Ma3101 Elementos de Álgebra **20 de Septiembre**

Pauta Examen

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

PROBLEMA 1:

(i).- Por contradicción, sea $n \in \mathbb{N} \setminus \{0\}$ el número compuesto más pequeño tal que $nr = 0$ para todo $r \in R$. Como n es compuesto, existen enteros $a, b > 1$ tales que $ab = n$ (en particular, $a, b < n$). Como $0 = n1_R = (ab)1_R = (a1_R)(b1_R)$ y R no posee divisores de 0, sigue que $a1_R = 0$ o $b1_R = 0$. Sin pérdida de generalidad, supongamos que $a1_R = 0$. Premultiplicando por $r \in R$, se obtiene que $ar = 0$. Esto último es válido para todo $r \in R$, contradiciendo la minimalidad de n.

(ii).- Por definición de p, sigue que $\mathbb{K} = \{a1_\mathbb{F} : a \in \mathbb{N}\}$ es un conjunto de tamaño p. Afirmamos que $\mathbb{K}$ es cuerpo. En efecto, claramente $(\mathbb{K}, +)$ es grupo abeliano. Además, $(a1_\mathbb{F})(a'1_\mathbb{F}) = b1_\mathbb{F}$ donde b es el resto de la división de aa' por p, y el inverso multiplicativo de $a1_\mathbb{F}$, $a \neq 0$, es $b1_\mathbb{F}$ donde $b \in \{1, \ldots, p-1\}$ es tal que ab es congruente a 1 módulo p (dicho b existe porque a es primo relativo con p). Se tiene entonces que $\mathbb{K}$ es cuerpo. Dado que $\mathbb{K}$ es subcuerpo de $\mathbb{F}$, contiene al cuerpo primo de $\mathbb{F}$. Más aún, afirmamos que es igual al cuerpo primo de $\mathbb{F}$. En efecto, como $1_\mathbb{F}$ está en el cuerpo primo de $\mathbb{F}$, por definición de $\mathbb{K}$ y cerradura de la adición en un cuerpo, sigue que $\mathbb{K} \subseteq \mathbb{F}$. Por minimalidad del cuerpo primo, se tiene que este debe ser igual a $\mathbb{K}$. Para concluir, basta verificar que $\varphi : \mathbb{K} \to \mathbb{Z}/(p)$ tal que $\varphi(a1_\mathbb{F}) = a$ para $a \in \{0, \ldots, p-1\}$ es un isomorfismo de cuerpos.

(iii).- Como $m1_\mathbb{F} \in \mathbb{F}$ cualquiera sea $m \in \mathbb{N}$, y dado que $\mathbb{F}$ es finito, deben existir $m, m' \in \mathbb{N}$, $m < m'$, tales que $m1_\mathbb{F} = m'1_\mathbb{F}$. Sigue que $(m'-m)1_\mathbb{F} = 0$. Multiplicando por $\alpha \in \mathbb{F}$, sigue que $(m'-m)\alpha = 0$ cualquiera que sea α. Luego, existe un entero positivo $n = m'-m$ tal que $n\alpha = 0$ cualquiera sea $\alpha \in \mathbb{F}$, i.e. $\mathbb{F}$ es de característica positiva.

Sea $\mathbb{K}$ el cuerpo primo de $\mathbb{F}$. Sigue que $\mathbb{F}$ es $\mathbb{K}$-espacio vectorial. Como $\mathbb{F}$ es finito, debe tener dimensión finita como $\mathbb{K}$-espacio vectorial, digamos $m \in \mathbb{N} \setminus \{0\}$. Luego, $|\mathbb{F}| = |\mathbb{K}|^m$. Si p es la característica de $\mathbb{F}$, como $\mathbb{K}$ es isomorfo a $\mathbb{Z}/(p)$, tenemos que $|\mathbb{K}| = p$ y que $|\mathbb{F}| = p^m$ como faltaba establecer.

(iv).- Por Teorema del Binomio (el cual sigue siendo valido sobre un cuerpo), tenemos que $(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p$. La conclusión deseada se obtiene del hecho que $\mathbb{F}$ es de característica p y observando que si $0 < i < p$, entonces $\binom{p}{i}$ es múltiplo de p (en efecto,

$p!/i!(p-i)!$ es múltiplo de p puesto que como p es primo, ni $i!$ ni $(p-i)!$ son divisibles por p, pero $p!$ si lo es).

PROBLEMA 2:

(i.1).- De la parte (iv) del problema anterior, sabemos que $(\beta+\gamma)^p = \beta^p + \gamma^p$, de donde es fácil concluir que $(\beta+\gamma)^{p^i} = \beta^{p^i} + \gamma^{p^i}$. Sumando sobre $i = 0, \ldots, m-1$ se obtiene la conclusión deseada.

