



UNIVERSIDAD COMPLUTENSE



5320646839

51
REU

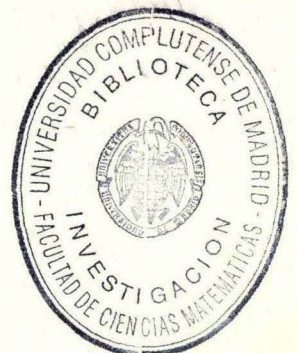
PUBLICACIONES DE LA SECCION DE MATEMATICA
DE LA UNIVERSIDAD DE MADRID

DONATIVO

ACTAS
DE LA
PRIMERA REUNION ANUAL
DE MATEMATICOS ESPAÑOLES

EN COLABORACION CON EL INSTITUTO
«JORGE JUAN» DEL CONSEJO SUPERIOR
DE INVESTIGACIONES CIENTIFICAS

R-61.311



MADRID

1961

UN LEMA SOBRE MODULOS

por

PEDRO ABELLANAS

1. Introducción.

Sea \mathfrak{M} un módulo libre con base finita sobre el anillo $A = k[x]$ de polinomios con una variable sobre un cuerpo de coeficientes, k , arbitrario.

Si \mathbf{x}^* e \mathbf{y}^* son homomorfismos de \mathfrak{M} en A y \mathbf{x} un elemento arbitrario de \mathfrak{M} , se define:

$$\text{I. } (\mathbf{x}^* + \mathbf{y}^*) \mathbf{x} = \mathbf{x}^* \mathbf{x} + \mathbf{y}^* \mathbf{x}.$$

Si $f(x)$ es un polinomio arbitrario de A se define:

$$\text{II. } (f(x) \mathbf{x}^*) \mathbf{x} = f(x) [\mathbf{x}^* \mathbf{x}].$$

Respecto de estas definiciones el conjunto \mathfrak{M}^* de todos los homomorfismos de \mathfrak{M} sobre k es otro módulo libre sobre A , llamado *dual* del módulo \mathfrak{M} .

Si

$$(1) \quad \mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$$

es una base de \mathfrak{M} , los homomorfismos:

$$(2) \quad \mathcal{B}^* = \{\mathbf{u}_1^*, \dots, \mathbf{u}_n^*\},$$

definidos por

$$(3) \quad \mathbf{u}_i^* \mathbf{u}_j = \delta_{ij},$$

en donde las δ_{ij} son las δ de Kronecker, constituyen una base de \mathfrak{M}^* , llamada *base dual* de la base \mathcal{B} de \mathfrak{M} .

Si \mathcal{L} es un submódulo de \mathfrak{M} y \mathbf{x}^* un homomorfismo arbitrario de \mathfrak{M} en A , se verifica [1] que $\mathbf{x}^* \mathcal{L}$ es un ideal de A .

2. Un lema.

LEMA. Si \mathbf{u}^* y \mathbf{v}^* son dos homomorfismos arbitrarios de \mathfrak{M}^* , se puede construir otro homomorfismo \mathbf{w}^* tal que se verifiquen las dos relaciones siguientes:

$$\mathbf{w}^* \mathcal{L} \supset \mathbf{u}^* \mathcal{L} \quad \text{y} \quad \mathbf{w}^* \mathcal{L} \supset \mathbf{v}^* \mathcal{L}.$$

DEMOSTRACIÓN. Por ser los ideales de $k[x]$ principales será:

$$(4) \quad \begin{cases} \mathbf{u}^* \mathcal{L} = A h, & \mathbf{v}^* \mathcal{L} = A l; \\ \mathbf{u}^* \mathbf{x} = h, & \mathbf{v}^* \mathbf{y} = l; \quad \mathbf{x}, \mathbf{y} \in \mathcal{L}. \end{cases}$$

Sea

$$A(d) = A(h, l), \quad d = ah + bl$$

y $h(x) = h_1(x)d(x)$, $l(x) = d(x)l_1(x)$; de donde $ah_1 + bl_1 = 1$.

