HOJA 2

1. Demostremos primero que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$:

Observemos que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

$\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ trivialmente ya que

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) := \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}$$

por lo que $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ tomando $a=0, b=1, c=1, d=0$

Ahora veamos que $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$: para ello probamos que $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Supongamos $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \{1, \sqrt{2}+\sqrt{3}, (\sqrt{2}+\sqrt{3})^2, (\sqrt{2}+\sqrt{3})^3\}$
(a priori, antes de terminar la demostración, podría ser mayor, pero con estos elementos nos llegarán para generar $\sqrt{2}, \sqrt{3}, \sqrt{6}$)

$$\sqrt{2} = a + b(\sqrt{2}+\sqrt{3}) + c(\sqrt{2}+\sqrt{3})^2 + d(\sqrt{2}+\sqrt{3})^3 =$$

$$= (a+5c)\cdot 1 + (b+11d)\sqrt{2} + (b+9c)\sqrt{3} + 2c\sqrt{6} \Rightarrow$$

$$\Rightarrow \begin{cases} a+5c=0 \\ b+11d=1 \\ b+9c=0 \\ 2c=0 \end{cases} \Rightarrow \begin{cases} c=0 \\ b=0 \\ d=\frac{1}{11} \\ a=0 \end{cases} \Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

Análogo para $\sqrt{3}, \sqrt{6}$.

Otra forma más corta: sabemos ya que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$:

$$\mathbb{Q} \xrightarrow{2\acute{o}4\,\circledast} \mathbb{Q}(\sqrt{2}+\sqrt{3}) \hookrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) \quad (4)$$

$\circledast$ Supongamos 2: $gr(Irr(\mathbb{Q}, \sqrt{2}+\sqrt{3})) = 2$

Sea $\underbrace{x^2+bx+c}_{p(x)} = 0$ pol. genérico de $\mathbb{Q}$ y $p(\sqrt{2}+\sqrt{3}) = 0$

$$\Leftrightarrow (\sqrt{2}+\sqrt{3})^2 + b(\sqrt{2}+\sqrt{3}) + c = 0 \quad \text{con} \quad b,c \in \mathbb{Q} \Rightarrow$$

$\Rightarrow$ Imposible $\Rightarrow gr(Irr(\mathbb{Q}, \sqrt{2}+\sqrt{3})) = 4 \Rightarrow$

$\Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

Ahora, ¿cómo calculamos $\mathrm{Irr}(\mathbb{Q}, \overbrace{\sqrt{2}+\sqrt{3}}^{\alpha})$?

Buscamos $p(x) = x^4 + ax^3 + bx^2 + cx + d$, $a,b,c,d \in \mathbb{Q}$

tal que $p(\alpha) = 0$:

$\alpha^4 + a\alpha^3 + b\alpha^2 + c\alpha + d = 0 \xrightarrow{\text{operaciones}} [\cdots] \Rightarrow$

$\Rightarrow (49+5b+d).1 + (11a+c)\sqrt{2} + (9a+c)\sqrt{3} + (20+2b)\sqrt{6} = 1$

Igualamos coef. a cero $\Rightarrow \begin{cases} a = 0 \\ c = 0 \\ b = -10 \\ d = 1 \end{cases} \Rightarrow p(x) = x^4 - 10x^2 + 1$

2. No es difícil ver que $\alpha = \sqrt[3]{9} + \sqrt[3]{3} - 1 \in \mathbb{Q}(\sqrt[3]{3})$

ya que $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[3]{3}) = \{1, \sqrt[3]{3}, \sqrt[3]{3^2} = \sqrt[3]{9}\}$

ya que $|\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}| = 3$ ($x^3 - 3$ irred. en $\mathbb{Q}$ y $\sqrt[3]{3}$ es raíz $\Rightarrow \mathrm{Irr}(\mathbb{Q}, \sqrt[3]{3})$).

