Ma31a Elementos de Álgebra **10 de Noviembre, 2007**

Pauta Control 3

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: R. Cortez*

PROBLEMA 1:

(i).- Primero, estableceremos la existencia de g. Como $\mathcal{C} \neq \{0\}$, existe $g \in \mathcal{C}$ mónico de grado minimal, necesariamente mayor o igual que 1. Afirmamos que g genera $\mathcal{C}$. En efecto, sea $p \in \mathcal{C}$ y supongamos que p no es divisible por g. Entonces, por el Teorema de la División sabemos que existen $q, r \in \mathbb{F}_2[x]$, $r \neq 0$ tales que $p = q \cdot g + r$ y donde el grado de r es estrictamente menor que el de g. Se verifica facilmente que tanto q como r deben deben tener un grado estrictamente menor que n, por lo que pertenecen a $\mathcal{P}_n(\mathbb{F}_2)$. Como $\mathcal{C}$ es un ideal, sigue que $r \in \mathcal{C}$ contradiciendo la minimalidad de g.

Ahora, veamos que g es único. En efecto, supongamos que existe $g' \in_\setminus (\mathbb{F}_\in)$ tal que $\mathcal{C} = (g'(x))$. Sigue que $g|g'$ y que $g'|g$. Como todo polinomio en $\mathbb{F}_2[x]$ de grado positivo es mónico, se concluye que $g = g'$.

(ii).- Nuevamente, si g no divide a $p(x) = x^n - 1$, entonces existen $q, r \in \mathbb{F}_2[x]$, $r \neq 0$ tales que $p = q \cdot g + r$ y donde el grado de r es estrictamente menor que el de g. Se verifica facilmente que tanto q como r deben deben tener un grado estrictamente menor que n, por lo que pertenecen a $\mathcal{P}_n(\mathbb{F}_2)$. Como $\mathcal{C}$ es un ideal, sigue que $r \in \mathcal{C}$ contradiciendo la minimalidad de g. Por lo tanto, g divide a $x^n - 1$.

(iii).- Evaluando en $x = 1$ vemos que 1 es raíz de $x^3 - 1$. Dividiendo sigue que

$$x^3 - 1 = (x+1)(x^2+x+1)\,.$$

Evaluando el polinomio $x^2 + x + 1$ en $\mathbb{F}_2$ vemos que este polinomio no posee raíces en $\mathbb{F}_2$, lo que basta para establecer irreducibilidad en el caso de polinomios cuadráticos en $\mathbb{F}_2[x]$. Sigue que los únicos divisores no triviales de $x^3 - 1$ son $g_1(x) = x + 1$ y $g_2(x) = x^2 + x + 1$ cada uno de ellos generadores de un código cíclico $\mathcal{C}_1$ y $\mathcal{C}_2$ respectivamente. Específicamente,

$$\begin{aligned} \mathcal{C}_1 &= \left\{0, x+1, x^2+x, x^2+1\right\}\,, \\ \mathcal{C}_2 &= \left\{0, x^2+x+1\right\}\,. \end{aligned}$$

Las tablas asociadas a cada código son:

$\mathcal{C}_1$	$i=0$	$i=1$	$i=2$
0	0	0	0
$x+1$	1	1	0
x^2+x	0	1	1
x^2+1	1	0	1

$\mathcal{C}_2$	$i=0$	$i=1$	$i=2$
0	0	0	0
x^2+x+1	1	1	1

PROBLEMA 2:

