GF(q^2)$ y $[GF(q^2) : GF(q)] = 2$, el grado de $p(x)$ puede ser $1, 2$. Concluimos por tanto que x^4+1 no es irreducible en $GF(q)[x]$.

20. Sea n un entero positivo y $f(x) = x^n - 2$ irreducible sobre $\mathbb{Q}$ por el criterio de Eisenstein. Determinar el cuerpo de escisión E de $f(x)$ sobre $\mathbb{Q}$. Si $n = p$, con p primo, razonar que $[E : \mathbb{Q}] = p(p-1)$.

Calculemos primero el cuerpo de escisión de $f(x)$ sobre $\mathbb{Q}$.

Si ω es una raíz n-ésima primitiva de la unidad, es claro que $E = \mathbb{Q}(\sqrt[n]{2}, \omega)$.

Supongamos que $n = p$. Expliquemos algo más este caso particular:
Las raíces de $f(x)$ son $\sqrt[p]{2}$, $\sqrt[p]{2}\omega, \ldots, \sqrt[p]{2}\omega^{p-1}$ siendo $\omega = e^{\frac{2\pi i}{p}}$ una raíz p-ésima primitiva de la unidad.
Entonces, el cuerpo de escisión E de $f(x)$ sobre $\mathbb{Q}$ viene dado por

$$E = \mathbb{Q}(\sqrt[p]{2}, \sqrt[p]{2}\omega, \ldots, \sqrt[p]{2}\omega^{p-1}) = \mathbb{Q}(\sqrt[p]{2}, \omega)$$

.
Veamos ahora que $[E : \mathbb{Q}] = p(p-1)$.

Como $E = \mathbb{Q}(\sqrt[p]{2}, \omega) = \mathbb{Q}(\sqrt[p]{2})(\omega)$, aparece la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{2}) \subseteq \mathbb{Q}(\sqrt[p]{2})(\omega) = E$$

Luego, por transitividad de grados

$$[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \cdot [E : \mathbb{Q}(\sqrt[p]{2})]$$

Como $\sqrt[p]{2}$ es algebraico, se tiene que
$[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = \delta(Irr(\sqrt[p]{2}, \mathbb{Q}) = \delta(x^p - 2) = p$.

Por otra parte, calculemos $[E : \mathbb{Q}(\sqrt[p]{2})]$. Para ello, como ω es algebraico, será suficiente con calcular $Irr(\omega, \mathbb{Q}(\sqrt[p]{2}))$ y ver cuál es su grado.

Sabemos que $Irr(\omega, \mathbb{Q}) = x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt[p]{2})[x]$, ya que como ω es raíz p-ésima primitiva de la unidad, es raíz del polinomio
$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, y por tanto, es raíz de $x^{p-1} + \cdots + x + 1$, que

es irreducible sobre $\mathbb{Q}$.

Como consecuencia de la definición de polinomio irreducible, y de que $Irr(\omega, \mathbb{Q}) = x^{p-1} + \cdots + x + 1 \in \mathbb{Q}(\sqrt[p]{2})[x]$ se tiene que

$$Irr(\omega, \mathbb{Q}(\sqrt[p]{2})) \mid x^{p-1} + \cdots + x + 1$$

$$\Downarrow$$

$$\delta(Irr(\omega, \mathbb{Q}(\sqrt[p]{2}))) \leq p - 1$$

Así, $[E : \mathbb{Q}] \leq p(p-1)$.

Por otro lado, como $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}]$ y $[\mathbb{Q}(\omega) : \mathbb{Q}]$ dividen a $[E : \mathbb{Q}]$ (por transitividad de grados) y p es primo, se tiene que $p \cdot (p-1) \mid [E : \mathbb{Q}]$

$\underbrace{\Longrightarrow}_{[E:\mathbb{Q}] \leq p(p-1)}$ $\quad [E : \mathbb{Q}] = p(p-1)$.

21. Sea $a \in \mathbb{C}$ satisfaciendo $a^2 = 1 + i$. Demostrar que cada cuerpo de la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, a)$$

es extensión de grado 2 de su anterior.

$$\mathbb{Q} \subseteq \mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, a)$$

$\underline{[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2}$

Es claro pues $i\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ y $Irr(i\sqrt{2}, \mathbb{Q}) = x^2 + 2$.

