Ma31a Elementos de Álgebra	**19 de Noviembre, 2005**

Pauta Control 3

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

PROBLEMA 1:

(i).- Suponiendo que q es potencia del primo p, se tiene que la característica de $\mathbb{F}$ es p. Luego, $(\beta+\gamma)^{p^n} = \beta^{p^n} + \gamma^{p^n}$ cualquiera sea $n \in \mathbb{N}$ y $\beta, \gamma \in \mathbb{F}$. En particular $(\beta+\gamma)^{q^i} = \beta^{q^i} + \gamma^{q^i}$ cualquiera sea $i \in \mathbb{N}$. Luego,

$$L(\beta+\gamma) = \sum_i \alpha_i (\beta+\gamma)^{q^i} = \sum_i \alpha_i \left(\beta^{q^i} + \gamma^{q^i}\right) = L(\beta) + L(\gamma)\,.$$

Por otro lado, para todo $c \in \mathbb{F}_q$ se tiene que $c^q = c$, y en general que $c^{q^i} = c$. Luego,

$$L(c\beta) = \sum_i \alpha_i (c\beta)^{q^i} = \sum_i c\alpha_i \beta^{q^i} = cL(\beta)\,.$$

Finalmente, como $\mathbb{F}$ es espacio vectorial sobre $\mathbb{F}_q$ y L es $\mathbb{F}_q$-lineal, el núcleo de L es un sub-espacio vectorial de $\mathbb{F}$ sobre $\mathbb{F}_q$. Pero el núcleo de L es exactamente el conjunto de raíces de $\mathbb{F}$.

(ii).- Si $\alpha_0 \neq 0$, entonces $L'(x)|_{x=0} = \sum_{i=0}^n \alpha_i q^i x^{q^i-1}\Big|_{x=0} = \alpha_0 \neq 0$ (porque q es un múltiplo de la característica de $\mathbb{F}$). Sigue que si $\alpha_0 \neq 0$ entonces todas las raíces de L son simples.

Supongamos ahora que $\alpha_0 \neq 0$. Sea $k \in \{0, \ldots, n\}$ el menor índice tal que $\alpha_k \neq 0$. Observar que $\alpha_0 \neq 0$ implica que $k > 0$. Además, como L es no nulo, se tiene que $k \leq n$. Sigue que cualquiera que sea $\alpha \in \mathbb{F}$ se tiene que

$$L(\alpha) = \sum_{i=k}^n \alpha_i \alpha^{q^i} = \sum_{i=k}^n \alpha_i^{q^k} \alpha^{q^{i-k} q^k} = \left(\sum_{i=k}^n \alpha_i \alpha^{q^{i-k}}\right)^{q^k}\,.$$

Por el argumento utilizado en el análisis del caso $\alpha_0 \neq 0$, sabemos que $\widetilde{L}(x) = \sum_{i=k} \alpha_i \alpha^{q^{i-k}}$ sólo tiene raíces simples. Sigue que L sólo posee raíces de multiplicidad q^k.

Cualquiera sea el caso, se tiene en particular que la multiplicidad de una raíz de L es una potencia de q.

(iii).- La existencia de C es directa del hecho que L es $\mathbb{F}_q$–lineal, y de hecho C corresponde a la traspuesta de la matriz representante de L con respecto a la base dada asociada al espacio de partida y de llegada. Por otro lado, $\beta \in \mathbb{F}$ se puede expresar como una combinación lineal de la base $\{\beta_1, \ldots, \beta_s\}$, digamos

$$\beta = \sum_j b_j \beta_j \,,$$

para $b_1, \ldots, b_s \in \mathbb{F}_q$. Análogamente, existen $a_1, \ldots, a_s \in \mathbb{F}_q$ tales que $\alpha = \sum_j a_j \beta_j$. Como $L(\beta) = \alpha$ y L es $\mathbb{F}_q$-lineal,

$$\sum_j a_j \beta_j = \sum_j b_j L(\beta_j) = \sum_j b_j \sum_k c_{j,k} \beta_k = \sum_k \left(\sum_j b_j c_{j,k} \right) \beta_k \,.$$

Por independencia lineal de la base, sigue que $\sum_j b_j c_{j,k} = \alpha_j$ para todo k. Equivalentemente, pero expresado en forma matricial, concluimos que $C^T b = a$ donde $b = (b_1, \ldots, b_s)^T$ y $a = (a_1, \ldots, a_s)^T$. La determinación de β se reduce entonces a resolver un sistema lineal (homogéneo en el caso que $\alpha = 0$).

