Irreducibilidad de polinomios

1) **Lema de Gauss.** Sea R DFU (ej $\mathbb{Z}$), $Q = \text{Quot}(R)$, $p(x) \in R[x]$.

Si $p(x)$ reducible en $F[x] \Rightarrow p(x)$ reducible en $R[x]$

Más precisamente, si $p(x) = A(x)B(x)$, $A, B \in F[x]$ (no constante)

$\Rightarrow \exists\ r, s \in F$ tq $rA(x) = a(x)$, $sB(x) = b(x)$; $a, b \in R[x]$

y $p(x) = a(x)b(x)$ factorización en $R[x]$

2) **Corolario.** Sea R DFU, $Q = \text{Quot}(R)$, $p(x) \in R[x]$. Si $p(x) = \sum_0^n a_i x^i$, $\text{mcd}\{a_i\} = 1$, entonces

$p(x)$ irreducible en $R[x] \iff p(x)$ irreducible en $F[x]$.

3) **Teorema.** R es DFU $\iff R[x]$ es DFU.

4) **Corolario.** Si R es DFU $\Rightarrow R[x_1, \dots x_n]$ es DFU.

5) **Proposición.** Sea F cuerpo, $p(x) \in F[x]$. $x - a \mid p(x) \iff p(a) = 0$.

6) **Proposición.** Un polinomio de grado 2 o 3 sobre $F[x]$ (F cuerpo) es reducible $\iff$ posee una raíz.

7) **Proposición.** Sea $p(x) = \sum_0^n a_i x^i$, $a_i \in \mathbb{Z}$. Si $\frac{r}{s} \in \mathbb{Q}$ $(\text{mcd}(r,s) = 1)$ es raíz de $p(x)$, entonces $r \mid a_0$, $s \mid a_n$. En particular, si $p(x)$ es mónico en $\mathbb{Z}[x]$ y $p(d) \neq 0$ $\forall d \in \mathbb{Z}$ tq $d \mid$ (término constante), entonces $p(x)$ no tiene raíces en $\mathbb{Q}$.

8) **Proposición.** Sea $I \subseteq R$ un ideal propio (R DI), $p(x) \in R[x]$ no constante. Si la imagen de $p(x)$ en $(R/I)[x]$ no puede ser factorizada en dos polinomios de grado menor, entonces $p(x)$ es irreducible en $R[x]$.

9) Proposición (Criterio de Eisenstein) Sea $P \subseteq R$ ideal primo (R DI), $f(x) = \sum_0^n a_i x^i$ polinomio en $R[x]$ ($n \geq 1$). Si $a_{n-1}, \dots, a_1, a_0 \in P$, $a_0 \notin P^2$, entonces $f(x)$ es irreducible en $R[x]$.

Corolario (Criterio de Eisenstein. Caso $\mathbb{Z}$) Sea $p \in \mathbb{Z}$ primo y $f(x) = \sum_0^n a_i x^i$ ($n \geq 1$). Si $p \mid a_i$ $\forall i \in \{0, \dots, n-1\}$, $p^2 \nmid a_0$, entonces $f(x)$ es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

Ejemplo. Consideremos el polinomio $p(x) = x^4 + 1$. No podemos aplicar criterio de Eisenstein sobre $p(x)$, pero considerando $q(x) = p(x+1)$, tenemos $q(x) = x^4 + 4x^3 + 6x^2 + 4x^2 + 2$. Por criterio de Eisenstein, $q(x)$ es irreducible, entonces $p(x)$ es irreducible.

En efecto, si: $p(x) = q(x)r(x) \Rightarrow q(x) = p(x+1) = q(x+1)r(x+1)$.
Luego $q(x)$ es reducible.

~~Sea $z \in \mathbb{C}$ tal que~~

Los conjugados también son raíces, o sea $z = \sqrt[4]{3}\, e^{-i\alpha/2}$, $z = \sqrt[4]{3}\, e^{-i(\frac{\alpha}{2}+\pi)}$ raíces de $p(x)$.

Afirmación. Si $z \in \mathbb{C}$ es raíz de $p(x) = \sum_{i=0}^{n} a_i x^i$, entonces $\bar{z}$ es raíz de $p(x)$. ($p(x) \in \mathbb{R}[x]$)

$$p(\bar{z}) = \sum_{i=0}^{n} a_i \bar{z}^i = \sum_{i=0}^{n} \overline{a_i z^i} = \overline{\sum_{i=0}^{n} a_i z^i} = \bar{0} = 0$$

Recordar que $\forall a \in \mathbb{C}$: $a \in \mathbb{R} \iff a = \bar{a}$.

¿Reducible por polinomios de grado 2?

$$x^4 - 2x^2 + 5 = (x^2 + ax + b)(x^2 + cx + d)$$
$$= x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd$$
$$= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$$

$$\Rightarrow \begin{cases} a+c=0 \longrightarrow ad+cd=0 \\ ac+b+d=-2 \\ ad+bc=0 \\ bd=5 \end{cases}$$

$$\Rightarrow \begin{cases} ad+bd=0 \\ ad+bc=0 \end{cases} \Rightarrow c(d-b)=0 \overset{c \in \mathbb{C}}{\Rightarrow} c=0 \Rightarrow a=0$$

$$\Rightarrow \begin{cases} b+d=-2 \longrightarrow b=-2-d \\ bd=5 \end{cases} ; \text{ reemplazando, } 5 = bd = (-2-d)d$$

$$\Rightarrow 5 = -d^2 - 2d \Rightarrow d^2 + 2d + 5 = 0 \; ; \; d = \frac{-2 \pm \sqrt{4-20}}{2}$$

$\therefore$ No existe $d \in \mathbb{C}$; $d^2 + 2d + 5 = 0$ $\therefore$ $p(x)$ no se puede factorizar por polinomios de grado 2. $\therefore$ $p(x)$ irreducible. ($\text{en } \mathbb{C}[x]$)

Otra manera. Afirmación. $x^2 + 2x + 5$ es irreducible en $\mathbb{C}[x]$.

+Demostración - $f(x) = x^2 + 2x + 1 + 1 = (x+1)^2 + 4 = g(x+1)$, donde $g(x) = x^2 + 4$.

$g(x)$ irreducible en $\mathbb{C}[x] \Rightarrow f$ irreducible en $\mathbb{C}[x]$.

Si $f(x) = g_1(x) g_2(x)$ Si $f(x) = f_1(x) f_2(x) \Rightarrow$ $g(x+1) = f_1(x) f_2(x)$

tomando $y = x+1$: $g(y) = f_1(y-1) f_2(y-1)$

Problema 8 (Guía 1)

Calcule el grado sobre $\mathbb{Q}$ de las siguientes extensiones

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

(b) $\mathbb{Q}(\sqrt{2},\sqrt{3})$ (d) $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$

- Desarrollo -

(a) Sea $a=\sqrt[4]{3}$, $a^4=3 \Rightarrow a^4-3=0$. a es raíz de $p(x)\in\mathbb{Q}[x]$

$p(x)=x^4-3$. Por criterio de einsenstein $p(x)$ es irreducible.

$$\therefore [\mathbb{Q}(\sqrt[4]{3}),\mathbb{Q}]=4$$

(b) $a=\sqrt{1+2i}$,

$$a^2=1+2i$$
$$\Rightarrow a^2-1=2i$$
$$\Rightarrow (a^2-1)^2=4i^2=-4$$
$$\Rightarrow a^4+1-2a^2=-4$$
$$\Rightarrow a^4-2a^2+5=0$$

a es raíz de $p(x)\in\mathbb{Q}[x]$, $p(x)=x^4-2x^2+5$.

Si $\frac{p}{q}$ (irreducible) es raíz de $p(x)$, $p|5$, $q|1$. Luego raíces racionales pueden ser ± 5.

$$p(5)=625-50+5\neq 0\ ,\quad p(-5)=p(5)$$

$y=x^2$: $x^4-2x^2+5=y^2-2y+5$; $y^2-2y+5=0$

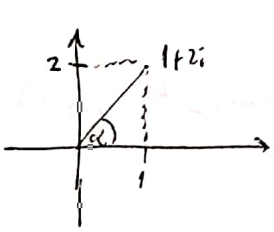
raíces: $y=\frac{2\pm\sqrt{4-20}}{2}=\frac{2\pm 4i}{2}=1\pm 2i$;

$$\Rightarrow x^2=1+2i\ ,\quad x^2=1-2i$$

$x^2=1+2i \Rightarrow x^2-(1+2i)=0 \Rightarrow (x+\sqrt{1+2i})(x-\sqrt{1+2i})=0$

$x^2=1-2i \Rightarrow x^2-(1-2i)=0 \Rightarrow (x+\sqrt{1-2i})(x+\sqrt{1-2i})=0$

2° Manera. Sea $z\in\mathbb{C}$ tq $z^2=1+2i$. Entonces $z=|1+2i|^{1/2}\,\mathrm{cis}\frac{1}{2}(\alpha+2\pi k)$, $0\le k\le 1$, donde $1+2i=|1+2i|\,\mathrm{cis}\,\alpha$.



$\tan\alpha=\frac{2}{1}=2$

$\cos\alpha=\frac{1}{\sqrt{5}}\approx 51$

$\mathrm{sen}\,\alpha=\frac{2}{\sqrt{5}}$

	0	π/4	π/2	3π/4	π
sen	0	1	2	3	4
cos	4	3	2	1	0
	4		2		

$$z=\sqrt[4]{5}\,\mathrm{cis}\,\tfrac{1}{2}(\alpha+2\pi k)$$

$$z=\sqrt[4]{5}\,\mathrm{cis}\,\tfrac{1}{2}\alpha\ ,\ \sqrt[4]{5}\,\mathrm{cis}\,\tfrac{\alpha}{2}+\pi$$

$$z_1=\sqrt[4]{5}\,e^{i\alpha/2}\ ,\quad z_2=\sqrt[4]{5}\,e^{i(\alpha/2+\pi)}$$

$$z_1z_2=\sqrt{5}\,e^{i\alpha/2}e^{i\alpha/2+i\pi}=\sqrt{5}\,e^{i\alpha}e^{i\pi}$$

Problema 5

E, F, L cuerpos, $E, F \subseteq L$. $[F : E \cap F] \leq \infty$. Entonces

$$EF = \left\{ \sum_{i=1}^{n} e_i f_i \;/\; e_i \in E,\ f_i \in F \text{ para } i = 1, \dots, n \right\}$$

es cuerpo (Sugerencia: primero considere caso $F = K(a)$, $K \subseteq E \cap F$)

– Demostración –

~~$F = K(a)$~~ $\Rightarrow [K(a) : E \cap K(a)] \leq \infty$

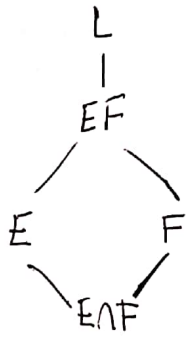
$K(a)$ cuerpo, entonces $\exists f(x) \in K[x]$; $f(a) = 0$. Sea $m_{a,K}(x) \in K[x]$ polinomio de menor grado que es satisfecho por a.

