Ma3101 Elementos de Álgebra **20 de Septiembre, 2011**

Examen

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: O. Rivera, D. Salas*

TIEMPO 4.5 HRS.

PROBLEMA 1: (40 %)

Si R es un anillo y existe $\mathbb{N} \setminus \{0\}$ tal que $nr = 0$ para todo $r \in R$, entonces al menor tal n se le llama característica de R, y se dice que R tiene característica positiva. Si no existe tal n se dice que R tiene característica 0.

Un cuerpo que no contiene subcuerpos propios se denomina cuerpo primo. Sea $\mathbb{F}$ cuerpo. Observe (no lo pruebe) que la intersección de todos los subcuerpos de $\mathbb{F}$ es un cuerpo primo. De hecho, es el único tal cuerpo y se denomina subcuerpo primo de $\mathbb{F}$.

(i).- (1.5 pts) Pruebe que todo anillo con unidad de característica positiva y sin divisores de 0 debe tener característica prima.

(ii).- (1.5 pts) Pruebe que si $\mathbb{F}$ es de característica positiva p, entonces el subcuerpo primo de $\mathbb{F}$ es isomorfo a $\mathbb{Z}/(p)$.

(iii).- (1.5 pts) Sea $\mathbb{F}$ finito. Pruebe que $\mathbb{F}$ tiene característica positiva. Concluya que para algún entero positivo m se tiene que $|\mathbb{F}| = p^m$ donde p es la característica de $\mathbb{F}$.

(iv).- (1.5 pts) Pruebe que si $\mathbb{F}$ tiene característica positiva p, entonces para todo $a, b \in \mathbb{F}$ se tiene que $(a+b)^p = a^p + b^p$.

PROBLEMA 2: (60 %)

Sea $\mathbb{F}_q$ un cuerpo de tamaño $q = p^m$ donde p es primo. Sea $\mathbb{F}_p$ el subcuerpo primo de $\mathbb{F}_q$. Para una indeterminada x definimos $\mathrm{Tr}_m(x) = x + x^p + x^{p^2} + \ldots + x^{p^{m-1}}$.

(i).- Sean $\beta, \gamma \in \mathbb{F}_q$ y $a \in \mathbb{F}_p$. Pruebe que:

(i.1).- (0.3 pts) $\mathrm{Tr}_m(\beta + \gamma) = \mathrm{Tr}_m(\beta) + \mathrm{Tr}_m(\gamma)$.

(i.2).- (0.3 pts) $\mathrm{Tr}_m(a\beta) = a\mathrm{Tr}_m(\beta)$.

Indicación: Recuerde que todo elemento de un grupo multiplicativo finito elevado al orden del grupo es igual a la identidad.

(i.3).- (0.3 pts) $(\mathrm{Tr}_m(\beta))^p = \mathrm{Tr}_m(\beta^p) = \mathrm{Tr}_m(\beta)$.

(ii).- (0.9 pts) Observe que todo elemento de $\mathbb{F}_p$ es una raíz de $x^p - x$ y demuestre que $\mathrm{Tr}_m(\beta) \in \mathbb{F}_p$ cualquiera sea $\beta \in \mathbb{F}_q$. Concluya que $\mathrm{Tr}_m : \mathbb{F}_q \to \mathbb{F}_p$ es $\mathbb{F}_p$-lineal y pruebe que no es idénticamente nula.

(iii).- (0.9 pts) Pruebe que para todo $a \in \mathbb{F}_p$ el cardinal de $\{\beta \in \mathbb{F}_q : \mathrm{Tr}_m(\beta) = a\}$ es p^{m-1}.

(iv).- (0.9 pts) Sea $a \in \mathbb{F}_p$. Pruebe que

$$\mathrm{Tr}_m(x) - a \;=\; \prod_{\beta \in \mathbb{F}_q : \mathrm{Tr}_m(\beta) = a} (x - \beta)\,,$$

y que

$$x^q - x \;=\; \prod_{a \in \mathbb{F}_p} (\mathrm{Tr}_m(x) - a)\,.$$

(v).- (0.9 pts) Considere el polinomio $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Verifique que $p(x)$ es irreducible. Sea α raíz de $p(x)$ y considere la representación de $\mathbb{F}_8$ dada por $\mathbb{F}_2(\alpha) = \langle 1, \alpha, \alpha^2 \rangle_{\mathbb{F}_2}$. Construya la tabla de multiplicación de la referida representación de $\mathbb{F}_8$, verifique que $\beta = \alpha^2$ genera el grupo multiplicativo $\mathbb{F}_8 \backslash \{0\}$, y construya la tabla de adición de los β^i (es decir, para $1 \leq i, j \leq 7$, determine k tal que $\beta^i + \beta^j = \beta^k$).

(vi).- (0.9 pts) Sea $n \in \mathbb{N}$, $n \geq 1$. Sea p primo, m el orden (multiplicativo) de p módulo n, $q = p^m$, y β de orden n en $\mathbb{F}_q$. Sea $c(\xi) = (\mathrm{Tr}_m(\xi), \mathrm{Tr}_m(\xi\beta^2), \ldots, \mathrm{Tr}(\xi\beta^{n-1}))$. Pruebe que $\mathcal{C} = \{c(\xi) : \xi \in \mathbb{F}_q\}$ es un código cíclico, i.e. un $\mathbb{F}_p$-subespacio vectorial de $\mathbb{F}_p^n$ tal que si $(c_0, \ldots, c_{n-1}) \in \mathcal{C}$, entonces $(c_1, c_2, \ldots, c_{n-1}, c_0) \in \mathcal{C}$.

(vii).- (0.6 pts) Para $n = 7$, $p = 2$, $m = 3$, β como en (v), y $\mathcal{C}$ como en (vi), determine todos los elementos de $\mathcal{C}$.