Sea ahora $p(x) = x^3 + ax^2 + bx + $, $a,b,c \in \mathbb{Q}$ pol. genérico

Buscamos $p(\alpha) = 0$ y $p(x)$ irred. en $\mathbb{Q}$:

$\alpha^3 + a\alpha^2 + b\alpha + c = 0 \Rightarrow$ operamos y despejamos a,b,c

Habría también que ver que el pol. obtenido es irreducible.

3. $\mathbb{Q}(i,\sqrt{2}) = \{a+bi+c\sqrt{2}+d\sqrt{2}i \;,\; a,b,c,d \in \mathbb{Q}\}$

$\mathbb{Q}(\sqrt{2}i) = \{a+b\sqrt{2}i \;,\; a,b \in \mathbb{Q}\}$

$\mathbb{Q}(\sqrt{2}+i) = \{a+b(\sqrt{2}+i)+c(\sqrt{2}+i)^2+d(\sqrt{2}+i)^3 \;,\; a,b,c,d \in \mathbb{Q}\}$

¿ $\mathbb{Q}(\sqrt{2},\sqrt{1+\sqrt{2}}) = \mathbb{Q}(\sqrt{1+\sqrt{2}})$?

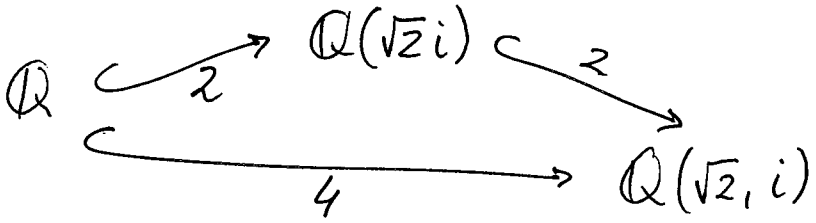
$\supset$ trivial

¿$\subset$?

Veamos que $\sqrt{2} \in \mathbb{Q}(\sqrt{1+\sqrt{2}})$:

$\sqrt{2} \in \mathbb{Q}(\sqrt{1+\sqrt{2}})$ porque $(\sqrt{1+\sqrt{2}})^2 = 1+\sqrt{2}$ y le podemos restar $1 \in \mathbb{Q}$ porque es cerrado por la operación suma.

Finalmente tener en cuenta:



4.

i) $\mathbb{Q}(\sqrt[6]{3})/\mathbb{Q}$

$\sqrt[6]{3}$ es raíz de $x^6-3=0$, que es un pol. irred. en $\mathbb{Q}$ por el criterio de Einsestein con $p=3$.

$\Rightarrow \mathrm{Irr}(\mathbb{Q},\sqrt[6]{3}) = x^6-3 \Rightarrow |\mathbb{Q}(\sqrt[6]{3}):\mathbb{Q}| = 6$

$\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[6]{3})$: $\{1, \sqrt[6]{3}, \sqrt[6]{9}, \sqrt[6]{27}, \sqrt[6]{81}, \sqrt[6]{243}\}$

ii) $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

$\mathbb{Q}(\sqrt{2},\sqrt{3}) = L(\sqrt{3})$

$|$

$\mathbb{Q}(\sqrt{2}) = L$

$|$

$\mathbb{Q}$

$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| =$

$= |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}):\mathbb{Q}|$

Sabemos que $p(x) = x^2 - 2$ es irred. en $\mathbb{Q}$ y que $\sqrt{2}$ es raíz $\Rightarrow \text{Irr}(\mathbb{Q},\sqrt{2}) = x^2 - 2$

$\Rightarrow |\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2$ $\quad$ $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$: $\{1, \sqrt{2}\}$