Sean

$$(5) \quad \mathbf{x} = x_1 \mathbf{u}_1 + \dots + x_n \mathbf{u}_n \quad \text{e} \quad \mathbf{y} = y_1 \mathbf{u}_1 + \dots + y_n \mathbf{u}_n,$$

las expresiones de \mathbf{x} e \mathbf{y} mediante la base \mathcal{B} (1) y

$$(6) \quad \mathbf{u}^* = u_1 \mathbf{u}_1^* + \dots + u_n \mathbf{u}_n^*, \quad \mathbf{v}^* = v_1 \mathbf{u}_1^* + \dots + v_n \mathbf{u}_n^*,$$

las de \mathbf{u}^* y \mathbf{v}^* respecto de su base dual (2). Supongamos que $x_n \neq 0$ e $y_n \neq 0$, y sea

$$(7) \quad A(y_n x_1 - y_1 x_n, y_n x_2 - y_2 x_n, \dots, y_n x_{n-1} - y_{n-1} x_n) = A(\zeta).$$

1. Vamos a construir dos homomorfismos, \mathbf{w}_1^* y \mathbf{w}_2^* , que verifiquen las siguientes condiciones:

$$(8) \quad \mathbf{w}_1^* \mathbf{x} = \zeta, \quad \mathbf{w}_1^* \mathbf{y} = 0; \quad \mathbf{w}_2^* \mathbf{x} = 0, \quad \mathbf{w}_2^* \mathbf{y} = \zeta.$$

Sea

$$(9) \quad \mathbf{w}_i^* = \tau_{i1} \mathbf{u}_1^* + \dots + \tau_{in} \mathbf{u}_n^*; \tau_{ij} \in A; i = 1, 2; j = 1, \dots, n.$$

Las condiciones (8) dan lugar a las siguientes relaciones en A:

$$(10) \quad (a) \begin{cases} \tau_{1i} x_i = \zeta, \\ \tau_{1i} y_i = 0, \end{cases} \quad (b) \begin{cases} \tau_{2i} x_i = 0, \\ \tau_{2i} y_i = \zeta. \end{cases}$$

Poniendo

$$\tau_{ji} = \tau'_{ji} y_n; j = 1, 2; i = 1, \dots, n-1,$$

resulta que los sistemas (10) se transforman en los siguientes:

$$(11) \quad \begin{cases} (a) \begin{cases} \tau'_{1i} (y_n x_i - y_i x_n) = \zeta, \\ \tau'_{1n} = -\tau'_{1i} y_i, \end{cases} \\ (b) \begin{cases} \tau'_{2n} = -\tau'_{2i} x_i, \\ \tau'_{2i} (y_n x_i - y_i x_n) = \zeta; i = 1, \dots, n-1; \end{cases} \end{cases}$$

lo que prueba que:

$$(12) \quad \tau'_{1i} = \tau'_{2i}; i = 1, \dots, n-1,$$

son los polinomios solución de la ecuación

$$(13) \quad X_1 (y_n x_1 - y_1 x_n) + \dots + X_{n-1} (y_n x_{n-1} - y_{n-1} x_n) = \zeta.$$

Ecuación que tiene solución, perteneciente a $k[x]$, en virtud de (7).

Sea

$$(14) \quad \zeta = \varphi_1^{a_1} \dots \varphi_r^{a_r},$$

la descomposición de ζ en producto de potencias de polinomios primos, $\varphi_1, \dots, \varphi_r$, sobre $k[x]$. De (7) y (14) se deduce:

$$y_n x_i - y_i x_n \equiv 0 (A \varphi_1)$$

y llamando \bar{x}_i e \bar{y}_i a las clases de restos de x_i e y_i , respectivamente, respecto de A_{φ_1} , y teniendo presente que por ser A_{φ_1} ideal primo máximo es A/A_{φ_1} un cuerpo, de

$$\bar{y}_n \bar{x}_i - \bar{y}_i \bar{x}_n = \bar{0},$$

se deduce

$$(15) \quad \frac{\bar{x}_i}{\bar{y}_i} = \frac{\bar{x}_n}{\bar{y}_n} = \bar{a},$$

de donde

$$\bar{x}_i - \bar{a} \bar{y}_i = \bar{0}, \quad i = 1, \dots, n,$$

lo que da lugar a la relación:

$$(16) \quad x_i = a y_i + z_i \varphi_1, \quad i = 1, \dots, n, \quad a \equiv \bar{a} (A_{\varphi_1}).$$

Poniendo

$$\mathbf{z} = z_i \mathbf{u}_i,$$

las igualdades (16) dan lugar a la igualdad:

$$(17) \quad \mathbf{x} = a \mathbf{y} + \varphi_1 \mathbf{z},$$

de donde:

$$(18) \quad y_n x_i - y_i x_n = \varphi_1 (y_n z_i - y_i z_n).$$

Llevando (18) a (7) y teniendo en cuenta (14), resulta:

$$(19) \quad A (y_n z_1 - y_1 z_n, \dots, y_n z_{n-1} - y_{n-1} z_n) = A (\varphi_1^{a_1-1} \varphi_2^{a_2} \dots \varphi_r^{a_r}).$$

