

Recordemos que $\sigma \in \text{Gal}((\mathbb{Q}(\zeta)/\mathbb{Q}))$ queda bien determinado según su acción sobre ζ . Luego tenemos dos candidatos:

$$\sigma(\zeta) = \zeta^{10}, \quad \tau(\zeta) = \zeta^{26}$$

(i) $\sigma(\zeta) = \zeta^{10}$:

$$\sigma(\zeta^{10}) = \zeta^{100} = \zeta^{37 \cdot 2 + 26} = \zeta^{26}$$

$$\sigma(\zeta^{26}) = \zeta^{260} = \zeta^{37 \cdot 7 + 1} = \zeta$$

$$\therefore \sigma(\alpha) = \zeta^{10} + \zeta^{26} + \zeta$$

(ii) $\tau(\zeta) = \zeta^{26}$

$$\tau(\zeta^{10}) = \zeta^{260} = \zeta$$

$$\tau(\zeta^{26}) = \zeta^{26 \cdot 26} = \zeta^{37 \cdot 18 + 10} = \zeta^{10}$$

$$\therefore \tau(\alpha) = \zeta^{26} + \zeta + \zeta^{10}$$

Ahora debemos calcular los órdenes de σ, τ

$$\sigma^2(\zeta) = \zeta^{100} = \zeta^{26}, \quad \sigma^3(\zeta) = \zeta^{260} = \zeta$$

$$\tau^2(\zeta) = \zeta^{26 \cdot 26} = \zeta^{10}, \quad \tau^3(\zeta) = \zeta^{260} = \zeta$$

$$\therefore \sigma^3 = \tau^3 = 1$$

Notar también que $\sigma^2 = \tau, \tau^2 = \sigma$

$$\therefore \sigma\tau = \sigma\sigma^2 = \sigma^3 = 1$$

$$\text{Así } H = \langle 1, 0, \sigma^3 \rangle \cong C_3 \cong \mathbb{Z}/3\mathbb{Z} = \langle \sigma \rangle$$

~~Por tanto, $H \leq \mathbb{Z}/36\mathbb{Z}$~~

$$\text{Como } H \leq \mathbb{Z}/36\mathbb{Z} : H = \langle \bar{12} \rangle = \mathbb{Z}/12\mathbb{Z}$$

$$\therefore \text{Gal}((\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/36\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$$

(b) Calcular el grupo de Galois de $(x^2+1)(x^2+2)(x^2+4)$ sobre \mathbb{F}_7 .

desarrollo

En \mathbb{F}_7 :

$$1^2 = 1$$

$$2^2 = 4$$

$$3^2 = 9 \equiv 2$$

$$\left. \begin{array}{l} 4^2 = 16 \equiv 2 \\ 5^2 = 25 \equiv 4 \\ 6^2 = 36 \equiv 1 \end{array} \right| \begin{array}{l} -1 \equiv 6 \\ -2 \equiv 5 \\ -4 \equiv 3 \end{array}$$

$\therefore 6, 5, 3$ no son \square 's en \mathbb{F}_7 .

$(x^2+1)(x^2+2)(x^2+4)$ irreducible sobre \mathbb{F}_7 .

Sea $\alpha \in \overline{\mathbb{F}_7}$: $\alpha^2 = -1 \iff \alpha^2 + 1 = 0$ (en \mathbb{F}_7)

Como $\mathbb{F}_7(\alpha)/\mathbb{F}_7$ es Galoiana, deberían estar las demás raíces del polinomio irreducible, en efecto:

$$-2 = (4\alpha)^2, \quad -4 = (5\alpha)$$

$$\therefore \beta^2 + 2 = 0, \quad \gamma^2 + 4 = 0$$

donde $\beta = 4\alpha, \quad \gamma = 5\alpha$.

Como ~~Gal($\mathbb{F}_7(\alpha)$)~~ $[\mathbb{F}_7(\alpha) : \mathbb{F}_7] = 2$

$$\therefore \text{Gal}\left(\mathbb{F}_7(\alpha)/\mathbb{F}_7\right) \cong C_2 = \langle \sigma \rangle$$

donde $\sigma^2 = 1, \quad \sigma: r \mapsto r^7, \quad \forall r \in \mathbb{F}_7(\alpha)$.

$$\sigma(\alpha) = \alpha^7 = \alpha^6 \alpha = -\alpha$$

$$\sigma^2(\alpha) = \sigma(-\alpha) = -\sigma(\alpha) = \alpha \quad \therefore \sigma^2 = 1$$

Problema 2

(a) Sea K/F finita y Galois y tal que $\text{Gal}(K/F) \cong S_4$. Considera

$$\mathcal{L} = \{L \mid L \text{ campo intermedio } F \subset L \subset K, [L:F]=12\}$$

Calcular $|\mathcal{L}|$ y determine todo $L \in \mathcal{L}$ tal que L/F es Galois.

(b) Calcule el orden del grupo de Galois de $x^{16}+1$ sobre \mathbb{Q} .

Dem.

(a) Debemos considerar L tal que

$$\begin{matrix} & K \\ 2 & \left\{ \begin{matrix} & 1 \\ & L \end{matrix} \right. \\ 12 & \left\{ \begin{matrix} & 1 \\ & F \end{matrix} \right. \end{matrix}$$

Por 2º teorema fundamental de la teoría de Galois, $\exists H \leq S_4$ tal que $L = K^H$, y $[K:L] = |H| = 2$. Luego basta encontrar todos los subgrupos $H \leq S_4 \cong \text{Gal}(K/F)$ de orden 2. Como estos elementos son trasposiciones, es fácil ver que

$$(42), (13), (14), (23), (24), (34)$$

son todas.

$$\therefore |\mathcal{L}| = 6$$

Ahora, si queremos que L/F sea Galois, por 2º teorema fundamental de la teoría de Galois,

$$L/F \text{ Galois} \Leftrightarrow H \trianglelefteq G$$

(b) Calcular el orden del grupo de Galois de $x^{16} + 1$ sobre \mathbb{Q} .

Desarrollo

Si $x^{16} + 1 = 0$, sus raíces vienen dadas por

$$x = e^{\frac{i(\pi + 2k\pi)}{16}}, \quad 0 \leq k \leq n-1. \quad \text{Luego, } n$$

K es el cdd de $x^{16} + 1$:

$$K = \mathbb{Q}(e^{\frac{i(\pi + 2k\pi)}{16}} \mid 0 \leq k \leq n-1)$$

$$= \mathbb{Q}(e^{i\pi/16}) = \mathbb{Q}(e^{2\pi i/32})$$

Sabemos que K/\mathbb{Q} Galoiana y

$$\begin{aligned} |\text{Gal}(K/\mathbb{Q})| &= [K : \mathbb{Q}] = \varphi(32) = \varphi(2^5) = (2-1)2^4 \\ &= 16 \end{aligned}$$

$$\therefore |\text{Gal}(K/\mathbb{Q})| = 16.$$

Problema 3

Sean K_1, K_2 finita y Galois sobre F .

- (a) Demuestre que $K_1 K_2 / F$ es Galois y que la aplicación

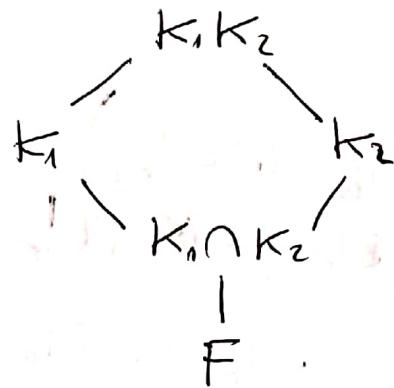
$$\Psi : \text{Gal}(K_1 K_2 / F) \longrightarrow \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$$

dada por $\Psi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$ define un isomorfismo de grupos.

- (b) Demuestre que : Ψ es isomorfismo $\Leftrightarrow K_1 \cap K_2 = F$.

Dem.

- (a) Tenemos



K_1 / F Galois $\Rightarrow K_1$ cdd de $p(x) \in F[x]$ separable

K_2 / F Galois $\Rightarrow K_2$ cdd de $q(x) \in F[x]$ separable.

Con esto, $K_1 K_2$ es cuerpo de descomposición de la parte libre de cuadrados de $p(x)q(x)$. $\therefore K_1 K_2 / F$ Galoisiana.

