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

Control 3

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

TIEMPO 5.0 HRS.

PROBLEMA 1: Sea $n \in \mathbb{N} \setminus \{0\}$. Sea $\mathcal{P}_n(\mathbb{F}_2)$ el conjunto de polinomios en $\mathbb{F}_2[x]$ de grado estrictamente menor que n. Observar (no lo pruebe) que $\mathcal{P}_n(\mathbb{F}_2)$ con la suma usual en $\mathbb{F}_2[x]$ y la multiplicación en $\mathbb{F}_2[x]$ módulo el polinomio $x^n - 1$ es un anillo conmutativo unitario. En lo que sigue, sea $\mathcal{C} \subseteq \mathcal{P}_n(\mathbb{F}_2)$, $\mathcal{C} \neq \{0\}$, un código cíclico, i.e. un ideal de $\mathcal{P}_n(\mathbb{F}_2)$.

(i).- (2.0 pts) Pruebe que existe un único polinomio g generador de $\mathcal{C}$, es decir tal que $\mathcal{C} = (g(x))$.

(ii).- (2.0 pts) Pruebe que el polinomio generador g de $\mathcal{C}$ divide a $x^n - 1$.

(iii).- (2.0 pts) Exprese $x^3 - 1$ como producto de polinomios irreducibles en $\mathbb{F}_2[x]$ y concluya que hay 2 códigos cíclicos no triviales en $\mathcal{P}_3(\mathbb{F}_2)$. Para cada uno de estos dos códigos cíclicos haga una tabla donde cada fila corresponda a un polinomio p en el código y la i-ésima columna corresponda al coeficiente que acompaña x^i en p, donde $i \in \{0, 1, 2\}$.

PROBLEMA 2:

(i).- (3.0 pts) Construya un cuerpo de característica 2 con 8 elementos (explicite su tabla de multiplicar).

(ii).- Considere la extensión $\mathbb{Q}(u)$ de $\mathbb{Q}$ generada por una raíz real u de $P(x) = x^3 - 6x^2 + 9x + 3 \in \mathbb{Q}[x]$.

(ii.1).- (1.0 pts) Pruebe que u no puede ser racional, i.e. no puede tener la forma a/b con a y b primos relativos.

(ii.2).- (1.0 pts) Pruebe que P es irreducible en $\mathbb{Q}[x]$.

Indicación: No necesita determinar el valor de u de manera exacta.

(ii.3).- (1.0 pts) Exprese $u^4, (u+1)^{-1} \in Q(u)$ como combinacion lineal de los elementos de la base $\{1, u, u^2\}$ de $\mathbb{Q}(u)$.

Problema 3:

(i).- (3.0 pts) Sean m y n primos relativos. Sea $\mathbb{K}$ una extension de $\mathbb{F}$ y $\alpha, \beta \in \mathbb{K}$ de grado algebráico m y n respectivamente. Pruebe que $[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = m \cdot n$.

Indicación: Considere argumentos puramente dimensionales.

(ii).- Sea $P \in \mathbb{F}[x]$ un polinomio irreducible de grado 6 y sea $\mathbb{K}$ un extensión de $\mathbb{F}$ tal que $[\mathbb{K} : \mathbb{F}] = 2$.

(ii.1).- (1.5 pts) Suponga que existe $Q \in \mathbb{K}[x]$ irreducible de grado 2. Pruebe que existe una extensión $\mathbb{L}$ de $\mathbb{K}$ tal que $[\mathbb{L} : \mathbb{F}] = 4$ y un $\alpha \in \mathbb{L}$ de grado algebráico 4 sobre $\mathbb{F}$.

(ii.2).- (1.5 pts) Pruebe que P es irreducible en $\mathbb{K}[x]$ o P es el producto de dos polinomios irreducibles en $\mathbb{K}[x]$ ambos de grado 3.