$\underline{[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(i\sqrt{2})] = 2}$

Para demostrarlo basta tener en cuenta que $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$, ya que entonces, por transitividad de grados se tiene que

$$4 = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(i\sqrt{2})] \cdot [\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(i\sqrt{2})] \cdot 2$$

$$\Downarrow$$

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(i\sqrt{2})] = \frac{4}{2} = 2$$

$\underline{[\mathbb{Q}(\sqrt{2}, a) : \mathbb{Q}(i, \sqrt{2})] = 2}$

Para probar que $[\mathbb{Q}(\sqrt{2}, a) : \mathbb{Q}(i, \sqrt{2})] = 2$, veamos que $[\mathbb{Q}(\sqrt{2}, a) : \mathbb{Q}] = 8$, ya que entonces, por transitividad de grados, se tiene que

$$8 = [\mathbb{Q}(\sqrt{2}, a) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{2}, a) : \mathbb{Q}(i, \sqrt{2})] = 4 \cdot [\mathbb{Q}(\sqrt{2}, a) : \mathbb{Q}(i, \sqrt{2})]$$

$$\Downarrow$$

$$[\mathbb{Q}(\sqrt{2}, a) : \mathbb{Q}(i, \sqrt{2})] = \frac{8}{4} = 2$$

Como $a^2 = 1 + i$ se tiene que $a^2 - 1 = i \Longrightarrow (a^2 - 1)^2 = -1 \Longrightarrow a^4 - 2a^2 + 2 = 0$. Las raíces de $x^4 - 2x^2 + 2 = 0$ son: $a_1 = a = \sqrt{1+i}, a_2 = -a_1, a_3 = \sqrt{1-i}, a_4 = -a_3$.

Como

$$a_1a_3 = \sqrt{2} \notin \mathbb{Q},\ \mathbb{Q}(a_1^2) = \mathbb{Q}(i) \neq \mathbb{Q}(\sqrt{2})$$

sabemos que si E es cuerpo de escisión de $x^4 - 2x^2 + 2$ sobre $\mathbb{Q}$, $[E : \mathbb{Q}] = 8$ ($G(E/\mathbb{Q}) \cong D_8$) y $E = \mathbb{Q}(a_1, a_1a_3) = \mathbb{Q}(a, \sqrt{2})$.

22. Sea $f(x) = (x^{12} - 16)(x^2 - 3) \in \mathbb{Q}[x]$. Probar
i) $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ es cuerpo de escisión sobre $\mathbb{Q}$ de $f(x)$ y que $[E : \mathbb{Q}] = 12$.
ii) $\exists\ M/\mathbb{Q}$ finita de Galois con $\mathbb{Q} \subseteq M \subseteq E$ tal que $[M : \mathbb{Q}] = 6$.
iii) $G(E/\mathbb{Q}) \ncong A_4$

i)Veamos en primer lugar que E es cuerpo de escisión sobre $\mathbb{Q}$ de $f(x)$.

∘ Las raíces de $x^{12} - 16$ son $a, a\varepsilon, a\varepsilon^2, \ldots, a\varepsilon^{11}$ siendo

$$\begin{cases} a = \sqrt[12]{16} = 2^{\frac{4}{12}} = 2^{\frac{1}{3}} = \sqrt[3]{2} \text{ (raíz real)} \\ \varepsilon = e^{\frac{2\pi i}{12}} = e^{\frac{\pi i}{6}} = \cos 30 + i \sin 30 = \dfrac{\sqrt{3}}{2} + \dfrac{i}{2} \\ (\varepsilon \text{ es raíz 12-ésima primitiva de la unidad }) \end{cases}$$

∘ Las raíces de $x^2 - 3$ son $\sqrt{3}$ y $-\sqrt{3}$.

Por tanto, el cuerpo de escisión de $f(x)$ sobre $\mathbb{Q}$ es

$$E = \mathbb{Q}(a, a\varepsilon, \ldots, a\varepsilon^{11}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$$

Veamos ahora que $[E : \mathbb{Q}] = 12$.

