**Ma31a Elementos de Álgebra** **01 de Diciembre, 2008**

# Examen

*Prof. Cátedra: M. Kiwi* *Prof. Auxiliar: E. Araya, O. Rivera*

TIEMPO 4.5 HRS.

PROBLEMA 1: El objetivo de este problema es establecer los siguientes resultados:

**Teorema 1** *Sea $G$ un grupo abeliano finito tal que la ecuación $x^n = 1_G$ se satisface para a lo más $n$ elementos de $G$, cualquiera sea $n \in \mathbb{N}$. Entonces, $G$ es cíclico.*

**Corolario 1** *Sea $\mathbb{F}$ un cuerpo y $G$ un subgrupo finito del grupo multiplicativo $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. Entonces, $G$ es cíclico.*

**Corolario 2** *Si $\mathbb{F}$ es un cuerpo finito, entonces el grupo multiplicativo $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ es cíclico.*

(i).- (1.5 pts) Demostrar el Teorema 1 para el caso en que $G$ es de orden $q$ potencia de un primo $p$.

Indicación: Considerar $g \in G$ elemento de orden maximal, digamos de orden $p^r$, y probar que $G = \{1, g, g^2, \ldots, g^{p^r-1}\}$.

(ii).- (2.0 pts) Demuestre el Teorema 1.

Indicación: Recordar que si $G$ es grupo abeliano de orden $m = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, los $p_i$'s primos distintos, entonces $G$ es isomorfo a $G_1 \times G_2 \times \ldots \times G_k$ donde $G_i$ es de orden $q_i = p_i^{e_1}$. Usar (i).

(iii).- (1.5 pts) Demuestre el Corolario 1.

(iv).- (1.0 pts) Demuestre el Corolario 2.

PROBLEMA 2: Sea $q$ una potencia de un primo $p$. Sea $n$ un entero positivo primo relativo a $p$. Un código cíclico es un ideal (potencialmente degenerado) $\mathcal{C} \neq \{0\}$ en $\mathbb{F}_q[x]/(x^n - 1)$.

(i).- (1.5 pts) Pruebe que existe $g(x) \in \mathbb{F}_q[x]$ de grado menor que $n$ tal que $\mathcal{C} = ([g(x)])$. Muestre que $g(x)$ es un divisor de $x^n - 1$.

(ii).- (1.0 pts) Sea $g(x)$ como en la parte anterior y $h(x) = (x^n - 1)/g(x)$. Pruebe que existen $a(x), b(x) \in \mathbb{F}_q[x]$ tal que $a(x)g(x) + b(x)h(x) = 1$ en $\mathbb{F}_q[x]$.

(iii).- (1.0 pts) Pruebe que existe un *idempotente* $i(x) \in \mathbb{F}[x]$ tal que $[i(x)] \in \mathcal{C}$ y $i(x)c(x) = c(x)(\text{mód} x^n - 1)$ cualquiera sea $[c(x)] \in \mathcal{C}$. Concluya que $i^2(x) = i(x)(\text{mód} x^n - 1)$.

(iv).- (0.75 pts) Sea $q = p = 2$ (luego $n$ impar). Para cada $a \in \{0, \ldots, n-1\}$ se define $I_a = \{(a2^s) \text{ mód } n : s \in \mathbb{N}\}$. Probar que $\mathcal{P}_n = \{I_0, I_1, \ldots, I_{n-1}\}$ es una partición de $\{0, \ldots, n-1\}$.

(v).- (1.0 pts) Sean $q$, $n$, y $\mathcal{P}_n$ como en la parte anterior. Probar que si un idempontente $i(x)$ de $\mathcal{C}$ contiene el término $x^i$ para algún $i \in I_a$, entonces contiene términos equivalentes módulo $x^n - 1$ a $x^j$ cualquiera sea $j \in I_a$. Concluya que existen $2^{|\mathcal{P}_n|}$ códigos cíclicos binarios de largo de bloque $n$.

(vi).- (0.75 pts) Liste todos los códigos cíclicos binarios de largo de bloque $n = 5$.