Universidad Autónoma de Madrid — Curso 2019-20

Matemáticas/ Ingeniería Informática-Matemáticas

Teoría de Galois

Primer examen parcial. Jueves, 17 de octubre de 2019

APELLIDOS: ____________________

NOMBRE: ____________________ DNI/NIE: ____________________ PROFESORA: ____________________

1. (16 puntos) Sea $R = \mathbb{F}_2[x]/\langle x^3+1\rangle$, donde $\langle x^3+1\rangle$ denota el ideal generado por x^3+1 en $\mathbb{F}_2[x]$. Contesta de manera razonada a las siguientes preguntas:

a) ¿Cuántos elementos tiene R? El homomorfismo natural: $\mathbb{F}_2 \to \mathbb{F}_2[x] \to R$, hace de R un espacio vectorial sobre $\mathbb{F}_2$. Cada $p(x) \in \mathbb{F}_2[x]$ se puede escribir como $p(x) = q(x)(x^3+1) + r(x)$, con $q(x)$, $r(x) \in \mathbb{F}_2[x]$ únicos con la propiedad de que $r(x) = 0$ ó $\deg(r(x)) < 3$. Por lo tanto $1, \bar{x}, \bar{x}^2$ generan R como $\mathbb{F}_2$-e.v. Por otro lado, si $a \cdot 1 + b\bar{x} + c\bar{x}^2 = 0 \in R$ con $a, b, c \in \mathbb{F}_2$, entonces $a \cdot 1 + bx + cx^2 \in \langle x^3+1\rangle$ en $\mathbb{F}_2[x]$. Como $\deg(x^3+1) = 3 \Rightarrow a + bx + cx^2 = 0 \in \mathbb{F}_2[x]$ $\Rightarrow a = b = 0 = c$, y por tanto $1, \bar{x}, \bar{x}^2$ son l.i. sobre $\mathbb{F}_2$. En consecuencia $\{1, \bar{x}, \bar{x}^2\}$ es base de $R/\mathbb{F}_2$ y R tiene 8 elementos.

b) ¿Cuántos ideales tiene R?

Hay una correspondencia biyectiva entre los ideales de R y los de $\mathbb{F}_2[x]$ que contienen a $\langle x^3+1\rangle$. Como $\mathbb{F}_2[x]$ es un D.I.P, un ideal I contiene a $\langle x^3+1\rangle$ si y sólo si está generado por un divisor de x^3+1. En $\mathbb{F}_2[x]$, $x^3+1 = (x+1)(x^2+x+1)$. $x+1$ es irred en $\mathbb{F}_2[x]$ por ser $\mathbb{F}_2$ cuerpo, y tener grado 1. Por otro lado, x^2+x+1 es irreducible en $\mathbb{F}_2[x]$ porque tiene grado 2, y no tiene ninguna raíz en $\mathbb{F}_2$. Así, en $\mathbb{F}_2[x]$ $\langle x^3+1\rangle \subset \langle x^3+1\rangle, \langle x+1\rangle, \langle x^2+x+1\rangle, \mathbb{F}_2[x]$. Luego en R hay 4 ideales distintos.

c) ¿Hay divisores de cero en R?

Primero observamos que $(\overline{x+1})(\overline{x^2+x+1}) \equiv 0$ en R.
Por otro lado $\overline{x+1}, \overline{x^2+x+1} \not\equiv 0$ en R porque $\{1, \bar{x}, \bar{x}^2\}$ es una base de R como $\mathbb{F}_2$-e.v.
En consecuencia $\overline{x+1}$ y $(\overline{x^2+x+1})$ son divisores de 0 en R.

d) ¿Es $\overline{x}$ invertible en R? Aquí, $\overline{x}$ denota la clase de $x \in \mathbb{F}_2[x]$ en R.

Basta observar que $\overline{x^3+1} \equiv 0 \in R \Rightarrow$

$\Rightarrow \overline{x^3} \equiv -1 \equiv 1 \in R \Rightarrow$

$\bar{x} \cdot \bar{x}^2 \equiv 1 \in R$

$\Rightarrow \bar{x}$ es invertible y su inverso es $\bar{x}^2$.