(iv).- Si Γ no fuese base de $\mathbb{F}_{81}$ como espacio vectorial de $\mathbb{F}_3$ tendríamos que existirían coeficientes $c_0, \ldots, c_3 \in \mathbb{F}_3$ tales que

$$c_0 + c_1\gamma + c_2\gamma^2 + c_3\gamma^3 = 0 \,.$$

Luego, el polinomio $P(x) = c_0 + c_1 x + c_2 x + c_3 x \in \mathbb{F}_3[x]$ tendría a γ como raíz. Por lo tanto, compartiría un divisor no nulo con $x^4 + x^3 + x^2 - x - 1$, contradiciendo así la irreducibilidad de este último polinomio.

(v).- Para verificar que $P(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$ es irreducible basta observar que $P(0) = -1$, $P(1) = 1$ y $P(2) = -1$, i.e., P no posee raíces en $\mathbb{F}_3$.

Determinemos como expresar γ^{10} como combinación lineal de la base Γ. Para ello, notar que se tiene que

$$\gamma^4 = 1 + \gamma - \gamma^2 - \gamma^3 \,.$$

Multiplicando ambos lados de la igualdad por γ y sustituyendo γ^4 por la anterior expresión se obtiene

$$\gamma^5 = \gamma + \gamma^2 - \gamma^3 - \gamma^4 = -1 + 2\gamma^2 = -1 - \gamma^2 \,.$$

Sigue que $\gamma^{10} = (\gamma^5)^2 = (-1-\gamma^2)^2 = 1+2\gamma^2+\gamma^4 = 2+\gamma+\gamma^2-\gamma^3 = -1+\gamma+\gamma^2-\gamma^3$. Además, $\gamma^{20} = (\gamma^{10})^2 = 1+\gamma-\gamma^2+\gamma^3-\gamma^4+\gamma^5+\gamma^6 = \gamma^2-\gamma^4 = -1-\gamma-\gamma^2+\gamma^3$. Sigue que $\gamma^{20}+\gamma^{10}-1 = 0$, i.e., γ^{10} es raíz de x^2+x-1.

(vi).- Para determinar $[L]_{\Gamma,\Gamma}$ notar que

$$L(1) \;=\; -\gamma^{10} = 1-\gamma-\gamma^2+\gamma^3\,.$$

Además,

$$\begin{aligned} L(\gamma) &= \gamma^9-\gamma^3-\gamma^{11}\,, && (1)\\ L(\gamma^2) &= \gamma^{18}-\gamma^6-\gamma^{12}\,, && (2)\\ L(\gamma^3) &= \gamma^{27}-\gamma^9-\gamma^{13}\,. && (3)\end{aligned}$$

Necesitamos determinar los valores de γ^6, γ^9, γ^{11}, γ^{12}, γ^{13}, γ^{18} y γ^{27}. Para ello, recordemos que $\gamma^4 = 1+\gamma-\gamma^2-\gamma^3$ y $\gamma^5 = -1-\gamma^2$. Luego,

$$\gamma^{-1} \;=\; -1+\gamma+\gamma^2+\gamma^3\,,$$

y además,

$$\begin{array}{rcccl} \gamma^6 &=& \gamma\cdot\gamma^5 &=& -\gamma-\gamma^3\,,\\ \gamma^9 &=& \gamma^{-1}\cdot\gamma^{10} &=& -1+\gamma^2-\gamma^3\,,\\ \gamma^{11} &=& \gamma\cdot\gamma^{10} &=& -1+\gamma-\gamma^2-\gamma^3\,,\\ \gamma^{12} &=& \gamma\cdot\gamma^{11} &=& -1+\gamma-\gamma^2\,,\\ \gamma^{13} &=& \gamma\cdot\gamma^{12} &=& -\gamma+\gamma^2-\gamma^3\,,\\ \gamma^{18} &=& (\gamma^6)^3 &=& 1-\gamma^2\,,\\ \gamma^{27} &=& (\gamma^9)^3 &=& -\gamma-\gamma^2\,. \end{array}$$

Reemplazando en (1), (2) y (3) se obtiene que

$$\begin{aligned} L(\gamma) &= -\gamma-\gamma^2-\gamma^3\,,\\ L(\gamma^2) &= -1+\gamma^3\,,\\ L(\gamma^3) &= 1-\gamma^3\,.\end{aligned}$$

Sigue que la matriz del enunciado es la matriz representante $[L]_{\Gamma,\Gamma}$.