Si $\deg m_{a,K} = p$, $\Rightarrow 1, a, a^2, \dots, a^{p-1}$ base de $K(a)$.

$$EK(a) = \left\{ \sum_{i=1}^{n} e_i f_i \;/\; e_i \in E,\ f_i \in \overset{K(a)}{\overset{\|}{F}} \right\} = \{\dots\}$$

$$f_i = k_i^0 + k_i^1 a + k_i^2 a^2 + \dots + k_i^{p-1} a^{p-1} = \sum_{j=0}^{p-1} k_i^j a^j$$

$$\sum_{i=1}^{n} e_i f_i = \sum_{\substack{i=1,\dots,n \\ j=0,\dots,p-1}} e_i k_i^j a^j$$



$1, 0 \in EF \therefore EF \neq \emptyset$

Sean $\alpha, \beta \in EF$

$$\alpha = \sum_{1}^{n} e_i^\alpha f_i^\alpha \quad , \quad \beta = \sum_{1}^{m} e_i^\beta f_i^\beta$$

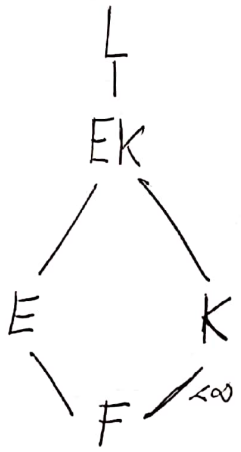
$n \leq m$: $\alpha + \beta = \sum_{n} \left(e_i^\alpha f_i^\alpha + e_i^\beta f_i^\beta \right)$

Esto se arregla con $F = K(a)$

Cuando $[F : E \cap F] < \infty \Rightarrow F = E \cap F(\alpha_1, \dots, \alpha_n)$

Ahora, $K = F(a) \subseteq L$

Pd: $[EK : E] \leq [K : F]$ $\forall E \subseteq L$ cuerpo, $F \subseteq E$



$[EK : F] = [EK : K][K : F]$

$[EK : F] = [EK : E][E : F]$

Supongamos que E/F finita, entonces

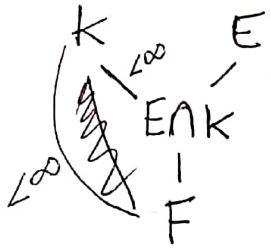
$$[EK : F] \leq [E : F][K : F]$$

$$[EK : E] = \frac{[EK : F]}{[E : F]} \leq \frac{[E : F][K : F]}{[E : F]} = [K : F]$$

Estudiar compósito EK

Por problema 5, EF compósito donde $[F : E \cap F] \leq \infty$

$[K : E \cap K] = ??$



Si $E, F \subset L$ cuerpos ¿$E \cap F$ cuerpo?

$a, b \in E \cap F \Rightarrow a, b \in E$; $a, b \in F$

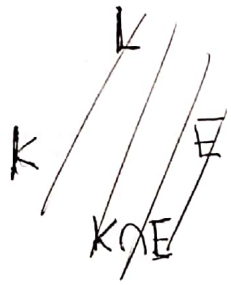
$\Rightarrow a+b \in E$; $a+b \in F$

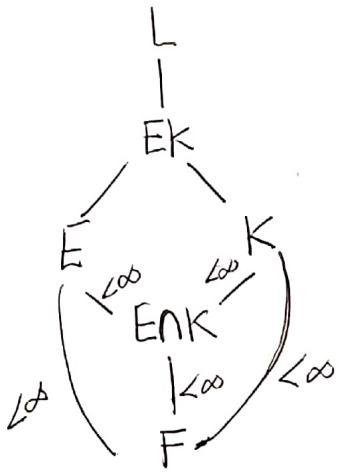
$\Rightarrow a+b \in E \cap F$

Análogo $ab \in E \cap F$

$a \in E \cap F \Rightarrow a \in E$, $a \in F$

$\Rightarrow \exists \hat{a} \in E : a\hat{a} = 1$, $\exists \tilde{a} \in F : a\tilde{a} = 1$ ✓



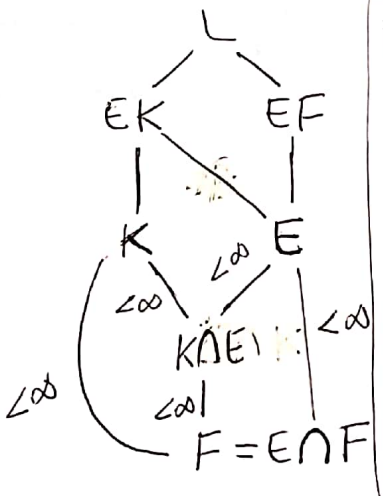


$[E : E \cap K] < \infty$

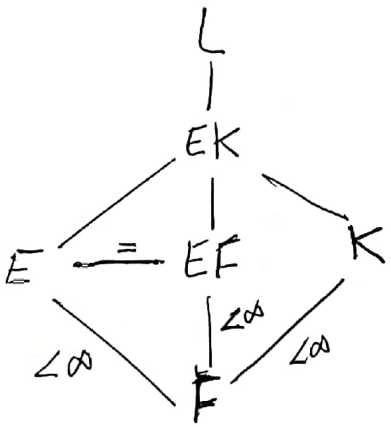
Problema 7 (Guía 2)

Probar que si K/F es extensión finita con $K \subseteq L$, entonces $[EK : EF] \leq [K : F]$ para todo cuerpo $E \subseteq L$ que contenga a F.

– Demostración –



Afirmación. Como $F \subseteq E$, $EF = E$



We have

~~$[EK : EF]$~~

$[EK : F] \leq [E : F][K : F]$

$[EF : F] \leq [E : F]$

$[EK : F] = [EK : EF][EF : F]$

$\Rightarrow [EK : EF][EF : F] \leq [E : F][K : F]$

$\Rightarrow [EK : EF] \leq \dfrac{[E : F][K : F]}{[EF : F]}$

$[EK : F] = [EK : E][E : F]$

$[EK : F] = [EK : K][K : F]$

K/F finita $\Rightarrow K = F(\alpha_1, \dots, \alpha_n)$

$\Rightarrow F = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$

$[E F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) : E] \leq [F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) : F] = [F(\alpha_1, \dots, \alpha_n) : F]$

$= [K : F]$

(8) Calcule el grado sobre $\mathbb{Q}$ de las siguientes extensiones

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

(b) $\mathbb{Q}(\sqrt{2},\sqrt{3})$ (d) $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$

- Desarrollo -

(a) Vemos que $\sqrt[4]{3}$ es raíz del polinomio $p(x)=x^4-3$ que es irreducible (einstein) $\therefore [\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}]=4$.

(b) ~~Se demuestra~~ Se verifica ~~$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$~~

Tenemos $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})$. Luego se puede demostrar que $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Si $x=\sqrt{2}+\sqrt{3}$

$x^2=2+3+2\sqrt{6} \Rightarrow x^2-5=2\sqrt{6} \Rightarrow x^4+25-10x^2=24$

$\Rightarrow x^4-10x^2+1=0 \quad \therefore p(x)=x^4-10x^2+1$ tiene como raíz a $x=\sqrt{2}+\sqrt{3}$. Falta demostrar que $p(x)$ es irreducible (sobre $\mathbb{Q}$)

$x^4-10x^2+1=(x+a)(x^3+bx^2+cx+d)$

$=x^4+bx^3$

$p(x)=x^4-10x^2+1 \Rightarrow p'(x)=4x^3-10 \Rightarrow p'(x)=0 \Leftrightarrow x=\sqrt[3]{\frac{10}{4}}$

$p''(x)=12x^2 \Rightarrow p''\left(\sqrt[3]{\frac{10}{4}}\right)>0$ (mínimo) $\Rightarrow p(x)$ no tiene raíces en $\mathbb{Q}$. ya que $p\left(\sqrt[3]{\frac{10}{4}}\right)>0$

$x^4-10x^2+1=(x^2+ax+b)(x^2+cx+d)$

$=x^4+cx^3+dx^2$

$p\left(\sqrt[3]{\frac{10}{4}}\right)=\frac{10}{4}\sqrt[3]{\frac{10}{4}}-10\left(\frac{10}{4}\right)^{2/3}+1$ ... puede tener raíces

$p(x)$ tiene discriminante $\Delta=\sqrt{100-4}=\sqrt{96}$

$=\sqrt{3\cdot 2^5}=2\sqrt{24}$

$96=48\cdot 2=6\cdot 8\cdot 2=2\cdot 3\cdot 2^4=3\cdot 2^5$

tiene raíces no racionales ✓

$$x^4-10x^2+1 = (x^2+ax+b)(x^2+cx+d)$$
$$= x^4+cx^3+dx^2+ax^3+acx^2+adx+bx^2+bcx+bd$$
$$= x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd$$

Tenemos
$$a+c=0 \longrightarrow a=-c$$
$$ac+b+d=-10$$
$$ad+bc=0 \longrightarrow -cd+bc=0 \Rightarrow c(b-d)=0$$
$$bd=1$$

Si $c=0 \Rightarrow a=0 \Rightarrow (b+d=-10,\ bd=1) \Rightarrow b+d=10=\frac{1}{d}+d=-10$

$\Rightarrow 1+d^2=-10d \Rightarrow 1+10d+d^2=0 \Rightarrow \Delta=100-4 \Rightarrow$ no tiene raíces en $\mathbb{Q}$.

Si $b-d=0 \Rightarrow b=d \Rightarrow b,d=1 \Rightarrow (a+c=0,\ ac=-12)$

$\Rightarrow 0=a+c=a-\frac{12}{a} \Rightarrow a^2-12=0 \Rightarrow$ no tiene raíces en $\mathbb{Q}$

$\therefore p(x)$ inducible

$\therefore [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}]=4$

(c) $\mathbb{Q}(\sqrt{1+2i})$; sea $x=\sqrt{1+2i} \Rightarrow x^2=1+2i \Rightarrow x^2-1=2i$

$\Rightarrow x^4-2x^2+1=-4 \Rightarrow x^4-2x^2-5=0$. $p(x)=x^4-2x^2-5$ inducible por criterio de eisenstein $\therefore [\mathbb{Q}(\sqrt{1+2i}) : \mathbb{Q}]=4$

(d) $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$

Tenemos $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}+i\sqrt[4]{2})$

$\sqrt[4]{2}(\sqrt[4]{2}+i\sqrt[4]{2})=\sqrt{2}+i\sqrt{2}$

$\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ splitting field of $p(x)$

$p(x)=x^4-2$ — $\mathbb{Q}(\sqrt[4]{2})$ — $\mathbb{Q}(i\sqrt[4]{2})$ → $p(x)=x^4-2$

$\mathbb{Q}(\sqrt[4]{2})$ — 4 — $\mathbb{Q}$ — 4

Problema 6

Probar que si $K=F(a)\subseteq L$, entonces $[EK:E]\leq[K:F]$ para todo cuerpo $E\subseteq L$ que contenga a F.