Sea $\sigma \in \text{Gal}(K_1 K_2 / F)$. Como σ fija F y K_1 / F es Galoisiana, ~~esta~~ queda bien definida por su acción sobre los generadores de K_1 , en particular lleva raíces de $p(x)$ en raíces de $p(x)$. \therefore tiene sentido la aplicación $\text{Gal}(K_1 K_2 / F) \rightarrow \text{Gal}(K_1 / F)$. Análogo para $\text{Gal}(K_1 K_2 / F) \rightarrow \text{Gal}(K_2 / F)$.

Si $\sigma, \tau \in \text{Gal}(K_1 K_2/F)$, $\sigma = \tau$
 $\Rightarrow \tau|_{K_1} = \sigma|_{K_1}, \tau|_{K_2} = \sigma|_{K_2}$
 $\therefore (\sigma|_{K_1}, \sigma|_{K_2}) = (\tau|_{K_1}, \tau|_{K_2})$
 $\therefore \Psi(\sigma) = \Psi(\tau)$ (Ψ bien definida).

Pd: Ψ homomorfismo de grupos.

dem. Sean $\sigma, \tau \in \text{Gal}(K_1 K_2/F)$.
 $\Psi(\sigma\tau) = ((\sigma\tau)|_{K_1}, (\sigma\tau)|_{K_2})$

Como $\sigma|_{K_1}, \tau|_{K_1} \in \text{Gal}(K_1/F) \rightarrow \sigma|_{K_1} \tau|_{K_1} = (\sigma\tau)|_{K_1}$
 $(\tau(K_1) = K_1, \sigma(K_1) = K_1)$. Análogo se cumple para
 $(\sigma\tau)|_{K_2} = \sigma|_{K_2} \tau|_{K_2}$

$$\begin{aligned}\therefore \Psi(\sigma\tau) &= ((\sigma\tau)|_{K_1}, (\sigma\tau)|_{K_2}) \\ &= (\sigma|_{K_1} \tau|_{K_1}, \sigma|_{K_2} \tau|_{K_2}) \\ &= (\sigma|_{K_1}, \sigma|_{K_2})(\tau|_{K_1}, \tau|_{K_2}) \\ &= \Psi(\sigma)\Psi(\tau)\end{aligned}$$

$\therefore \Psi$ homomorfismo de grupos

Pd: $\ker \Psi = \{1\}$

Tenemos que ~~$\ker \Psi = \{(\sigma, \tau) \in \text{Gal}(K_1/F) \times \text{Gal}(K_2/F) \mid (\sigma|_{K_1}, \sigma|_{K_2}) = (\tau|_{K_1}, \tau|_{K_2})\}$~~

$\ker \Psi = \{\sigma \in \text{Gal}(K_1 K_2/F) \mid (\sigma|_{K_1}, \sigma|_{K_2}) = (1|_{K_1}, 1|_{K_2})\}$

pero si σ fija a K_1 y a $K_2 \rightarrow \sigma$ fija a $K_1 K_2$

$$\therefore \sigma = \text{id}_{K_1 K_2}$$

$\therefore \Psi$ monomorfismo.

(b) Pd: φ es un isomorfismo $\Leftrightarrow K_1 \cap K_2 = F$

Afirmación: $K_1 K_2 / K_2$ es Galoisiana y

$$\text{Gal}(K_1 K_2 / K_2) \cong \text{Gal}(K_1 / K_1 \cap K_2)$$

dem. La aplicación $\varphi: \text{Gal}(K_1 K_2 / K_2) \xrightarrow{\sigma \mapsto \sigma|_{K_1}} \text{Gal}(K_1 / F)$ es un ~~isomorfismo~~ de grupos. Sea $H = \varphi(\text{Gal}(K_1 K_2 / K_2))$, debemos demostrar que $H = \text{Gal}(K_1 / K_1 \cap K_2)$, o de manera equivalente (por correspondencia del teorema de Galois), $K_1 \cap K_2 = K_1^H$. En efecto, si $\sigma \in \text{Gal}(K_1 K_2 / K_2)$ fija K_2 , y $\sigma|_{K_1} \in H$

$$\therefore K_1 \cap K_2 \subseteq K_1^H$$

Falta demostrar que $K_1^H \subseteq K_1 \cap K_2$. ~~ya que~~
~~Sabemos que $\sigma \in \text{Gal}(K_1 K_2 / K_2)$ fija a K_2 por definición,~~
~~y como $\sigma|_{K_1} \in H$ $\Rightarrow \sigma|_{K_1}$ fija a K_1^H ,~~
~~luego σ fija a K_1^H .~~

$$K_1^H \subseteq K_1 \cap K_2 \Leftrightarrow (K_1^H \subseteq K_1, K_1^H \subseteq K_2)$$

Por definición $K_1^H \subseteq K_1$.

Afirmación: $\text{Gal}(K_1 K_2 / K_2)$ fija a $K_1^H K_2$.

dem $\sigma \in \text{Gal}(K_1 K_2 / K_2)$ fija a K_2 por definición,

y como $\sigma|_{K_1} \in H \Rightarrow \sigma|_{K_1}$ fija a K_1^H ,

En particular σ fija a K_1 .

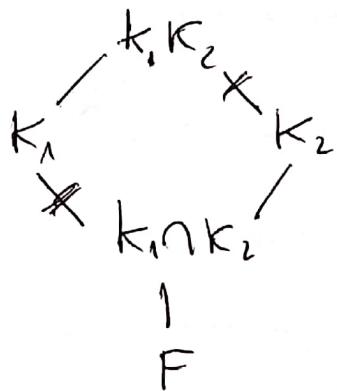
\therefore Por correspondencia Galoisiana, $K_1^H K_2 = K_2$

$$\therefore K_1^H \subseteq K_2$$

$$\text{Finalmente } K_1^H = K_1 \cap K_2$$

Se comprueba así que $\text{Gal}(K_1 K_2 / F) \cong \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$.

Nuevamente el diagrama



$$[K_1 K_2 : F] = [K_1 K_2 : K_2] [K_2 : F]$$

~~$$[K_1 K_2 : F] = [K_1 : K_1 \cap K_2] [K_2 : F]$$~~

$$= \frac{[K_1 : F] [K_2 : F]}{[K_1 \cap K_2 : F]}$$

Pd: Ψ isomorfismo $\Leftrightarrow K_1 \cap K_2 = F$

$$\Leftrightarrow [K_1 \cap K_2 : F] = 1$$

$$\therefore [K_1 K_2 : F] = [K_1 : F] [K_2 : F]$$

Por (a), $\text{Gal}(K_1 K_2 / F) \hookrightarrow \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$

y $|\text{Gal}(K_1 K_2 / F)| = [K_1 K_2 : F]$. Además

$$\begin{aligned} |\text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)| &= |\text{Gal}(K_1 / F)| |\text{Gal}(K_2 / F)| \\ &= [K_1 : F] [K_2 : F] \end{aligned}$$

$$\therefore \text{Gal}(K_1 K_2 / F) \cong \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$$

(\Rightarrow) Supongamos que $\text{Gal}(K_1 K_2 / F) \cong \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$

$$\Rightarrow |\text{Gal}(K_1 K_2 / F)| = |\text{Gal}(K_1 / F)| |\text{Gal}(K_2 / F)|$$

$$\Rightarrow \frac{|\text{Gal}(K_1 K_2 / F)|}{|\text{Gal}(K_1 / F)| |\text{Gal}(K_2 / F)|} = 1$$

$$= \frac{[K_1 K_2 : F]}{[K_1 : F][K_2 : F]} = \frac{1}{[K_1 \cap K_2 : F]}$$

$$\therefore [K_1 \cap K_2 : F] = 1$$

$$\therefore K_1 \cap K_2 = F$$



CUADERNILLO DE 6 HOJAS

NOTA:

5,3

Firma Corrector

(Escriba con letra de imprenta y lápiz pasta)

APELLIDO PATERNO	APELLIDO MATERNO	NOMBRES
GODOY	VALDEBENITO	MARCO ALEJANDRO

FECHA				
SIGLA	SECCION N°	DIA	MES	AÑO

CONTROL N°	NOMBRE DEL PROFESOR
INTERROGACION N°	SR. ERDAL EMSIZ

IMPORTANTE

- El artículo Nº 33 del reglamento del alumno establece.

