Universidad Autónoma de Madrid — Curso 2019-20

Matemáticas/ Ingeniería Informática-Matemáticas

Teoría de Galois

Segundo examen parcial. Martes, 17 de noviembre de 2020

---

1. Problema 2A. Responde de manera razonada a las siguientes preguntas.

a) (0,5 puntos) Demuestra que $E = \mathbb{F}_5[x]/\langle x^2 + x + 1\rangle$ es el cuerpo de descomposición de $t^3 - 1$ sobre $\mathbb{F}_5$.

b) (0,25 puntos) Escribe una base de E sobre $\mathbb{F}_5$.

c) (0,25 puntos) Escribe, en términos de la base del apartado (a), todas las raíces de $t^3 - 1$.

d) (0,25 puntos) Sea M el cuerpo de descomposición de $t^3 - 2$ sobre K. Demuestra que M y E son isomorfos.

e) (0,25 puntos) Usando el apartado (c) y que 3 es una raíz cúbica de 2 en $\mathbb{F}_5$, encuentra todas las raíces de $t^3 - 2$ en E.

f) (0,5 puntos) Sea $\alpha \in M$ una raíz cúbica de 2, de modo que $M = \mathbb{F}_5(\alpha)$. Escribe de manera explítica un isomorfismo entre M y E indicando cuál sería la imagen de $\overline{x} \in E$ en términos de α. ¿Cuántos isomorfismos distintos puedes construir?

a) $t^3-1 = (t-1)(t^2+t+1) \in \mathbb{F}_5[t]$

t^2+t+1 es irred / $\mathbb{F}_5$ (porque no tiene raíces en $\mathbb{F}_5$).

Por lo tanto $\mathbb{F}_5[x]/\langle x^2+x+1\rangle$ es el cuerpo más pequeño que contiene a $\mathbb{F}_5$ y 1 raíz de t^2+t+1, pero como el polinomio es de grado dos, tiene sus dos raíces y es también a su cuerpo de descomposición / $\mathbb{F}_5$.

b) $[E:\mathbb{F}_5] = 2$ Base: $\{\overline{1}, \overline{x}\}$.

c) $\bar{x}$ es una raíz cúbica de 1 en $E \setminus \mathbb{F}_5$. $Fr: E \to E$ lleva una raíz cúbica de 1 en otra raíz cúbica de 1: $\bar{x} \to \bar{x}^5$ en otra raíz.

- $\bar{x}^2 = -\bar{x} - 1 = 4\bar{x} + 4$
- $\bar{x}^3 = 1$
- $\bar{x}^4 = \bar{x}$; $\boxed{\bar{x}^5 = \bar{x}^2 = 4\bar{x} + 4}$

d) $t^3 - 2 = (t-3)(t^2+3t+4)$ pred/$\mathbb{F}_5$ (simples)

$\Rightarrow M = \mathbb{F}_5[y]/\langle y^2+3y+4 \rangle$ es el cuerpo de descomposición de $t^3 - 2/\mathbb{F}_5$ (mismo argumento que en (a)).

Como $[M : \mathbb{F}_5] = 2$ y sólo hay una extensión de grado 2 sobre $\mathbb{F}_5$ (salvo isom. en $\mathbb{F}_{5^2}$) necesariamente $M \cong E$.

e) $\bar{3}^3 \equiv \bar{2} \mod 5$
$\bar{x}^3 = 1$ en E

$\Rightarrow (\overline{3x})^3 = \overline{2}$ en E

$\Rightarrow \overline{3x}$ es una raíz cúbica de $\overline{2}$ en $E \setminus \mathbb{F}_5$. La otra se obtiene aplicando Frobenius: $F_r(\overline{3x}) =$

$= \overline{3}^5 \cdot \overline{x}^5 = \overline{3}\,\overline{x}^5 = \overline{3}(4x+4) =$

$= \boxed{\overline{2x+2}}$

Raíces cúbicas de $\overline{2}$: $\{\overline{3}, \overline{3x}, \overline{2x+2}\}$

