MA-31A Elementos de Álgebra	15 de Noviembre, 2003

Pauta Control 3

Prof. Cátedra: M. Kiwi — *Prof. Auxiliar: H. Castro, J. Soto*

PROBLEMA 1:

(i).- Sabemos que $\theta \notin \mathbb{F}_3$ y que $\theta^2 + \theta + 2 = 0$ (luego $\theta^2 = 2\theta + 1$). Sigue que $\{1, \theta\}$ es una base de $\mathbb{F}_9$ como espacio vectorial sobre $\mathbb{F}_3$. La tabla de multiplicación correspondientes es

$+$	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	0	0	0	0	0	0	0	0
1		1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
2			1	2θ	$2\theta+2$	$2\theta+1$	θ	$\theta+2$	$\theta+1$
θ				$2\theta+1$	1	$\theta+1$	$\theta+2$	$2\theta+2$	2
$\theta+1$					$\theta+2$	2θ	2	θ	$2\theta+1$
$\theta+2$						2	$2\theta+2$	1	$\theta+1$
2θ							$2\theta+1$	$\theta+1$	1
$2\theta+1$								2	2θ
$2\theta+2$									$\theta+2$

Finalmente, como $x^2 + x + 2 = (x - \theta)(x + \theta + 1) = (x - \theta)(x - (2\theta + 2))$, la otra raíz pedida es $2\theta + 2$.

(ii).- Claramente $x^2 - 2$ y $x^2 - 3$ son polinomios irreducibles sobre $\mathbb{Q}$ cuyas raíces en $\mathbb{R}$ son $\sqrt{2}$ y $\sqrt{3}$ respectivamente. Luego, $\sqrt{2}, \sqrt{3} \in \mathbb{R}$ son ambos de grado algebráico 2. Como $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \leq 4$.[1]

Por otro lado, se tiene que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ divide a $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$. Luego, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ puede ser igual a 2 o a 4. Supongamos que fuese 2. Entonces, $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, i.e., existirían racionales a y b tales que $\sqrt{3} = a + b\sqrt{2}$. Luego, $3 = a^2 + 2ab\sqrt{2} + 2b^2$. Como $\sqrt{2}$ no es racional debe necesariamente tenerse que a o b son iguales a 0. Como $\sqrt{3}$ es irracional y $\sqrt{3} = a + b\sqrt{2}$, se tiene que b no puede ser 0, i.e., $a = 0$. Sigue que $\sqrt{6} = 2b \in \mathbb{Q}$, un absurdo.

PROBLEMA 2: Ver apuntes de clases.

[1] Un argumento alternativo sería exhibir un polinomio en $\mathbb{Q}[x]$ de grado 4 para el cual $\sqrt{2} + \sqrt{3}$ fuese raíz.

PROBLEMA 3:

(i).- Sean $\alpha, \beta \in \mathbb{K}$, $c \in \mathbb{F}$. Debemos comprobar que $\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha+\beta) = \mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha) + \mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\beta)$ y que $\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(c\alpha) = c\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha)$. En efecto,

$$\begin{aligned}
\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \ldots + (\alpha+\beta)^{q^{m-1}} \\
&= \alpha + \beta + \alpha^q + \beta^q + \ldots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\
&= \mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha) + \mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\beta)\,,
\end{aligned}$$

donde la segunda igualdad se tiene por el hecho que q es una potencia de la característica de $\mathbb{F}$.

Por otro lado, cualquiera que sea $c \in \mathbb{F}$ se tiene que $c^{|\mathbb{F}|} = c$, luego

$$\begin{aligned}
\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(c\alpha) &= (c\alpha) + (c\alpha)^q + \ldots + (c\alpha)^{q^{m-1}} \\
&= c\left(\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}\right) \\
&= c\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha)\,.
\end{aligned}$$

(ii).- Observar que $\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha) = 0$ sí y sólo si α es raíz de $x^{q^{m-1}} + \ldots + x^q + x \in \mathbb{F}[x]$. Pero este polinomio posee a lo más $q^{m-1} < |\mathbb{K}|$ raíces. Luego existe en $\mathbb{K}$ un α tal que $\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha) \neq 0$.

(iii).- Una transformación $\mathbb{F}$-lineal de $\mathbb{K}$ en $\mathbb{F}$ queda definida (de manera única) por los valores que toma en una base de $\mathbb{K}$. Como una base de $\mathbb{K}$ tiene m elementos, sigue que hay q^m tales transformaciones lineales.

(iv).- Por (iii) bastará verificar que para $\beta, \gamma \in \mathbb{K}$, $\alpha \neq \beta$, se tiene que $L_\alpha \neq L_\beta$. En efecto,

$$L_\beta(\gamma) - L_\alpha(\gamma) = \mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\beta\gamma) - \mathbf{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha\gamma) = \mathbf{Tr}_{\mathbb{K}/\mathbb{F}}((\beta-\alpha)\gamma)\,.$$

Como $\beta - \alpha \neq 0$ y $\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}$ es sobreyectiva, para γ elegido apropiadamente se debe tener que $\mathbf{Tr}_{\mathbb{K}/\mathbb{F}}((\beta-\alpha)\gamma) \neq 0$, i.e., $L_\alpha \neq L_\beta$.