"Todo acto realizado por el alumno durante el control académico, que lo viole, será sancionado a lo menos con la suspensión inmediata del control y con la aplicación de la nota mínima. Sin perjuicio de lo anterior, el profesor del curso deberá entregar los antecedentes a la Facultad de que depende el Alumno".

- Por ningún motivo debe arrancar hojas al cuadernillo. Si hay necesidad de hacer cálculos o anotaciones, utilice la contratapa de la última hoja, luego crúcela diagonalmente.

- 1.- 6
- 2.- 4
- 3.- 3
- 4.-
- 5.-
- 6.-

TOTAL: _____


FIRMA DEL ALUMNO

Desarrollo Problema 3

• Tenemos $f(x) = x^2 + x + 2$, $g(x) = x^2 - 2$

(a) Por demostrar que $f(x)$, $g(x)$ irreducibles en $\mathbb{F}_5[x]$.

Dem. como $\deg(f(x)) = 2$, $f(x)$ es reducible si y sólo si $f(x)$ tiene una raíz en \mathbb{F}_5 , ya que ~~f(x)~~ $f(x)$ se descompone en factores lineales. Lo ~~se~~ mismo ocurre para $g(x)$.

Luego basta demostrar que ni $f(x)$, ni $g(x)$ tienen raíces en \mathbb{F}_5 .

$$f(0) = 0^2 + 0 + 2 = 2$$

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

$$f(2) = 4 + 2 + 2 = 8 = 3$$

$$f(3) = 9 + 3 + 2 = 14 = 4$$

$$f(4) = 16 + 4 + 2 = 1 + 4 + 2 = 7 = 2$$

$$g(0) = 0^2 - 2 = -2 = 3$$

$$g(1) = 1^2 - 2 = -1 = 4$$

$$g(2) = 4 - 2 = 2$$

$$g(3) = 9 - 2 = 7 = 2$$

$$g(4) = 16 - 2 = 14 = 4$$

$\therefore f(x), g(x)$ no tienen raíces en \mathbb{F}_5

③

$\therefore g(x), f(x)$ irreducibles en $\mathbb{F}_5[x]$.

(b) $K_1 = \mathbb{F}_5(\alpha)$, $K_2 = \mathbb{F}_5(\beta)$, donde $f(\alpha) = 0$, $g(\beta) = 0$.

Objetivo: Construir isomorfismo explícito entre K_1 y K_2 .

Desarrollo.

(Como $f(x) \in \mathbb{F}_5[x]$ irreducible y ~~f(x)~~ $f(\alpha) = 0$, entonces

$\mathbb{F}_5[x]/(f(x)) \cong \mathbb{F}_5(\alpha)$, donde el isomorfismo viene dado por

$$\begin{aligned} \varphi : \mathbb{F}_5[x]/(f(x)) &\longrightarrow \mathbb{F}_5(\alpha) \\ \overline{p(x)} &\longmapsto p(\alpha) \end{aligned}$$

donde $\alpha \in \mathbb{F}_5$, y , $\bar{x} = x \pmod{f(x)}$. Evidentemente es un isomorfismo de cuerpos ya que $\varphi(\bar{1}_{\mathbb{F}_5}) = \bar{1}_{\mathbb{F}_5}$, y en particular,

donde $\bar{p(x)} = p(x) \pmod{f(x)}$. Evidentemente φ es homomorfismo de anillos, pues

$$\begin{aligned}\varphi(\bar{p(x)} + \bar{q(x)}) &= \varphi(\bar{p(x) + q(x)}) \\ &= p(\alpha) + q(\alpha) \\ &= \varphi(\bar{p(x)}) + \varphi(\bar{q(x)})\end{aligned}$$

$$\begin{aligned}\varphi(\bar{p(x)} \bar{q(x)}) &= \varphi(\bar{p(x)q(x)}) \\ &= p(\alpha)q(\alpha) \\ &= \varphi(\bar{p(x)}) \varphi(\bar{q(x)})\end{aligned}$$

$\forall \bar{p(x)}, \bar{q(x)} \in \mathbb{F}_5[x]/(f(x))$

~~dominio euclídeo~~

~~Como $\mathbb{F}_5[x]$ es un dominio euclídeo, $\ker \varphi$ es generado por un elemento de $\mathbb{F}_5[x]$ digamos $\ker \varphi = (g(x))$~~

φ es inyectiva, ya que $\varphi(\bar{p(x)}) = 0$ implica $p(\alpha) = 0$. Pero por el algoritmo de la división, $\exists q(x), r(x) \in \mathbb{F}_5[x]$:

$$p(x) = f(x)q(x) + r(x)$$

Afirmamos que $r(x) = 0$, en caso contrario, $r(\alpha) = 0$ y $(x-\alpha)$ divisor común de $f(x)$ y $r(x)$ (\Rightarrow), ya que $f(x)$ es irreducible.

$$\therefore \not\exists r(x) = 0$$

$$\therefore f(x) \mid p(x)$$

$$\therefore \overline{p(x)} = \overline{0}$$

Así, φ es inyectiva.

Ψ es epíyectiva, ya que recordando $\mathbb{F}_5(\alpha) = \left\langle \frac{A(\alpha)}{B(\alpha)} \mid A(\alpha), B(\alpha) \in \mathbb{F}_5[x] \right\rangle$, siempre podemos dejar $\frac{A(\alpha)}{B(\alpha)}$ como combinación lineal de elementos $1, \alpha, \alpha^2, \dots, \alpha^m$

$$1, \alpha. \therefore \exists C(x) \in \mathbb{F}_5[x] : \frac{A(\alpha)}{B(\alpha)} = C(\alpha).$$

Tomando $C(x) \in \mathbb{F}_5[x]$,

$$\Psi(\overline{C(x)}) = C(\alpha).$$

$\therefore \Psi$ es un isomorfismo

Análogamente tenemos el isomorfismo $\mathbb{F}_5[x]/(g(x)) \cong \mathbb{F}_5(\beta)$,

$\Psi: \overline{p(x)} \mapsto p(\beta)$. Ahora si consideramos el siguiente diagrama

$$\begin{array}{ccc}
 \mathbb{F}_5(\alpha) & \xrightarrow{\delta} & \mathbb{F}_5(\beta) \\
 \downarrow \psi^{-1} & \swarrow ? & \uparrow \psi \\
 \mathbb{F}_5[x]/(f(x)) & \xrightarrow{id} & \mathbb{F}_5[x]/(g(x))
 \end{array}$$

Existe isomorfismo $\sigma: \mathbb{F}_5(\alpha) \longrightarrow \mathbb{F}_5(\beta)$, dado por

$\sigma = \psi \circ \text{id} \circ \psi^{-1}$, en el cual ~~$\sigma(f(\alpha))$~~

$$\sigma(f(\alpha)) = f(\beta), \quad f(x) \in \mathbb{F}_5[x], \text{gr}(f) \leq 1.$$

Más específicamente, $\sigma: \begin{cases} a \longmapsto a & \forall a \in \mathbb{F}_5 \\ \alpha \longmapsto \beta. \end{cases}$

$$\begin{aligned}
 &\text{no es homom. de anillo} \\
 &\text{ya que } 2^2 + 2 + 2 = 0 \xrightarrow{\sigma} \beta + \beta + 2 \neq 0
 \end{aligned}$$

Problemas 2

- (a) Construir el cuerpo de descomposición $K \supset \mathbb{Q}$ para $x^5 - 18 \in \mathbb{Q}$. Calcular $[K : \mathbb{Q}]$.

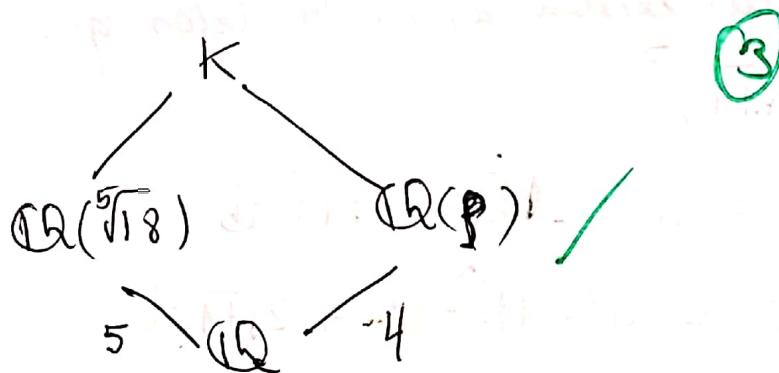
Desarrollo. Es sabido que en \mathbb{C} , las raíces de $x^5 - 18$ son:

$$\sqrt[5]{18}, \sqrt[5]{18} p, \sqrt[5]{18} p^2, \sqrt[5]{18} p^3, \sqrt[5]{18} p^4$$

donde $\rho = e^{\frac{2\pi i}{5}}$.