(i.2).- Como $\mathbb{F}_p$ es cuerpo, tenemos que $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ es grupo multiplicativo de orden $p-1$. Luego, por la indicación, sigue que $a^{p-1} = 1$ para todo $a \in \mathbb{F}_p^*$. Por lo tanto, $a^p = a$ cualquiera sea $a \in \mathbb{F}_p^*$, identidad que se cumple trivialmente cuando $a = 0$. Elevando sucesivamente a la potencia p ambos lados de esta última identidad, sigue que $a^{p^i} = a$ cualquiera que sea $i \in \mathbb{N}$ y que $a \in \mathbb{F}_p$. Luego,

$$\mathrm{Tr}_m(a\beta) = \sum_{i=1}^{m-1} (a\beta)^{p^i} = \sum_{i=1}^{m-1} (a^{p^i})\beta^{p^i} = \sum_{i=1}^{m-1} a\beta^{p^i} = a\mathrm{Tr}_m(\beta)\,.$$

(i.3).- La primera igualdad es consecuencia directa de la parte (iv) del Problema 1. La segunda igualdad se tiene trivialmente si $\beta = 0$. Si $\beta \neq 0$, dado que $\mathbb{F}_q \setminus \{0\}$ es un grupo multiplicativo de orden $q-1$, sabemos que $(\beta^p)^{p^{m-1}} = \beta^{q-1}\beta = \beta$. Se concluye fácilmente que $\mathrm{Tr}_m(\beta^p) = \mathrm{Tr}_m(\beta)$.

(ii).- Veamos primero que $\mathrm{Tr}_m(\beta) \in \mathbb{F}_p$ para todo $\beta \in \mathbb{F}_q$. Como ya vimos en la demostración de la parte (i.2), todo $a \in \mathbb{F}_p$ satisface $a^p = a$, luego es raíz de $x^p - x$. Como $x^p - x$ es un polinomio de grado p, tiene a lo más p raíces distintas. Sigue que los elementos de $\mathbb{F}_p$ son las únicas raíces de $x^p - x$. De la parte (i.3), sabemos que $\mathrm{Tr}_m(\beta)$ es raíz de $x^p - x$ cualquiera sea $\beta \in \mathbb{F}_q$. Sigue que $\mathrm{Tr}_m(\beta) \in \mathbb{F}_p$, como se quería demostrar. De (i.1) y (i.2) se tiene que Tr_m es $\mathbb{F}_p$ lineal. Solo falta establecer que Tr_m no es idénticamente nula. En efecto, si $\mathrm{Tr}_m(\beta) = 0$ cualquiera fuese $\beta \in \mathbb{F}_q$, entonces el polinomio $\mathrm{Tr}_m(x)$, cuyo grado es p^{m-1}, tendría $q = p^m > p^{m-1}$ raíces, lo que es imposible.

(iii).- Observar primero que $\mathbb{F}_p$ y $\mathbb{F}_q$ son $\mathbb{F}_p$-espacios vectoriales de dimensión 1 y m respectivamente. Dado que Tr_m es lineal y no es idénticamente nula, por Teorema Núcleo Imágen, sigue que Tr_m es sobreyectiva y su núcleo tiene dimensión $m-1$. Por resultados conocidos concernientes a operadores lineales, las soluciones del sistema $\mathrm{Tr}_m(x) = a$ son todas de la forma $\beta + \mathrm{Ker}(\mathrm{Tr}_m)$ donde β es un elemento fijo de $\mathbb{F}_q$ tal que $\mathrm{Tr}_m(\beta) = a$. Como $\mathrm{Ker}(\mathrm{Tr}_m)$ es un $\mathbb{F}_p$-espacio vectorial de dimensión $m-1$, posee exactamente p^{m-1} elementos. La conclusión deseada sigue de manera inmediata.

Nota: Una respuesta alternativa sería argumentar que dado que $\mathrm{Tr}_m(\cdot)$ no es idénticamente

nula, entonces para algún $\beta \in \mathbb{F}_q$ se tiene que $a = \mathrm{Tr}_m(\beta) \neq 0$, $a \in \mathbb{F}_p$ por (ii). Luego, por (i.2), para cualquier $b \in \mathbb{F}_p$ se tiene que $\mathrm{Tr}_m(ba^{-1}\beta) = b$, i.e. $\mathrm{Tr}_m(\cdot)$ es sobreyectiva. El resto del argumento sigue como arriba, pero no requiere aplicar el Teorema Núcleo Imágen.

(iv).- Para probar la primera identidad, basta observar que $\mathrm{Tr}_m(x) - a$ es un polinomio mónico de grado p^{m-1} que tiene por raíces los $\beta \in \mathbb{F}_q$ tales que $\mathrm{Tr}_m(\beta) = a$. Por (iii), hay p^{m-1} tales raíces. Luego, $\mathrm{Tr}_m(x) - a$ se factoriza completamente como producto de los polinomios lineales $x - \beta$ donde β varía sobre los elementos de $\mathbb{F}_q$ tales que $\mathrm{Tr}_m(\beta) = a$.

La segunda identidad se obtiene del hecho que a ambos lados de la igualdad aparecen polinomios de grado q y tales que cualquier $\beta \in \mathbb{F}_q$ es raíz de dichos polinomios (en efecto, por resultado ya mencionado $\beta^q = \beta$ cualquiera sea $\beta \in \mathbb{F}_q$, y claramente se tiene que β es raíz de $\mathrm{Tr}_m(x) - \mathrm{Tr}_m(\beta)$). Como dos polinomios de grado q que comparten q raíces distintas deben necesariamente ser iguales, se concluye la identidad deseada.