(f) $E = \dfrac{\mathbb{F}_5[x]}{\langle x^2+x+1\rangle}$ $\quad M = \dfrac{\mathbb{F}_5[y]}{\langle y^2+3y+4\rangle}$

Para ver un isomorfismo escribimos $L = \mathbb{F}_5(\alpha)$, $\alpha^3 = 2$, basta definir primero

$$\begin{array}{ccc} \mathbb{F}_5[y] & \xrightarrow{\varphi} & E \\ a & \longrightarrow & a \quad \text{si } a \in \mathbb{F}_5 \\ y & \longrightarrow & \overline{3x} \end{array}$$

φ es sobreyectiva y $\ker \varphi = \langle y^2+3y+4\rangle$ por ser $\overline{3x}$ una raíz cúbica de $\overline{2}$.

$\Rightarrow \varphi$ define un isomorfismo $\dfrac{\mathbb{F}_5[y]}{\ker\varphi} \xrightarrow{\sim} E$, $\overline{y} \mapsto \overline{3x}$

Luego el isomorfismo pedido será el inverso: $\overline{x} \mapsto 2y$. Solo hay otro que sale enviando y a la otra raíz única de t^2+4x+4..

2. Problema 2B. Responde de manera razonada a las siguientes preguntas.

a) (0,5 puntos) Demuestra que $E = \mathbb{F}_5[x]/\langle x^2+4x+1\rangle$ es el cuerpo de descomposición de t^3-4 sobre $\mathbb{F}_5$.

b) (0,25 puntos) Escribe una base de E sobre $\mathbb{F}_5$.

c) (0,25 puntos) Demuestra que el orden de $\overline{x}$ en el grupo multiplicativo E^* es 6.

d) (0,25 puntos) Escribe, en términos de la base del apartado (b), todas las raíces de t^3-4.

e) (0,25 puntos) Sea M el cuerpo de descomposición de t^3-1 sobre $\mathbb{F}_5$. Demuestra que M y E son isomorfos.

f) (0,5 puntos) Sea $\alpha \in M$ una raz cúbica de 1 de modo que $M = \mathbb{F}_5(\alpha)$. Escribe de manera explícita un isomorfismo entre M y E describiendo la imagen de $\overline{x}$ por el isomorfismo. *Sugerencia: Usa el apartado (c).* ¿Cuntos isomorfismos puedes construir entre los dos cuerpos?

a) $t^3-4 = (t-4)(t^2+4t+1)$

t^2+4t+1, en irred / $\mathbb{F}_5$ porque tiene raíces en $\mathbb{F}_5$.

Ahora $E = \mathbb{F}[x] / \langle x^2+4x+1 \rangle$ es el cuerpo + pequeño que contiene a $\mathbb{F}_5$ y a una raíz de t^2+4t+1. Como el polinomio tiene grado 2, E contiene sus dos raíces y en particular el c.d.d. de t^3-4 / $\mathbb{F}_5$.

b) $[E:\mathbb{F}_5] = 2$ $B = \{1, \overline{x}\}$

c) $\overline{x}^3 = 4$ y $|\overline{4}| = 2$ en $\mathbb{F}_5$

$\Rightarrow \overline{x}^6 = 1$

$\Rightarrow |\bar{x}| \leq 6 \Rightarrow |\bar{x}| = 1, 2, 3, 6.$

Pero $\bar{x} \neq 1$; $\bar{x}^2 = -4x - 1 = x + 4 \neq 1$

$\bar{x}^3 = \bar{x}^2 + 4\bar{x} = \bar{x} + 4 + 4\bar{x} = \bar{4} \neq \bar{1}$

$\Rightarrow |\bar{x}| = 6.$

d) $\bar{4}, \bar{x}$ son raíces cúbicas de $\bar{4}$. La sala de $F_7(\bar{x}) = \bar{x}^5$