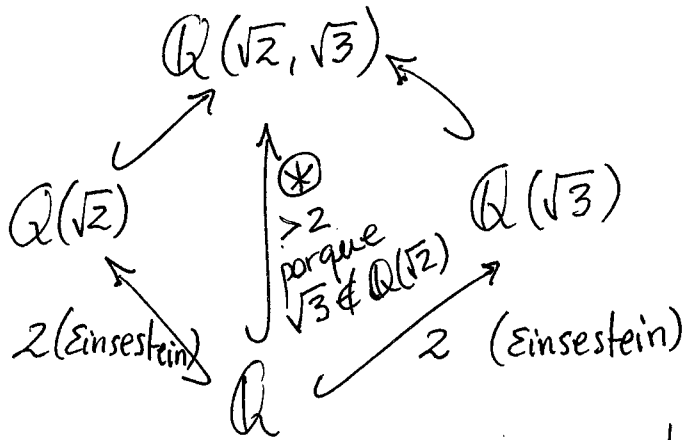
Ahora bien, $x^2 - 3$ es irreducible en L: (y en $\mathbb{Q}$):

R.A. $\sqrt{3} = a + b\sqrt{2}$ (tratamos de escribir $\sqrt{3}$ en términos de la $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$):

$3 \in (a+b\sqrt{2})^2 = \underbrace{a^2 + 2b^2}_{\in \mathbb{Q}} + \underbrace{2ab\sqrt{2}}_{\in \mathbb{Q}}$

$\in \mathbb{Q}$ $\quad$ $\hookrightarrow$ tiene que estar en $\mathbb{Q}$ $\not\Rightarrow$ $\sqrt{2} \notin \mathbb{Q}$

Entonces:



(*) También como $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2$ y $|\mathbb{Q}(\sqrt{3}):\mathbb{Q}| = 2 \Rightarrow$

$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| \leq 4$ y al mismo tiempo $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| > 2$

$\Rightarrow |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| = 4$

$\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

iii) $\mathbb{Q}(\sqrt{2},\sqrt{3},i)\,/\,\mathbb{Q}$

$\mathbb{Q}(\sqrt{2},\sqrt{3},i)$

(2) $\{$ $\Big|$ $\mathbb{Q}(\sqrt{2},\sqrt{3})$

4 $\{$ $\Big|$

$\uparrow$ $\mathbb{Q}$

apartado ii)

Sea $p(x)=x^2+1$, pol. que tiene como raíz i.

Veamos que $p(x)$ es irreducible en $\mathbb{Q}(\sqrt{2},\sqrt{3})$: veamos que no tiene raíces en $\mathbb{Q}(\sqrt{2},\sqrt{3})$:

Elemento genérico de $\mathbb{Q}(\sqrt{2},\sqrt{3})$:

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$$

$$(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})^2+1=0 \iff \dots \iff$$

$\iff$ llegaremos a una contradicción $\Rightarrow x^2+1$ irreducible en $\mathbb{Q}(\sqrt{2},\sqrt{3}) \Rightarrow \mathrm{Irr}(\mathbb{Q}(\sqrt{2},\sqrt{3}),i)=x^2+1 \Rightarrow$

$$|\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}(\sqrt{2},\sqrt{3})| = gr(x^2+1)=2 \Rightarrow$$

$$\Rightarrow |\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}| = 4\cdot 2 = 8$$

$\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2},\sqrt{3},i)$: $\{1,\sqrt{2},\sqrt{3},\sqrt{6},\sqrt{2}i,\sqrt{3}i,\sqrt{6}i,i\}$

iv) $\mathbb{Q}(\sqrt{2}i)\,/\,\mathbb{Q}$

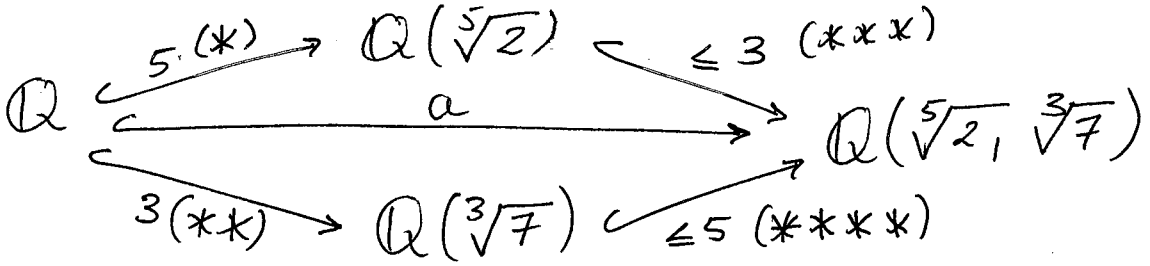
$p(x)=x^2+2$ es un pol. que $\sqrt{2}i$ es raíz