Ahora, K viene dado por $K = \mathbb{Q}(\sqrt[5]{18}, \sqrt[5]{18}\rho, \sqrt[5]{18}\rho^2, \sqrt[5]{18}\rho^3, \sqrt[5]{18}\rho^4)$
o bien $K = \mathbb{Q}(\sqrt[5]{18}, \rho)$.

Ahora debemos calcular $[K : \mathbb{Q}]$



Se sabe que $[(\mathbb{Q}(\sqrt[5]{18})) : \mathbb{Q}] = 5$ ya que $m(x) = x^5 - 18$ es irreducible (18 no es una 5 -potencia), además $m(\sqrt[5]{18}) = 0$.

Por otro lado, $[(\mathbb{Q}(\rho)) : \mathbb{Q}] = \varphi(5) = 4$, ya que ρ es raíz 5^{th} de la unidad (primitiva) (φ función de Euler).

$$\text{Como } \text{mcd}(5,4) = 1$$

$$[K:\mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{8}, p) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{8})\mathbb{Q}(p) : \mathbb{Q}] \\ = [\mathbb{Q}(\sqrt[5]{8}) : \mathbb{Q}] [\mathbb{Q}(p) : \mathbb{Q}] = 5 \cdot 4 = 20$$

~~1. [K : Q]~~

$$\therefore [K : \mathbb{Q}] = 20$$

(b) Por demostrar que $\mathbb{Q}(\sqrt{7})$ y $\mathbb{Q}(\sqrt{11})$ no son isomorfos como cuerpos.

Demonstración.

Si existiera isomorfismo $\varphi : \mathbb{Q}(\sqrt{7}) \rightarrow \mathbb{Q}(\sqrt{11})$, entonces $\varphi(\sqrt{7}) \in \mathbb{Q}(\sqrt{11})$, y

$7 = \varphi(\sqrt{7})$ (ya que $\varphi(1) = 1 \Rightarrow \varphi(q) = q \quad \forall q \in \mathbb{Q}$), pero $7 = \varphi(\sqrt{7}) \varphi(\sqrt{7}) = \varphi(\sqrt{7})^2$. Luego $\sqrt{7}$ es cuadrado en $\mathbb{Q}(\sqrt{11})$. Vamos a probar que esto no es posible.

Supongamos que existen $a, b \in \mathbb{Q}$ tales que

$$\sqrt{7} = (a + b\sqrt{11})^2$$

(3)

$$\therefore \sqrt{7} = a^2 + 11b^2 + 2\sqrt{11}ab$$

$$\therefore 0 = a^2 + 11b^2 - 7 + 2\sqrt{11}ab$$

Obtenemos el siguiente sistema de ecuaciones

$$\begin{cases} a^2 + 11b^2 - 7 = 0 \\ 2\sqrt{11}ab = 0 \end{cases}$$

$$2\sqrt{11}ab = 0 \Rightarrow a=0 \text{ o } b=0.$$

$$\text{Si } a=0 : 11b^2 - 7 = 0 \quad \therefore b^2 = \frac{7}{11} (\Leftrightarrow)$$

(No existe $b \in \mathbb{Q}$ tal que $b^2 = \frac{7}{11}$)

$$\text{Si } b=0 : \quad a^2 - 7 = 0 \quad \therefore a^2 = 7 \Leftrightarrow (\exists)$$

(No existe $a \in \mathbb{Q}$ tal que $a^2 = 7$)

$\therefore \mathbb{Q}[\sqrt{7}], \mathbb{Q}[\sqrt{11}]$ no son isomórfos
como cuerpos.

Problema 2.

(a) K cuerpo de característica $p > 0$.

Pd: $f(x) = x^p - x - a$ es reducible en $F[x]$,

$\Rightarrow f(x)$ se descompone en factores lineales distintos en $F[x]$

Demonstración.

Primero veamos que si $f(x) = x^p - x - a$,

$$Df(x) = p \cdot x^{p-1} - 1 = -1$$

Luego $f(x)$ no puede tener raíces dobles en K

$\because f(x)$ se descompone en factores lineales distintos en K

Sea $f(x) = f_1(x) \cdots f_r(x)$, donde $f_i(x) \in F[x]$

$\forall i = 1, \dots, r$, son los factores irreducibles de $f(x)$

Si $x_{i_1}, x_{i_2}, \dots, x_r \in K$ tales que $f_i(x_{i_1}) = f_i(x_{i_2})$

Como $\text{char } K = p > 0$, entonces $\mathbb{F}_p \subset K$.

Ademas ~~$\forall \alpha \in \mathbb{F}_p$~~ $\forall \alpha \in \mathbb{F}_p : \alpha^p = \alpha$. (*)

Por otro lado, si $\alpha \in \mathbb{F}_p$ es raíz de $f(x)$, entonces $\alpha + 1 \in \mathbb{F}_p$ también es raíz de $f(x)$. Ya que

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^p - (\alpha+1) - a \\ &= \alpha^p + 1 - \alpha - 1 - a \\ &= \alpha^p - \alpha - a \\ &\equiv 0 \end{aligned}$$



$$\therefore f(0) = 0$$

$$\therefore a = 0$$

Por lo tanto, si $a=0$, $f(x)$ se descompone en factores lineales del tipo $(x-b)$, $b \in F_p$.

Supongamos ahora que $a \in F \setminus F_p$ ($a \notin F_p$).

$$a \notin F_p \Rightarrow a \in F^*$$

~~Si asumimos a la complejación algebraica~~

①

Si asumimos que existe una raíz α_j que no está en K , entonces

$$x^p - x - a = (x - \alpha_1) \cdots (x - \alpha_{j-1})(x - \alpha_j)(x - \alpha_{j+1}) \cdots (x - \alpha_p)$$

entonces

$$x^p - x = (x - \alpha_1) \cdots (x - \alpha_j) \cdots (x - \alpha_p) + a$$

pero $\alpha_j^p - \alpha_j = 0 + a$

$$\alpha_j^p - \alpha_j - a = 0 \iff$$

ya que asumimos que α_j es raíz de $x^p - x - a$

(b) Por demostrar que para cada primo p , $x^p - x - 1$ es irreducible en $\mathbb{Q}[x]$

Dem.: Por lema de Gauss, si $f(x)$ es irreducible en $\mathbb{Z}[x]$, entonces es irreducible en $\mathbb{Q}[x]$. Ahora basta ver que $x^p - x - 1$ es irreducible en $\mathbb{Z}[x]$.

Si $x^p - x - 1 = A(x)B(x)$, donde $A(x), B(x)$ enteros en módulo p (i.e., con coeficientes en $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$) serían reducible. Demostraremos que $x^p - x - 1$ no tiene raíces en \mathbb{F}_p . Aplicando desarrollo en (a), lcm($x^p - x - 1$, $x^p - x - 1$) = 1 y $x^p - x - 1$ no se descompone en factores lineales en \mathbb{F}_p 3

$\therefore x^p - x - 1$ es irreducible en \mathbb{F}_p

Con lo anterior, se tiene que $x^p - x - 1$ es irreducible en $\mathbb{Z}[x]$.

$\therefore x^p - x - 1$ es irreducible en $\mathbb{Q}[x]$ \mathbb{F}_p (p primo).

Álgebra 2 para postgrado

Prueba 1 Miércoles 10 de Septiembre, 2014

Se espera que explique su respuesta: motive su respuesta, mencione el teorema, proposición, lema, etc. que usted utiliza.