(i).- Basta con econtrar un polinomio $P \in \mathbb{F}_2[x]$ irreducible de grado 3 y adjuntar a $\mathbb{F}_2$ una raíz de dicho polinomio. Notar que todo polinomio en $\mathbb{F}_2[x]$ reducible de grado 3 tiene un raíz en $\mathbb{F}_2$. Sea entonces $P(x) = x^3 + x + 1$. Como $P(0) = P(1) = 1 \neq 0$ sigue que P es irreducible en $\mathbb{F}_2[x]$. Sea entonces α raíz de P, i.e. tal que $\alpha^3 = \alpha + 1$. El cuerpo $\mathbb{K}$ con las características solicitadas lo construimos como un espacio vectorial de dimensión 3 sobre $\mathbb{F}_2$ con base $\{1, \alpha, \alpha^2\}$. Específicamente $\mathbb{K} = \langle\{1, \alpha, \alpha^2\}\rangle_{\mathbb{F}_2}$ dotado de la suma

$$(a + b\alpha + c\alpha^2) +_{\mathbb{K}} (a' + b'\alpha + c'\alpha^2) = (a +_2 +a') + (b +_2 +b')\alpha + (c +_2 +c')\alpha^2 \,,$$

donde $a, b, c, a', b', c' \in \mathbb{F}_2$ y $+_2$ denota la suma en $\mathbb{F}_2$. El producto en $\mathbb{K}$ esta dado por la siguiente tabla:

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1		1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α			α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$				α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2					$\alpha^2+\alpha$	α	α^2+1	1
α^2+1						$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$							α	α^2
$\alpha^2+\alpha+1$								$\alpha+1$

(ii.1) Supongamos que $u = a/b$ con $a \in \mathbb{Z}$ y $b \in \mathbb{N} \setminus \{0\}$ primos relativos. Como u es raíz de P sigue que

$$a^3 = 6a^2b - 9ab^2 - 3b^3 \,. \tag{1}$$

Luego, a^3 es un múltiplo de 3, por lo que a debe ser divisible por 3, i.e. $a = 3\widetilde{a}$ para algún $\widetilde{a} \in \mathbb{Z}$. Sustituyendo en (1) obtenemos que

$$27\widetilde{a}^3 \;=\; 54\widetilde{a}^2 b - 27\widetilde{a}b^2 - 3b^3\,,$$

o sea,

$$b^3 \;=\; 9\widetilde{a}^3 - 18\widetilde{a}^2 b + 9\widetilde{a}b^2\,.$$

Concluimos ahora que b también es múltiplo de 3, contradiciendo nuestra elección de a y b como primos relativos.

(ii.2).- Derivando, obtenemos que $P'(x) = x^2 - 4x + 3 = (x-1)(x-3)$. Como $P(x) \to -\infty$ cuando $x \to -\infty$ y $P(x) \to \infty$ cuando $x \to \infty$ se debe tener que $x = 1$ es un máximo y $x = 3$ es un mínimo de P. El mínimo valor que toma $P(x)$ cuando $x \geq 0$ debe ser igual a $\min\{P(0), P(3)\} = 3$. Luego, P no tiene raíces positivas. Como $P(0) = 3$, $P(x) \to -\infty$ cuando $x \to -\infty$, y P no posee puntos críticos negativos, sigue que P tiene una única raíz negativa que llamaremos u. De la parte (ii.1) sabemos que u no puede ser racional. Pero por un argumento similar al descrito en la pate (i), todo polinomio en $\mathbb{Q}[x]$ reducible de grado 3 debe tener al menos una raíz racional. Sigue que P es irreducible.

(ii.3).- Como $P(u) = 0$, tenemos que $u^3 = 6u^2 - 9u - 3$. Sigue que

$$u^4 = u \cdot u^3 = u \cdot (6u^2 - 9u - 3) = 6u^3 - 9u^2 - 3u = 3(9u^2 - 19u - 6)\,.$$

Para encontrar el inverso de $(u+1)$ determinaremos los valores de $a, b, c \in \mathbb{Q}$ tales que se tiene la siguiente igualdad en $\mathbb{Q}(u)$:

$$(au^2 + bu + c)(u+1) = 1\,.$$

Cómo $u^3 = 6u^2 - 9u - 3$ obtenemos que

$$1 = a(6u^2 - 9u - 3) + (a+b)u^2 + (c+b)u + c = (7a+b)u^2 + (-9a+c+b)u + (-3a+c)\,.$$