Por Einsestein con $p=2$ vemos que es irreducible en $\mathbb{Q}$

$$\Rightarrow \mathrm{Irr}(\mathbb{Q},\sqrt{2}i)=x^2+2 \Rightarrow |\mathbb{Q}(\sqrt{2}i):\mathbb{Q}|=2$$

$\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}i)$: $\{1,\sqrt{2}i\}$

v) $\mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{7}) \,/\, \mathbb{Q}(\sqrt[3]{2})$



(*) $|\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}| = 5$ ya que $x^5 - 2$ es irred. en $\mathbb{Q}$ por Einsestein con $p = 2 \Rightarrow \text{Irr}(\mathbb{Q}, \sqrt[5]{2}) = x^5 - 2$

(**) $|\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}| = 3$ ya que $x^3 - 7$ es irred. en $\mathbb{Q}$ por Einsestein con $p = 7 \Rightarrow \text{Irr}(\mathbb{Q}, \sqrt[3]{7}) = x^3 - 7$

Por lo tanto, $a \geq 3 \cdot 5 = 15$ por el teorema de transitividad de grados. Por otro lado, si $\mathbb{Q}(\sqrt[3]{7})$ extiende $\mathbb{Q}$ con grado 3, $\mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{7})$ extiende a $\mathbb{Q}(\sqrt[5]{2})$ con grado ≤ 3 (***).

Finalmente, si $\mathbb{Q}(\sqrt[5]{2})$ extiende $\mathbb{Q}$ con grado 5, $\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2})$ extiende a $\mathbb{Q}(\sqrt[3]{7})$ con grado ≤ 5 (****).

$$\Rightarrow |\mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{7}) : \mathbb{Q}| = 3 \cdot 5 = 15$$

La $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{7})$ es:

$$\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \beta^2, \alpha\beta, \alpha^2\beta, \alpha^3\beta, \alpha^4\beta, \alpha\beta^2, \alpha^2\beta^2, \alpha^3\beta^2, \alpha^4\beta^2\}$$

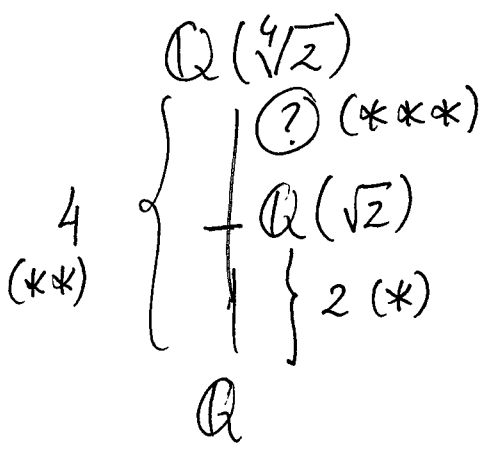
con $\alpha = \sqrt[5]{2}$ y $\beta = \sqrt[3]{7}$.

Por el T^me transitividad de grados: $|\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt[5]{2})| = 3$

$\mathbb{Q}(\sqrt[5]{2})$-base de $\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2})$: $\{1, \beta, \beta^2\}$

Habría que ver que $\beta, \beta^2 \notin \mathbb{Q}(\sqrt[5]{2})$ para demostrar que es esta base

vi) $\mathbb{Q}(\sqrt[4]{2}) \,/\, \mathbb{Q}(\sqrt{2})$



(*) Como hemos visto, $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2$ usando x^2-2 y viendo por Einsestein que es irred. en $\mathbb{Q}$