2. (16 puntos) Considera la extensión $\mathbb{Q}(\sqrt{1+\sqrt{7}})/\mathbb{Q}$.

a) Calcula su grado. Razona tu respuesta. Sea $\alpha = \sqrt{1+\sqrt{7}}$. Hay dos maneras de calcular el grado. O bien calculando $Irr(\mathbb{Q},\alpha)$ y usando que por el Teorema del Elemento Algebraico $|\mathbb{Q}(\alpha):\mathbb{Q}| = \delta(Irr(\mathbb{Q},\alpha))$ o bien notemos que $\alpha^2-1=\sqrt{7}\in\mathbb{Q}(\alpha)$ y usando el Teorema de transitividad de grados (finitud). Quizá en este caso, lo más sencillo sería la primera opción, así que desarrollo la segunda.

$\sqrt{7}$ es raíz de $x^2-7\in\mathbb{Q}[x]$ irreducible

$\sqrt{1+\sqrt{7}}$ es raíz de $x^2-(1+\sqrt{7})\in\mathbb{Q}(\sqrt{7})[x]$, es también irreducible pues si $\pm\sqrt{1+\sqrt{7}}\in\mathbb{Q}(\sqrt{7})$, entonces $\exists a,b\in\mathbb{Q}$: $\pm\sqrt{1+\sqrt{7}}=a+b\sqrt{7}$, de donde $1+\sqrt{7}=a^2+2ab\sqrt{7}+7b^2$ y operando obtendríamos la contradicción $\sqrt{7}=\dfrac{a^2+7b^2-1}{1-2ab}\in\mathbb{Q}$ (siempre que $1\neq 2ab$, si $1=2ab$ la contradicción viene de $1=a^2+7b^2$). Por el teorema de transitividad de grados $\mathbb{Q}(\alpha)/\mathbb{Q}$ es finita y
$|\mathbb{Q}(\alpha):\mathbb{Q}|=|\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{7})||\mathbb{Q}(\sqrt{7}):\mathbb{Q}|$
$=2\cdot 2=4$

b) Calcula una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{1+\sqrt{7}})$. Razona tu respuesta.

Por el apartado a)

sabemos que $|\mathbb{Q}(\alpha):\mathbb{Q}|=4$

En particular, α es algebraico sobre $\mathbb{Q}$

y por el Teorema del Elemento Algebraico

$\{1,\alpha,\alpha^2,\alpha^3\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$.

También podríamos calcular una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$ usando la transitividad de grados (finitud)

$\{1,\sqrt{7}\}$ es $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{7})$

$\{1,\sqrt{1+\sqrt{7}}\}$ es $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{1+\sqrt{7}})$ $\Big\} \to$

$\{1,\sqrt{7},\sqrt{1+\sqrt{7}},\sqrt{1+\sqrt{7}}\sqrt{7}\}$ es $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{1+\sqrt{7}})$

c) Calcula el polinomio mínimo de $\sqrt{1+\sqrt{7}}$ sobre $\mathbb{Q}$. Razona tu respuesta.

Sea $\alpha = \sqrt{1+\sqrt{7}}$ como en apartados anteriores, se tiene $(\alpha^2-1)^2 = 7$ de donde α es raíz del polinomio $p(x) = x^4 - 2x^2 - 6$.
Como p es mónico e irreducible por el criterio de Eissestein, tenemos que x^4-2x^2-6 es el polinomio mínimo de α sobre $\mathbb{Q}$.
(En caso de haber obtenido un polinomio del que α fuera raíz del que no fuera fácil decidir su irreducibilidad, podríamos haber concluido que era el irreducible usando que el grado coincide con el grado de la ext previamente calculado)

d) Sea $\alpha = \sqrt{1+\sqrt{7}}$. Calcula α^{-1} en función de la base que has encontrado en el apartado b).

