Ma31a Elementos de Álgebra **24 de Octubre de 2008**

Pauta Control 2

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

PROBLEMA 1:

(i.1).- Sabemos que los ideales de $\mathbb{Z}$ son $n\mathbb{Z}$ con $n \in \mathbb{N}$, $n \neq 1$. Si $n \geq 2$ no es primo, entonces existen $a,b \in \mathbb{N}$, $a,b > 1$ tales que $n = a \cdot b$. Como $a,b \notin n\mathbb{Z}$, sigue que $n\mathbb{Z}$ no es ideal primo. Luego, los únicos candidatos a ideales primos de $\mathbb{Z}$ son $\{0\}$ y $p\mathbb{Z}$ con p primo. Claramente $\{0\}$ es ideal primo. Sea entonces p un primo y $ab \in p\mathbb{Z}$. Sigue que $p|ab$. Por primalidad de p tenemos que $p|a$ o $p|b$, i.e. $a \in p\mathbb{Z}$ o $b \in p\mathbb{Z}$. Concluimos que los ideales primos de $\mathbb{Z}$ son $\{0\}$ y $p\mathbb{Z}$ con p primo.

(i.2).- Sea P ideal primo de R. Sean $[a]_P, [b]_P \in R/P$ tales que $[a]_P[b]_P = P$. Sigue que $P = (a+P)(b+P) = ab + aP + Pb + P$. Pero como P es ideal, se tiene que $aP, bP \subseteq P$. Se concluye que $ab \in P$. Como P es ideal primo, sigue que $a \in P$ o $b \in P$, i.e. $[a]_P = P$ o $[b]_P = P$. Por lo tanto, R/P es dominio de integridad.

Supongamos ahora que R/P es dominio de integridad y que $ab \in P$. Sigue que $P = [ab]_P = [a]_P[b]_P$. Pero como R/P es dominio de integridad, se debe tener que $[a]_P = P$ o $[b]_P = P$, i.e. $a \in P$ o $b \in P$. Por lo tanto, P es ideal primo.

(ii).- Sea I el ideal generado por $\{a,b\}$. Como R es un dominio de integridad principal, sigue que existe $c \in R$ tal que $I = (c)$. Por caracterización de ideal generado, se tiene que existen $s,t \in R$ tales que $sa + tb = c$. Afirmamos que c es un máximo común divisor de a y b. En efecto, $a,b \in I = (c)$ implica que $c|a$ y $c|b$. Además, si $c' \in R$ es tal que $c'|a$ y $c'|b$, sigue que $c'|(sa+tb) = c$. Por lo tanto, c es un máximo común divisor de a y b.

(iii.1).- Supongamos que W es un submódulo de V que no es finitamente generado. Sigue que W no es vacío. Sea $w_1 \in W \setminus \{0\}$. Como W no es finitamente generado, w_1 no genera W. Luego, existe w_2 en $W \setminus \langle\{w_1\}\rangle_R$. Como W no es finitamente generado, $\{w_1, w_2\}$ no genera W. Luego, existe w_3 en $W \setminus \langle\{w_1,w_2\}\rangle_R$, ... y así sucesivamente. Si definimos $W_i = \langle\{w_1,\ldots,w_i\}\rangle_R$, entonces tenemos que $W_1 \subsetneq W_2 \subsetneq W_3 \subsetneq \ldots$ es una cadena creciente infinita de submódulos en V.

Veamos ahora que el converso se tiene. Supongamos que todo submódulo de V es finitamente generado y que existe una cadena creciente infinita $W_1 \subsetneq W_2 \subsetneq W_3 \subsetneq \ldots$ de submódulos de V. Sea U la unión de todos los W_i's. Es fácil ver que U es submódulo de V, y por lo tanto es finitamente generado, digamos por $\{u_1,\ldots,u_r\}$. Pero por definición de U y dado que $\{u_1,\ldots,u_r\}$ está contenido en U, debe existir un i tal que $\{u_1,\ldots,u_r\} \subseteq W_i$. Sigue que $U = W_i = W_{i+1} = \ldots$ y que la cadena de los W_i's no es creciente.