Supongamos demostrado que

$$(20) \quad \begin{cases} \mathbf{x} = (a + a_1 \varphi_1 + \dots + a_s \varphi_1^{a_1} \dots \varphi_i^{a_i} \varphi_{i+1}^{\gamma}) \mathbf{y} \\ \quad + \varphi_1^{a_1} \dots \varphi_i^{a_i} \varphi_{i+1}^{\gamma+1} \mathbf{t}, \quad \gamma < x_{i+1}, \mathbf{t} \in \mathfrak{M}, \end{cases}$$

siendo

$$(21) \quad \left\{ \begin{array}{l} A (y_n t_1 - y_1 t_n, \dots, y_n t_{n-1} - y_{n-1} t_n) \\ = A (\varphi_{i+1}^{\alpha_{i+1} - (\gamma+1)} \varphi_{i+2}^{\alpha_{i+2}} \dots \varphi_r^{\alpha_r}). \end{array} \right.$$

En virtud de (17) y (19) se puede construir un elemento $\mathbf{s} \in \mathfrak{M}$ tal que

$$(22) \quad \mathbf{t} = b \mathbf{y} + \varphi_{i+1} \mathbf{s},$$

en donde, si $\alpha_{i+1} = \gamma + 1$ figuraría φ_{i+2} en lugar de φ_{i+1} , siendo:

$$\begin{aligned} & A (y_n s_1 - y_1 s_n, \dots, y_n s_{n-1} - y_{n-1} s_n) \\ & = A (\varphi_{i+1}^{\alpha_{i+1} - (\gamma+2)} \varphi_{i+2}^{\alpha_{i+2}} \dots \varphi_r^{\alpha_r}). \end{aligned}$$

Por consiguiente, queda demostrado que se puede construir un elemento $\mathbf{q} \in \mathfrak{M}$, tal que:

$$(23) \quad \mathbf{x} = (a + a_1 \varphi_1 + \dots + a_m \varphi_1^{\alpha_1} \dots \varphi_{r-1}^{\alpha_{r-1}} \varphi_r^{\alpha_r - 1}) \mathbf{y} + \zeta \mathbf{q},$$

siendo

$$(24) \quad A (y_n q_1 - y_1 q_n, \dots, y_n q_{n-1} - y_{n-1} q_n) = A.$$

De (15) se obtiene:

$$\frac{\overline{y_i}}{\overline{x_i}} = \frac{\overline{y_n}}{\overline{x_n}} = \overline{b}, \quad \overline{b} = \overline{\alpha}^{-1},$$

de donde

$$\overline{y_i} - \overline{b} \overline{x_i} = \overline{0}, \quad i = 1, \dots, n,$$

y si $b \equiv \overline{b} (A \varphi_1)$,

$$(25) \quad y_i = b x_i + z'_i \varphi_1.$$

Procediendo a partir de (25) de modo análogo a como se ha procedido a partir de (17), se obtiene:

$$(26) \quad \mathbf{y} = (b + b_1 \varphi_1 + \dots + b_m \varphi_1^{a_1} \dots \varphi_{r-1}^{a_{r-1}} \varphi_r^{a_r-1}) \mathbf{x} + \zeta \mathbf{q}'$$

$$(27) \quad A(x_n q'_1 - x_1 q'_n, \dots, x_n q'_{n-1} - x_{n-1} q'_n) = A.$$

Poniendo

$$(28) \quad \begin{cases} p(x) = a + a_1 \varphi_1 + \dots + a_m \varphi_1^{a_1} \dots \varphi_{r-1}^{a_{r-1}} \varphi_r^{a_r-1}, \\ q(x) = b + b_1 \varphi_1 + \dots + b_m \varphi_1^{a_1} \dots \varphi_{r-1}^{a_{r-1}} \varphi_r^{a_r-1}, \end{cases}$$

se pueden escribir (23) y (26) del siguiente modo:

$$(29) \quad \mathbf{x} = p(x) \mathbf{y} + \zeta \mathbf{q}, \quad \mathbf{y} = q(x) \mathbf{x} + \zeta \mathbf{q}'.$$

De (24) se deduce que se pueden calcular los polinomios w'_{1i} , $i = 1, \dots, n-1$, de modo que

$$(30) \quad \tau'_{11}(y_n q_1 - y_1 q_n) + \dots + \tau'_{1n-1}(y_n q_{n-1} - y_{n-1} q_n) = 1.$$