Dado que $\{1, u, u^2\}$ es base de $\mathbb{Q}(u)$ obtenemos el siguiente sistema de ecuaciones lineales $7a + b = 0$, $-9a + c + b = 0$ y $-3a + c = 1$. Luego, sustituyendo por $b = -7a$ sigue que $c = 16a$ por lo que $13a = 1$. En resumen

$$(u+1)^{-1} = \frac{1}{13}u^2 - \frac{7}{13}u + \frac{16}{13}\,.$$

Problema 3:

(i).- Sea $\mathbb{K} = \mathbb{F}(\alpha, \beta)$. Recordar que $[\mathbb{K} : \mathbb{F}] \leq [\mathbb{K} : \mathbb{F}(\alpha)] \cdot [\mathbb{F}(\alpha) : \mathbb{F}]$ por lo que $\mathbb{K}$ es una extensión finita de $\mathbb{F}$. Por resultado visto sigue que

$$\begin{aligned} [\mathbb{K} : \mathbb{F}] &= [\mathbb{K} : \mathbb{F}(\alpha)] \cdot [\mathbb{F}(\alpha) : \mathbb{F}] \,, \\ [\mathbb{K} : \mathbb{F}] &= [\mathbb{K} : \mathbb{F}(\beta)] \cdot [\mathbb{F}(\beta) : \mathbb{F}] \,. \end{aligned}$$

Reemplazando por m y n, se obtiene que

$$[\mathbb{K} : \mathbb{F}(\alpha)] \cdot m = [\mathbb{K} : \mathbb{F}(\beta)] \cdot n \,.$$

Como m y n son primos relativos, se tiene que m divide a $[\mathbb{K} : \mathbb{F}(\beta)]$. Pero $1 \leq [\mathbb{K} : \mathbb{F}(\beta)] \leq m$, donde la primera desigualdad se tiene porque $\mathbb{K}$ es una extensión de $\mathbb{F}(\beta)$ y la segunda desigualdad porque $[\mathbb{K} : \mathbb{F}(\beta)] \leq [\mathbb{F}(\alpha) : \mathbb{F}] = m$. Necesariamente sigue que $[\mathbb{K} : \mathbb{F}(\beta)] = m$ por lo que

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}(\beta)] \cdot [\mathbb{F}(\beta) : \mathbb{F}] = m \cdot n \,.$$

(ii.1).- Sea $\mathbb{L} = \mathbb{K}[x]/(Q)$. Como Q es irreducible de grado 2 sigue que $\mathbb{L}$ es extensón de $\mathbb{K}$ tal que $[\mathbb{L} : \mathbb{K}] = 2$. Por resultado visto, $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}] = 4$. Por otro lado, podemos ver $\mathbb{L}$ como el generado por $\mathbb{K}$ y una raíz α del polinomio Q. Sigue que $[\mathbb{K}(\alpha) : \mathbb{F}] = [\mathbb{L} : \mathbb{F}] = 4$, i.e. α tiene grado algebráico 4 sobre $\mathbb{F}$.

(ii.2).- Supongamos que P tiene algún factor irreducible $Q \in \mathbb{K}[x]$ de grado a lo más 2. Si Q tiene grado 1, sigue que Q tiene una raíz en $\mathbb{K} \setminus \mathbb{F}$. Como P es irreducible en $\mathbb{F}[x]$ y Q es un factor de P la referida raíz debe ser de grado algebráico 2 sobre $\mathbb{F}$. Si Q tiene grado 2, por la parte anterior se tiene que existe una raíz de Q de grado algebráico 4 sobre $\mathbb{F}$. En cualquier caso, y dado que toda raíz de Q es también raíz de P, se concluye que existe una extensión en que P tiene una raíz de grado algebráico 4 sobre $\mathbb{F}$. Esto contradice que P es un polinomio irreducible en $\mathbb{F}[x]$ de grado 6, luego sus raíces tienen grado algebráico 6 sobre $\mathbb{F}$.