1.
 - a) Construye un cuerpo de descomposición $K \supset \mathbb{Q}$ para $x^5 - 18 \in \mathbb{Q}[x]$. Calcule $[K : \mathbb{Q}]$.
 - b) Demuestre que $\mathbb{Q}[\sqrt{7}]$ y $\mathbb{Q}[\sqrt{11}]$ no son isomorfos como cuerpos.
2.
 - a) Sea K un cuerpo de característica $p > 0$. Demuestre que si $f(x) = x^p - x - a$ es reducible en $F[x]$, entonces $f(x)$ se descompone en factores lineales distintos en $F[x]$.
 - b) Para cada primo p demuestre que $x^p - x - 1$ es irreducible en $\mathbb{Q}[x]$.
3. Considere $f(x) = x^2 + x + 2$ y $g(x) = x^2 - 2$.
 - a) Demostrar que $f(x)$ y $g(x)$ son irreducibles en $\mathbb{F}_5[x]$.
 - b) Sea $K_1 = \mathbb{F}_5(\alpha)$ con $f(\alpha) = 0$ y $K_2 = \mathbb{F}_5(\beta)$ con $g(\beta) = 0$. Construye un isomorfismo explícito entre K_1 y K_2 .

Duración: 2 horas

Problema 1

(a) K es el campo de descomposición de $x^5 - 18 \in \mathbb{Q}[x]$. Las raíces de $x^5 - 18$ ($\in \mathbb{C}$) son $\sqrt[5]{18}, \sqrt[5]{18}\rho, \sqrt[5]{18}\rho^2, \sqrt[5]{18}\rho^3, \sqrt[5]{18}\rho^4$, donde $\rho = e^{2\pi i/5}$. Luego

$$K = \mathbb{Q}(\sqrt[5]{18}, \sqrt[5]{18}\rho, \sqrt[5]{18}\rho^2, \sqrt[5]{18}\rho^3, \sqrt[5]{18}\rho^4) = \mathbb{Q}(\sqrt[5]{18}, \rho).$$

Para calcular $[K : \mathbb{Q}]$ veamos lo siguiente:

$$\begin{array}{ccc} K & = & \mathbb{Q}(\sqrt[5]{18}, \rho) \\ & \swarrow & \searrow \\ \mathbb{Q}(\sqrt[5]{18}) & & \mathbb{Q}(\rho) \\ & \searrow^5 & \swarrow^4 \\ & \mathbb{Q} & \end{array}$$

$\sqrt[5]{18}$ es raíz de $x^5 - 18 \in \mathbb{Q}[x]$ (irreducible por Eisenstein).

Como $\text{mcd}(5, 4) = 1$, se tiene

$$\begin{aligned} [K : \mathbb{Q}] &= [\mathbb{Q}(\sqrt[5]{18}, \rho) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{18})(\mathbb{Q}(\rho)) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt[5]{18}) : \mathbb{Q}] [\mathbb{Q}(\rho) : \mathbb{Q}] = 5 \cdot 4 = 20 \end{aligned}$$

$$\therefore \cancel{[K : \mathbb{Q}]} = 20.$$

(b) Por demostrar que $\mathbb{Q}(\sqrt{7})$ y $\mathbb{Q}(\sqrt{11})$ no son isomorfos.

En efecto, en caso de que existiera un isomorfismo $\varphi: \mathbb{Q}(\sqrt{7}) \rightarrow \mathbb{Q}(\sqrt{11})$ $\varphi(\sqrt{7}) \in \mathbb{Q}(\sqrt{11})$, $\varphi(\sqrt{7}) = \sqrt{7} = \varphi(\sqrt{7})^2$. Es decir, $\sqrt{7}$ es un cuadrado en $\mathbb{Q}(\sqrt{11})$. Sean $a, b \in \mathbb{Q}$:

$$\sqrt{7} = (a + b\sqrt{11})^2$$

$$\Rightarrow \sqrt{7} = a^2 + 11b^2 + 2ab\sqrt{11} \Leftrightarrow 0 = a^2 + 11b^2 - 7 + 2ab\sqrt{11}$$

Así tenemos sistema de ecuaciones

$$\begin{cases} a^2 + 11b^2 - 7 = 0 \\ 2ab\sqrt{11} = 0 \end{cases}$$

$$\therefore ab = 0$$

$$\therefore a = 0 \quad \text{o} \quad b = 0.$$

Si $a=0 \Rightarrow b^2 = \frac{7}{11} \Leftrightarrow (\text{No existe } b \in \mathbb{Q} \text{ tal que } b^2 = \frac{7}{11})$

Si $b=0 \Rightarrow a^2 = 7 \Leftrightarrow (\text{No existe } a \in \mathbb{Q} \text{ tal que } a^2 = 7)$

$\therefore (\mathbb{Q}(\sqrt{7})) \text{ y } (\mathbb{Q}(\sqrt{11})) \text{ no son isomorfos}$

Problema 3

(a) Por demostrar que $f(x) = x^2 + x + 2$, $g(x) = x^2 - 2$ son irreducibles en $\mathbb{F}_5[x]$.

Como son de grado 2, en caso de que fueran reducibles implicaría que tienen una raíz en \mathbb{F}_5 . Veámos que no es así.

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\},$$

$$\begin{aligned} f(0) &= 0^2 + 0 + 2 = 2 \\ f(1) &= 1^2 + 1 + 2 = 4 \\ f(2) &= 2^2 + 1 + 2 = 7 = 2 \\ f(3) &= 3^2 + 1 + 2 = 12 = 2 \\ f(4) &= 4^2 + 1 + 2 = 19 = 4 \end{aligned}$$

$$\left. \begin{array}{l} g(0) = 0^2 - 2 = -2 = 3 \\ g(1) = 1^2 - 2 = -1 = 4 \\ g(2) = 2^2 - 2 = 2 \\ g(3) = 3^2 - 2 = 7 = 2 \\ g(4) = 4^2 - 2 = 14 = 4. \end{array} \right\}$$

$\therefore f, g$ sin raíces en \mathbb{F}_5 .

$\therefore f, g$ irreducibles en \mathbb{F}_5 .

(b) Construir isomorfismos explícitos entre K_1 y K_2 .

Tenemos $f(\alpha), g(\beta) = 0$. Sea $\varphi: K_1 \rightarrow K_2$ isomorfismo

$$\alpha^2 + \alpha + 2 = 0 \Rightarrow \varphi(\alpha^2 + \alpha + 2) = 0$$

$$\Rightarrow \varphi(\alpha)^2 + \varphi(\alpha) + 2 = 0$$

$$\Rightarrow \varphi(\alpha)^2 + \varphi(\alpha) + \beta^2 = 0 \quad (\beta^2 - 2 = 0)$$

Como $\det \mathbb{F}_5 \neq 2$, podemos usar expresión clásica para desarrollar ecuaciones de grado 2:

$$\varphi(\alpha) = \frac{-1 \pm \sqrt{1 - 4\beta^2}}{2}$$

$$\text{Supongamos que } \varphi(x) = \frac{-1 + \sqrt{1 - 4\beta^2}}{2}$$

$$\varphi(x) = \frac{-1 + \sqrt{1 - 4\beta^2}}{2} = \frac{-1 + \sqrt{-7}}{2} = \frac{-1 + \sqrt{-2}}{2} = \frac{-1 + \sqrt{\beta^2}}{2} = \frac{-1 + \beta}{2}$$

$$= 3 \cdot 4 + 3\beta = 12 + 3\beta = 2 + 3\beta$$

$$\therefore \forall a, b \in \mathbb{Q} : \varphi(a+b\alpha) = a+b\varphi(\alpha) = \cancel{a+\cancel{b}(\cancel{1}+\cancel{\beta})}$$

$$= a+b(2+3\beta) = (a+2b)+3b\beta$$

$$\therefore \varphi(\alpha+b\alpha) = (a+2b)+3b\beta$$

Análogamente se puede calcular un segundo isomorfismo, considerando

$$\varphi(x) = \frac{-1 - \sqrt{1 - 4\beta^2}}{2} \dots$$

Cuerpos y Álgebra
Desarrollo Puebla 2
Marco Godoy V.

(4,2)

Problema 1

(1) Si $b \in L$ es entero sobre B , entonces $B[b]$ es finitamente generado como B -módulo. En particular, si $a_1, \dots, a_n \in B[b]$ son los generadores

$$b = \sum_{i=1}^n l_i a_i, \quad l_i \in B.$$

Por otro lado, B es entero sobre D , lo que implica que ~~B es entero sobre D~~ B es finitamente generado como D -módulo.

Es más, si b_1, \dots, b_m son los generadores ($\in B$)

$$B = D[b_1, \dots, b_m]$$

Ahora $B[b] = D[b_1, \dots, b_m][b] = D[b_1, \dots, b_m, b]$ es finitamente generado como D -módulo, y esto quiere decir

que b_1, \dots, b_m, b son enteros sobre D

$\therefore b$ es entero sobre D .