Sea $\tau_{1i} = \tau'_{1i} y_n$, $i = 1, \dots, n-1$ y $\tau_{1n} = -\tau'_{1i} y_i$. De estas relaciones y de (30) se deduce que si

$$(31) \quad \mathbf{w}_1^* = \tau_{11} \mathbf{u}_1^* + \dots + \tau_{1n} \mathbf{u}_n^*,$$

se verifica que

$$(32) \quad \mathbf{w}_1^* \mathbf{q} = 1, \quad \mathbf{w}_1^* \mathbf{y} = 0,$$

y teniendo en cuenta (29):

$$(33) \quad \mathbf{w}_1^* \mathbf{x} = p(x) \mathbf{w}_1^* \mathbf{y} + \zeta \mathbf{w}_1^* \mathbf{q} = \zeta.$$

Análogamente, de (27) se deduce que se pueden calcular los polinomios w'_{2i} , $i = 1, \dots, n-1$, de modo que

$$w'_{21}(x_n q'_1 - x_1 q'_n) + \dots + w'_{2,n-1}(x_n q'_{n-1} - x_1 q'_n) = 1.$$

Poniendo

$$\tau w'_{2i} = \tau w'_{2i} x_n, \quad i = 1, \dots, n-1, \quad \tau w'_{2n} = -\tau w'_{2i} x_i, \quad \mathbf{w}_2^* = \tau w'_{2i} \mathbf{u}_i^*,$$

resulta que

$$(34) \quad \mathbf{w}_2^* \mathbf{y} = \zeta, \quad \mathbf{w}_2^* \mathbf{x} = \mathbf{0}.$$

Las expresiones (32), (33) y (34) demuestran la proposición 1.

Aplicando \mathbf{u}^* a (29) se obtiene:

$$(35) \quad \mathbf{u}^* \mathbf{x} = p(x) \mathbf{u}^* \mathbf{y} + \zeta \mathbf{u}^* \mathbf{q},$$

o bien, recordando que $\mathbf{u}^* \mathbf{x} = h$, y poniendo $\mathbf{u}^* \mathbf{y} = h_1(x)$, $\mathbf{u}^* \mathbf{q} = h_2(x)$:

$$(36) \quad h(x) = p(x) h_1(x) + \zeta h_2(x).$$

Sea el homomorfismo:

$$(37) \quad \mathbf{w}_3^* = p(x) \mathbf{u}^* + h_2(x) \mathbf{w}_2^*.$$

De (36) y (37) se deduce que:

$$(38) \quad \mathbf{w}_3^* \mathbf{y} = p(x) \mathbf{u}^* \mathbf{y} + h_2(x) \mathbf{w}_2^* \mathbf{y} = p(x) h_1(x) + h_2(x) \zeta = h(x).$$

2. El homomorfismo:

$$(39) \quad \mathbf{w}^* = a \mathbf{w}_3^* + b \mathbf{v}$$

cumple las condiciones del lema. En efecto:

$$(40) \quad \mathbf{w}^* \mathbf{y} = a \mathbf{w}_3^* \mathbf{y} + b \mathbf{v} \mathbf{y} = a(x) h(x) + b(x) l(x) = d(x),$$

de donde resulta que

$$d(x) \equiv \mathbf{0} (\mathbf{w}^* \mathcal{L}),$$

y como $d(x) \mid h(x)$ y $d(x) \mid l(x)$, resulta:

$$\mathfrak{u}^* \mathfrak{R} = A \mid h \subset A \mid d \subset \mathfrak{w}^* \mathfrak{R}, \quad \mathfrak{v}^* \mathfrak{R} = A \mid d \subset A \subset \mathfrak{w}^* \mathfrak{R}.$$

Q. E. D

De este lema se deduce inmediatamente que entre todos los ideales $\mathfrak{u}^* \mathfrak{R}$, cuando \mathfrak{u}^* recorre \mathfrak{M}^* existe uno máximo absoluto.

El ideal máximo absoluto $\mathfrak{u}_1^* \mathfrak{R} = A \mid f_1(x)$ determina de modo único el polinomio $f_1(x)$, siempre que se suponga éste normalizado de modo que el coeficiente del término de mayor grado sea la unidad. El polinomio $f_1(x)$, que está únicamente determinado por \mathfrak{R} , se llama el primer factor invariante (el último factor invariante) del submódulo \mathfrak{R} .

LITERATURA CITADA

- [1] N. BOURBAKI: *Algèbre*. Chap. VII. «Actualités scientifiques et industrielles», 1179 (1952).