- Demostración -

(i) Supongamos que $K\subseteq E$.

$$EK=E \Rightarrow [EK:E]=[E:E]\leq 1\leq [K:F]$$

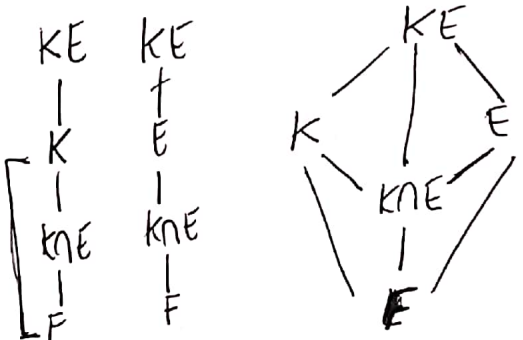
(ii) Supongamos que $E\subseteq K$:

$EK=K$.

$$[K:F]=[K:E][E:F]$$
$$\| \quad (*)$$
$$[EK:E]$$

Automáticamente $[EK:E]\leq[K:F]$.

(iii) Supongamos que $E\not\subseteq K$, $K\not\subseteq E$



$$[KE:F]=[KE:E][E:K\cap E][K\cap E:F]$$
$$=[KE:K][K:K\cap E][K\cap E:F]$$

$$[KE:F]=[KE:E][E:F]=[KE:K][K:F]$$

$$[KE:E]\leq[KE:K\cap E]$$
$$\leq[KE:K\cap E][K\cap E:F]$$
$$\leq[KE:F]$$

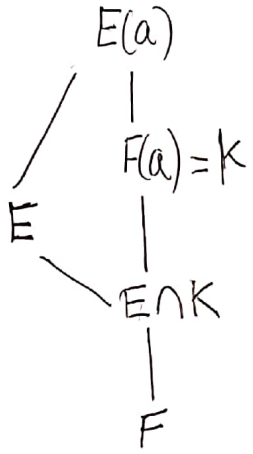
$$[K:K\cap E]\leq[K:F]$$

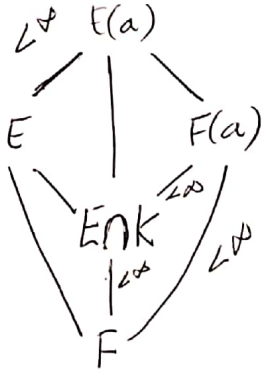
$[KE:F]=[KE:K\cap E][K\cap E:F]$ $\Rightarrow$

$[KE:E]\leq[KE:K\cap E]$ $\rightarrow$ $[KE:E]\leq[KE:K][K:K\cap E]$

$KE=E(a)$,

$K E = E(a)$
$\cup$
$F(a)$





Tenemos $[E:F]$, $[E(a):F(a)]$

$$[E(a):F] = [E(a):K][K:F]$$
$$\| $$
$$[E(a):E][E:F]$$

$$[F(a):F] = [F(a):E\cap K][E\cap K:F]$$

$$[E(a):E][E:E\cap K][E\cap K:F] \leq [E(a):E][E:E\cap K][E\cap K:F]$$
$$[K:E\cap K]$$

$$[E(a):E][E:F] \leq [E(a):E\cap K][K:F]$$

$[E(a):E]$

~~Ap. $[E:F] = [E(a):F(a)]$ $\forall E \supseteq F$~~

$$[EK:E] = [E(a):E] \leq [E(a):E\cap K][E\cap K:F]$$

$$[EK:E] \leq [EK:E\cap K]$$
$$\leq [EK:E\cap K][E\cap K:F]$$
$$= [EK:F]$$

$$[E:F] = [E(a):F(a)] \quad \forall E \supseteq F$$

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

$$[F(a):F] \geq [E\cap K:F]$$
$$\geq [F(a):E\cap K]$$

$$[E(a):F(a)][F(a):F] \geq [E(a):F(a)]$$
$$[F(a):E\cap K]$$

$$[E(a):E][E:F] = [E(a):F(a)][F(a):F]$$

$$\left|\frac{PN}{N}\right| = \frac{|PN|}{|N|} = \frac{|P||N|}{|P \cap N||N|}$$

$$= \frac{|P|}{|P \cap N|} = \frac{p^a}{p^b}$$

Problema 6

Probar que si $K = F(a) \subseteq L$, entonces

$$[EK : E] \leq [K : F] \quad \forall E \subseteq L \text{ cuerpo tq } F \subseteq E$$

$$EK = \left\{ \sum_{i=1}^{n} e_i k_i \;/\; e_i \in E,\ k_i \in K \ \ \forall i \in \{1, \dots, n\} \right\}$$

Tenemos que $E \subseteq EK$

$\{1, a, \dots, a^m\}$ base de $F(a)$ sobre F $\left(K = F(a)\right)$

$$\sum_{i=1}^{n} e_i k_i = \sum_{i=1}^{n} e_i \sum_{j=1}^{m} f_{ij} a^{j-1} = \sum_{\substack{i=1,\dots,n \\ j=1,\dots,m}} e_i f_{ij} a^{j-1}$$

Como $e_i, f_{ij} \in E$, $e_i f_{ij} \in E$

Como $F \subseteq E$: $e_i f_{ij} \in E \Rightarrow$ ¿ $EK = EF(a) = (EF)(a) \overset{?}{=} E(a)$?

$$[EK : F] = [EK : K][K : F]$$
$$[EK : F] = [EK : E][E : F]$$

$[E(a) : E]$

$\{1, a, \dots, a^m\}$ base de $F(a) = K$ sobre F : $\forall k$, $k = \sum_{i=1}^{m} f_i a^{i-1}$

Sea $\left\{1, \sum_{i=1}^{n_1} e_{i1} k_{i1}, \sum_{i=1}^{n_2} e_{i2} k_{i2}, \dots, \sum_{i=1}^{n_\ell} e_{i\ell} k_{i\ell}\right\}$

Sea $\left\{1, \sum_{i=1}^{n_1} e_{i1} k_{i1}, \sum_{i=1}^{n_2} e_{i2} k_{i2}, \dots, \sum_{i=1}^{n_\ell} e_{i\ell} k_{i\ell}\right\}$ base de EK/E

$\forall w \in EK$

$$w = \tilde{e}_1 \sum_{i=1}^{n_1} e_{i1} k_{i1} + \tilde{e}_2 \sum_{i=1}^{n_2} e_{i2} k_{i2} + \dots + \tilde{e}_\ell \sum_{i=1}^{n_\ell} e_{i\ell} k_{i\ell}$$

$$\sum_{i=1}^{n} e_i f_i = \sum_{i=1}^{n} e_i k_i^1 + a \sum_{i=1}^{n} e_i k_i^2 + \cdots + a^{m-1} \sum_{i=1}^{n} e_i k_i^{m-1}$$

cerrado bajo suma y producto ✓
también está el inverso aditivo

Como $\sum_{i=1}^{n} e_i k_i^1 \in E$, $\exists A \in E : A \sum_{i=1}^{n} e_i k_i^1 = 1$

$$a^m + b_{m-1} a^{m-1} + b_{m-2} a^{m-2} + \cdots + b_1 a + b_0 = 0$$

$$a^m + b_{m-1} a^{m-1} + \cdots + b_1 a = -b_0$$

$$a\left(a^{m-1} + b_{m-1} a^{m-2} + \cdots + b_1\right) = -b_0$$

$$\Rightarrow a^{-1} = -\frac{1}{b_0}\left(a^{m-1} + b_{m-1} a^{m-2} + \cdots + b_1\right)$$

$$\therefore \left(\sum_{i=1}^{n} e_i f_i\right)^{-1} = -\frac{1}{b_0}\left(\left(\sum_{i=1}^{n} e_i f_i\right)\right)$$

$$= \left(\sum_{i=1}^{n} e_i k_i^1 + a \sum_{i=1}^{n} e_i k_i^2 + \cdots + a^{m-1} \sum_{i=1}^{n} e_i k_i^{m-1}\right)^{-1} \quad \text{etc.}$$

$\therefore$ $Ek(a)$ es cuerpo.

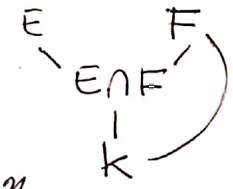
Caso general : listo!

Problema 5

E, F subcuerpos de L : $[F : E \cap F] \leq \infty$

Afirmación . $EF = \left\{ \sum_{i=1}^{n}{}' e_i f_i \;/\; e_i \in E,\ f_i \in F \right\}$ cuerpo.

Caso 1: $F = k(a)$, $k \subseteq E \cap F$



$$EF = Ek(a) = \left\{ \sum_{i=1}^{n}{}' e_i f_i \;/\; e_i \in E,\ f_i \in k(a) \right\}$$

$f_i = k_i^1 + k_i^2 a + \dots + k_i^m a^{m-1}$; $k_i^j \in k$ $\left([k(a) : k] = m \right)$

$$\sum_{i=1}^{n}{}' e_i f_i = \sum_{i=1}^{n}{}' e_i \left(\sum_{j=1}^{m}{}' k_i^j a^{j-1} \right) = \sum_{i=1}^{n}{}' \sum_{j=1}^{m}{}' e_i k_i^j a^{j-1} = \sum_{i,j=1}^{n,m}{}' e_i k_i^j a^{j-1}$$

$\forall (i,j) \in \{1, \dots, n\} \times \{1, \dots, m\}$: $e_i k_i^j \in E \cap k = k$

~~$\therefore EK(a) = (E \cap K)(a)$~~

¿~~Af. $EK(a) = (E \cap K)(a)$~~ ?

Afirmación ¿$Ek(a) = (E \cap k)(a)$?

$k \subseteq E \cap F \Rightarrow k_i \in k \subseteq E$

$e_i k_i^j \in E$ | $Ek(a) \subseteq E(a)$

Como $[k(a) : k] = m$; $a^m + b_{m-1} a^{m-1} + b_{m-2} a^{m-2} + \dots + b_1 a + b_0 = 0$

(*) $\Rightarrow a^m = -b_{m-1} a^{m-1} - b_{m-2} a^{m-2} - \dots - b_1 a - b_0$

$\Rightarrow 1 = a^{-m} \left(-b_{m-1} a^{m-1} - b_{m-2} a^{m-2} - \dots - b_1 a - b_0 \right)$

En particular : $Ek(a) = E(a)$

$$\sum_{i=1}^{n}{}' e_i f_i = \sum_{i=1}^{n}{}' e_i \left(k_i^1 + k_i^2 a + \dots + k_i^m a^{m-1} \right)$$

$$= e_1 \left(k_1^1 + k_1^2 a + \dots + k_1^m a^{m-1} \right) + e_2 \left(k_2^1 + k_2^2 a + \dots + k_2^m a^{m-1} \right) + \dots + e_n \left(k_n^1 + k_n^2 a + \dots + k_n^m a^{m-1} \right)$$

$$= \sum_{i=1}^{n}{}' e_i k_i^1 + a \sum_{i=1}^{n}{}' e_i k_i^2 + \dots + a^{m-1} \sum_{i=1}^{n}{}' e_i k_i^m$$

Cerrado bajo suma y producto.

$E(a)$ / $k(a)$

~~$E(k(a)) = (Ek)(a)$~~

$Ek(a) = (Ek)(a)$

Problema 6.

Encuentre el menor entero r tal que $\mathbb{F}_{7^r}$ contiene una raíz onceava primitiva de la unidad.