Sea $L = \mathbb{Q}(\sqrt{3}, i)$. Aparece la cadena

$$\mathbb{Q} \subseteq L \subseteq E = L(\sqrt[3]{2})$$

con lo que

$$[E : \mathbb{Q}] = [E : L][L : \mathbb{Q}]$$

∘ $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$ puesto que:

- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, i)$
- $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$
- $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ ya que $\sqrt{3}$ es algebraico y $Irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3$
- $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] = 2$ pués i es algebraico y $Irr(i, \mathbb{Q}(\sqrt{3})) = x^2 + 1$ (ya que i no está en $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$)

∘ Calculemos $[E : L]$. Para ello, obtengamos el $Irr(\sqrt[3]{2}, L)$.

Sabemos que $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$.

Recordar que $o(\varepsilon) = 12$ así $o(\varepsilon^4) = 3$ y las raíces de $x^3 - 2$ son $\sqrt[3]{2}$, $\sqrt[3]{2}\varepsilon^4$ y $\sqrt[3]{2}\varepsilon^8$. Si llamamos $\omega = \varepsilon^4$, se tiene que las raíces son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ y $\sqrt[3]{2}\omega^2$.

Si $\sqrt[3]{2} \in L \Longrightarrow \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq L$ y entonces $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, dividiría a $4 = [L : \mathbb{Q}]$.

De forma totalmente análoga sucede para $\sqrt[3]{2}\omega$ y $\sqrt[3]{2}\omega^2$.

Luego, $Irr(\sqrt[3]{2}, L) = x^3 - 2 \Longrightarrow [E : L] = 3$.

Por lo tanto, $[E : \mathbb{Q}] = [E : L][L : \mathbb{Q}] = 3 \cdot 4 = 12$.

ii) Consideremos el cuerpo de escisión M de $x^3 - 2$ sobre $\mathbb{Q}$.
Hemos visto antes que sus raíces son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ y $\sqrt[3]{2}\omega^2$ ($\omega = -1/2 + i\sqrt{3}/2$), con lo que

$$M = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$$

Como $car\mathbb{Q} = 0$, $x^3 - 2$ es separable, y así , la extensión $M/\mathbb{Q}$ es de Galois (por ser M cuerpo de escisión de un polinomio separable).

Por otra parte, calculemos $[M : \mathbb{Q}]$.

Tenemos la cadena

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq M$$

con lo que

$$[M : \mathbb{Q}] = [M : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

$\circ$ $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ya que $\sqrt[3]{2}$ es algebraico y $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$.

$\circ$ Sabemos que $Irr(i\sqrt{3}, \mathbb{Q}) = x^2 + 3$.
Además, como $i\sqrt{3}$ no pertenece a $\mathbb{Q}(\sqrt[3]{2})$, se tiene que $Irr(i\sqrt{3}, \mathbb{Q}(\sqrt[3]{2})) = x^2 + 3$ luego $[M : \mathbb{Q}(\sqrt[3]{2})] = 2$.

Por lo tanto, $[M : \mathbb{Q}] = [M : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$.

iii) Como $M/\mathbb{Q}$ es finita de Galois, sabemos por el teorema fundamental de Galois, que

$$G(M/\mathbb{Q}) \cong \frac{G(E/\mathbb{Q})}{G(E/M)}$$

Además, $|G(M/\mathbb{Q})| = [M : \mathbb{Q}] = 6$.

Por otra parte, notar que $E/\mathbb{Q}$ también es una extensión finita de Galois, ya que $f(x)$ es separable por ser $car\mathbb{Q} = 0$, y E es su cuerpo de escisión. Como consecuencia, $|G(E/\mathbb{Q})| = [E : \mathbb{Q}] = 12$.

Entonces

$$6 = |G(M/\mathbb{Q})| = \frac{|G(E/\mathbb{Q})|}{|G(E/M)|} = \frac{12}{|G(E/M)|}$$

$$\Downarrow$$

$$|G(E/M)| = \frac{12}{6} = 2$$

Luego, $G(E/M)$ es un subgrupo de orden 2 normal en $G(E/\mathbb{Q}) \Longrightarrow$
$G(E/\mathbb{Q}) \ncong A_4$ puesto que los únicos subgrupos normales de A_4 son 1, V_4 y A_4, ninguno de ellos es de orden 2.