(iii.2).- Sea I un ideal (no degenerado) de R que no está contenido en un ideal maximal. Como $I_1 = I$ no está contenido en un ideal maximal, entonces esta estrictamente contenido en un ideal no degeneraod I_2. Si I_2 no está contenido en un ideal maximal, entonces esta estrictamente contenido en un ideal no degenerado I_3, ... y así sucesivamente. Sigue que $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$ es una cadena creciente de ideales de R. Como todo ideal de R es un R-submódulo de R y todo submódulo de R es finitamente generado (porque R es noetheriano), la cadena creciente debe ser finita. Sigue que I está contenido en I_k ideal maximal para algún k.

(iv).- Supongamos $\{u_1,\ldots,u_k\}$ genera el $\mathrm{Ker}(\varphi)$ y que $\{w_1,\ldots,w_\ell\}$ genera $\mathrm{Im}(\varphi)$. Como $w_i\in\mathrm{Im}(\varphi)$, existen $v_1,\ldots,v_\ell\in V$ tales que $\varphi(v_i)=w_i$. Afirmamos que $\{u_1,\ldots,u_m,v_1,\ldots,v_\ell\}$ generan V. En efecto, sea $v\in V$ cualquiera. Como $\varphi(v)$ está en $\mathrm{Im}(\varphi)$, sigue que existen $b_1,\ldots,b_\ell\in R$ tales que

$$\varphi(v)=b_1\cdot w_1+\ldots b_\ell\cdot w_\ell=\varphi(b_1\cdot v_1+\ldots b_\ell\cdot v_\ell)\,.$$

Sea $v'=b_1\cdot v_1+\ldots+b_\ell\cdot v_\ell$. Sigue que $v-v'\in\mathrm{Ker}(\varphi)$. Luego, existen $a_1,\ldots,a_k\in R$ tales que

$$v-v'=a_1\cdot u_1+\ldots+a_k\cdot u_k\,.$$

Despejando obtenemos que $v=a_1\cdot u_1+\ldots+a_k\cdot u_k+b_1\cdot w_1+\ldots b_\ell\cdot w_\ell$. Se concluye que $\{u_1,\ldots,u_k,v_1,\ldots,v_\ell\}$ genera V.

PROBLEMA 2:

(i).- Como $M=m_0\mathbb{F}[x]$, sigue que M es finitamente generado. Como $\mathbb{F}[x]$ es un dominio de integridad principal y los resultados vistos de caracterización de R-módulos finitiamente generados con R dominio de integridad principal, tenemos que existen $\delta_1|\delta_2|\ldots|\delta_k$, con $\delta_1,\ldots,\delta_k\in\mathbb{F}[x]$ y $\delta_1\not\sim 1$, tales que

$$M\quad\cong\quad\mathbb{F}[x]/(\delta_1(x))\oplus\ldots\oplus\mathbb{F}[x]/(\delta_k(x))\oplus F\,,$$

con F un $\mathbb{F}[x]$-módulo libre. Como M es de torsión, sabemos que $F=\{0\}$. Pero $\mathbb{F}[x]/(\delta_1(x))\oplus\ldots\oplus\mathbb{F}[x]/(\delta_k(x))$ es cíclico sólo si $k=1$. Lueo, si $\alpha\in\mathbb{F}$ denota el coeficiente de δ_1 que acompaña al termino de mayor grado, concluimos que existe $\delta=\delta_1/\alpha$ polinomio mónico tal que $M\cong\mathbb{F}[x]/(\delta(x))$.