-Desarrollo- ~~Sea $p(x) = x^{11} - 1$~~

$\mathbb{F}_{7^r}$ es el campo de descomposición de $p(x) = x^{7^r} - x$. $x \neq 0$, $g(x) = x^{7^r - 1} - 1$

$\forall x \in \mathbb{F}_{7^r}$, $g(x) = 0$ (raíces de la unidad)

Sea G el grupo de las raíces onceavas de la unidad ($\forall g \in G : g^{11} - 1 = 0$)

Si $\mathbb{F}_{7^r}$ posee raíz onceava de la unidad, entonces $G \leq \mathbb{F}_{7^r}$

$$\therefore \quad 11 \mid 7^r - 1 \quad \text{(Lagrange)}$$

Resolver $7^r \equiv 1 \,(11)$:

$$7^r \equiv 1 \,(11)$$

$$\Rightarrow 7^r \cdot 8^r \equiv 8^r \,(11)$$

$$(56)^r \equiv 8^r \,(11) \iff 8^r \equiv 1 \,(11)$$

$$\iff 2^{3r} \equiv 1 \,(11)$$

Resolver $2^t \equiv 1 \,(11)$

$$2^t \equiv 1 \iff 2^t - 1 \equiv 0 \iff (2-1)(2^{t-1} + \dots + 1) \equiv 0$$

$$\iff 2^{t-1} + \dots + 1 \equiv 0$$

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16 \equiv 5$
$2^5 = 10$
$2^6 = 9$
$2^7 = 18 \equiv 7$
$2^8 = 14 \equiv 3$
$2^9 = 6$
$2^{10} = 12 \equiv 1$

Por lo tanto, para $t = 10$: $2^t \equiv 1 \,(11)$

$\forall n \in \mathbb{N}$: $2^{nt} \equiv 1 \,(11)$

$$\therefore \quad 8^t \equiv 1 \,(11)$$

$$\therefore \quad 7^t \equiv 1 \,(11)$$

Problema 4. (Guía 3)

$p(x) = x^6 + x + 1 \in \mathbb{F}_4[x]$. Averiguar si es o no es con raíz en $\mathbb{F}_4$

$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \{a + b\alpha / a, b \in \mathbb{F}_2\}$

$0, 1, \alpha, 1+\alpha$, donde $\alpha^2 = \alpha + 1$

$\in \mathbb{F}_4$

$0^6 = 0$, $1^6 = 1$, $\alpha^6 = \alpha^6 = (\alpha^2)^3 = (\alpha+1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1$

$= \alpha(\alpha+1) + 3\alpha^2 + 3\alpha + 1$

$= \alpha^2 + \alpha + \alpha^2 + \alpha + 1 = 1$

$p(\alpha) = \alpha^6 + \alpha + 1 = 1 + \alpha + 1 = \alpha$

$(\alpha+1)^6 = \left((\alpha+1)^2\right)^3 = (\alpha^2+1)^3 = (\alpha^2+1)(\alpha^2+1)^2 = \alpha(\alpha^4+1)$

$= \alpha\left((\alpha^2+1)^2+1\right) = \alpha(\alpha^2+1+1) = \alpha^3 = \alpha$

$p(\alpha+1) = (\alpha+1)^6 + (\alpha+1) + 1 = \alpha + \alpha + 1 + 1 = 0$

$\therefore$ $\alpha+1$ raíz de $p(x)$.

Ahora para $q(x) = x^5 + x + 1$

$q(0) = 0 + 0 + 1$

$q(1) = 1 + 1 + 1 = 1$

$q(\alpha) = \alpha^5 + \alpha + 1$

$\alpha^5 = \alpha^3\alpha^2 = \alpha^3(\alpha+1) = \alpha\alpha^4 = \alpha(\alpha+1)^2 = \alpha(\alpha^2+1) = \alpha^3 + 1$

$= \alpha(\alpha+1) + 1 = \alpha^2 + \alpha + 1 = 0$

$\therefore$ $q(\alpha) = \alpha + 1$

$q(\alpha+1) = (\alpha+1)^5 + (\alpha+1) + 1 = (\alpha+1)^5 + \alpha$

$(\alpha+1)^5 = \alpha(\alpha+1)^4 = \alpha(\alpha^4+1) = \alpha^5 + \alpha = \alpha$

$\therefore$ $q(\alpha+1) = \alpha + \alpha = 0$.

$\therefore$ $\alpha+1$ raíz de $q(x)$.

$$\alpha^6+\alpha+1 = \alpha^6+\alpha^2 = \left((\alpha^3)^2+\alpha^2\right) = (\alpha^3+\alpha)^2$$
$$= (\alpha(\alpha+1)+\alpha)^2$$
$$= (\alpha^2+\alpha+\alpha)^2$$
$$= \alpha^4$$

Problema 13

Sea $f(x)$ un polinomio con coeficientes en $\mathbb{F}_p$. Probar que $f'(x)=0$ ssi $f(x)=g(x)^p$ para algún polinomio g con coeficientes en $\mathbb{F}_p$.

- Demostración -

$$f(x)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0 \quad , \quad a_i\in\mathbb{F}_p .$$

$$f'(x)=na_nX^{n-1}+(n-1)a_{n-1}X^{n-2}+\cdots+a_1$$

$$f'(x)=0 \iff ia_i=0 \quad \forall i\in\{1,\dots,n\}$$

en $\mathbb{F}_p$: $f'(x)=0 \iff p\mid ia_i \quad \forall i\in\{1,\dots,n\}$.

en $i=n$, $p\mid ia_i \iff p\mid i$

$\therefore$ ~~$f(x)\neq a_nX^{ph_1}+a$~~

$\therefore$ ~~$f(x)=a_nX^{pp_n}+a_{n-1}X$~~

$$f'(x)=0 \iff f(x)=a_0+a_pX^p+a_{2p}X^{2p}+\cdots+a_{kp}X^{kp} \quad ; \quad kp=n$$

¿ $\forall a\in\mathbb{F}_p$, $\exists b\in\mathbb{F}_p$: $b^p=a$?

Sabemos que $\mathbb{F}_p^*$ grupo multiplicativo

$\mathbb{F}_5=\{0,1,2,3,4\} \to \mathbb{F}_5^*=\{1,2,3,4\}$ ✓

$2, 4, 3, 1$

$3, 4, 7, 1$

$4, 1$

$\mathbb{F}_4=\{0,1,2,3\}$

$$\boxed{\forall x\in\mathbb{F}_p : x^p-x=0}$$

$$f'(x)=0 \iff f(x)=a_0^p+a_pX^p+\cdots+a_{kp}X^{kp}$$

$$=\underbrace{\left(a_0+a_pX+\cdots+a_{kp}X^k\right)}_{g(x)}{}^p .$$

(1) Muestre que $p(x) = x^3 + 9x + 6$ es irreducible en $\mathbb{Q}[x]$. Sea θ una raíz de $p(x)$. Encuentre el inverso de $1+\theta$ en $\mathbb{Q}(\theta)$

- Demostración -

Raíces de $p(x) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$

$p(1) = 1+9+6$
$p(-1) = -1-9+6$
$p(-2) = -8-18+6$
$p(-3) = -27-27+6$
$p(-6) = -6^3 - 54 + 6$

$\therefore$ $p(x)$ irreducible en $\mathbb{Q}[x]$

θ raíz de $p(x) \Rightarrow p(\theta) = \theta^3 + 9\theta + 6 = 0 \Rightarrow \theta = \frac{1}{9}(-6-\theta^3)$

$\theta = \frac{1}{9}(-6-\theta^3)$

$\theta^3 + 9\theta + 6 = 0 \Leftrightarrow \theta(\theta^2+9) = -6 \Rightarrow \theta^{-1} = -\frac{1}{6}(\theta^2+9)$

Luego $(1+\theta)^{-1} = -\frac{1}{6}((1+\theta)^2+9) = -\frac{1}{6}(1+2\theta+\theta^2+9) = -\frac{1}{6}\theta^2 - \frac{1}{3}\theta - \frac{5}{3}$

$\therefore (1+\theta)^{-1} = -\frac{1}{6}\theta^2 - \frac{1}{3}\theta - \frac{5}{3}$

Verificación: $(1+\theta)(1+\theta)^{-1} = (1+\theta)\left(-\frac{1}{6}\theta^2 - \frac{1}{3}\theta - \frac{5}{3}\right)$

$= -\frac{1}{6}\theta^2 - \frac{1}{3}\theta - \frac{5}{3} - \frac{1}{6}\theta^3 - \frac{1}{3}\theta^2 - \frac{5}{3}\theta$

$= -\frac{1}{6}\theta^3 - \frac{1}{2}\theta^2 - 2\theta - \frac{5}{3} = -\frac{1}{6}(\theta^3 + 3\theta^2 + 12\theta + 10)$

$= -\frac{1}{6}(\theta^3 + 9\theta + 6 + 3\theta^2 + 3\theta + 4) = -\frac{1}{6}(3\theta^2 + 3\theta + 4)$

$p(x) = x^3 + 9x + 6$ irreducible en $\mathbb{Q}[x]$. $\mathbb{Q}[x]/(p(x)) = \{a + b\theta + c\theta^2 / a, b \in \mathbb{Q}\}$

$\theta^3 + 9\theta + 6 = 0$.

$q(x) = 1 + x$, $a(x)q(x) \equiv 1 \ (p(x)) \Leftrightarrow a(x)q(x) + b(x)p(x) = 1$; $b(x) \in \mathbb{Q}[x]$

$x^3 + 9x + 6 : x + 1 = x^2 - x + 10$
$x^3 + x^2$
$-x^2 + 9x + 6$
$-x^2 - x$
$10x + 6$
$10x + 10$
-4

$\Leftrightarrow (x+1)(x^2 - x + 10) - 4 = x^3 + 9x + 6$

$\Leftrightarrow (x+1)(x^2 - x + 10) - (x^3 + 9x + 6) = 4$

$\Leftrightarrow (x+1)\underbrace{\left(\frac{1}{4}x^2 - \frac{1}{4}x + \frac{5}{2}\right)}_{a(x)} - \underbrace{\frac{1}{4}}_{b(x)}(x^3 + 9x + 6) = 1$

$a(x) \in \mathbb{Q}[x]/(p(x))$; $a(x)q(x) \equiv 1 \ (p(x))$ $\therefore (1+\theta)^{-1} = \frac{1}{4}\theta^2 - \frac{1}{4}\theta + \frac{5}{2}$

Verificación: $(1+\theta)\left(\frac{1}{4}\theta^2-\frac{1}{4}\theta+\frac{5}{2}\right) = \frac{1}{2}\theta^2-\frac{1}{2}\theta+1+\frac{1}{2}\theta^3-\frac{1}{2}\theta^2+4\theta$

$= \frac{1}{2}\theta^3+\frac{7}{2}\theta+1 = \frac{1}{2}(\theta^3+7\theta+8) = \frac{1}{2}(\theta^3+9\theta+6-2\theta+2)$

$= \frac{1}{2}(2-2\theta)$

$(1+\theta)\left(\frac{1}{4}\theta^2-\frac{1}{4}\theta+\frac{5}{2}\right) = \frac{1}{4}\theta^2-\frac{1}{4}\theta+\frac{5}{2}+\frac{1}{4}\theta^3-\frac{1}{4}\theta^2+\frac{5}{2}\theta$

$= \frac{1}{4}\theta^3+\frac{9}{4}\theta+\frac{5}{2} = \frac{1}{4}(\theta^3+9\theta+10)$

$= \frac{1}{4}(\theta^3+9\theta+6+4) = \frac{1}{4}\cdot 4 = 1$ ✓ □

(2) Demuestre que x^3-2x-2 es irreducible sobre $\mathbb{Q}$. Si θ es raíz de este polinomio, calcule $(1+\theta)(1+\theta+\theta^2)$ y $\frac{1+\theta}{1+\theta+\theta^2}$ en $\mathbb{Q}(\theta)$.