Supongamos que nuestra base es $\{1, \alpha, \alpha^2, \alpha^3\}$.
De nuevo hay dos formas de proceder.
Podemos expresar α^{-1} en función de la base

$$\alpha^{-1} = a + b\alpha + c\alpha^2 + d\alpha^3 \quad , \; a,b,c,d \in \mathbb{Q}$$

y usar

$$1 = \alpha\alpha^{-1} = a\alpha + b\alpha^2 + c\alpha^3 + d\alpha^4$$

$$= a\alpha + b\alpha^2 + c\alpha^3 + 2d\alpha^2 + 6d$$

$\alpha^4 = 2\alpha^2 + 6$ de donde $\begin{cases} 6d = 1 & \Rightarrow d = 1/6 \\ (2d+b) = 0 & \Rightarrow b = -1/3 \\ a = 0 = c \end{cases}$

$\alpha^{-1} = -1/3\,\alpha + 1/6\,\alpha^3$.

De otro modo, si $f(x) = x$, $f \in \mathbb{Q}[x]$, como $mcd(f,p) = 1$ ($f(\alpha) \neq 0$ y p es irreducible).
Podíamos calcular una identidad de Bézout, en este caso: $-1/6\, p(x) + x\left(\frac{x^3-2x}{6}\right) = 1$. Evaluando en α obtenemos $\alpha\left(\frac{\alpha^3 - 2\alpha}{6}\right) = 1$, de donde, $\alpha^{-1} = -1/3\,\alpha + 1/6\,\alpha^3$

3. (8 puntos) Decide razonadamente[1] si las siguientes afirmaciones son verdaderas o falsas.

a) Si $L = \mathbb{Q}(\sqrt[3]{2})$, entonces el polinomio x^2+x+1 es irreducible en $L[x]$. VERDADERO.

Supongamos que $\alpha \in L$ es una raíz de $f(x) = x^2+x+1$.
$\alpha \notin \mathbb{Q}$ porque las posibles raíces racionales de f serían enteros divisores de 1, y ± 1 no son raíces.
Entonces $|\mathbb{Q}(\alpha):\mathbb{Q}| > 1$. Como f es irreducible sobre $\mathbb{Q}$, $f(x) = \mathrm{Irr}(\mathbb{Q},\alpha)$; luego

$$|\mathbb{Q}(\alpha):\mathbb{Q}| = 2 \text{; pero}$$

$$\begin{array}{c} L \\ | \\ \mathbb{Q}(\alpha) \\ 2\ | \\ \mathbb{Q} \end{array} \Bigg) 3$$

$|L:\mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}| = 3$ porque $x^3-2 \in \mathbb{Q}[x]$ es irreducible por Einsestein (por ejemplo)
y $\underbrace{|\mathbb{Q}(\alpha):\mathbb{Q}|}_{=2} \mid |L:\mathbb{Q}| = 3$ es una contradicción.

Como f no tiene raíces en L y es de grado 2, es irred. en $L[x]$.

b) Existe un homomorfismo de anillos entre los cuerpos $\mathbb{Q}(\sqrt{5}i)$ y $\mathbb{Q}(\sqrt{5})$. FALSO.

Supongamos que existe un hom. $f: \mathbb{Q}(\sqrt{5}i) \to \mathbb{Q}(\sqrt{5})$.
Como $f(1) = 1 \Rightarrow \forall m \in \mathbb{Z}$, $f(m) = m$ y $\forall r \in \mathbb{Q}$, $f(r) = r$. Luego f fija $\mathbb{Q}$.
Como f es homomorfismo de anillos:

$$-5 = f(-5) = f(\sqrt{5}i\sqrt{5}i) = f(\sqrt{5}i)\cdot f(\sqrt{5}i)$$

Luego $f(\sqrt{5}i) \in \mathbb{Q}(\sqrt{5})$ tiene que ser una raíz de -5, pero eso es imposible porque $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$.
También se puede comprobar directamente que ningún elemento de $\mathbb{Q}(\sqrt{5})$ puede ser una raíz de -5, porque la ecuación: $(a+b\sqrt{5})^2 = -5$ con $a, b \in \mathbb{Q}$ no tiene solución:

[1] Prueba la afirmación si es verdadera, y da un contraejemplo o razona por reducción al absurdo si es falsa.

$$a^2+5b^2+2ab\sqrt{5} = -5$$
$$\Rightarrow a^2+5b^2 = -5 \ \text{(imposible)}$$

y además usando que $\{1, \sqrt{5}\}$ a base de $\mathbb{Q}(\sqrt{5})$