(**) Por lo mismo, $|\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}| = 4$ usando que $\sqrt[4]{2}$ es raíz de x^4-2 (irred. por Einsestein en $\mathbb{Q}$

(***) Usando el teorema de transitividad de grados:

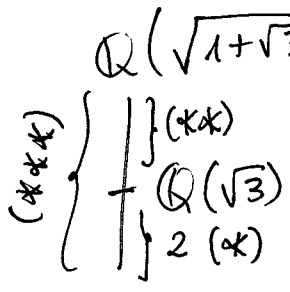
$$|\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})| = |\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}| \,/\, |\mathbb{Q}(\sqrt{2}):\mathbb{Q}| =$$

$$= 4/2 = 2$$

$\mathbb{Q}(\sqrt{2})$-base de $\mathbb{Q}(\sqrt[4]{2})$: $\{1, \sqrt[4]{2}\}$

Vamos a ver que $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$: $\sqrt[4]{2} = a + b\sqrt{2}$ para algún $a,b \in \mathbb{Q}$. Llegaremos a contradicción ##.

vii) $\mathbb{Q}(\sqrt{1+\sqrt{3}}) \,/\, \mathbb{Q}$



(*) Como llevamos visto $\overbrace{x^2-\sqrt{3}-1}^{p(x)}$,

(**) $\sqrt{1+\sqrt{3}}$ es raíz de $p(x)$, que es un polinomio mónico en $\mathbb{Q}(\sqrt{3})$. Nos preguntamos si es irred:

$\mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3} : a,b \in \mathbb{Q}\}$ $\quad B := \{1, \sqrt{3}\}$ $\mathbb{Q}(\sqrt{3})$ base

¿ $\exists a,b \in \mathbb{Q}$: $(a+b\sqrt{3})^2 - \sqrt{3} - 1 = 0$?

$a^2 + 2ab\sqrt{3} + 3b^2 - \sqrt{3} - 1 \Rightarrow (2ab-1)\sqrt{3} + (a^2+3b^2-1).1 = 0$

$$\Rightarrow \begin{cases} 2ab = 1 \longrightarrow b = \frac{1}{2a} \text{ (ya sabíamos que } a \neq 0) \\ a^2+3b^2-1 = 0 \longrightarrow a^2 - 1 = \frac{-3}{4a^2} \end{cases} \longrightarrow 4a^4 - 4a^2 = -3$$

$$\longrightarrow 4\alpha^2 - 4\alpha + 3 = 0 \Rightarrow \alpha = \frac{4 \pm \sqrt{16-4.4.3}}{2.4} \notin \mathbb{Q} \;\; \# \Rightarrow p(x) \text{ irred. en } \mathbb{Q}(\sqrt{3})$$

(***) $\Rightarrow |\mathbb{Q}(\sqrt{1+\sqrt{3}}):\mathbb{Q}| = |\mathbb{Q}(\sqrt{3}):\mathbb{Q}| \cdot |\mathbb{Q}(\sqrt{1+\sqrt{3}}):\mathbb{Q}(\sqrt{3})| = 2.2 = 4$ (**)

$\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{1+\sqrt{3}})$: $\{1, \beta, \beta^2, \beta^3\}$ con $\beta = \sqrt{1+\sqrt{3}}$

viii) $\mathbb{Q}(e^{\frac{2\pi i}{5}}) / \mathbb{Q}$

Sea $p(x) = \frac{x^5-1}{x-1}$ pol. ciclotómico $\Rightarrow$ irred. en $\mathbb{Q}$ (visto en clase)

todo pol. ciclotómico es irred. en $\mathbb{Q}$ (teorema)

$e^{\frac{2\pi i}{5}}$ es raíz de $p(x)$

$\Rightarrow |\mathbb{Q}(e^{\frac{2\pi i}{5}}) : \mathbb{Q}| = gr\left(\frac{x^5-1}{x-1}\right) = gr\left(Irr(\mathbb{Q}; e^{\frac{2\pi i}{5}})\right) = m$