- Demostración - $p(x) = x^3-2x-2$. raíces de $p = \{\pm 1, \pm 2\}$

$p(2) = 8-4-2 = 2$, $p(-2) = -8+4-2 = -6$ ∴ $p(x)$ irreducible

$\mathbb{Q}[x]/(p(x)) = \{a+b\theta+c\theta^2 / a,b,c \in \mathbb{Q} ;\ \theta^3-2\theta-2=0\}$

$(1+\theta)(1+\theta+\theta^2) = 1+\theta+\theta^2+\theta+\theta^2+\theta^3 = \theta^3+2\theta^2+2\theta+1$

$= 2\theta+2+2\theta^2+2\theta+1$

$= 2\theta^2+4\theta+3$

$q(x) = 1+x+x^2$, hal $r(x)$, $q(x)r(x) \equiv 1\ (p(x))$

$\Updownarrow$

(*) $q(x)r(x)+p(x)s(x) = 1$, algún $s(x) \in \mathbb{Q}[x]$.

$p(x)$ irreducible $\Rightarrow (p(x), q(x)) = 1 \Rightarrow$ (*) ✓

$x^3-2x-2 : x^2+x+1 = x-1$

x^3+x^2+x

$-x^2-2x-2$

$-x^2-x-1$

$-2x-1$

$\Leftrightarrow (x-1)(x^2+x+1)+(-2x-1) = x^3-2x-2$

$x^2+x+1 : x+1 = x$ $\Leftrightarrow$ $x(x+1)+1 = x^2+x+1$

x^2+x

1

$\Rightarrow (x^2+x+1) - x(x+1) = 1$

$\Rightarrow (x^2+x+1) - x\left((x^3-2x-2) - (x-1)(x^2+x+1)\right) = 1$

$q(x) - x\left(p(x) - (x-1)q(x)\right) = 1$

$\Rightarrow q(x) - xp(x) + (x^2+x)q(x) = 1$

$\Rightarrow (x^2+x+1)q(x) - xp(x) = 1$

$\therefore (x^2+x+1)\,q(x) \equiv 1 \;(p(x))$

$\therefore (1+\theta+\theta^2)^{-1} = 1+\theta+\theta^2$

$x^2+x+1 : -2x-1 = -\frac{1}{2}x - \frac{1}{4}$

$x^2+\frac{1}{2}x$

$\frac{1}{2}x+1$

$\frac{1}{2}x+\frac{1}{4}$

$3/4$

$\Leftrightarrow (-2x-1)\left(-\frac{1}{2}x-\frac{1}{4}\right)+\frac{3}{4} = x^2+x+1$

$\Leftrightarrow (-2x-1)\left(-\frac{1}{2}x-\frac{1}{4}\right) - (x^2+x+1) = -\frac{3}{4}$

$\Leftrightarrow (-2x-1)\left(\frac{2}{3}x+\frac{1}{3}\right) + \frac{4}{3}(x^2+x+1) = 1$

$\Leftrightarrow \left(p(x) - (x-1)q(x)\right)\left(\frac{2}{3}x+\frac{1}{3}\right) + \frac{4}{3}(x^2+x+1) = 1$

$\Leftrightarrow p(x)\left(\frac{2}{3}x+\frac{1}{3}\right) + q(x)\underbrace{\left(\frac{4}{3} - (x-1)\left(\frac{2}{3}x+\frac{1}{3}\right)\right)}_{r(x)} = 1$

$r(x) = \frac{4}{3} - \left(\frac{2}{3}x^2 + \frac{1}{3}x - \frac{2}{3}x - \frac{1}{3}\right) = \frac{4}{3} - \frac{2}{3}x^2 + \frac{1}{3}x + \frac{1}{3} = -\frac{2}{3}x^2 + \frac{1}{3}x + \frac{5}{3}$

$\therefore r(x)q(x) \equiv 1 \;(p(x))$

$\therefore (1+\theta+\theta^2)^{-1} = -\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3}$

Verificamos! : $\beta = (1+\theta+\theta^2)\left(-\frac{2}{3}\theta^2+\frac{1}{3}\theta+\frac{5}{3}\right) = -\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3} - \frac{2}{3}\theta^3 + \frac{1}{3}\theta^2$

$+ \frac{5}{3}\theta - \frac{2}{3}\theta^4 + \frac{1}{3}\theta^3 + \frac{5}{3}\theta^2$

$= -\frac{2}{3}\theta^4 - \frac{1}{3}\theta^3 + \frac{4}{3}\theta^2 + \frac{6}{3}\theta + \frac{5}{3} = \frac{1}{3}\left(-2\theta^4 - \theta^3 + 4\theta^2 + 6\theta + 5\right)$

$-\theta^3 = -2\theta - 2 \Rightarrow -\theta^4 = -2\theta^2 - 2\theta$

$\beta = \frac{1}{3}\left(-2\theta^2 - 2\theta - 2\theta - 2 + 4\theta^2 + 6\theta + 5\right) = \frac{1}{3}\left(2\theta^2 + 2\theta + 1\right)$

$= \frac{1}{3}(3) = 1$

Por lo tanto

$$\frac{1+\theta}{1+\theta+\theta^2} = (1+\theta)\left(-\frac{2}{3}\theta^2+\frac{1}{3}\theta+\frac{5}{3}\right) = -\frac{2}{3}\theta^2+\frac{1}{3}\theta+\frac{5}{3}-\frac{2}{3}\theta^3+\frac{1}{3}\theta^2+\frac{5}{3}\theta$$

$$= -\frac{2}{3}\theta^3-\frac{1}{3}\theta^2+\frac{6}{3}\theta+\frac{5}{3} = \frac{1}{3}\left(-2\theta^3-\theta^2+6\theta+5\right)$$

$$= \frac{1}{3}\left(-4\theta-4-\theta^2+6\theta+5\right) = \frac{1}{3}\left(-\theta^2+2\theta+1\right) = -\frac{1}{3}\theta^2+\frac{2}{3}\theta+\frac{1}{3}$$

---

(3) L/K una extensión cuadrática, Probar que si $\mathrm{char}\, K \neq 2$, entonces existe $a \in L$ con $a \notin K$ y $a^2 \in K$.

-Demostración-. Sea $\alpha \in L$, $p(\alpha)=0$ donde $p(x)=x^2+\omega_1 x+\omega_2 \in K[x]$ irreducible.

$$\alpha^2+\omega_1\alpha+\omega_2=0 \Rightarrow \alpha^2+\omega_1\alpha = -\omega_2$$

$$\Rightarrow \alpha^2+\omega_1\alpha+\frac{\omega_1^2}{4} = -\omega_2+\frac{\omega_1^2}{4}$$

$$(\mathrm{char}\, K \neq 2)$$

$$\Rightarrow \left(\alpha+\frac{\omega_1}{2}\right)^2 = \frac{\omega_1^2-4\omega_2}{4}$$

Tomando $a = \alpha+\frac{\omega_1}{2} \in L \setminus K$, $a^2 = \frac{\omega_1^2-4\omega_2}{4} \in K$

En particular, $L = K[\sqrt{a}] = K\left[\sqrt{\frac{\omega_1^2-4\omega_2}{2}}\right] = K\left[\sqrt{\omega_1^2-4\omega_2}\right]$.

(4) Calcule el grado sobre $\mathbb{Q}$ de las siguientes extensiones:

(i) $\mathbb{Q}(\sqrt[n]{p})$ (p primo)

(ii) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$

(iii) $\mathbb{Q}(\sqrt{a+bi})$ ($a^2+b^2=p$ primo)

(iv) $\mathbb{Q}(\sqrt[9]{2}, i\sqrt[4]{2})$

- Desarrollo -

(i) $\sqrt[n]{p}$ raíz de x^n-p (irreducible por Einsestein) $\therefore [\mathbb{Q}(\sqrt[n]{p}):\mathbb{Q}] = n$

(ii) $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}] = ??$

$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) = L$

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

4 |

$\mathbb{Q}$

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

$(\sqrt{2}+\sqrt{3})^2 = 5+\sqrt{6}$, $(\sqrt{2}+\sqrt{3})^3 = (\sqrt{2}+\sqrt{3})(\sqrt{2}+\sqrt{3})^2 = (\sqrt{2}+\sqrt{3})(5+\sqrt{6})$

$= 5\sqrt{2}+2\sqrt{3}+5\sqrt{3}+3\sqrt{2}$ ok!

$\sqrt{5} = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

$\Rightarrow 5 = a^2+2b^2+3c^2+6d^2+2\sqrt{2}ab+2\sqrt{3}ac+2\sqrt{6}ad+2\sqrt{6}bc+4\sqrt{3}bd+6\sqrt{2}cd$

Puede resolverse por este método (estudiar combinaciones)

(iii) $\mathbb{Q}(\sqrt{a+bi})$; $x = \sqrt{a+bi} \Rightarrow x^2 = a+bi$

$\Rightarrow x^2 - a = bi$

$\Rightarrow x^4 + a^2 - 2ax^2 = -b^2$

$\Rightarrow x^4 - 2ax^2 + a^2 + b^2 = 0$

$\Rightarrow x^4 - 2ax^2 + p = 0$

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

| $\mathbb{Q}$ |

Para ver si es irreducible

$\sqrt{a+bi} = c+di \Rightarrow a+bi = c^2-d^2+2icd \Rightarrow \begin{cases} a = c^2-d^2 \\ b = 2cd \end{cases}$

$c = \frac{b}{2d} \Rightarrow a = \frac{b^2}{4d^2} - d^2 \Rightarrow 4ad^2 = b^2 - 4d^4$

$\Rightarrow b^2 = 4d^2(a+1)$

$\Rightarrow b = 2d\sqrt{a+1}$

$a^2+b^2 = p \Rightarrow a^2 = p-b^2 \Rightarrow a = \frac{p-b^2}{a}$

$p = a^2+b^2 = \frac{b^4}{16d^4} + d^4 - \frac{b^2}{2} + b^2$

$a^2+b^2 = c^4+d^2+4c^2d^2 = (c^2+d^2)^2 = p \ (\Rightarrow\Leftarrow) \quad \therefore [\mathbb{Q}(a+bi):\mathbb{Q}] = 4$

(iv) $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$

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

2

$i \notin \mathbb{Q}(\sqrt[4]{2}) \qquad \mathbb{Q}(i\sqrt[4]{2})$

4

$\mathbb{Q}$

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

---

(5) - Probar que si $\alpha \in \mathbb{C}$, entonces α es algebraico sobre $\mathbb{Q}$ ssi existe un polinomio $f(x)$ con coeficientes racionales tq $f(\alpha) = \frac{1}{\alpha^2}$

- Dem - $\alpha \in \mathbb{C}$ algebraico sobre $\mathbb{Q} \iff \exists g(x) \in \mathbb{Q}[x] : g(\alpha) = 0$

Sea $m_{\alpha,\mathbb{Q}}(x)$ minimal $\iff (x-\alpha)(x-\bar{\alpha})\tilde{q}(x) = g(x)$

$f(\alpha) = \frac{1}{\alpha^2} \iff f(\alpha)\alpha^2 - 1 = 0$

($\Rightarrow$) α algebraico $\iff \mathbb{Q}(\alpha)$ cuerpo $\Rightarrow \alpha^2$ tiene inverso en $\mathbb{Q}(\alpha) \iff \exists f(\alpha) \in \mathbb{Q}(\alpha)$ tq $\alpha^2 f(\alpha) = 1$

Sup. $\exists f(x) \in \mathbb{Q}[x]$, $f(\alpha) = \frac{1}{\alpha^2} \Rightarrow \alpha^2 f(\alpha) - 1 = 0 \Rightarrow \alpha$ raíz de $g(x) = x^2 f(x) - 1$

$\therefore$ α algebraico sobre $\mathbb{Q}$.