$\bar{x}^5 = \bar{x}^3 \cdot \bar{x}^2 = \bar{4} \cdot (\bar{x} + \bar{4}) = \underline{\bar{4}\bar{x} + \bar{1}}$

Raíces: $2\bar{4}, \bar{x}, \bar{4}\bar{x} + \bar{1}$ ✓

e) $t^3 - 1 = (t-1)\underbrace{(t^2 + t + 1)}_{\text{irred}/\mathbb{F}_5}$

Sabemos, por el mismo argumento que en (a) $M = \mathbb{F}_5[y]/\langle y^2 + y + 1 \rangle$ es el cuerpo de descomposición de $t^3 - 1/\mathbb{F}_5$ pues $[M : \mathbb{F}_5] = 2$ y, salvo isom., sólo hay un cuerpo de grado 2 sobre

$\mathbb{F}_5$) que en $\mathbb{F}_5^2 \Rightarrow M \simeq E$.

(f) $M = \mathbb{F}_5(\alpha) = \mathbb{F}_5(\bar{y})$

Como $\bar{x}^6 = \bar{1}$ en $E \Rightarrow \bar{x}^2$

es una raíz cúbica de 1 en E.

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

Ahora: escribimos el siguiente homomorfismo de anillos:

$$\mathbb{F}_5[y] \xrightarrow{\varphi} E$$

$$a \longrightarrow a \text{ si } a \in \mathbb{F}_5$$

$$y \longrightarrow \underbrace{\bar{x}^2 = \bar{x} + \bar{4}}_{\text{raíz cúbica de 1}}$$

Ahora $\ker \varphi = \langle y^2 + y + 1 \rangle$ y

φ es sobreyectiva $\Rightarrow$

$$M = \mathbb{F}[y] / \langle y^2 + y + 1 \rangle \simeq E$$

y por tanto la inversa $\bar{x} \longrightarrow \bar{y} - \bar{4} = \bar{y} + \bar{1}$

$$\boxed{\text{es } \bar{y} \to \bar{x} + \bar{4}}$$

Hay sólo dos isomorfismos que salen al mandar $\overline{x}$ a la otra raíz ubicada 1 distinto de 1.

3. Problema 2C. Responde de manera razonada a las siguientes preguntas.

a) (0,5 puntos) Demuestra que $E = \mathbb{F}_5[x]/\langle x^2+3x+4\rangle$ es el cuerpo de descomposición de t^3-2 sobre $\mathbb{F}_5$.

b) (0,25 puntos) Escribe una base de E sobre $\mathbb{F}_5$.

c) (0,25 puntos) Calcula, en términos de la base del apartado anterior, todas las raíces de t^3-2

d) (0,25 puntos) Escribe, en términos de la base del apartado (a), todas las raíces de t^3-4. *Sugerencia: fjate en que* $2^2 = 4$.

e) (0,25 puntos) Sea M el cuerpo de descomposición de t^3-4 sobre $\mathbb{F}_5$. Demuestra que M y E son isomorfos.

f) (0,5 puntos) Sea $\alpha \in M$ una raz cbica de 4 de modo que $M = \mathbb{F}_5(\alpha)$. Escribe de manera explítica un isomorfismo entre M y E describiendo la imagen de $\overline{x}$ en términos de α. ¿Cuántos isomorfismos distintos puedes construir entre los dos cuerpos?

a) $t^3-2 = (t-3)(t^2+3t+4)$

irred/$\mathbb{F}_5$ (no tiene raíces en $\mathbb{F}_5$). Cuerpo $\mathbb{F}_5[x]/\langle x^2+3x+4\rangle$ es el cuerpo + pequeño que contiene a $\mathbb{F}_5$ y a una raíz de t^2+3t+4. Como el polinomio tiene grado 2, tiene las 2 y por tanto $E = \mathbb{F}_5[x]/\langle x^2+3x+4\rangle$ es el cdd de $t^3-2/\mathbb{F}_5$.

