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

Examen

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

PROBLEMA 1:

(i).- Sea $g \in G$ de orden maximal. Como el orden de un elemento de G debe dividir el orden de G, sigue que g tiene orden p^r para algún $r \in \mathbb{N}$. Como g es de orden p^r, se tiene que $(g^i)^{p^r} = (g^{p^r})^i = 1_G$ cualquiera sea $i \in \mathbb{N}$ y que $1, g, g^2, \ldots, g^{p^r-1} \in G$ son todos distintos. Por hipótesis, $x^{p^r} = 1_G$ tiene a lo más p^r soluciones en G. Sigue que $H = \{1, g, g^2, \ldots, g^{p^r-1}\} \subseteq G$ son todas las p^r soluciones en G de la ecuación $x^{p^r} = 1_G$. Veamos ahora que $G \subseteq H$. En efecto, si $b \in G$, por maximalidad del orden de g se tiene que b tiene orden p^s para algún $s \leq r$. Luego, b es solución de la ecuación $x^{p^r} = 1_G$, y por lo tanto pertenece a H.

(ii).- Bastará ver que $G' = G_1 \times \ldots \times G_k$ como en la indicación es un grupo cíclico. Vía el isomorfismo entre G y G', cualquier solución de $x_i^n = 1_{G_i}$ en G_i se puede identificar con $x = (1_{G_1}, \ldots, x_i, \ldots, 1_{G_k})$ solución de $x^n = 1_G$ en G. Luego, existen a lo más n soluciones en G_i de la ecuación $x^n = 1_{G_i}$. Por (i), sigue que cada G_i es cíclico de orden q_i. Sea g_i un generador de G_i, y $g' = (g_1, \ldots, g_k) \in G'$. Afirmamos que g' genera G'. En efecto, sea m' el orden de g'. Sigue que $(g')^{m'} = (g_1^{m'}, \ldots, g_k^{m'}) = (1_{G_1}, \ldots, 1_{G_k})$. Como $g_i^{m'} = 1_{G_i}$ se debe tener que q_i divide m'. Como los q_i's son primos relativos, se tiene que $m = q_1 q_2 \ldots q_m$ es divisor de m'. Pero m' es a lo más menor o igual que el orden de G, i.e. $m' \leq m$. Luego, $m = m'$ y por lo tanto g' es generador de G'. Sigue que G' es cíclico.

(iii).- Basta ver que se cumplen las hipótesis del Teorema 1. En efecto, $x^n - 1 \in \mathbb{F}[x]$ tiene a lo más n raíces en $\mathbb{F}$, luego con más razón en G. Claramente, $x^n = 1_G$ tiene a lo más n soluciones en G.

(iv).- Basta considerar en (iii) el grupo $G = \mathbb{F}^*$, el cual es claramente un grupo finito.

PROBLEMA 2:

(i).- Sea $g(x) \in \mathbb{F}_q[x]$, $[g(x)] \in \mathcal{C} \setminus \{0\}$ de grado mínimo. Afirmamos que $\mathcal{C} = ([g(x)])$ y que $g(x)$ tiene grado estrictamente menor que n. En efecto, si $g(x)$ tuviese grado mayor o igual que n, entonces el resto $r(x)$ de la división de $g(x)$ por $x^n - 1$ sería de grado menor que $g(x)$ y tal que $[r(x)] = [g(x)]$. Luego, $\mathcal{C} = ([r(x)])$ contradiciendo la minimalidad de

$g(x)$. Supongamos ahora que existe $[c(x)] \in \mathcal{C}$ tal que $c(x)$ no es múltiplo de $g(x)$. Por Teorema de la División existen $q(x)$ y $r(x)$ tal que $c(x) = q(x)g(x) + r(x)$ con $r(x)$ no nulo de grado estrictamente menor que $g(x)$. Como $\mathcal{C}$ es ideal, sigue que $[r(x)] = q(x)[g(x)] - [c(x)]$ está en $\mathcal{C}$, contradiciendo nuevamente la minimalidad de $g(x)$.

Para concluir que $g(x)$ es divisor de $x^n - 1$ basta observar que $[x^n - 1] = [0]$, que $[0] \in \mathcal{C}$ dado que $\mathcal{C}$ es ideal, y usar el hecho recién demostrado que garantiza que si $[c(x)] \in \mathcal{C}$, entonces $g(x)$ es divisor de $c(x)$.

(ii).- Por Lema de Bezout, basta demostrar que $g(x)$ y $h(x)$ son primos relativos. En efecto, si $g(x)$ y $h(x)$ no fuesen primos relativos, entonces existiría un factor $p(x)$ de $g(x)$ y $h(x)$ de grado mayor o igual a 1. Luego, $g(x)$ y $h(x)$ compartirían raíces en alguna extensión $\mathbb{K}$ de $\mathbb{F}_q$ (por ejemplo, el cuerpo de descomposición de $g(x)$). Como $g(x)h(x) = x^n - 1$, sigue que $(p(x))^2$ sería divisor de $x^n - 1$. En particular, $x^n - 1$ tendría raíces múltiples en $\mathbb{K}$. Pero la derivada formal de $x^n - 1$ es nx^{n-1} que es distinto de 0 en $\mathbb{F}_q[x]$ dado que n es primo relativo con p. Sigue que nx^{n-1} y $x^n - 1$ no comparten raíces, luego $x^n - 1$ no tiene raíces múltiples en ninguna extensión de $\mathbb{F}_q$, lo que da una contradicción.