(6) Encuentre todos los polinomios irreducibles de grado 2, 3 y 4 en $\mathbb{F}_2[x]$.

-Desarrollo-

Grado 2: x^2, x^2+1, x^2+x+1, x^2+x

Grado 3: x^3+x^2+x+1 no!

x^3+x+1

x^3+x^2+1

Grado 4: no debe tener raíces,

$x^4+x^3+x^2+x+1$

x^4+x+1

x^4+x^2+1

x^4+x^3+1

No deben ser factorizable por polinomios cuadráticos

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

$x^2(x^2+x+1) = x^4+x^3+x$

$x^2(x^2+x) = x^4+x^3$

$(x^2+1)(x^2+x+1) = x^4+x^3+x^2+x^2+x+1 = x^4+x^3+x+1$

$(x^2+1)(x^2+x) = x^4+x^3+x^2+x$

$(x^2+x+1)(x^2+x) = x^4+x^3+x^3+x^2+x^2+x = x^4+x$

$(x^2+x+1)^2 = x^4+x^2+1$ ✗

$\therefore$ irreducibles grado 4 son x^4+x+1, x^4+x^3+1

---

(7) Calcule cuántos polinomios irreducibles de grado 8 hay en $\mathbb{F}_2[x]$.
Calcule cuantos polinomios irreducibles de grado 6 hay en $\mathbb{F}_3[x]$.

-Desarrollo-

Sea $p(x)$ irreducible en $\mathbb{F}_2[x]$, $\deg(p(x)) = 8$. $\mathbb{F}_2[x]/(p(x)) = \mathbb{F}_2(\alpha)$

$[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \dim_{\mathbb{F}_2} \mathbb{F}_2(\alpha) = 8$. Particular, $\{1, \alpha, \dots, \alpha^7\}$ base.

$\mathbb{F}_2(\alpha) \ni v = a_0 + a_1\alpha + \cdots + a_7\alpha^7 \quad \therefore |\mathbb{F}_2(\alpha)| = 2^8 \quad (\mathbb{F}_2(\alpha) = \mathbb{F}_{2^8})$

($\mathbb{F}_{2^8}$ cuerpo de descomposición de $x^{2^8}-x$)

$x^{2^8}-x = x(x^{2^8-1}-1) = x(x-1)(x^{2^8-2} + x^{2^8-3} + \cdots + x+1)$

$\{\alpha \in \mathbb{F}_{2^8} / \mathbb{F}_2(\alpha) = \mathbb{F}_{2^8}\} = A$

$\mathbb{F}_{2^8}$
| 2
$\mathbb{F}_{2^4}$
| 2
$\mathbb{F}_{2^2}$
| 2
$\mathbb{F}_2$

Cada polinomio de grado 8 tiene 8 raíces (distintas)

(nº polinomios irreducibles)(deg polinomio) = A

$\Rightarrow N = \frac{A}{\text{deg polinomio}}$

$|\{\alpha \in \mathbb{F}_{2^2} / \mathbb{F}_2(\alpha) = \mathbb{F}_{2^2}\}| = |\mathbb{F}_{2^2}| - |\{\alpha \in \mathbb{F}_{2^2} / \mathbb{F}_2(\alpha) = \mathbb{F}_2\}| = 2$

$\mu_p(n) = |\{\alpha \in \mathbb{F}_{p^n} / \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}\}|$.

$\mu_2(2) = |\mathbb{F}_{2^2}| - \mu_p(1) = 4 - 2 = 2$

~~$\mu_2(4) = |\mathbb{F}_{2^4}| - \mu_2(2) = 14$~~

~~$\mu_2(8) = |\mathbb{F}_{2^8}| - \mu_2(4) = 2^8 - 14 = 2^4 \cdot 2^4 - 14$~~
~~$= 256 - 14 =$~~ 256

$2^4 \cdot 2^4$ ~~tiene~~ cuenta mal hecha!

$\mu_2(4) = |\mathbb{F}_{2^4}| - \mu_2(2) - 2 = 16 - 2 - 2 = 12$

$\mu_2(8) = |\mathbb{F}_{2^8}| - \mu_2(4) - 2 = 2^8 - 14 = 256 - 14 = 242$

$\#\{\alpha / \mathbb{F}_2(\alpha) = \mathbb{F}_{2^8}\} = 2^8 - (2^2 - 2) - (2^4 - 2) - 2$
$= 256 - 2 - 14 - 2 = 240$

$\mu_2(2) = |\mathbb{F}_{2^2}| - \mu_2(1) = 4 - 2 = 2$

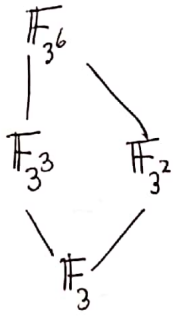
$\mu_2(4) = |\mathbb{F}_{2^4}| - \mu_2(2) - 2 = 16 - 4 = 12$

$\mu_2(8) = |\mathbb{F}_{2^8}| - \mu_2(4) - \mu_2(2) - 2$
$= 256 - 12 - 2 - 2 = 256 - 16 = 240$

$\therefore$ Hay 30 polinomios irreducibles de grado 8.

¿Cuantos polinomios irreducibles de grado 6 hay en $\mathbb{F}_3[x]$?

$\#\{\alpha \in \mathbb{F}_{3^6} / \mathbb{F}_3(\alpha) = \mathbb{F}_{3^6}\} = \mu_3(6)$



$\mu_3(6) = |\mathbb{F}_{3^6}| - \mu_3(3) - \mu_3(2) - 3 = |\mathbb{F}_{3^6}| - (3^3 - 3) - (3^2 - 3) - 3$

$= 3^6 - 3^3 - 3^2 - 9$

$3^6 = 3^3 \cdot 3^3 = 27 \cdot 27$

189
54
729

684 : 6 = 114
08
24
0

$\mu_3(6) = 729 - 27 - 18 = 729 - 45 = 684$

nº polinomios irreducibles deg 6 $= \frac{684}{6} = 114$

---

(8) Sea $\alpha \in \mathbb{F}_8 - \{0, 1\}$ tal que $\alpha^3 \neq \alpha + 1$. Probar que $\alpha^3 = \alpha^2 + 1$

- Demostración - $\mathbb{F}_8 = \mathbb{F}_{2^3} = \mathbb{F}_2(\alpha) \cong \mathbb{F}_2[x]/(p(x))$; $p(x)$ irreducible, $\deg p(x) = 3$. $p(\alpha) = 0$

Por problema (6): $p(x) = x^3 + x + 1$
$p(x) = x^3 + x^2 + 1$.

Como $\alpha^3 \neq \alpha + 1 \Rightarrow \alpha^3 + \alpha^2 + 1 = 0 \Rightarrow \alpha^3 = \alpha^2 + 1$.

(9) Sea α raíz de x^5+x^2+1 en $\mathbb{F}_{32}$. Encuentre un polinomio f de grado no mayor a 4 tal que $\alpha^8 = f(\alpha)$

- Desarrollo -

$$\alpha^8 = f(\alpha) \iff \alpha^8 f(\alpha)^{-1} = 1 \iff (\alpha^8)^{-1} f(\alpha) = 1$$

Debemos encontrar inverso de α^8 en $\mathbb{F}_{32}$

$$\alpha^8 = \alpha^5\alpha^3 = (\alpha^2+1)\alpha^3 = \alpha^5+\alpha^3 = (\alpha^2+1)+\alpha^3 = \alpha^3+\alpha^2+1$$

$$\therefore f(x) = x^3+x^2+1 \in \mathbb{F}_2[x] \quad ; \quad f(\alpha) = \alpha^8$$

---

(10) Sea $\text{char}(K) = p$, $a \in K$. $F(x) = x^p - x + a$

(a) Demuestre α raíz de $F \Rightarrow \alpha+1$ también.
Concluya que tiene raíces distintas

(b) Si F tiene raíz en $K \Rightarrow$ tiene todas sus raíces en K

(c) Suponga $K = \mathbb{F}_p$, $a = 1$. Demuestre que F no tiene raíces en K.

(d) Con hipótesis de (c), entonces $\forall \alpha$, $F(\alpha) = 0 \Rightarrow \alpha^{p^p} = \alpha$.
Concluya que $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^p}$.

- Demostración -

(a) $F(\alpha+1) = (\alpha+1)^p - (\alpha+1) + a = \alpha^p + 1 - \alpha - 1 + a = \alpha^p - \alpha + a = 0$

$\alpha = \beta$ raíces $\Rightarrow \alpha = \alpha + n$, algún $n < p$

$\Rightarrow n = 0$

F tiene p raíces, a saber, $\alpha, \alpha+1, \alpha+2, \ldots, \alpha+(p-1)$
las cuales son distintas.

(b) Si $\alpha \in K$ raíz de $F \Rightarrow \alpha+1 \in K$ raíz de F

$$\therefore \alpha, \alpha+1, \ldots, \alpha+(p-1) \in K$$

(c) $F(x) = x^p - x + 1$, $F(x) = x^p + (p-1)x - 1 = x + (p-1)x - 1 = px - 1 = -1$ $\forall x \in K$

(d) $F(\alpha) = \alpha^p - \alpha + 1 = 0 \iff \alpha^p + 1 = \alpha$

$\alpha^p = (\alpha^p + 1)^p = \alpha^{p^2} + 1$, $(\alpha^p)^p = (\alpha^{p^2} + 1)^p = \alpha^{p^3} + 1 = \alpha^{p^2}$

Inductivamente: $\forall n \in \mathbb{N}$, $\alpha^{p^n} = \alpha^{p^{(n+1)}} + 1$

$\underline{p = n}$ / $\alpha^{p^p} = \alpha^{p^{(p+1)}} + 1$

$\alpha^{p^{(p+1)}} = \alpha^{p \cdots p} = \big(\big((\alpha^p)^p\big)^{\cdots}\big)^p = \big(\big((\alpha-1)^p\big)^{\cdots}\big)^p$ ($p+1$ vezes; p vezes)

$= \big(\big((\alpha^p - 1)^p\big)^{\cdots}\big)^p = \alpha^{p^p} - 1$ ($p-1$ vezes)

$\underline{\text{H}}$. $\alpha^{p^{(p+1)}} = \alpha^{p^p} - 1$

$\alpha^{p^{(p+1)}} + 1 = \alpha^{p^p p} + 1 = \alpha^{p\left(\alpha^{p^p}\right)} + 1$

$\alpha^p = \alpha - 1$, $\alpha^{p^2} = \alpha^{p^{(p-1)}} - 1 = \alpha^{p^{(p-2)}} - 2 = \alpha^{p^{(p-3)}} - 3$

$\#$- Inductivamente: $\alpha^{p^p} = \alpha^{p^{(p-n)}} - n$, $n \leq p$

$\therefore \alpha^{p^p} = \alpha^{p^{(p-p)}} - p = \alpha^{p^0} - p = \alpha^1 - 0 = \alpha$.

