Ma31a Elementos de Álgebra **2 de Diciembre, 2005**

Pauta Examen

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

(i).- Supongamos que C es cíclico. Luego, C es lineal, en particular si $c(x)$ y $c'(x)$ están en C sigue que $(c+c')(x)$ está en C. Consideremos ahora $p(x) \in \mathbb{F}_q[x]$ y probemos que $(p \cdot c)(x)$ está en C. Por la linealidad de C, bastará mostrar que si $c(x)$ está en C, entonces $x \cdot c(x)$ también está en C. Para probar esto último, simplemente observar que módulo $x^n - 1$,

$$x \cdot c(x) = c_0 x + c_1 x^2 + \ldots + c_{n-1} x^n = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2} x^{n-1} .$$

Supongamos ahora que C es un ideal. Luego, si $c(x)$ está en C, se tiene que $x \cdot c(x) \in C$, i.e., $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

(ii).- Sea g el polinimio mónico de grado mínimo en C. Como C es ideal, $(g) \subseteq C$. Supongamos entonces que $f(x)$ está en C. Del Teorema de la División sabemos que exiten $q(x)$ y $r(x)$ tales que $f(x) = q(x)g(x) + r(x)$ donde $\mathrm{grd}(r) < \mathrm{grd}(g)$. Si $f(x)$ no fuese divisible por $g(x)$ entonces $r(x) = f(x) - q(x)g(x)$ sería un elemento no nulo de C de grado menor que g. Esto contradice la minimalidad de g. Hemos concluido que $C = (g)$.

(iii.1).- Del Teorema de la División sabemos que existen $q(x)$ y $r(x)$ polinomios tales que $x^n - 1 = q(x)g(x) + r(x)$ donde $\mathrm{grd}(r) < \mathrm{grd}(g)$. Si g no divide a $x^n - 1$, entonces $r(x) = (x^n - 1) - q(x)g(x) \in C$ es un polinomio no nulo de grado menor al de g, contradiciendo así la minimalidad de g.

(iii.2).- Si $c(x) \in C$, entonces de (ii) sabemos que $c(x) = f(x)g(x)$ para algún $f(x) \in \mathbb{F}_q[x]$. Como $c(x)$ es un polinomio de grado a lo más $n-1$, se debe tener que x es un polinomio de grado a lo más $(n-1) - \mathrm{grd}(g) < n - \mathrm{grd}(g)$. Como el conjunto de polinomios de grado a lo más $n - \mathrm{grd}(g)$ es un $\mathbb{F}_q[x]$–espacio vectorial de dimensión $n - \mathrm{grd}(g)$ se tiene que C es de dimensión $n - \mathrm{grd}(g)$.

(iii.3).- Como C es un ideal generado por g, entonces $\mathcal{G} = \{g(x), x \cdot g(x), \ldots, x^{n-d-1}g(x)\} \subseteq C$. Más aún, por (iii.2), cualquier $c(x) \in C$ si y sólo si es combinación $\mathbb{F}_q$–lineal de $\mathcal{G}$. Como la i–ésima fila de la matriz G del enunciado corresponde al polinomio $x^i g(x)$, hemos establecido que G genera C.

(iv).- En $\mathbb{F}_q^n$ habrá tantos códigos cíclicos como elecciones posibles para el polinomio generador g hayan. Sabemos que dicho polinomio debe dividir a $x^n - 1$. Luego, la cantidad de códigos cíclicos corresponderá a $2^m - 1$ donde m es igual al número de términos en la factorización de $x^n - 1$ en $\mathbb{F}_q[x]$ (el -1 corresponde a excluir el código vacio). Veamos entonces cuantos polinomios irreducibles aparecen en la factorización de $x^n - 1$. Para ello, notar que

$$x^7 - 1 = (x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)\,.$$

Sigue que hay 7 códigos cíclicos no vacios distintos en $\mathbb{F}_2^7$.

(v.1).- Sea g el polinomio minimal de α. Como $\mathbb{F}_{2^m}$ es de característica 2 sigue que $g(\alpha) = 0$ implica que $g(\alpha^{2^i}) = (g(\alpha))^{2^i} = 0$, i.e., α^{2^i} también es raíz de g. Como α es elemento primitivo de $\mathbb{F}_{2^m}$, tiene orden $2^m - 1$ en $\mathbb{F}_{2^m}^*$. Luego, $\alpha^{2^i} \neq \alpha^{2^j}$ si $0 \le i < j \le m-1$, luego

$$\{\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{m-1}}\} = \left\{\alpha^{2^i} \,:\, i \in \mathbb{N}\right\}\,.$$

Dado que α es un elemento primitivo de $\mathbb{F}_{2^m}$, se tiene que $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^m}$. Luego, el polinomio minimal de α debe tener grado m. Luego $\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{m-1}}$ es una colección completa de las raíces del polinomio minimal, i.e.,

$$g(x) = \prod_{i=0}^{m-1}\left(x - \alpha^{2^i}\right)\,.$$

(v.2).- Como el grado algebráico de α es m, toda potencia α^{j-1} con $j > m$ puede expresarse de manera única como combinación lineal de $\{1, \alpha, \ldots, \alpha^{m-1}\}$. Sigue que H existe y esta definida de manera única.