b) $[E:\mathbb{F}_5] = 2$ y $B = \{1, \overline{x}\}$ es base

(c) Ya tenía dos raíces: $\bar{2}, \bar{x}$.
La tercera sale de aplicar Frobenius a $\bar{x}$: $\bar{x}^5 = ?$

$\bar{x}^3 = \bar{2}$, $\bar{x}^4 = 2\bar{x}$, $\bar{x}^5 = 2\bar{x}^2 =$

$= \bar{2}(-3x - 4) = -6x - 3 =$

$= \boxed{4\bar{x} + \bar{2}}$ Raíces: $\{\bar{2}, \bar{x}, 4\bar{x}+\bar{2}\}$

(d) Raíces de $t^3 - 4$:

$t^3 - 4 = (t-4) \cdot \underbrace{(t^2 + 4t + 1)}_{\text{irred } /\#_5 \text{ (sin raíces)}}$

$\bar{x} \in E$ es tq $\bar{x}^3 = \bar{2} \Rightarrow$

$\Rightarrow (\bar{x}^3)^2 = \bar{4} \Rightarrow \boxed{\bar{x}^2 = 2\bar{x} + \bar{1}}$

es una raíz cúbica de 4. La otra es $(\overline{4x+2})^2 = \bar{x}^2 + \bar{4} + \bar{x} = 2\bar{x} + \bar{1} + \bar{4} + \bar{x}$

$= \underline{3\bar{x}}$

Raíces cúbicas de $\bar{4}$: $\{\bar{4}, 2\bar{x}+\bar{1}, 3\bar{x}\}$

e) $t^3-4 = (t-4)\underbrace{(t^2+4t+1)}_{\text{irred}/\mathbb{F}_5}$

y por el mismo argumento del apartado (a) $\mathbb{F}_5[y]/\langle y^2+4y+1\rangle = M$ es el c.d.d. de $t^3-4/\mathbb{F}_5$.

Que $[M:\mathbb{F}_5]=2$, y, como hay isomorfismo solo hay que extensión de grado 2 de $\mathbb{F}_5$ ($\mathbb{F}_{5^2}$) solo hay uno así $M\cong E$.

f) $M=\mathbb{F}_5(\bar{y})$. Primero definimos:

$$\mathbb{F}_5[x] \xrightarrow{\varphi} \mathbb{F}_5(\bar{y})$$
$$a \longrightarrow a \text{ si } a\in\mathbb{F}_5$$
$$x \longrightarrow ?$$

Pues que $2x+1 \to y \Rightarrow x \to 6(y-1)$

Ahora se comprueba que $\ker\varphi = \langle x^2+3x+4\rangle$ y por el 1er Tmo de isomorfía.

$$\frac{\mathbb{F}_5[x]}{\langle x^2+3x+4\rangle} \cong \mathbb{F}_5(\bar{y})$$ porque φ es sobre.

Hay dos morfismos posible: hacer que $3\bar{x} \to 4$ i.e. $\bar{x} \to 2\bar{4}$. Y no hay + papeo no hay más raíces ubicando 4 en $E \setminus \#_5$.

4. Problema 2D. Responde de manera razonada a las siguientes preguntas.

a) (0,5 puntos) Demuestra que $E = \mathbb{F}_5[x]/\langle x^2+2x+4\rangle$ es el cuerpo de descomposición de t^3-3 sobre $\mathbb{F}_5$.

b) (0,25 puntos) Escribe una base de E sobre $\mathbb{F}_5$.

c) (0,25 puntos) Calcula, en términos de la base del apartado anterior, todas las raíces de t^3-3.

d) (0,25 puntos) Demuestra, de manera razonada, que el orden de $\overline{x}$ en el grupo multiplicativo E^* es 12.

e) (0,25 puntos) Sea M el cuerpo de descomposición de t^3-1 sobre $\mathbb{F}_5$. Demuestra que M y E son isomorfos.

f) (0,5 puntos) Sea $\alpha \in M$ una raíz cúbica de 1 de modo que $M = \mathbb{F}_5(\alpha)$. Escribe de manera explítica un isomorfismo entre M y E describiendo la imagen de $\overline{x}$ en trminos de α. Sugerencia: usa el apartado (d). ¿Cuántos isomorfismos distintos puedes construir entre los dos cuerpos?