Por lo tanto, $\forall \alpha$ raiz de F, $\alpha \in \mathbb{F}_{p^p}$ $\left(\mathbb{F}_p[\alpha] \subseteq \mathbb{F}_{p^p}\right)$

~~pero $[\mathbb{F}_p[\alpha] : \mathbb{F}_p] = p$~~ $\mathbb{F}_p[\alpha]$ cuerpo de p^n elementos

pero $n \mid p \Rightarrow n = p$ $\therefore \mathbb{F}_p[\alpha] = \mathbb{F}_{p^p}$

~~(10) Sea q primo que divide a $p-1$.~~
~~Pd: existe $\alpha \in \mathbb{F}_{p^q}$, $\alpha^q = \mathbb{F}_p$ y $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^q}$~~
~~Sugerencia: (*) podría ser $\mathbb{F}$~~

(11) q primo, $q \mid p-1$. Demostrar que existe $\alpha \in \mathbb{F}_{p^q}$, $\alpha^q \in \mathbb{F}_p$, $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^q}$

(Sugerencia: $q^t \mid p-1 \Rightarrow q^{t+1} \mid p^q - 1$)

$$p^q - 1 = (p-1)(p^{q-1} + \cdots + p + 1) = q^t r (p^{q-1} + \cdots + p + 1)$$

$$= q^t r \frac{p^q - 1}{p - 1}$$

$$q \mid p-1 \Rightarrow p - 1 = qs \Rightarrow (p-1)^t = q^t s^t$$

$$q^t \mid p-1 \ \& \ q^t \mid (p-1)^t \Rightarrow q^t \mid (p-1) + (p-1)^t$$

$$p^q - 1 = qs(p^{q-1} + \cdots + p + 1) = q^t r (p^{q-1} + \cdots + p + 1)$$

$$q^t r (p^{q-1} + \cdots + p + 1) = qs(p^{q-1} + \cdots + p + 1)$$

$$q^t r = qs$$

$$q^{t+1} r (p^{q-1} + \cdots + p + 1) = q^2 s (p^{q-1} + \cdots + p + 1)$$

$$q^{t+1} \alpha = q(p^q + 1)$$

—o—

$\mathbb{F}_{p^q}$ / $\mathbb{F}_p$

Tenemos $[\mathbb{F}_{p^q} : \mathbb{F}_p] = q \Rightarrow \mathbb{F}_{p^q} = \mathbb{F}_p[\alpha]$; $\alpha \in \mathbb{F}_{p^q}$

$\mathbb{F}_p^{\times} \cong \mathbb{F}_{p-1}$, tomamos $\alpha^{p-1/q} = \tilde{\alpha}$, $\tilde{\alpha} \in \mathbb{F}_{p^q}$ y $\tilde{\alpha}^q$ ...

(12) Sea $K/\mathbb{F}_p$ una extensión finita. Probar que $\varphi: K \to K$ definida por $\varphi(u) = u^p$ es un automorfismo de K que fija $\mathbb{F}_p$. Probar que los elementos de $\mathbb{F}_p$ son los únicos elementos fijos por φ.

- Demostración -

$K = \mathbb{F}_p(\alpha_1, \dots, \alpha_n)$, $\operatorname{char} K = p$

$$\varphi(u+v) = (u+v)^p = \sum_{i=0}^{p} \binom{p}{i} u^{p-i} v^i = u^p + v^p$$

$$\varphi(uv) = (uv)^p = u^p v^p = \varphi(u)\varphi(v)$$

$\varphi(u) = u^p = 0 \iff u = 0 \Rightarrow \varphi$ 1-1

Como K finito $\Rightarrow \varphi$ sobre $\therefore \varphi$ automorfismo.

Como $u^p = u \ \forall u \in \mathbb{F}_p \Rightarrow \varphi(u) = u$.

Sea $\operatorname{irr}_{\alpha_i}(x) = a_0 + a_1 x + \dots + a_{n_i} x^{n_i}$, $\operatorname{irr}_{\alpha_i}(\alpha_i) = 0$

$$\Rightarrow \varphi(0) = \varphi(\operatorname{irr}_{\alpha_i}(\alpha_i)) = a_0 + a_1 \alpha_i + \dots + a_{n_i} \alpha_i^{n_i}$$

$$= a_0 + a_1 \varphi(\alpha_i) + \dots + a_{n_i} \varphi(\alpha_i)^{n_i} \Rightarrow \operatorname{irr}_{\alpha_i}(\varphi(\alpha_i)) = 0$$

$\therefore \varphi(\alpha_i)$ raíz de $\operatorname{irr}_{\alpha_i}(x)$. (puede ser $\neq \alpha_i$)

---

(13) Sea K un cuerpo de característica p. Probar que para todo par de elementos $a, b \in K$, se tiene que $a^p = b^p \Rightarrow a = b$

- Demostración -

$a^p = b^p \iff a^p - b^p = 0 \iff (a-b)^p = 0$.

$\iff (a-b) = 0 \iff a = b$

Cuando $p = 2$ $-b^p = b^p$

(14) Probar que la aplicación $\phi : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ definida por $\phi(a) = a^p$ es un homomorfismo epiyectivo para todo entero r.

- Demostración - $\forall r \in \mathbb{N}$, $\mathbb{F}_{p^r}/\mathbb{F}_p$ finita. Luego aplicamos resultado de (12).

---

(15) Probar que si p es primo impar, el cuerpo $\mathbb{F}_{p^r}$ tiene $\frac{p^r+1}{2}$ cuadrados perfectos.

- Demostración -

a cuadrado perfecto $\Leftrightarrow \exists b,\ a = b^2$

$\Omega = \{ a \in \mathbb{F}_{p^r} / a \text{ cuadrado perfecto en } \mathbb{F}_{p^r} \}$ es grupo multiplicativo.

Lagrange $\Rightarrow |\Omega| \mid |\mathbb{F}_{p^r}^{\times}| \Rightarrow m \mid p^r - 1$

$\mathbb{F}_{p^r}$ cuerpo de descomposición de $X^{p^r} - X$; $\forall x \in \mathbb{F}_{p^r} : x^{p^r} = x$

$\Rightarrow$ 0 también es cuadrado perfecto $\Rightarrow$

~~La ecuación $X^2 - a$ tiene soluciones distintas~~

~~m = nº de cuadrados perfectos $\neq 0$ $\Rightarrow$ $2m$ = nº elementos que al cuadrado dan un cuadrado perfecto.~~

$|\Omega| = m$. Como $\mathbb{F}_{p^r}^{\times}$ es cíclico, $|\mathbb{F}_{p^r}^{\times}| = p^r - 1$; $\exists a \in \mathbb{F}_{p^r}^{\times}$, $\langle a \rangle = \mathbb{F}_{p^r}^{\times}$

Af. $\langle a^2 \rangle = \Omega$

Como $\Omega \leq \mathbb{F}_{p^r}^{\times}$, Ω también es cíclico, luego $\forall b \in \Omega$ ~~existe~~ t ~~tal que~~ $b = \tilde{b}^2 = (a^t)^2 = (a^2)^t$

Como $|a^2|^m = a^{2m} = a^{p^r-1} = 1 \Rightarrow 2m = p^r - 1 \Rightarrow m = \frac{p^r-1}{2}$

total de cuadrados perfectos es $m+1 = \frac{p^r-1}{2} + 1 = \frac{p^r+1+2}{2} = \frac{p^r+1}{2}$ ∎

16) Sea $L = k(\alpha_0, \dots, \alpha_r)$. L/k algebraica. Son equivalentes

(i) L/k normal

(ii) $\forall \alpha_i$, $i \in \{1, \dots, r\}$, α_i/k es normal (L contiene todas las raíces de $irr_{k,\alpha_i}(x)$)

(iii) Para todo homomorfismo $\varphi : L \to \bar{k}$, tq $\varphi|_k = id_k$. Se tiene $\varphi(L) = L$

Por 1° teorema fundamental de la teoría de Galois

$$L/L^{\langle\sigma\rangle} \text{ Galoisiana}, \quad Gal\left(L/L^{\langle\sigma\rangle}\right) = \langle\sigma\rangle$$

$$[L : L^{\langle\sigma\rangle}] = 3, \quad [L : \mathbb{Q}] = 6 \Rightarrow [L^{\langle\sigma\rangle} : \mathbb{Q}] = 2$$

$$\therefore \quad L = \mathbb{Q}(\sqrt{D})$$

Falta encontrar D

Tomar $L^{\langle\sigma\rangle} = \mathbb{Q}(\rho + \rho^2 + \rho^4)$

Debemos demostrar que $\rho+\rho^2+\rho^4 \in L^{\langle\sigma\rangle}$

$$\sigma_2(\rho+\rho^2+\rho^4) = \sigma_2(\rho) + \sigma_2(\rho^2) + \sigma_2(\rho^4)$$
$$= \rho^2 + \rho^4 + \rho$$
$$\sigma_4(\rho+\rho^2+\rho^4) = \sigma_4(\rho) + \sigma_4(\rho^2) + \sigma_4(\rho^4)$$
$$= \rho^4 + \rho + \rho^2$$
$$id(\rho+\rho^2+\rho^4) = \rho+\rho^2+\rho^4 \quad \checkmark \text{ ok!}$$

Ahora, $(\rho+\rho^2+\rho^4)^2 = \rho^2+\rho^4+\rho+2(\rho^3+\rho^5+\rho^6)$

Tenemos que $u^2 = u + 2(-u-1) = u - 2u - 2 = -u - 2$

$$\therefore \quad u^2 + u + 2 = 0$$
$$\therefore \quad u = \frac{-1 \pm \sqrt{1-8}}{2} = \frac{-1 \pm \sqrt{-7}}{2}$$

$$\therefore \quad D = -7$$

Considerar ahora $\tau(\rho) = \rho^3$. Encontrar $L^{\langle\tau\rangle}$.