(iii).- Sean $a(x)$, $b(x)$, $g(x)$, y $h(x)$ como en la parte (ii). Afirmamos que $i(x) = a(x)g(x) = 1 - b(x)h(x)$ es tal que para todo $[c(x)] \in \mathcal{C}$ se tiene que $i(x)c(x) = c(x)$ en $\mathbb{F}_q[x]/(x^n - 1)$. En efecto, como $[c(x)] \in \mathcal{C} = ([g(x)])$, entonces $c(x) = p(x)g(x)$ para algún $p(x) \in \mathbb{F}_q[x]$. Sigue que

$$i(x)c(x) = c(x) - b(x)p(x)g(x)h(x) = c(x) - b(x)p(x)(x^n - 1)\,,$$

de donde se concluye que $i(x)c(x) = c(x)$ en $\mathbb{F}_q[x]/(x^n - 1)$.

Como $i(x) \in \mathcal{C}$, entonces tomando $c(x) = i(x)$ en la identidad $i(x)c(x) = c(x)$ en $\mathbb{F}_q[x]/(x^n - 1)$ se obtiene la igualdad $i^2(x) = i(x) (\operatorname{mód} x^n - 1)$.

(iv).- Claramente $a \in I_a$, por lo que la unión de los I_a's es $\{0, 1, \ldots, n-1\}$. Veamos ahora que si $I_a \neq I_b$, entonces $I_a \cap I_b = \emptyset$. En efecto, si $i \in I_a \cap I_b$, entonces existen s_a y s_b en $\mathbb{N}$ tales que $i = a2^{s_a} = b2^{s_b} \pmod{n}$. Como n es primo relativo a 2, sigue que 2 es invertible módulo n. Suponiendo sin pérdida de generalidad que $s_a \geq s_b$, sigue que $b = 2^{s_a - s_b}a \pmod{n}$, i.e. $b \in I_a$. Sigue que $I_b \subseteq I_a$. Analogamente se tiene que $I_a \subseteq I_b$. Luego $I_a = I_b$, por lo que se concluye que la intersección de I_a y I_b debe ser vacía.

De la discusión anterior se desprende que $\mathcal{P}_n$ es partición de $\{0, 1, \ldots, n-1\}$.

(v).- Sea $i(x)$ un idempotente de $\mathcal{C}$ que contiene el término x^i tal que $i \in I_a$. Como $i^2(x) = i(x) \pmod{x^n - 1}$, sigue en particular que $i^2(x)$ contiene el término $x^{2i} \pmod{x^n - 1}$, y en general que contiene el término $x^{2^s i} \pmod{x^n - 1}$. Luego, $i(x)$ contiene todos los términos $x^j \pmod{x^n - 1}$ con $j \in I_i$. Como $\mathcal{P}_n$ es partición, se tiene que $I_i = I_a$ y por lo tanto se cumple la primera parte del enunciado.

Vimos que todo código cíclico $\mathcal{C}$ de largo de bloque n tiene asociado un idempotente. Dicho idempotente es único (módulo x^n-1) puesto que si $i(x)$ y $i'(x)$ son idempotentes de $\mathcal{C}$, entonces $[i(x)],[i'(x)] \in \mathcal{C}$ y por lo tanto, por propiedades de idempotentes, sigue que $i(x) = i(x)i'(x) = i'(x) (\bmod x^n-1)$.

Todo idempotente $i(x)$ queda completamente especificado por el conjunto de índices $I \subseteq \{0,\ldots,n-1\}$ tal que x^i aparece en $i(x)$. De la discusión anterior se desprende que I debe ser unión de elementos de $\mathcal{P}_n$. Dado que hay $2^{|\mathcal{P}_n|}$ uniones distintas que se pueden hacer con los elementos de $\mathcal{P}_n$, se concluye que hay igual número de códigos cíclicos binarios disintos.

(vi).- Basta observar que $\mathcal{P}_n = \{I_0, I_1\}$ donde $I_0 = \{0\}$ y $I_1 = \{1,2,3,4\}$. Definimos entonces $i_0(x) = 1$ y $i_1(x) = x+x^2+x^3+x^4$. Sigue que los posibles idempontentes de códigos cíclicos binarios de largo de bloque $n=5$ son 0, $i_0(x)$, $i_1(x)$, y $i_0(x)+i_1(x)$. Los ideales de $\mathbb{F}_2[x]/(x^n-1)$ generados por cada uno de estos idempontentes son (usando la convención de denotar el polinomio $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ por $c_0c_1\ldots c_{n-1}$):

$$
\begin{aligned}
\mathcal{C}_{\emptyset} &= \{0\}\,, \\
\mathcal{C}_0 &= \{0,1\}^5\,, \\
\mathcal{C}_1 &= \{01111, 10111, 11011, 11101, 11110, 11100, 01110, 00111, 10011, 11001\}\,, \\
\mathcal{C}_{0,1} &= \{00000, 11111\}\,.
\end{aligned}
$$