1	14
2	10
3	8
4	-

(K, +, ·) ~~para datos~~

Primero demostraremos que \mathcal{O}_K es un dominio.

En efecto, sean $a, b \in \mathcal{O}_K$ tales que $a \cdot b = 0$

y $a \neq 0$. Se tiene que $ab \in \mathcal{O}_K$ y además

$$a^n b^n + z_{n-1} a^{n-1} b^{n-1} + \dots + z_1 ab + z_0 = 0, \quad z_i \in \mathbb{Z}$$

como $ab = 0$, inmediatamente $z_0 = 0$

$$\Rightarrow a^n b^n + z_{n-1} a^{n-1} b^{n-1} + \dots + z_1 ab = 0$$

Sin pérdida de generalidad, podemos suponer que $z_1 \neq 0$ (en caso contrario tomamos j tal que a^j es la menor potencia). Dividiendo la igualdad por a se tiene que

$$a^{n-1} b^{n-1} + z_{n-1} a^{n-2} b^{n-2} + \dots + z_1 b = 0$$

como $ab = 0$, $\Rightarrow z_1 b = 0$

¡¡ Es dominio

porque está

contenido en

un cuerpo !!

Afirmación: \mathcal{O}_K es normal

Para demostrar que \mathcal{O}_K es normal es suficiente verificar que

$$\mathcal{O}_K = K_{\text{ent}}$$

donde $K_{\text{ent}} = \{a \in K / a \text{ entero sobre } \mathcal{O}_K\}$ (Recordar que $\mathbb{Z} \subset \mathcal{O}_K \subset K$)



Primero veamos que automáticamente se tiene la
contención

$$\mathcal{O}_K \subset K_{\text{ent}} \quad (K_{\text{ent}} \subset K)$$

Ahora, sea $b \in K_{\text{ent}}$. Como b es entero sobre \mathcal{O}_K
y \mathcal{O}_K es entero sobre \mathbb{Z} , por resultado (7.1) se tiene que
 b es entero sobre \mathbb{Z} .

$$\therefore b \text{ es entero sobre } \mathbb{Z}$$

$$\therefore b \in \mathcal{O}_K$$

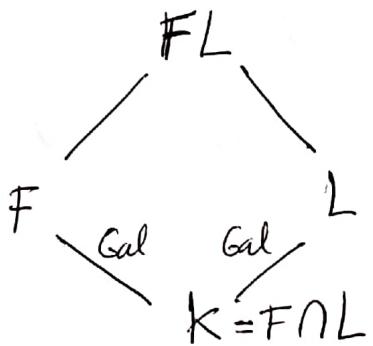
$$\therefore \mathcal{O}_K = K_{\text{ent}}$$

Se concluye así que \mathcal{O}_K es un dominio normal.

14/15

Problema 2

Veamos el siguiente diagrama



Afirmación. FL/K es Galoiana

~~En efecto, tomando $\in FL \setminus (F \cap K)$ nos queda que~~

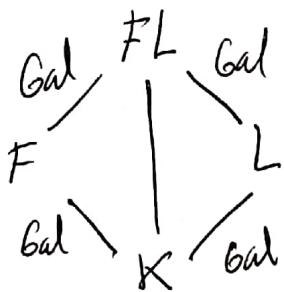
En efecto, como F/K es galosiana, F es el cuerpo de descomposición de un polinomio $f_1(x) \in K[x]$ separable,
análogamente, L/K Galoiana implica

Luego $f_1(x)$ puede verse como polinomio en $L[x]$ ($K \hookrightarrow L$)
y como $F \subset FL$, entonces FL es el cuerpo de descomposición
de un polinomio $f_1(x) \in L[x]$ separable

$\therefore FL/L$ Galoiana

Análogamente, se demuestra que FL/F Galoiana. Observando
nuestro diagrama otra vez, se tiene

Cuidado!! la
propiedad de ser
Galoiana no
se preserva en
torno.



$\therefore FL/K$ Galoiana

Por demostrar que

$$\text{Gal}(FL/k) \cong \text{Gal}(F/k) \times \text{Gal}(L/k)$$

-Demostración-

Consideremos la aplicación

$$\varphi: \text{Gal}(FL/k) \longrightarrow \text{Gal}(F/k) \times \text{Gal}(L/k)$$
$$\sigma \longmapsto (\sigma|_F, \sigma|_L)$$

Es evidente que φ está bien definida, ya que $F, L \subset FL$ y un automorfismo $\sigma \in \text{Gal}(FL/k)$ sigue siendo un automorfismo en F y en L .

También es claro que φ es un homomorfismo de grupos

$$\begin{aligned}\varphi(\sigma \cdot \tau) &= (\sigma \cdot \tau|_F, \sigma \cdot \tau|_L) \\ &= (\sigma|_F \cdot \tau|_F, \sigma|_L \cdot \tau|_L) = (\sigma|_F, \sigma|_L) \cdot (\tau|_F, \tau|_L) \\ &= \varphi(\sigma) \varphi(\tau)\end{aligned}$$

Veamos que

$$\ker \varphi = \{\sigma \in \text{Gal}(FL/k) \mid (\sigma|_F, \sigma|_L) = (1, 1)\} \quad (1 = \text{id})$$

Del hecho de que $\sigma|_F, \sigma|_L = 1$ implica que $\sigma|_{F \cap L} = 1$, en particular, σ fija el producto FL ($\sigma|_{FL} = 1$)

$$\therefore \sigma = 1$$

$\therefore \varphi$ inyectiva



Sea ahora $(\sigma, \tau) \in \text{Gal}(F/k) \times \text{Gal}(L/k)$.

esto dice

$$\sigma \in \text{Gal}(F/k), \tau \in \text{Gal}(L/k)$$

Se sigue, por el teorema de extensión de homomorfismos,

que σ, τ se pueden extender a homomorfismos

$$\hat{\sigma}, \hat{\tau}: FL \longrightarrow \overline{FL} \quad \text{Pero por otro lado } FL/F, FL/L$$

son Galoisianas, lo que dice que estas extensiones satisfacen

$$\hat{\sigma}(FL) \subset FL \quad (\text{por normalidad})$$

$$\hat{\tau}(FL) \subset FL \quad (\text{de } FL/F, FL/L)$$

10/
15

cuidado!!

¿Cuál serán la pre-imagen

de (σ, τ) ?

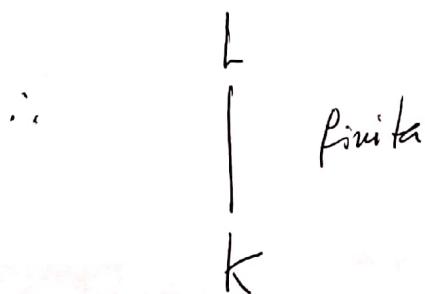
¿Sobre qué sucede levantamiento?

Problema 3

Tenemos

$$\mathbb{F}_2 \subsetneq K \subseteq L = \mathbb{F}_2(x)$$

En el caso de que $K = \mathbb{F}_2(f)$, $f \in \mathbb{F}_2[x]$,
 se tiene que $[\mathbb{F}_2(x) : K] = \max\{\deg g, \deg h\}$
 donde $f = \frac{g}{h}$ ($g, h \in \mathbb{F}_2[x]$, $h \neq 0$)



Por lo tanto existe cantidad finita de cuerpos F

$$\text{con } K \subseteq F \subseteq L$$

8/15

~~Supongamos~~ Podemos ver que si \hat{F} es un cuerpo finito tal que $\mathbb{F}_2 \subsetneq \hat{F}$, entonces $\hat{F} \not\subset \mathbb{F}_2(x)$. Luego los cuerpos intermedios entre \mathbb{F}_2 y $\mathbb{F}_2(x)$ son cuerpos de fracciones nacionales (con coeficientes en \mathbb{F}_2)

Hebría que probar que $\mathbb{F}_2 \subsetneq F \subseteq K$

$\Rightarrow F = \mathbb{F}_2(f')$ para algún f' . (Es cierto,
 pero no evidente)

(6,0)

(1) Tenemos $[L : K] = 2$. Considerando $\alpha \in L, \alpha \notin K$ tenemos

$$z \begin{pmatrix} L \\ | \\ k[\alpha] \\ | \\ K \end{pmatrix}$$

1	15
2	15
3	12
4	8
5	-

Luego se cumple que $L = k(\alpha)$ ($[L : K] = [L : k(\alpha)][k(\alpha) : K]$).