Por teo. fundamental de Galois, $L/L^{\langle\tau\rangle}$ Galoisiana, $Gal\left(L/L^{\langle\tau\rangle}\right) = |\langle\tau\rangle|$

~~$\tau^2(\rho) = \rho^9$, $\tau^3(\rho) = \rho^{18} = \rho^4$, $\tau^4(\rho) = \rho^{12} = \rho^5$, $\tau^5(\rho) = \rho^{15} = \rho$~~

~~$\therefore \tau^5 = id$~~

$\tau^2(\rho) = \rho^9 = \rho^2$, $\tau^3(\rho) = \rho^6$, $\tau^4(\rho) = 18 = 4$, $\tau^5(\rho) = \rho^{12} = \rho^5$, $\tau^6(\rho) = \rho^{15} = \rho$

$\therefore \tau^6 = id$; $|\langle\tau\rangle| = 6$ y $[L : L^{\langle\tau\rangle}] = 6 \Rightarrow [L^{\langle\tau\rangle} : \mathbb{Q}] = 1 \Rightarrow L^{\langle\tau\rangle} = \mathbb{Q}$

(16) Sea $\rho = e^{2\pi i/7}$, $\text{irr}_{\mathbb{Q},\rho}(x) = \dfrac{x^7-1}{x-1} = x^6+x^5+x^4+x^3+x^2+x+1$. (16

Automáticamente se obtiene que $\mathbb{Q}(\rho)/\mathbb{Q}$ es Galoisiana.

$$\left|\text{Gal}\left(\mathbb{Q}(\rho)/\mathbb{Q}\right)\right| = [\mathbb{Q}(\rho):\mathbb{Q}] = \varphi(7) = 6$$

Hay 6 homomorfismos $\sigma: L = \mathbb{Q}(\rho) \to \overline{\mathbb{Q}}$, $\sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}$ y $\sigma(L) = L$.
Podemos determinarlos, a saber

$$\forall i \in \{1,\dots,6\} \;;\quad \sigma_i(\rho) = \rho$$

Propiedades:

$$\sigma_i(\sigma_j(\rho)) = \sigma_i(\rho^j) = (\rho^j)^i = \rho^{ji} = \rho^{ij} = \sigma_{ij}(\rho)$$

$$\therefore \sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i = \sigma_{ij}$$

$$\text{Gal}\left(\mathbb{Q}(\rho)/\mathbb{Q}\right) = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\} \cong C_6 \cong \left(\mathbb{Z}/7\mathbb{Z}\right)^\times \quad (id = \sigma_1)$$

Tomando $\sigma: L \to L$, $\sigma(\rho) = \sigma^2$; $|\langle\sigma\rangle| = 3$

Calculan $L^{\langle\sigma\rangle} = \{u \in L / \alpha(u) = u \;\; \forall \alpha \in \langle\sigma\rangle\}$

$$\langle\sigma\rangle = \{\sigma_2,\sigma_4,\sigma_1\} = \{\sigma_2,\sigma_4,id\}$$

Observación. $\rho, \rho^2, \rho^3, \rho^4, \rho^5, \rho^6$ (y $1, \rho, \rho^2, \rho^3, \rho^4, \rho^5$) es una base de $L/\mathbb{Q}$

$$\sigma(a\rho+b\rho^2+c\rho^3+d\rho^4+e\rho^5+f\rho^6) = a\rho^2+b\rho^4+c\rho^6+d\rho+e\rho^3+f\rho^5$$

$\sigma(\lambda) = \lambda \iff a\rho+b\rho^2+c\rho^3+d\rho^4+e\rho^5+f\rho^6 = a\rho^2+b\rho^4+c\rho^6+d\rho+e\rho^3+f\rho^5$

$\lambda \in \mathbb{Q}$

$$\Rightarrow a = d = b \;,\quad c = e = f$$

$$\therefore \lambda = a\rho+a\rho^2+c\rho^3+a\rho^4+c\rho^5+e\rho^6 = a(\rho+\rho^2+\rho^4)+c(\rho^3+\rho^5+\rho^6)$$

Si $a = c = -1$, $\lambda = 1$ (ver $\text{irr}_{\mathbb{Q},\rho}(x)$)

Tomando $u = \rho+\rho^2+\rho^4$, $v = \rho^3+\rho^5+\rho^6 \Rightarrow 1 = -u-v$ $(v = -u-1)$

Encontrar $L^{\langle\varphi\rangle}$ para $\varphi(\rho)=\rho^4$

$\varphi^2(\rho)=\rho^{16}=\rho^2$, $\varphi^3(\rho)=\rho^8=\rho$ $\therefore |\varphi|=3 \Rightarrow |\langle\varphi\rangle|=3$

Se sigue que $[L^{\langle\varphi\rangle}:\mathbb{Q}]=2$

$\therefore L^{\langle\varphi\rangle}=\mathbb{Q}(\sqrt{F})$

Encontrar F.

$$\varphi(a\rho+b\rho^2+c\rho^3+d\rho^4+e\rho^5+f\rho^6)=a\rho^4+b\rho+c\rho^5+d\rho^2+e\rho^6+f\rho^3$$

$\varphi(\lambda)=\lambda \iff a=b=d$, $c=f=e$

$$\lambda=a\rho+a\rho^2+c\rho^3+a\rho^4+c\rho^5+c\rho^6=a(\rho+\rho^2+\rho^4)+c(\rho^3+\rho^5+\rho^6)$$

cuando $a,c=-1 \Rightarrow \lambda=1$

$$\varphi(\rho+\rho^2+\rho^4)=\varphi(\rho)+\varphi(\rho^2)+\varphi(\rho^4)=\rho^4+\rho+\rho^2=\rho+\rho^2+\rho^4$$

$$\therefore L^{\langle\varphi\rangle}=\mathbb{Q}(\rho+\rho^2+\rho^4)=\mathbb{Q}(\sqrt{-7})$$

Los casos restantes son evidentes.

~~$h \in \mathbb{C}(x)$~~

~~$h \in \mathbb{C}(z)$, $h(z) = h(z^{-1})$ $\forall$~~

$h \in \mathbb{C}(x)$; $h(z) = h(z^{-1})$ $\forall z \in \mathbb{C}$.

Pd: $\exists\, g \in \mathbb{C}(x)$ tq $h(z) = g(z + z^{-1})$

Ej. $h(z) = cte$

$F = \{ h \in \mathbb{C}(x) \,/\, h(z) = h(z^{-1}) \ \forall z \in \mathbb{C} \}$

subcuerpo de $\mathbb{C}(x)$

$f(x)$
$=$

$x + \frac{1}{x} = \frac{x^2+1}{x} \Rightarrow g\left(x + \frac{1}{x}\right) = g\left(\frac{x^2+1}{x}\right)$

$\mathbb{C}(x)$
$|2$
$\mathbb{C}(f)$
$|$
$\mathbb{C}$

$f(z) = f(z^{-1})$ $\forall z$ $(\forall x) \Rightarrow \mathbb{C}(f) \subseteq F$

$\Rightarrow$ ~~$[F : \mathbb{C}(f)] =$~~

$\mathbb{C}(x)$
$|$
F (2)
$|$
$\mathbb{C}(f)$

$\therefore F = \mathbb{C}(f)$

$\exists\, g(x) \in \mathbb{C}(x)$: $h(x) = g(f(x)) = g\left(x + \frac{1}{x}\right)$

en particular $h(z) = g\left(z + \frac{1}{z}\right)$ $\forall z$.

$L = \mathbb{F}_p(x_1^{1/p}, x_2)$, $K = \mathbb{F}_p(\sigma_1, \sigma_2)$, $\sigma_1 = x_1 + x_2$
$\sigma_2 = x_1 x_2$

Pd: L_{sep}/K galoisiana pero L/K ↑ normal

$$irr_{K, x_1^{1/p}}(T) = T^{2p} - \sigma_1 T^p + \sigma_2$$
$$= (T - x_1^{1/p})^p (T - x_2^{1/p})^p$$

$K(x_1^{1/p})$
p | $\to$ t.i
$K(x_1)$
2 |
K

$2p$

$$(T - x_1)(T - x_2)$$
$$= T^2 - T x_2 - T x_1 + x_1 x_2$$
$$= T^2 - (x_1 + x_2) T + x_1 x_2$$
$$= T^2 - \sigma_1 T + \sigma_2 \in K[T]$$

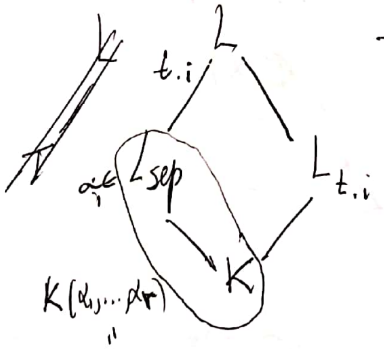
$\Rightarrow$

$K(x_1)$ $K(x_2)$
2 2
K

$$T^p - x_1 = (T - x_1^{1/p})^p$$
$\uparrow$
$K(x_1)[T]$

$x_2^{1/p} \notin L$ | $K(x_1, x_2) = K(x_1) = F$

$K(\alpha_1, \dots \alpha_n) = L$
| $< \infty$
K



Tenemos que $|Gal(L/K)| \leq [L:K]$

Tenemos que L_{sep}/K separable $\Rightarrow$ L/L_{sep} t.i.

$irr_{K, \alpha_i}(x)$ tiene ↑ raíces $\neq$ en L_{sep}

$K = \mathbb{Q}(\sqrt{d})$ d libre de cuadrados

$$(x-a-b\sqrt{d})(x-a+b\sqrt{d}) = (x-a)^2 - b^2 d$$
$$= x^2 + a^2 - 2ax - b^2 d$$
$$= x^2 - 2ax + a^2 - b^2 d$$

$a+b\sqrt{d} \in \mathcal{O}_K$ entero algebraico ssi $2a,\ a^2-b^2d \in \mathbb{Z}$

$$2a = t,\quad a^2 - b^2 d = s \quad ;\quad t, s \in \mathbb{Z}.$$

$$2a = t \Rightarrow a = \frac{t}{2}$$

$$a^2 - b^2 d = \frac{t^2}{4} - b^2 d = s \Rightarrow t^2 - 4b^2 d = 4s$$
$$\Rightarrow t^2 - 4s = 4b^2 d = (2b)^2 d$$
$$\in \mathbb{Z}.$$

$$t^2 - 4s = (2b)^2 d$$
↓ no puede cancelar (libre de cuadrados)

$$2b = \frac{p}{q} \Rightarrow t^2 - 4s = \frac{p^2}{q^2} d \Rightarrow \frac{q^2}{p^2}(t^2 - 4s) = d \quad (\Rightarrow\Leftarrow)$$
$$q^2\left(\frac{1}{p^2}(t^2-4s)\right) = d$$

$\therefore \quad 2b \in \mathbb{Z} \quad \left(b = \frac{s'}{2}\right)$

$$\Rightarrow a^2 - b^2 d = \frac{t^4}{4} - \frac{s'^2 d}{4} = \frac{t^4 - s'^2 d}{4}$$

$$\Rightarrow x^2 - 2ax + a^2 - b^2 d = x^2 - tx + \frac{t^4 - s'^2 d}{4}$$

$d = 2n$ (par) $\Rightarrow n$ impar $\Rightarrow$ t par $(a \in \mathbb{Z})$

$$\frac{t^2 - s'^2 d}{4} = \frac{4a^2 - s'^2(2n)}{4} = \frac{4a^2 - 2s'^2 n}{4} = \frac{2a^2 - s'^2 n}{2} \Rightarrow s' \text{ par}.$$