Además, si $c(x) \in C$, entonces c es múltiplo de g. En particular, como α es raíz de g se debe tener que $c(\alpha) = 0$. Si suponemos ahora que $c(\alpha) = 0$, entonces g y c comparten una raíz. Como g es minimal, debe ser irreducible. Sigue entonces que c debe ser múltiplo de g (de lo contrario el máximo común divisor de g y c sería un polinomio en $\mathbb{F}_q[x]$ de grado menor que g y con α como raíz). Como c es múltiplo de g se concluye que c está en C.

Observemos ahora que si $f = (f_0, \ldots, f_{n-1})^T$, entonces $(Hf)_i = \sum_{j=1}^n h_{i,j} f_{j-1}$. Luego,

$$\sum_{i=0}^{m-1} (Hf)_i \alpha^i = \sum_{j=1}^{n}\left(\sum_{i=0}^{m-1} h_{i,j}\alpha^i\right) f_{j-1} = \sum_{j=1}^{n} \alpha^{j-1} f_{j-1} = \sum_{j=0}^{n-1} \alpha^j f_j = f(\alpha)\,.$$

Luego, $c(\alpha) = 0$ equivale a decir que $Hc^T = 0$. Por lo tanto, $c \in C$ si y sólo $Hc^T = 0$.

(v.3).- Como $\alpha^i \neq \alpha^j$ si $1 \leq i < j \leq 2^m - 1$ sigue que todas las columnas de H deben ser distintas. Como hay a lo más $2^m - 1$ posibles tuplas de largo m a coordenadas en $\mathbb{F}_2$ no todas nulas, todas ellas deben aparecer como columnas de H. Sigue que (salvo por permutaciones de las columnas),

$$H = \begin{pmatrix} 1 & & & 1 & 1 & & 1 \\ & 1 & & 1 & & 1 & 1 \\ & & 1 & & 1 & 1 & 1 \end{pmatrix}.$$

Una matriz G esta dada por una base del núcleo de H. Como la matriz H tiene 3 filas linealmente independientes, tiene un núcleo de dimensión 4. Para construir G basta entonces encontrar 4 vectores linealmente independientes en el núcleo de H. Por prueba y error se llega a por ejemplo

$$G = \begin{pmatrix} 1 & & & & & 1 & 1 \\ & 1 & & & 1 & & 1 \\ & & 1 & 1 & & & 1 \\ 1 & 1 & 1 & & & & 1 \end{pmatrix}.$$

(vi).- Si $e(x) = x^{a_1}$, entonces $S_1 = \alpha_1^{a_1}$, luego $x = \alpha^{-a_1}$ es tal que $1 + S_1 x = 0$.

Si $e(x) = x^{a_1} + x^{a_2}$, entonces

$$\begin{aligned} S_1 &= \alpha^{a_1} + \alpha^{a_2}. \\ S_2 &= \alpha^{3a_1} + \alpha^{3a_2}. \end{aligned}$$

Denotaremos α^{a_1} y α^{a_2} por η_1 y η_2 respectivamente. Luego, $S_1 = \eta_1 + \eta_2$ y $S_2 = \eta_1^3 + \eta_2^3$. Se pide mostar que η_1^{-1} y η_2 son raíces de $1 + S_1 x + (S_1^2 + S_2 S_1^{-1})x^2$. En particular, dado que $S_1^2 = (\eta_1 + \eta_2)^2 = \eta_1^2 + \eta_2^2$, debemos mostar que

$$1 + (\eta_1 + \eta_2)\eta_1^{-1} + (\eta_1^2 + \eta_2^2 + (\eta_1^3 + \eta_2^3)(\eta_1 + \eta_2)^{-1})\eta_1^{-2} = 0.$$

Multiplicando por η_1^2 y reagrupando, lo anterior equivale a pedir que

$$\eta_1^2 + (\eta_1 + \eta_2)\eta_1 + \eta_1^2 + \eta_2^2 = (\eta_1^3 + \eta_2^3)(\eta_1 + \eta_2)^{-1},$$

o equivalentemente, que $\eta_1^2 + \eta_1\eta_2 + \eta_2^2 = (\eta_1^3 + \eta_2^3)(\eta_1 + \eta_2)^{-1}$. Como $(\eta_1^2 + \eta_1\eta_2 + \eta_2^2)(\eta_1 + \eta_2) = \eta_1^3 + \eta_2^3$, se obtiene la conclusión deseada. Por simetría, también se concluye que η_2 es otra raíz.