(vi).- Para comprobar que $p(x)$ es irreducible, basta verificar que su evaluación en $0, 1 \in \mathbb{F}_2$ es no nula.

En la representación de $\mathbb{F}_8$ a considerar se tiene que $\alpha^3 = \alpha + 1$, luego la tabla del producto en $\mathbb{F}_8$ queda dada por:

$\times$	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
α	α^2	$\alpha+\alpha^2$	$1+\alpha$	1	$1+\alpha+\alpha^2$	$1+\alpha^2$
$1+\alpha$		$1+\alpha^2$	$1+\alpha+\alpha^2$	α^2	1	α
α^2			$\alpha+\alpha^2$	α	$1+\alpha^2$	1
$1+\alpha^2$				$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$
$\alpha+\alpha^2$					α	α^2
$1+\alpha+\alpha^2$						$1+\alpha$

Si $\beta = \alpha^2$, de acuerdo a la tabla del producto de la representación de $\mathbb{F}_8$, sigue que $\beta^2 = \alpha+\alpha^2$, $\beta^3 = 1+\alpha^2$, $\beta^4 = \alpha$, $\beta^5 = 1+\alpha$, $\beta^6 = 1+\alpha+\alpha^2$, $\beta^7 = 1$. Luego, β genera $\mathbb{F}_8 \setminus \{0\}$. Se verifica que la tabla de adición de los β^i queda dada por:

$+$	β	β^2	β^3	β^4	β^5	β^6	β^7
β	0	β^4	1	β^2	β^6	β^5	β^3
β^2		0	β^5	β	β^3	1	β^6
β^3			0	β^6	β^2	β^4	β
β^4				0	1	β^3	β^5
β^5					0	β	β^4
β^6						0	β^2
β^7							0

(vi).- Veamos primero que $\mathcal{C}$ es un $\mathbb{F}_p$-subespacio vectorial de $\mathbb{F}_p^n$. En efecto, sean $\xi, \xi' \in \mathbb{F}_q$ y $a, a' \in \mathbb{F}_p$. Notar que, por definición de $c(\cdot)$ y linealidad de $\mathrm{Tr}_m(\cdot)$ (de acuerdo a lo demostrado en (ii)),

$$\begin{aligned} ac(\xi) + ac(\xi') &= (a\mathrm{Tr}_m(\xi\beta^i) + a'\mathrm{Tr}_m(\xi'\beta^i) : i = 0, \ldots, n-1) \\ &= (\mathrm{Tr}_m(a\xi\beta^i + a'\xi'\beta^i) : i = 0, \ldots, n-1) \\ &= c(a\xi + a'\xi'). \end{aligned}$$

Sigue que $\mathcal{C}$ es un $\mathbb{F}_p$-subespacio vectorial de $\mathbb{F}_p^n$

Veamos ahora que $\mathcal{C}$ es cíclico. En efecto, tomando $\xi' = \xi\beta \in \mathbb{F}_q$, y observando que $\beta^n = 1$ (dado que el orden de β es n), sigue que

$$\begin{aligned} c(\xi') &= (\mathrm{Tr}_m(\xi\beta), \mathrm{Tr}_m(\xi\beta^2), \ldots, \mathrm{Tr}_m(\xi\beta^{n-1}), \mathrm{Tr}_m(\xi\beta^n)) \\ &= (\mathrm{Tr}_m(\xi\beta), \mathrm{Tr}_m(\xi\beta^2), \ldots, \mathrm{Tr}_m(\xi\beta^{n-1}), \mathrm{Tr}_m(\xi)) \\ &= (c_1, c_2, \ldots, c_{n-1}, c_0). \end{aligned}$$

Luego, $(c_1, c_2, \ldots, c_{n-1}, c_0) \in \mathcal{C}$ como se quería establecer.

(vii).- Notar que $c(0) = (0,0,0,0,0,0,0)$. Además $c(1) = (\mathrm{Tr}_3(\beta^i) : i = 0, \ldots, 6)$. Dado que $p = 2$, tenemos que $\mathrm{Tr}_3(\beta^i) = \beta^i + \beta^{2i} + \beta^{4i}$. Evaluando en $i = 0, 1, \ldots, 6$ y usando la tabla de adición para las potencias de β construida en la parte (v), sigue que $c(1) = (1,0,0,1,0,1,1)$. De la demostración de la parte (vi) sabemos que $c(\beta^j)$ se obtiene a partir de $c(1)$ vía j shifts cíclicos. Como todo $\xi \in \mathbb{F}_8$ es una potencia de β, sigue que $\mathcal{C}$ es igual a los shifts cíclicos ditintos de $c(1)$, es decir

$$\begin{aligned} \mathcal{C} = \{&(1,0,0,1,0,1,1), (0,0,1,0,1,1,1), (0,1,0,1,1,1,0), (1,0,1,1,1,0,0), \\ &(0,1,1,1,0,0,1), (1,1,1,0,0,1,0), (1,1,0,0,1,0,1)\}. \end{aligned}$$