$\mathbb{Q}$-base de $\mathbb{Q}(e^{\frac{2\pi i}{5}})$: $\{1, \beta, \dots, \beta^{m-1}\}$ con $\beta = e^{\frac{2\pi i}{5}}$

x) $\mathbb{R}(\sqrt[4]{-3}) / \mathbb{R}$

Como $\sqrt[4]{-3} \notin \mathbb{R}$ (de hecho $\sqrt[4]{-3} \in \mathbb{C}$) $\Rightarrow$ se genera $\mathbb{C}$

$\Rightarrow |\mathbb{R}(\sqrt[4]{-3}) : \mathbb{R}| = 2 = |\mathbb{C} : \mathbb{R}|$

$\Rightarrow$ $\mathbb{R}$-base de $\mathbb{C} = \{1, i\}$ = $\mathbb{R}$-base de $\mathbb{R}(\sqrt[4]{-3})$

5.

$\mathbb{F}_7(t)$

$\mathbb{F}_7(t^2)$

$x^2 - t^2 \in \mathbb{F}_7(t^2)[x]$

t es raíz de $x^2 - t^2$ y además $\pm t \notin \mathbb{F}_7(t^2)$:

R.A. si $t \in \mathbb{F}_7(t^2) \Rightarrow t = \frac{f(t^2)}{g(t^2)} \Rightarrow$

$\Rightarrow t\,g(t^2) = f(t^2) \quad g \neq 0$

contradicción viendo que $tg(t^2)$ tiene grado impar y $f(t^2)$ grado par.

$\longrightarrow |\mathbb{F}_7(t) : \mathbb{F}_7(t^2)| = 2 \Rightarrow \mathbb{F}_7(t^2)$ - base de $\mathbb{F}_7(t)$: $\{1, t\}$

Ahora vamos a calcular t^{-1} y $(1+t)^{-1}$ en función de $\{1, t\}$

$t = f(t) \longleftrightarrow f(x) = x$ ($f(x) \in \mathbb{F}_7(t^2)$)

$x^2 - t^2 = 0, \quad \underbrace{x}_{f(x)} x = t^2 \Rightarrow x \cdot \frac{1}{t^2} x = 1$

Evaluando en t: $t \cdot \underbrace{\frac{1}{t^2}}_{t^{-1}} \cdot t = 1$

$f(x) = 1 + x$; $\text{mcd}(f(x), x^2 - t^2) = 1$

Aplicamos Bezout + algoritmo de la división

$$\begin{array}{r|l} x^2 - t^2 & x+1 \\ \hline -x^2 - x & x-1 \\ \hline -x - t^2 & \\ -(-x-1) & \\ \hline 1 - t^2 & \end{array}$$

$\Rightarrow x^2 - t^2 = \overbrace{(x+1)}^{f(x)}(x-1) + (1-t^2) \Rightarrow$

$\Rightarrow (x^2 - t^2) + f(x)(1-x) = 1 - t^2 \in \mathbb{F}_7(t^2)$

$\Rightarrow \frac{1}{1-t^2}(x^2 - t^2) + f(x)\frac{1-x}{1-x^2} = 1$

Iden. Bezout: evaluando en t: $f(t) \cdot \frac{1-t}{1-t^2} = 1 \Rightarrow$

$\Rightarrow (t+1)^{-1} = \frac{1}{1-t^2} \cdot 1 + \frac{1}{t^2 - 1} t \in \mathbb{F}_7(t^2)$

6.1 Apuntes

7. $K \subseteq K(a_0) \subseteq K(a_0, a_1, \dots, a_n) \subseteq K(a_0, a_1, \dots, a_n)[u]$

u alg sobre $K(a_0, \dots, a_n)$ porque es raíz para algún polinomio

Usamos el teorema de extensiones finitas y está demostrado. (↳ con elem. algebraicos)

8.

$\Leftarrow$ Se dice que es lo fácil.

