Universidad de El Salvador. 12.12.2018
Álgebra II. Examen parcial 2 (repetido). Soluciones

Problema 1 (2 puntos)**.** Encuentre el polinomio mínimo de $\sqrt{2}+\sqrt[3]{2}$ sobre $\mathbb{Q}$.

Solución. Primero, se puede considerar el cuerpo

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

Este tiene grado 6 sobre $\mathbb{Q}$ y como su base se pueden tomar los elementos

$$1,\ \sqrt{2},\ \sqrt[3]{2},\ \sqrt[3]{4},\ \sqrt{2}\,\sqrt[3]{2},\ \sqrt{2}\sqrt[3]{4}.$$

Calculamos

$$\begin{aligned} 1\cdot(\sqrt{2}+\sqrt[3]{2}) &= \sqrt{2}+\sqrt[3]{2},\\ \sqrt{2}\cdot(\sqrt{2}+\sqrt[3]{2}) &= 2+\sqrt{2}\sqrt[3]{2},\\ \sqrt[3]{2}\cdot(\sqrt{2}+\sqrt[3]{2}) &= \sqrt[3]{4}+\sqrt{2}\sqrt[3]{2},\\ \sqrt[3]{4}\cdot(\sqrt{2}+\sqrt[3]{2}) &= 2+\sqrt{2}\sqrt[3]{4},\\ \sqrt{2}\sqrt[3]{2}\cdot(\sqrt{2}+\sqrt[3]{2}) &= 2\sqrt[3]{2}+\sqrt{2}\sqrt[3]{4},\\ \sqrt{2}\sqrt[3]{4}\cdot(\sqrt{2}+\sqrt[3]{2}) &= 2\sqrt{2}+2\sqrt[3]{4}. \end{aligned}$$

Entonces, la matriz de multiplicación por $\sqrt{2}+\sqrt[3]{2}$ sobre K viene dada por

$$\begin{pmatrix} 0 & 2 & 0 & 2 & 0 & 0\\ 1 & 0 & 0 & 0 & 0 & 2\\ 1 & 0 & 0 & 0 & 2 & 0\\ 0 & 0 & 1 & 0 & 0 & 2\\ 0 & 1 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

El polinomio característico de esta matriz es

$$X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4.$$

Se ve que el grado de $\sqrt{2}+\sqrt[3]{2}$ tiene que ser igual a 6, así que lo que acabamos de encontrar es el polinomio mínimo de $\sqrt{2}+\sqrt[3]{2}$. ∎

Problema 2 (2 puntos)**.** Consideremos el polinomio $f := X^2+X+2 \in \mathbb{F}_p[X]$.

a) ¿Para cuáles primos p el polinomio es irreducible? [1 *punto*]

b) ¿Para cuáles primos p el polinomio es separable? [1 *punto*]

Solución. Si $p=2$, el polinomio es reducible y separable: tenemos $f = X\,(X+1)$. Si $p\neq 2$, las raíces de f en un cuerpo de descomposición vienen dadas por

$$\frac{-1\pm\sqrt{-7}}{2}.$$

El polinomio es irreducible si $\sqrt{-7}\notin\mathbb{F}_p$, es decir, si $\left(\frac{-7}{p}\right)=-1$. Tenemos por la ley de reciprocidad cuadrática

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}}\,(-1)^{\frac{7-1}{2}}\,(-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right) = -\left(\frac{p}{7}\right).$$

Entonces, f es irreducible si y solo si $p\equiv 3,5,6 \pmod 7$.