Para determinar las raíces de L debemos calcular el núcleo de la matriz $[L]_{\Gamma,\Gamma}$. Es fácil verificar que $\delta_1 = (1,-1,1,0)^T$ y $\delta_2 = (0,0,1,1)^T$ pertenecen a dicho núcleo y son linealmente independientes. Además, las dos primeras columnas de $[L]_{\Gamma,\Gamma}$ son claramente linealmente independientes. Sigue necesariamente que el núcleo de $[L]_{\Gamma,\Gamma}$

está generado por $\{\delta_1, \delta_2\}$. Las raíces de L son entonces aquellos elementos de $\mathbb{F}_{81}$ que corresponden a combinaciones lineales sobre $\mathbb{F}_3$ de estos vectores, i.e., son los siguientes 9 valores:

$$\begin{aligned}
\theta_1 &= 0\,,\\
\theta_2 &= 1-\gamma+\gamma^2\,,\\
\theta_3 &= -1+\gamma-\gamma^2\,,\\
\theta_4 &= \gamma^2+\gamma^3\,,\\
\theta_5 &= 1-\gamma-\gamma^2+\gamma^3\,,\\
\theta_6 &= -1+\gamma+\gamma^3\,,\\
\theta_7 &= -\gamma^2-\gamma^3\,,\\
\theta_8 &= 1-\gamma-\gamma^3\,,\\
\theta_9 &= -1+\gamma+\gamma^2-\gamma^3\,.
\end{aligned}$$

(vii).- Para que $Q(x) = \sum_{i=0}^{n-1} \alpha_i R_i(x)$ sea un polinomio constante, se deben anular todos los coeficientes que acompañan a los términos x^j con $j \in \{1, \ldots, n-1\}$. Equivalentemente, y denotando por $R_{i,j} \in \mathbb{F}_{q^m}$ el coeficiente del polinomio $R_i(x)$ que acompaña el término x^j, debe ocurrir que para todo $j \in \{1, \ldots, n-1\}$,

$$\sum_{i=0}^{n-1} \alpha_i R_{i,j} = 0$$

Para encontrar los α_i's basta entonces resolver este sistema lineal homogéneo de $n-1$ ecuaciones en las n variables $\alpha_0, \ldots, \alpha_{n-1}$. Dicho sistema siempre posee como solución un sub-espacio vectorial de $\mathbb{F}_{q^m}$ de dimensión al menos 1, luego existen escalares no todos nulos que satisfacen las condiciones pedidas.

(viii).- Dado $P \in \mathbb{F}^{q^m}$ polinomio no nulo de grado n. Para encontrar una raíz de P en $\mathbb{F}$ extensión finita de $\mathbb{F}_{q^m}$ se procede como sigue:

- Utilizando el mecanismo descrito en (vii) determinar los α_i's de manera que $\sum_i \alpha_i R_i(x)$ sea un polinomio constante, digamos igual a $\alpha \in \mathbb{F}_{q^m}$. Sigue que,

  $$\sum_{i=0}^{n-1} \alpha_i x^{q^i} = \alpha \pmod{P}\,.$$

  Equivalentemente, P es un divisor de $A(x) = \displaystyle\sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha$.

- Utilizando el mecanismo descrito en (iii) determinar todas las raíces en $\mathbb{F}$ del polinomio $A(x)$.
- Como $P(x)$ divide a $A(x)$, todas sus raíces en $\mathbb{F}$ son también raíces de $A(x)$. Por lo tanto, evaluando $P(x)$ en todas las raíces en $\mathbb{F}$ de $A(x)$ se obtienen las raíces en $\mathbb{F}$ de $P(x)$.