Sea $m_{K, \alpha}(x)$ el polinomio minimal satisfecho por α . Como $[k(\alpha) : K] = 2$, $m_{K, \alpha}(x) = x^2 + \alpha x + b$. Por otro lado, $\alpha^2 + \alpha\alpha + b = 0$, y ademárs

$$\alpha^2 + \alpha\alpha + b = 0 \iff \alpha^2 + \alpha\alpha = -b$$

$$\begin{aligned} & \underset{K[x]}{\Rightarrow} \alpha^2 + \alpha\alpha + \frac{\alpha^2}{4} = -b + \frac{\alpha^2}{4} \quad \left(\text{ya que } \alpha \in K \neq 2, \text{ podemos dividir por 4} \right) \\ & \Rightarrow \left(\alpha + \frac{\alpha}{2} \right)^2 = \frac{\alpha^2 - 4b}{4} \end{aligned}$$

Luego tomamos $\omega = \alpha + \frac{\alpha}{2}$. Evidentemente $\omega \notin K$ y $\omega^2 = \frac{\alpha^2 - 4b}{4}$ que sí está en K . Ahora podemos definir $\tilde{\omega} = \sqrt{\frac{\alpha^2 - 4b}{4}}$, teniendo así:

$$L = K(\omega) = K\left(\sqrt{\frac{\alpha^2 - 4b}{4}}\right) = K\left(\sqrt{\alpha^2 - 4b}\right)$$

$\sqrt{\alpha^2 - 4b} \in K$, entonces

Si $\tilde{\omega} = \sqrt{\alpha^2 - 4b}$, entonces $\tilde{\omega} \in K$, pero $\sqrt{\tilde{\omega}} = \sqrt{\sqrt{\alpha^2 - 4b}} = \omega \notin K$,

y

$$L = K(\sqrt{\tilde{\omega}})$$

→ continua
en pag (*)

(2) Sea $p(x)$ polinomio monico irreducible en $\mathbb{F}_5[x]$, $\deg p = 6$. Si $\alpha \in \overline{\mathbb{F}_5}$ es raíz de $p(x)$, entonces

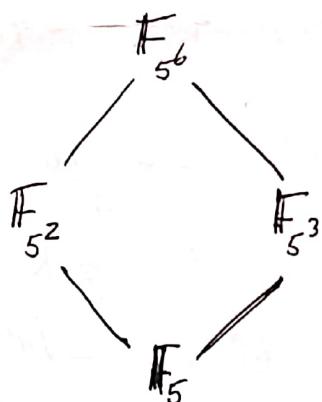
$$\mathbb{F}_5(\alpha) \cong \mathbb{F}_5[x]/(p)$$

donde $\mathbb{F}_5(\alpha)$ campo y $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 6$. Como $\mathbb{F}_5(\alpha)$ tiene 5^6 elementos, entonces $\mathbb{F}_5(\alpha) \cong \mathbb{F}_{5^6}$.

Sea $A = \#\{\alpha \in \overline{\mathbb{F}_5} / \mathbb{F}_5(\alpha) \cong \mathbb{F}_{5^6}\}$, B el numero de polinomios irreducibles en $\mathbb{F}_5[x]$ de grado 6, y como cada polinomio irreducible tiene raíces distintas (\mathbb{F}_5 es perfecto), entonces

$$B = \frac{A}{6}$$

Ahora,



$$\#\{\alpha \in \overline{\mathbb{F}_5} / \mathbb{F}_5(\alpha) \cong \mathbb{F}_{5^2}\} = 5^2 - 5, \text{ ya que } \mathbb{F}_5(\alpha) \cong \mathbb{F}_{5^2} \Leftrightarrow \alpha \in \mathbb{F}_{5^2}.$$

$$\text{Análogamente, } \#\{\alpha \in \overline{\mathbb{F}_5} / \mathbb{F}_5(\alpha) \cong \mathbb{F}_{5^3}\} = 5^3 - 5. \text{ Con lo anterior}$$

$$A = |\mathbb{F}_{5^6}| - (5^2 - 5) - (5^3 - 5) - 5 = 5^6 - (5^2 - 5) - (5^3 - 5) - 5$$

$$5^6 = (5^2)^3 = 25^3 = 15625, \quad 5^2 - 5 = 20, \quad 5^3 - 5 = 120$$

$$\therefore A = 15625 - 145 = 15480$$

$$\therefore B = \frac{15480}{6} = 2580 \quad (\text{polinomios irreducibles en } \mathbb{F}_5[x] \text{ de grado 6})$$

Falta la restricción a la característica

Página (*)

Sea $K = \mathbb{F}_2$, $L = \mathbb{F}_{2^2}$, tenemos que $[L : K] = 2$

Pero $\mathbb{F}_{2^2} = \mathbb{F}_2[x]/(x^2 + x + 1)$ ($x^2 + x + 1$ único polinomio irreducible en $\mathbb{F}_2[x]$ de grado 2)

$$\mathbb{F}_{2^2} = \{0, 1, \alpha, 1+\alpha \mid \alpha^2 + \alpha + 1 = 0\}$$

Tenemos que $0^2 = 0$, $1^2 = 1$, $\alpha^2 = 1 + \alpha \notin \mathbb{F}_2$,

$(1+\alpha)^2 = 1 + \alpha^2 = \alpha \notin \mathbb{F}_2$. Luego no existe $\omega \in L$ tal que $\omega^2 \in K$, o de manera equivalente, no existe ~~$\omega \in L$~~ $a \in \mathbb{F}_2$ tal que $\mathbb{F}_{2^2} = \mathbb{F}_2(\sqrt{a})$



(3) Por demostrar que $[\mathbb{Q}(\sqrt{2+i}) : \mathbb{Q}] = 4$

Sea $\alpha = \sqrt{2+i}$

$$\begin{aligned}\alpha^2 &= 2+i \\ \Rightarrow \alpha^2 - 2 &= i \\ \Rightarrow \alpha^4 - 4\alpha^2 + 4 &= -1 \\ \Rightarrow \alpha^4 - 4\alpha^2 + 5 &= 0\end{aligned}$$

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

Afirmación: $p(x)$ es irreducible

12/15

- Demostración - Primero veamos que $p(x)$ no tiene raíces. Como $p(5) = p(-5) = 625 - 100 + 5 \neq 0$, luego por el criterio de las raíces racionales, $p(x)$ no tiene raíces. ~~Ahora~~ (hay que probar con 1 y -1)

Ahora veamos que $p(x)$ no se puede factorizar como polinomios cuadráticos.

Para ello, sean $a, b, c, d \in \mathbb{Q}$

$$\begin{aligned}p(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd \\ &= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd\end{aligned}$$

Luego se tiene:

$$\left\{ \begin{array}{l} a+c=0 \\ ac+b+d=-4 \\ ad+bc=0 \\ bd=5 \end{array} \right.$$

Como $b, d \neq 0$, podemos multiplicar $a+c=0$ por $-b$ y sumarla a $ad+bc=0$, quedando así

$$\left. \begin{array}{l} a+b=0 \\ -ab-bc=0 \\ ad+bc=0 \end{array} \right\} \Rightarrow a(d-b)=0$$

De $bd=5$, tenemos que $d \neq b$ (5 no es cuadrado perfecto, es más, no existe $q \in \mathbb{Q}$ tq $q^2=5$). $\therefore a=0$

Por lo tanto $c=0$ y nos quedamos con

$$\begin{cases} b+d = -4 \\ bd = 5 \end{cases}$$

$$\Rightarrow b^2 + bd = -4b \Rightarrow b^2 + 5 = -4b$$

$$\Rightarrow b^2 + 4b + 5 = 0, \text{ con } b \in \mathbb{Q}$$

pero las raíces de $x^2 + 4x + 5$ son $\frac{-4 \pm \sqrt{16-20}}{2} \notin \mathbb{Q}$ ($\Rightarrow \Leftarrow$)

$\therefore p(x)$ es irreducible

$$\therefore [\mathbb{Q}(\sqrt{2+i}) : \mathbb{Q}] = 4 \quad \checkmark$$

(4)