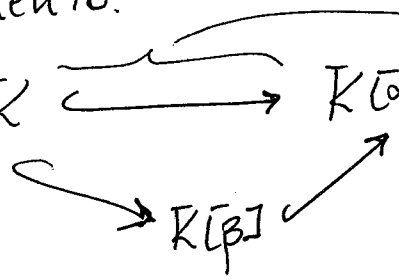
$\Rightarrow$ Supongamos que $K[\alpha]$ es un cuerpo

R.A.: supongamos que para llegar a una contradicción que α no es alg. sobre K.

$\Rightarrow K[\alpha] \cong K[x]$ no es un cuerpo $\Rightarrow$ contradicción ✱

$\Rightarrow \alpha$ alg. sobre K.

Resulta que solo lo hemos demostrado para α, no $\forall$ elemento.



$\Rightarrow$ grado $= gr(Irr(K, \alpha)) < \infty$

$\Rightarrow$ la extensión es finita de grado n $\Rightarrow$

$\Rightarrow 1, \beta, \dots, \beta^n$ son lin. dep. sobre K.

9. a) fácil usando que $a_i \in K$ (cuerpo) $\Rightarrow \exists\, a_i^{-1}$

b) $\mathbb{A} \to$ algebraicos de los $\mathbb{C}/\mathbb{Q}$

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}] \subseteq \cdots \subseteq \mathbb{A}$$

$x^2 - 2$
$x^3 - 3$
$x^4 - 4$
$\vdots$

extensión de grado infinito

10. Probar que $\underset{\| \; q(x)}{\mathrm{Irr}(L, \alpha)} \;\Big|\; \underset{\| \; p(x)}{\mathrm{Irr}(K, \alpha)}$

En particular: $|L(\alpha) : L| \leq |K(\alpha) : K|$

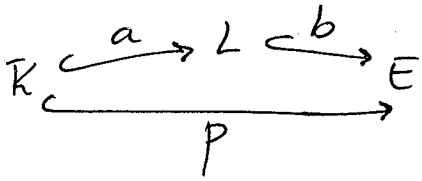
$p(x) \in K[x] \subseteq L[x]$

Como $p(\alpha) = 0$, por el T^ma del elemento algebraico,

$q(x) \mid p(x) \Rightarrow |L[\alpha] : L| = gr(q(x)) \leq gr(p(x)) = |K(\alpha) : K|$

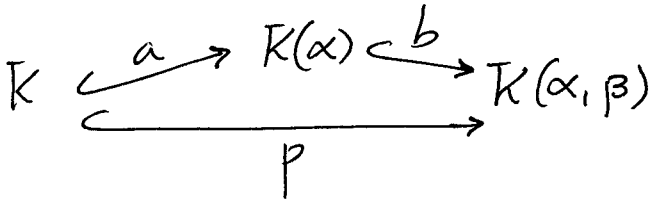
12.

a)



$$p = ab \Rightarrow \begin{cases} a = p \wedge b = 1 \\ \text{ó} \\ b = p \wedge a = 1 \end{cases}$$

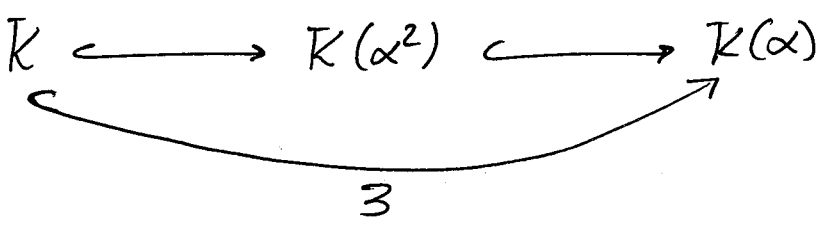
b) Sup. $E = K(a,b)$ (sin pérdida de generalidad)



$$p = ab \Rightarrow \begin{cases} a = p \wedge b = 1 \\ \text{ó} \\ a = 1 \wedge b = p \end{cases}$$

