Ma31a Elementos de Álgebra **06 de Octubre, 2007**

Pauta Control 2

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

Problema 1:

(i).- Lo único que le falta a R para ser cuerpo es que todo elemento no nulo de R sea invertible. Como $R \setminus \{0\}$ es finito, entonces para todo $r \in R$, $r \neq 0$, existen $i, j \geq 1$ tales que $r^{i+j} = r^i$. Como R es dominio de integridad, r es cancelable, luego $r^j = 1$. Si $r \neq 1$, necesariamente se debe tener que $j > 1$ y por lo tanto $rr^{j-1} = r^{j-1}r = 1$, i.e. r es invertible.

(ii).- Sea I un dip en R. Si $I = \{0\}$, entonces es obviamente un ideal principal. Supongamos entonces que existe $b \in I$, $b \neq 0$, minimal con respecto a $d(b)$. Afirmamos que $I = (b)$. En efecto, como $b \in I$, ciertamente que $(b) \subseteq I$. Supongamos que existe $a \in I \setminus (b)$. Notar en particular que b no es divisor de a. Como R es Euclideano, existen $t, r \in R$ tales que $a = tb + r$ donde $r = 0$ o $d(r) < d(b)$. Pero $r \neq 0$ pues en caso contrario tendríamos que $b|a$. Sigue, dado que a y b estan en I, que $r = a - tb \in I$, contradiciendo la minimalidad de $d(b)$.

(iii).- Hay muchas maneras probar el isomorfismo, en particular exhibiendo un isomorfismo. Aquí seguiremos otro camino. Específicamente, demostraremos la isomorfia como una aplicación del Teorema del Factor para anillos. Sea $f : R \to R/(\beta)$ tal que $f(r) = [\alpha r] \in R/(\beta)$. Se verifica facilmente que f es un morfismo de anillos. Luego, por Teorema del Factor para anillos, $\mathrm{Im}\,(f) \cong R/\,\mathrm{Ker}\,(f)$ (isomorfismo de anillos). Claramente $\mathrm{Im}\,(f) = \alpha R/(\beta)$. Sea δ un máximo común divisor de α y β. Veamos entonces que $\mathrm{Ker}\,(f) = (\beta/\delta)$. En efecto, si $r \in \mathrm{Ker}\,(f)$, entonces existe $r' \in R$ tal que $\alpha r = \beta r'$. Sabemos que existen $s, t \in R$ tales que $s\alpha + t\beta = \delta$. Sigue que $r\delta = (sr' + tr)\beta$. Luego $r \in (\beta/\delta)$. Por otro lado, $f(\beta/\delta) = \beta(\alpha/\delta) \in (\beta)$, i.e. $\beta/\delta \in \mathrm{Ker}\,(f)$ y por lo tanto $(\beta/\delta) \subseteq \mathrm{Ker}\,(f)$.

Problema 2:

(i).- Sea M el módulo de torsión de V. Sabemos que $V \cong M \oplus L$ donde L es un módulo libre de rango finito. En particular, como V es un $\mathbb{F}[t]$ módulo, $L \cong (\mathbb{F}[t])^s$ para algún entero no–negativo s. Pero, V es un espacio vectorial sobre $\mathbb{F}$ de dimensión finita, mientras que $(\mathbb{F}[t])^s$ es un espacio vectorial sobre $\mathbb{F}$ de dimensión infinita si $s \geq 1$. Sigue que la única posibilidad es que $s = 0$, i.e., $L \cong \{0\}$. Esto último es equivalente a decir que $V \cong M$, i.e., V es de torsión.

Por resultado visto, y como V es en particular $\mathbb{F}[t]$–módulo de torsión finitamente generado (por ser de dimensión finita), sabemos que existen $p_1, \ldots, p_r$ primos en $\mathbb{F}[t]$ (no necesariamente distintos) y enteros no–negativos $e_1, \ldots, e_r$ tales que

$$V \cong \mathbb{F}[t]/(p_i^{e_i}) \oplus \ldots \oplus \mathbb{F}[t]/(p_r^{e_r})\,.$$

(ii).- Sea φ el morfismo cuya existencia esta garantizada por la parte (i). Sea W_i la pre–imágen de $\mathbb{F}[t]/(p_i^{e_i})$ vía φ. Es fácil ver que W_i es un $\mathbb{F}[t]$–módulo cíclico generado por $\varphi^{-1}(\widehat{x}_i)$ donde $\widehat{x}_i$ denota el elemento de $\mathbb{F}[t]/(p_i^{e_i}) \oplus \ldots \oplus \mathbb{F}[t]/(p_r^{e_r})$ que se obtiene como la suma de $x_j \in \mathbb{F}[t]/(p_j^{e_j})$ donde x_j es igual a 1 si $j = i$ y 0 en caso contrario.

Finalmente, dado que W_i es un $\mathbb{F}[t]$–sub–módulo de V, sabemos que W_i es estable bajo T, i.e., $T(W_i) \subseteq W_i$.

(iii).- Sea $n_i = |\beta_i|$ y supongamos que $\beta_i = \{b_{i,j} \,:\, j = 1, \ldots, n_i\}$.