(ii).- Sea $m\in M$ tal que $m=p(x)m_0$ con $p(x)\in\mathbb{F}[x]$. Por Teorema de la División, existen $q,r\in\mathbb{F}[x]$ tales que $p=q\cdot\delta+r$ con $\mathrm{grado}(r)<\mathrm{grado}(\delta)=n$. Sigue que $m=p(x)m_0=[q(x)\circ\delta(x)+r(x)](m_0)$. Pero $\delta(x)m_0=0$ (para ver esto último, notar que si φ es el isomorfismo entre los $\mathbb{F}[x]$-módulos M y $\mathbb{F}[x]/(\delta(x))$, entonces $\varphi(\delta(x)m_0)=\delta(x)\varphi(m_0)=0$ en $\mathbb{F}[x]/(\delta(x))$, y como φ es isomorfismo se concluye que $\delta(x)m_0=0$ en M).

Luego, sin pérdida de generalidad podemos asumir que $p(x)$ tiene grado menor que n. Sigue que $m=p(x)m=\sum_{i=0}^{n-1}p_iT^i(m_0)$ por lo que $m\in\langle\{m_0,T(m_0),\ldots,T^{n-1}(m_0)\}\rangle_{\mathbb{F}}$, i.e. M está generado por $\beta=\{m_0,T(m_0),T^2(m_0),\ldots,T^{n-1}(m_0)\}$.

(iii).- Sean $\lambda_0,\lambda_1,\ldots,\lambda_{n-1}\in\mathbb{F}$ tales que $\lambda_0m_0+\lambda_1T(m_0)+\ldots+\lambda_{n-1}T^{n-1}(m_0)=0$. Definimos $p(x)=\lambda_0+\lambda_1x+\ldots+\lambda_{n-1}x^{n-1}\in\mathbb{F}[x]$. Notar en particular que $p(x)m_0=0$. Como $M=m_0\mathbb{F}[x]$, sigue que $p(x)M=\{0\}$. Como $M\cong\mathbb{F}[x]/(\delta(x))$, necesariamente se debe tener $\delta(x)|p(x)$. Pero $\mathrm{grado}(p)<\mathrm{grado}(\delta)$, luego $p(x)=0$ en $\mathbb{F}[x]$, i.e. $\lambda_0=\lambda_1=\ldots=\lambda_{n-1}=0$. Hemos concluido que β es una familia linealmente independiente en M como $\mathbb{F}$-espacio vectorial.

(iv).- Sea $v_i=T^i(m_0)$ con $i=0,\ldots,n-1$. Como ya se ha indicado, $\delta(x)m_0=0$. Luego, $\delta(T)m_0=0$, o equivalentemente

$$T(v_{n-1})\;=\;T^n(m_0)\;=\;-c_0\cdot m_0-c_1\cdot T(m_0)-\ldots-c_{n-1}\cdot T^{n-1}(m_0)\,.$$

Luego,

$$\begin{array}{rcrcrcrcrcccr}
T(v_0) & = & - & 0\cdot v_0 & + & 1\cdot v_1 & + & 0\cdot v_2 & + & \ldots & + & 0\cdot v_{n-1}\,, \\
T(v_1) & = & - & 0\cdot v_0 & + & 0\cdot v_1 & + & 1\cdot v_2 & + & \ldots & + & 0\cdot v_{n-1}\,, \\
 & \vdots & & & & & & & & & & \\
T(v_{n-2}) & = & - & 0\cdot v_0 & + & 0\cdot v_1 & + & 0\cdot v_2 & + & \ldots & + & 1\cdot v_{n-1}\,, \\
T(v_{n-1}) & = & - & c_0\cdot v_0 & - & c_1\cdot v_1 & - & c_2\cdot v_2 & - & \ldots & - & c_{n-1}\cdot v_{n-1}\,.
\end{array}$$

Sigue que

$$[T]_{\beta,\beta} \quad = \quad \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & 0 & -c_1 \\ 0 & 1 & & 0 & 0 & -c_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ 0 & 0 & & 1 & 0 & -c_{n-2} \\ 0 & 0 & \dots & 0 & 1 & -c_{n-1} \end{pmatrix}.$$