$$\Rightarrow \begin{cases} K(\alpha) = K \Rightarrow K(\beta) = K(a,b) \\ \text{ó} \\ K(a) = K(a,b) \end{cases}$$

c) $p(x) = x^3 + x - 1$, $p(\alpha) = 0$, $\alpha \in E / K$



$K(\alpha^2) = K(\alpha)$ porque $K(\alpha^2) \neq K$ ya que $\alpha^2 \notin K$

Base: $\{1, \alpha, \alpha^2\}$

$\Rightarrow |Irr(K, \alpha^2)| = 3$

$q(x) = x^3 + ax^2 + bx + c$ (pol. genérico)

$q(\alpha^2) = \alpha^6 + a\alpha^4 + b\alpha^2 + c = 0$

Sabemos que $p(\alpha) = 0 \Rightarrow \alpha^3 + \alpha - 1 = 0 \Rightarrow$

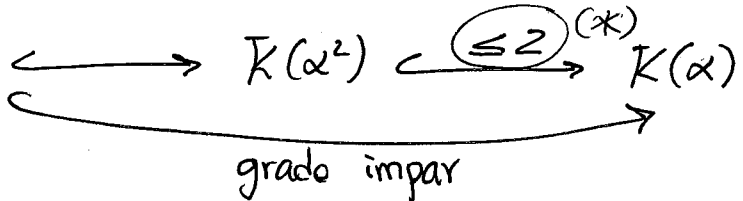
$\Rightarrow \boxed{\alpha^3 = 1 - \alpha} \Rightarrow \boxed{\begin{array}{l} \alpha^6 = \alpha^2 - 2\alpha + 1 \\ \alpha^4 = -\alpha^2 + \alpha \end{array}}$

$\Rightarrow$ Sustituimos en $q(\alpha^2)$:

$q(\alpha^2) = (1 - a + b)\alpha^2 + (-2 + a)\alpha + (1 + c) \cdot 1 = 0$

$\Rightarrow \begin{cases} 1 - a + b = 0 \\ -2 + a = 0 \\ 1 + c = 0 \end{cases} \Rightarrow \begin{cases} b = 1 \\ a = 2 \\ c = -1 \end{cases}$

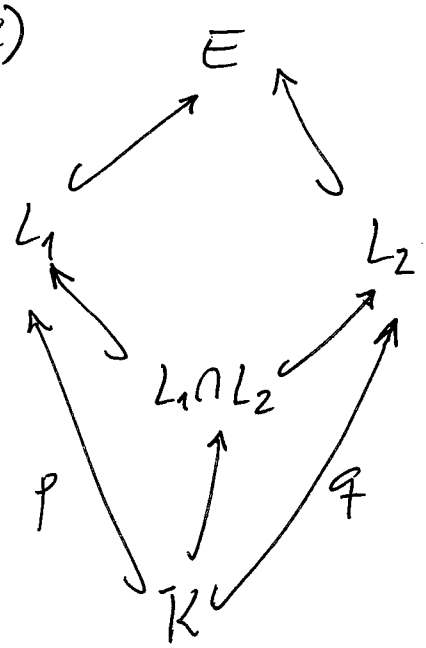
$\boxed{q(x) = x^3 + 2x^2 + x - 1}$

d) 

Como $|K(\alpha) : K|$ = grado impar $\Rightarrow |K(\alpha) : K(\alpha^2)| = 1 \Rightarrow K(\alpha) = K(\alpha^2)$

(*) Es ≤ 2 porque $x^2 - \alpha^2$ es un pol. en $K(\alpha^2)$ tal que α es raíz $\Rightarrow gr(Irr(K(\alpha^2), \alpha)) \leq 2$.

e)



Como p y q son primos entre sí

$|L_1 : L_1 \cap L_2| = p$ y $|L_2 : L_1 \cap L_2| = q$

porque p y q no tienen primos comunes en su descomp. factorial

$\Rightarrow |L_1 \cap L_2 : K| = 1$.