MA-31A Elementos de Álgebra **18 de Octubre, 2003**

Pauta Control 2

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

Problema 1:

(i).- Es evidente que $X \subseteq \langle X \rangle$. Como la intersección de grupos abelianos se sabe es también grupo abeliano, sigue que $\langle X \rangle$ debe ser grupo abeliano.

Sea entonces $x \in \langle X \rangle$ y $r \in R$. Sigue que $x \in L$ para todo R-cuasi-módulo L que contenga a X, i.e., $r \cdot x \in L$ para todos los L con las propiedades recién mencionadas. Luego, $r \cdot x \in \langle X \rangle$. Verificar que $\langle X \rangle$ cumple todas las otras propiedades de un R-cuasi-módulo se establece de forma análoga.

(ii).- Sea W un R-módulo. Supongamos que $W \neq \langle 0 \rangle$. Luego, existe $w \in W$, $w \neq 0$. Sigue que $0 \neq w \in \langle w \rangle$. Por lo tanto $\langle w \rangle \neq \{0\}$. Como M es simple se concluye que $W = \langle w \rangle$, es decir, W es cíclico.

(iii).- Supongamos que $r \cdot m \neq 0$ para algún $r \in R$ y $m \in M$. Sigue que $0 \neq r \cdot m \in \langle r \cdot m \rangle$, i.e., $\langle r \cdot m \rangle \neq \{0\}$. Como M es simple se concluye que $\langle r \cdot m \rangle = M$, o sea, M es cíclico.

(iv).- Como $r \cdot m \neq 0$ por (ii) tenemos que M es cíclico. Digamos, $M = \langle m' \rangle$ para algún $m' \in M$. Si $T(m') = 0$, entonces $T(r \cdot m') = r \cdot T(m') = r \cdot 0 = 0$ para todo $r \in R$.[1] Sigue que $T(m) = 0$ para todo $m \in M$, i.e., $T(M) = \{0\}$. Supongamos entonces que $T(m') \neq 0$. Luego $0 \neq T(m') \in \langle T(m') \rangle$. Sigue que $\{0\} \neq \langle T(m') \rangle \subseteq M$. Como M es simple se concluye que $\langle T(m') \rangle = M$. Luego $T(M) = T(\langle m' \rangle) = \langle T(m') \rangle = M$, i.e., T es epiyectiva.

Queda establecer que T es inyectiva. Para ello, basta determinar que el núcleo de T es $\{0\}$. En efecto, es fácil ver que el núcleo de T es un cuasi-submódulo de M que no contiene a m'. Luego, como M es simple, el núcleo de T debe ser igual a $\langle 0 \rangle = \{0\}$, i.e., T es inyectiva.

(v).- Basta considerar para la suma la adición usual de funciones y para la multiplicación la composición de funciones.

Para establecer que bajo las hipótesis del Lema de Schur se tiene que $\mathcal{L}(M)$ es un

[1] Aquí hemos usado los siguientes hechos facilmente demostrables; (1) para todo R-morfismo T entre R-cuasi-módulos $T(0) = 0$, y (2) en un R-cuasi-módulo $r \cdot 0 = 0$ para todo $r \in R$.

anillo de división basta ver que $T \in \mathcal{L}(M)$, $T \neq 0$, es invertible (puesto que $T = 0$ es el neutro aditivo en $\mathcal{L}(M)$). En efecto, por (iv) y dado que $T \neq 0$, se tiene que T es un isomorfismo, luego invertible con inverso en $\mathcal{L}(M)$.

Problema 2:

(i).- Sea I un ideal en R que es además un R-módulo libre. Sea B base de I. Como $I \neq (0)$, entonces $B \not\subseteq \{0\}$. Supongamos que existiesen $b_0, b_1 \in B$, $b_0 \neq b_1$, no nulos. Entonces, para $\alpha_0 = b_1$ y $\alpha_1 = -b_0$ tendríamos que $\alpha_0 b_0 + \alpha_1 b_1 = 0$ y $\alpha_0, \alpha_1 \neq 0$, i.e., $\{b_0, b_1\}$ es linealmente dependiente. Sigue que B debe tener un sólo elemento no nulo, digamos r. Tenemos entonces que $I = (r)$. Si r fuese divisor de cero, entonces B no sería linealmente independiente, contradiciendo el hecho que B es base. Se concluye que I es un ideal principal generado por un elemento que no es divisor de cero.

Para establecer el converso, recordar que un ideal I de R es un R-módulo. Supongamos que I fuese ideal principal generado por un r que no es divisor de cero. Para concluir que I es un R-módulo libre bastará verificar que $\{r\}$ es base de I. En efecto $\{r\}$ claramente genera I. Si $\rho r = 0$ para algún $\rho \in R$, como r no es divisor de cero, necesariamente se tiene que $\rho = 0$, i.e., $\{r\}$ es linealmente independiente. Esto concluye la demostración de que $\{r\}$ es base de I.

Finalmente, sea I el ideal en $R = \mathbb{C}[x, y]$ generado por $\{x, y\}$. Por la equivalencia recién establecida bastará probar que I no es un ideal principal generado por un elemento que no es divisor de cero. En efecto, supongamos que $I = (r)$. Como $r \in I \subseteq R = \mathbb{C}[x, y]$ y R no posee divisores de cero, entonces r no puede ser un divisor de cero. Como $x, y \in I$, deben existir $P, Q \in \mathbb{C}[x, y]$ tales que $x = P(x, y)r(x, y)$ e $y = Q(x, y)r(x, y)$. Es fácil ver que la existencia de tales P y Q implican que $r \in \mathbb{C}$. Luego $r \in \mathbb{C} \cap I$. Pero esto es absurdo pues $\mathbb{C} \cap I = \emptyset$.

(ii).- Sean $u, r \in R$ no nulos tales que $ru = 0$. Como (u) es finitamente generado, existe por hipótesis $B \subseteq (u)$ base de (u). Es fácil ver que $B = \{b\}$ para algún elemento $b \neq 0$. Sea entonces $\beta \in R$ tal que $b = \beta u$. Sigue que $rb = r(\beta u) = \beta(ru) = 0$. Pero como $\{b\}$ es base, debemos tener que $r = 0$, contradicción.

(iii.1).- Es fácil ver que $\{2\}$ es una familia linealmente independiente que no genera $\mathbb{Z}$. De cualquier forma que se extienda esta familia de manera de generar todo $\mathbb{Z}$ se obtendrá una familia linealmente dependiente, y por lo tanto no cumplirá los requisitos para ser base.

(iii.2).- La afirmación es falsa. Veamos un contraejemplo. Como $(\mathbb{Z}^2, +)$ es grupo abeliano, entonces es un $\mathbb{Z}$-módulo. Además es fácil convencerse que tiene dimensión 2. En el mencionado módulo, $\{(2, 0)\}$ es linealmente independiente y no puede ser extendido a una base de $\mathbb{Z}^2$. En efecto, supongamos que $B = \{(2,0),(a,b)\}$ es base de $\mathbb{Z}^2$. Como $(1,1)$ debe poder expresarse como combinación lineal de los elementos en B, sigue inmediatamente que $b = \pm 1$. Supongamos sin pérdida de generalidad que $b = 1$. Consideremos entonces el elemento $(1,2)$ y supongamos que existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$\alpha(2,0) + \beta(a,1) = (1,2)\,.$$

Igualando coordenadas se tiene que $\beta = 2$ y que $1 = 2\alpha + 2a$, i.e., que 1 es par, un absurdo.