MA-31A Elementos de Álgebra **15 de Octubre, 2005**

Pauta Control 2

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: H. Castro, J. Soto*

Problema 1:

(i).- El subgrupo H tiene orden 4, que es el cuadrado de un primo, luego es abeliano. Por el Teorema de Estructura de los Grupos Abelianos, se tiene que existen tantas clases isomorfas de grupos abelianos como particiones de 4, o sea, hay dos clases. Cada clase esta asociada a una de las particiones de 4. En particular, $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ o $H \cong \mathbb{Z}_4$.

El subgrupo K tiene orden 3, luego es cíclico y por unicidad (salvo isomorfismos) de los grupos cíclicos de orden finito, se tiene que $K \cong \mathbb{Z}_3$.

(ii).- El número de 3-subgrupos de Sylow debe ser un divisor de 12 congrutente a 1 módulo 3. Luego, necesariamente el número de 3-subgrupos de Sylow es 1 o 4. Si $K \ntriangleleft G$, entonces K no es el único 3–subgrupo de Sylow. Sigue que existen 4 subgrupos de Sylow de orden 3, digamos $K_1, \ldots, K_4$.

Para todo $i \neq j$ se tiene que $K_i \cap K_j$ es un subgrupo propio de K_i. Luego, por Lagrange $K_i \cap K_j = \{1\}$. Análogamente se tiene que $K_i \cap H = \{1\}$ para todo i. Como H tiene orden 4 y comparte un sólo elemento con $K_1 \cup K_2 \cup K_3 \cup K_4$ cuyo tamaño es 9, necesiaramente se debe tener que

$$H \setminus \{1\} = G \setminus (K_1 \cup K_2 \cup K_3 \cup K_4)\,.$$

En resumen se tiene una situación como la ilustrada en la figura del enunciado. Más aún, H es único. Luego, todo conjugado de H es igual a H, i.e., $H \triangleleft G$.

Como $K \ntriangleleft G$ o $K \triangleleft G$, sigue que $H \triangleleft G$ o $K \triangleleft G$.

(iii).- Si $K, H \triangleleft G$, entonces G es abeliano y $G \cong N \times K$. De la parte (i) sigue que $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ o $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

(iv).- Como $K \cong \mathbb{Z}_3$, se tiene que $(Aut(K), \circ) \cong (Aut(\mathbb{Z}_3), \circ) \cong (\mathbb{Z}_3^*, \circ)$. El grupo $\mathbb{Z}_3^*$ tiene orden 2. Luego, $Aut(\mathbb{Z}_3)$ tiene sólo dos elementos, la identidad id y ϕ tal que $\phi(n) = 2n$. Sigue que la única acción no trivial por automorfismos de $\mathbb{Z}_4$ en $\mathbb{Z}_3$ es

$\varphi : \mathbb{Z}_4 \to \mathbb{Z}_3$ tal que $\varphi(1) = \phi$. Como $K \cong \mathbb{Z}_3$, $H \cong \mathbb{Z}_4$, y $K \ntrianglelefteq G$ (en particular G no es abeliano), sigue que $G \cong \mathbb{Z}_3 \times_\varphi \mathbb{Z}_4$. Luego,

$$(k,h) \cdot (k',h') = (k +_3 \varphi(h)(k'), h +_4 h') = (k +_3 2^h k', h +_4 h')\,.$$

Observar que $(0,0)$ es el neutro de $\mathbb{Z}_3 \times_\varphi \mathbb{Z}_4$. Sean $x, y \in \mathbb{Z}_3 \times \mathbb{Z}_4$ tales que $x = (0,1)$ e $y = (1,0)$. Se verifica que

$$\begin{aligned} x^2 &= (0,2)\,,\\ x^3 &= (0,3)\,,\\ x^4 &= (0,0)\,,\\ y^2 &= (2,0)\,,\\ y^3 &= (0,0)\,,\\ xy &= (2,1)\,,\\ y^2x &= (2,1)\,. \end{aligned}$$

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 torsón.

Por resultado visto, y como V es en particular $\mathbb{F}[t]$–módulo de torsión finitamente generado, 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.

(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.

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

(iv).- Veamos primero que β es base. Para ello probaremos por inducción que t^j puede expresarse como una $\mathbb{F}$ combinación lineal de $\beta_j = \{(t-\alpha)^i : i = 0, \ldots, j\}$. En efecto, la afirmación es obvia para $j = 0$. Supongamos que se tiene para j. Como $t^{j+1} = (t-\alpha)t^j + \alpha t^j$ y por hipótesis de inducción t^j puede expresarse como una $\mathbb{F}$ combinación lineal de β_j, digamos $t^j = c_0 + c_1(t-\alpha) + \cdot + c_j(t-\alpha)^j$, sigue que

$$t^{j+1} = \alpha c_0 + (\alpha c_1 + c_0)(t-\alpha) + \ldots + (\alpha c_j + c_{j-1})(t-\alpha)^j + c_j(t-\alpha)^{j+1} .$$

En particular t^{j+1} puede escribirse como una $\mathbb{F}$ combinación lineal de β_{j+1}. Esto concluye la inducción.

Del párrafo anterior sigue que $\{(t-\alpha)^n : n \in \mathbb{N}\}$ es una base de $\mathbb{F}[t]$. Luego, $\{[(t-\alpha)^n]_I : n \in \{0, \ldots, m-1\}\} = \{[(t-\alpha)^n : n \in \mathbb{N}\}$ 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 $q_i(t-\alpha)^i]_I$ es estrictamente menor que m. Sigue que existe $q \in \mathbb{F}[t]$ tal que

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

Como los polinomios a la izquierda y la derecha de la anterior igualdad son de grado menor que m y 0 o m respectivamente, necesariamente se debe tener que $q_0 = \ldots = q_{m-1} = q = 0$. 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 $[L]_{\beta',\beta'} = [\varphi^{-1} \circ L \circ \varphi]$ donde $\beta' = \varphi(\beta)$.