Si $v \in V$, entonces existen $w_i \in W_i$ para $i = 1, \ldots, r$, tales que $v = w_1 + w_2 + \ldots + w_r$. Como V es un espacio vectorial sobre $\mathbb{F}$, se tiene que existen también $\alpha_{i,j}$'s en $\mathbb{F}$ tales que $w_i = \sum_j \alpha_{i,j} b_{i,j}$ Sigue facilmente que β genera V.

Por otro lado, supongamos que $\sum_{i,j} \alpha_{i,j} b_{i,j} = 0$ donde los $\alpha_{i,j} \in \mathbb{F}$. Como V es suma directa de los W_i y $\sum_j \alpha_{i,j} b_{i,j} \in W_i$, sigue que $\sum_j \alpha_{i,j} b_{i,j} = 0$ para todo i. Como β_i es base de W_i, se concluye que $\alpha_{i,j} = 0$ para todo $i \in \{1, \ldots, r\}$ y $j \in \{1, \ldots, n_i\}$. Luego, β es una familia linealmente independiente en V. Esto concluye la demostración de que β es base V.

Como $T(W_i) \subseteq W_i$ se tiene que $T(b_{i,j})$ puede expresarse como combinación lineal de los elementos en β_i. Se concluye facilmente que $[T]_{\beta,\beta}$ es una matriz diagonal por bloques donde cada bloque tiene tamaño $n_i \times n_i$.

(iv).- Veamos primero que β es base. Como $\{(t-\alpha)^n \,:\, n \in \mathbb{N}\}$ es una base de $\mathbb{F}[t]$, sigue que $\beta_i = \{[(t-\alpha)^n]_I \,:\, n \in \{0, \ldots, m-1\}\} = \{[(t-\alpha)^n \,:\, n \in \mathbb{N}\}$ genera $\mathbb{F}[t]/((t-\alpha)^m)$.

Falta establecer que β es una colección linealmente independiente. En efecto, sean $q_0, \ldots, q_{m-1} \in \mathbb{F}[t]$ tales que

$$0 = \sum_{i=0}^{m-1} q_i[(t-\alpha)^i]_I = [\sum_{i=0}^{m-1} q_i(t-\alpha)^i]_I\,.$$

Notar que sin pérdida de generalidad podemos asumir que el grado de $\sum_{i=0}^{m-1} q_i(t-\alpha)^i$ es estrictamente menor que m. Sigue que existe $q \in \mathbb{F}[t]$ tal que

$$\sum_{i=0}^{m-1} q_i(t-\alpha)^i = q(t-\alpha)^m .$$

El polinomio a la izquierda de la igualdad tiene grado menor que m. El que está a la derecha, tiene grado múltiplo de m. Luego, necesariamente que ambos son nulos, en particular $q_0 = \ldots = q_{m-1} = q = 0$. Esto concluye la demostración de independencia.

Sea entonces la transformación L como en el enunciado. Observemos que para todo i,

$$L\left((t-\alpha)^i\right) = \left[t(t-\alpha)^i\right]_I = \alpha\left[(t-\alpha)^i\right]_I + \left[(t-\alpha)^{i+1}\right]_I .$$

Luego, de la definición de matriz representante sigue inmediatamente que $[L]_{\beta,\beta}$ es un bloque de Jordan como el del enunciado.

(v).- En $\mathbb{C}[x]$ los polinomios irreducibles son los de grado 1. Luego, si V es un espacio vectorial sobre $\mathbb{C}$ de dimensión n, se tiene que como $\mathbb{F}[t]$–módulos

$$V \cong \mathbb{F}[t]/\left((x-\alpha_1)^{e_1}\right) \oplus \ldots \oplus \mathbb{F}[t]/\left((x-\alpha_r)^{e_r}\right) ,$$

donde $e_1, \ldots, e_r \in \mathbb{N}$ y $e_1 + \ldots + e_r = n$. Sea φ el morfismo cuya existencia acabamos de establecer. Sea $\beta = \beta_1 \cup \ldots \cup \beta_r$ donde $\beta_i = \{[(t-\alpha_i)^j]_{I_i} : j = 0, \ldots, e_i - 1\}$ e $I_i = ((t-\alpha_i)^{e_i})$ para $i = 1, \ldots, r$. De la parte (iii) tenemos que β es base de $\mathbb{F}[t]/\left((x-\alpha_1)^{e_1}\right) \oplus \ldots \oplus \mathbb{F}[t]/\left((x-\alpha_r)^{e_r}\right)$ y que $[\varphi^{-1} \circ L \circ \varphi]_{\beta,\beta}$ es una matriz diagonal por bloques de tamaños $e_i \times e_i$, $i = 1, \ldots, r$. De la parte (iv) sabemos que el i–ésimo de estos bloques es un bloque de Jordan, específicamente

$$\begin{pmatrix} \alpha_i & & & \\ 1 & \alpha_i & & \\ & \ddots & \ddots & \\ & & 1 & \alpha_i \end{pmatrix} .$$

El resultado deseado sigue del hecho que $[L]_{\beta',\beta'} = [\varphi^{-1} \circ L \circ \varphi]_{\beta,\beta}$ donde $\beta' = \varphi(\beta)$.