El polinomio no es separable solo cuando sus dos raíces en un cuerpo de descomposición coinciden; es decir, cuando $\sqrt{-7}=0$. Esto sucede solo para $p=7$ cuando $f=(X-3)^2$. ∎

Problema 3 (2 puntos)**.** Sean p un número primo y $n = 1, 2, 3, \ldots$ Para $\alpha \in \mathbb{F}_{p^n}$ definamos

$$N(\alpha) := \alpha\, \alpha^p\, \alpha^{p^2} \cdots \alpha^{p^{n-1}}.$$

a) Demuestre que $N(\alpha) \in \mathbb{F}_p$ para todo $\alpha \in \mathbb{F}_{p^n}$. [$\frac{1}{2}$ *punto*]

b) Demuestre que

$$N(\alpha\beta) = N(\alpha)\, N(\beta), \quad N(a\alpha) = a^n\, N(\alpha)$$

para cualesquiera $a \in \mathbb{F}_p$, $\alpha, \beta \in \mathbb{F}_{p^n}$. [$\frac{1}{2}$ *punto*]

c) Demuestre que el homomorfismo de grupos multiplicativos $N\colon \mathbb{F}_{p^n}^\times \to \mathbb{F}_p^\times$ es sobreyectivo. [1 *punto*]

Indicación: demuestre que $|\ker N| = \frac{p^n-1}{p-1}$ e use el primer teorema de isomorfía.

Solución. Recordamos que un elemento $x \in \mathbb{F}_{p^n}$ pertenece al subcuerpo $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ si y solo si $x^p = x$. En este caso calculamos que

$$N(\alpha)^p = \alpha^p\, \alpha^{p^2}\, \alpha^{p^3} \cdots \alpha^{p^n} = \alpha^p\, \alpha^{p^2}\, \alpha^{p^3} \cdots \alpha = N(\alpha),$$

usando que $\alpha^{p^n} = \alpha$ (el orden del grupo $\mathbb{F}_{p^n}^\times$ es $p^n - 1$). Esto establece la parte a). Para la parte b), la identidad $N(\alpha\beta) = N(\alpha)\, N(\beta)$ está clara de la definición, mientras que para $a \in \mathbb{F}_p$ se tiene

$$N(a\alpha) = N(a)\, N(\alpha) = a\, a^p\, a^{p^2} \cdots a^{p^{n-1}}\, N(\alpha) = a^n\, N(\alpha),$$

puesto que $a^p = a$ (y luego por inducción $a^{p^i} = a$ para cualquier i).

En la parte c), notamos que

$$\ker N = \{\alpha \in \mathbb{F}_{p^n} \mid N(\alpha) = 1\} = \{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{\frac{p^n-1}{p-1}} = 1\}.$$

Tenemos

$$\frac{p^n - 1}{p - 1} \mid p^n - 1,$$

donde $p^n - 1$ es el orden del grupo cíclico $\mathbb{F}_{p^n}^\times$, así que la ecuación $x^{\frac{p^n-1}{p-1}} = 1$ tiene precisamente $\frac{p^n-1}{p-1}$ soluciones en $\mathbb{F}_{p^n}^\times$. Esto nos permite concluir que

$$|\ker N| = \frac{p^n - 1}{p - 1},$$

y luego por el primer teorema de isomorfía

$$|\operatorname{im} N| = |\mathbb{F}_{p^n}^\times| \Big/ \frac{p^n - 1}{p - 1} = p - 1 = |\mathbb{F}_p^\times|,$$

lo que significa que el homomorfismo $N\colon \mathbb{F}_{p^n}^\times \to \mathbb{F}_p^\times$ es sobreyectivo. ■

Problema 4 (2 puntos)**.** Sean p un número primo y $n = 1, 2, 3, \ldots$ Consideremos el endomorfismo de Frobenius $F\colon x \mapsto x^p$ sobre $\mathbb{F}_{p^n}$. Hemos probado en clase que es una aplicación $\mathbb{F}_p$-lineal. Encuentre su polinomio característico.

Solución. De hecho, ya probamos en clase que F es un automorfismo de $\mathbb{F}_{p^n}$ que preserva a $\mathbb{F}_p$. Para calcular el polinomio característico, bastaría notar que este debe tener grado $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ y

$$F^n := \underbrace{F \circ \cdots \circ F}_{n} = \mathrm{id}.$$

Entonces, el polinomio característico viene dado por $X^n - 1$. ■