~~(4)~~

$$\mathcal{Q}(\rho) \cong (\mathbb{Z}/7\mathbb{Z})^* = C_6$$

$$(\mathbb{Z}/7\mathbb{Z})^* = \cancel{\{1, 2, 3, 4, 5, 6\}}$$

1	2	3	4	5	6	elementos de $(\mathbb{Z}/7\mathbb{Z})^*$
↓	↓	↓	↓	↓	↓	orden
1	3	6	3	6	2	

Por lo visto en clases, $\mathcal{Q}(\sqrt{-7}) = \mathcal{Q}(\rho + \rho^2 + \rho^4)$. En efecto, para

$\sigma(\rho) = \rho^2$ tenemos

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

para $\sigma(\lambda) = \lambda$

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

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

$$\Rightarrow \lambda = \underbrace{a(\rho + \rho^2 + \rho^4)}_u + \underbrace{c(\rho^3 + \rho^5 + \rho^6)}_v$$

$$a = b = -1, \text{ tenemos } -\rho - \rho^2 - \rho^3 - \rho^4 - \rho^5 - \rho^6 = 1$$

$$\therefore 1 = -u - v$$

$$\therefore u = -1 - v$$

$$\text{Luego } u^2 = (\rho + \rho^2 + \rho^4)^2 = \rho^2 + \rho^4 + \rho + 2(\rho^3 + \rho^5 + \rho^6)$$

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

$$u^2 = -u - 2$$

$$u^2 + u + 2 = 0$$

$$\therefore u = \frac{-1 \pm \sqrt{1 - 8}}{2} = \frac{-1 \pm \sqrt{-7}}{2}$$

$$\therefore \mathcal{Q}(u) = \mathcal{Q}(\sqrt{-7})$$

Tenemos que

$$6 \left(\begin{array}{c} \mathbb{Q}(p) \\ | \\ \mathbb{Q}(p+p^2+p^4) = \mathbb{Q}(\sqrt{-7}) \\ | \\ \mathbb{Z} \\ | \\ \mathbb{Q} \end{array} \right)$$



Luego $[\mathbb{Q}(p) : \mathbb{Q}(p+p^2+p^4)] = 3$

~~Algo~~ $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ es el polinomio irreducible de p minimal de p .

$$\begin{array}{r} x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 : x^2 + x + 2 = x^4 - x^2 + 2x \\ \hline x^6 + x^5 + 2x^4 \\ \hline -x^4 + x^3 + x^2 + x + 1 \\ \hline -x^4 - x^3 - 2x^2 \\ \hline 2x^3 + 3x^2 + x + 1 \\ \hline 2x^3 + 2x^2 + 4x \\ \hline x^2 - 3x + 1 \end{array}$$

8/15

$$1 + p + p^2 + p^3 + p^4 + p^5 + p^6 = 0$$

$$1 + p + p^2 \notin \mathbb{Q}(\sqrt{-7}),$$

$$\underbrace{(1 + p + p^2)}_{=0} + p^3 + (p^4 + p^5 + p^6) = 0$$

$$1 + p^2 + p^3$$

$$(1 + p + p^2) + p^3 + p^4(1 + p + p^2) = 0$$

$$u + p^3 + p^4 u = 0$$

Luego p es raíz de $ux^4 + x^3 + u \in \mathbb{Q}(\sqrt{-7}) = \mathbb{Q}(p+p^2+p^4)$

Nota

58

Grupos de Lie lineales 2º semestre de 2011:

Prueba 1

Nombre: Marco Godoy V.

Problema	Puntaje
1	70
2	60
3	4,5
Total	77,5

Desarrollo prueba 1

Problema 1.

$$G \subseteq GL_m(\mathbb{C}), H \subseteq GL_k(\mathbb{C})$$

grupos de Lie de matrices

por demostrar que

$$\phi(G \times H) \subseteq GL_{m+k}(\mathbb{C})$$

es grupo de Lie de matriz

Demonstración.

Por demostrar que $\phi(G \times H)$ es grupo

como $I_m \in G, I_k \in H$, entonces

$$\phi(I_m, I_k) = \begin{pmatrix} I_m & \\ & I_k \end{pmatrix} = I_{m+k} \in \phi(G \times H)$$

$$\therefore \phi(G \times H) \neq \emptyset$$

Si $z_1, z_2 \in \phi(G \times H) \Rightarrow \exists (x_1, y_1), (x_2, y_2) \in G \times H,$

$$\phi(x_1, y_1) = z_1 \wedge \phi(x_2, y_2) = z_2$$

$$\phi(x_1, y_1) = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \phi(x_2, y_2) = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

$$\Rightarrow z_1 z_2 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 x_2 \\ y_1 y_2 \end{pmatrix}$$

como $x_1, x_2 \in G \quad \left\{ \begin{array}{l} x_1 x_2 \in G \\ y_1, y_2 \in H \end{array} \right. \quad (G, H \text{ grupos})$

$$\therefore z_1 z_2 = \begin{pmatrix} x_1 x_2 \\ y_1 y_2 \end{pmatrix} = \phi(x_1 x_2, y_1 y_2) \in \phi(G \times H)$$

$$\therefore z_1 z_2 \in \phi(G \times H)$$

Si $z \in \phi(G \times H), \exists (x, y) \in G \times H : \phi(x, y) = \begin{pmatrix} x \\ y \end{pmatrix} = z$

como $x \in G, y \in H \Rightarrow x^{-1} \in G, y^{-1} \in H$ y existe

$$z^{-1} = \begin{pmatrix} x \\ y \end{pmatrix}^{-1} = \begin{pmatrix} x^{-1} \\ y^{-1} \end{pmatrix} = \phi(x^{-1}, y^{-1}) \in \phi(G \times H)$$

$$\therefore z^{-1} \in \phi(G \times H)$$

Como G, H son grupos de matrices bajo multiplicación

$$\forall x \in G, \forall y \in H ; \det(x) \neq 0 \\ \det(y) \neq 0$$

Además $(x, y) \in G \times H \Rightarrow \phi(x, y) \in \phi(G \times H)$

$$\det(\phi(x, y)) = \det \begin{pmatrix} x & \\ & y \end{pmatrix} = \det(x) \det(y) \neq 0$$

$$\therefore \forall z \in \phi(x, y) ; \det(z) \neq 0$$

se concluye que $\phi(G \times H) \subseteq GL_{m+k}(\mathbb{C})$ es grupo

Falta demostrar que $\phi(G \times H)$ es de Lie.

Sean $(x_n)_{n=1}^{\infty}, (y_n)_{n=1}^{\infty}$ sucesiones en G y H respectivamente. Como G, H son grupos de Lie:

$$x_n \xrightarrow[n \rightarrow \infty]{} x \quad \Rightarrow \quad x \in G$$

$$y_n \xrightarrow[n \rightarrow \infty]{} y \quad \Rightarrow \quad y \in H$$

$$\Rightarrow \phi(x_n, y_n) = \begin{pmatrix} x_n & \\ & y_n \end{pmatrix} \xrightarrow[n \rightarrow \infty]{} \begin{pmatrix} x & \\ & y \end{pmatrix} = \phi(x, y) \in \phi(G \times H)$$

$\therefore \phi(G \times H)$ es grupo de Lie

Por demostrar que si G, H son caminos conexos, entonces $\phi(G \times H)$ es camino conexo.

Dem. $\forall x \in G, \forall y \in H, \exists \alpha: [0, 1] \rightarrow G, \exists \beta: [0, 1] \rightarrow H$ continuas tales que

$$\alpha(0) = I_m \quad ; \quad \beta(0) = I_k$$

$$\alpha(1) = x \quad ; \quad \beta(1) = y$$

Definimos el camino $\gamma: [0, 1] \rightarrow \phi(G \times H)$ por $\gamma(t) = \begin{pmatrix} \alpha(t) & \\ & \beta(t) \end{pmatrix}$

Evidentemente γ es continua en $[0, 1]$

$$\gamma(0) = \begin{pmatrix} \alpha(0) & \\ & \beta(0) \end{pmatrix} = \begin{pmatrix} I_m & \\ & I_k \end{pmatrix} = I_{m+k}$$

$$\gamma(1) = \begin{pmatrix} \alpha(1) & \\ & \beta(1) \end{pmatrix} = \begin{pmatrix} x & \\ & y \end{pmatrix}$$