a) $t^3-3 = (t-2)\underbrace{(t^2+2t+4)}_{\text{irred/}\mathbb{F}_5 \text{ (sin raíces)}}$

$\Rightarrow E = \mathbb{F}_5[x]/\langle x^2+2x+4\rangle$ en el cuerpo + pequeño que contiene a $\mathbb{F}_5$ y a una raíz de t^2+2t+4. Como el polinomio tiene grado 2 E contiene todas sus raíces y por tanto E es el c.d.d. de t^3-3.

b) $[E:\mathbb{F}_5] = 2$, basis: $B = \{\bar{1}, \bar{x}\}$

c) La otra raíz cúbica de 3 es el resultado de aplicar Frobenius a $\bar{x}$:

$Fr(\bar{x}) = \bar{x}^5 = \bar{x}^3\cdot\bar{x}^2 = 3\cdot\bar{x}^2 =$

$= 3(-2x-4) = -6x-12 = \overline{4x+3}$

Raíz cúbica de 3: $\{\overline{2}, \overline{x}, \overline{4x+3}\}$.

d) $|\overline{x}| \mid 24$ pues $|E^*| = 24$.

Ahora $\overline{x}^3 = 3$ y $|3| = 4 \Rightarrow$

$\Rightarrow \overline{x}^{12} = 1 \Rightarrow |\overline{x}| \mid 12$.

$\Rightarrow |\overline{x}| \in \{1, 2, 3, 6, 12\}$.

pero $\overline{x} \neq 1$, $\overline{x}^2 = \overline{-2x-4} \neq 1$;

$\overline{x}^3 = 3 \neq 1$, $\overline{x}^6 = (\overline{x}^3)^2 = \overline{9} = \overline{4} \neq 1$

$\Rightarrow |\overline{x}| = 12$.

e) $t^3 - 1 = (t-1)\underbrace{(t^2+t+1)}_{\text{irred}/\mathbb{F}_5} \Rightarrow$

$\Rightarrow M$ es el c.d.d. de t^3-1.

↳ mismo argumento que en (d)

Como $[M:\mathbb{F}_5] = 2$ y, salvo isomorfismo sólo hay un cuerpo degrado 2 sobre $\mathbb{F}_5$ ($\mathbb{F}_{5^2}$) $\Rightarrow M \simeq E$.

(f) $M = \mathbb{F}_5(\alpha)$; $M = \mathbb{F}_5[y] / \langle y^2+y+1 \rangle$

Tomamos $\alpha = \overline{y}$.
Como $\overline{x}^{12} = 1 \Rightarrow \overline{x}^4$ es una raíz cúbica de 1 en E
Pero $\overline{x}^4 = \overline{x}^3 \cdot x = 3\overline{x}$.
Ahora construimos el isomorfismo entre E y M. Para ello primero construimos:

$$\mathbb{F}_5[x] \xrightarrow{\varphi} M$$
$$a \longrightarrow a \text{ si } a \in \mathbb{F}_5$$

y que $3\overline{x} \longrightarrow y$ así que definimos $\varphi(x) = 2\overline{y}$. El homomorfismo φ es sobreyectivo y se puede comprobar que $\langle x^2+2x+4 \rangle \subset \ker \varphi$
y como el ideal es maximal $\Rightarrow$

$$\langle x^2+2x+4 \rangle = \ker \varphi$$

y $\dfrac{\mathbb{F}_5[x]}{\langle x^2+x+4 \rangle} \overset{\varphi}{\cong} M$

Sólo hay dos isomorfismos que mandan la otra raíz cúbica de 1 a $\overline{y}$: $(3\overline{x})^2 = 3\overline{x}^4 = 3 \cdot 3\overline{x} = 4\overline{x}$. $\overline{x} \longrightarrow 4\overline{y}$.