

Álgebra II

PRIMER CUATRIMESTRE 2005

PRÁCTICA 3

1) *Propiedad universal del grupo asociado a un semigrupo conmutativo.*

Sea $(N, +)$ un semigrupo conmutativo, sea $G(N)$ el grupo asociado a N y sea $j : N \rightarrow G(N)$ (ver ejercicio 1 de la práctica 2). Probar que si G es un grupo y $f : N \rightarrow G$ es un morfismo de semigrupos, entonces existe un único morfismo $\bar{f} : G(N) \rightarrow G$ tal que $f = \bar{f} \circ j$.

2) *Propiedad universal del cuerpo de fracciones de un dominio.*

Sea A un dominio y $K(A)$ el cuerpo de fracciones de A (ver ejercicio 2 de la práctica 2). Sea $j : A \rightarrow K(A)$ definida por $j(a) =$ clase de $(a, 1)$. Probar que j es un morfismo de anillos y que si K es un cuerpo y $f : A \rightarrow K$ es un morfismo de anillos, entonces existe un único morfismo de cuerpos $\bar{f} : K(A) \rightarrow K$ tal que $f = \bar{f} \circ j$.

3) *Observación.*

En el ejercicio 7 de la práctica 2 se definió el álgebra del semigrupo S con coeficientes en un anillo A como un subanillo del anillo $A[[S]]$.

Observar que para definir el álgebra de semigrupo no es necesario pedir que para todo $s \in S$ el conjunto $\{(u, v) \in S \times S : u * v = s\}$ sea finito, ya que al ser los elementos de $A[S]$ funciones $\alpha : S \rightarrow A$ de soporte finito, dadas $\alpha, \beta \in A[S]$ el conjunto

$$\{(u, v) \in S \times S : u * v = s, \alpha(u) \neq 0, \beta(v) \neq 0\}$$

es finito.

Por ejemplo, el semigrupo $(\mathbb{Z}, +)$ (que es un grupo) no verifica esa propiedad.

Probar que si A es un anillo conmutativo, entonces $A[\mathbb{Z}]$ es isomorfo a $A[x, y]/(xy-1)$ (polinomios de Laurent con coeficientes en A).

Propiedad universal del álgebra de semigrupo.

Sea A un anillo $(S, *)$ un semigrupo y $A[S]$ el álgebra del semigrupo S con coeficientes en A (ver ejercicio 7 de la práctica 2 y ejercicio 3 de esta práctica). Sea B un anillo. Es equivalente dar:

- i) Un morfismo de anillos $f : A[S] \rightarrow B$
- ii) Un morfismo de anillos $f_A : A \rightarrow B$ y un morfismo de semigrupos $f_S : S \rightarrow B$ (donde B es un semigrupo con la operación de multiplicación del anillo).

Explicitar el caso en que $S = \mathbb{N}^r$ y deducir la propiedad universal del álgebra de polinomios en r variables con coeficientes en A (ejercicio 4 de esta práctica).

4) a) *Propiedad universal del álgebra de polinomios.*

Sea A un anillo conmutativo y $A \rightarrow B$ una A -álgebra conmutativa. Verificar que dar un morfismo de A -álgebras $A[x] \rightarrow B$ es equivalente a dar un elemento

$b \in B$ (el morfismo correspondiente a $b \in B$ se denomina especialización en b). Generalización al caso de morfismos $A[x_1, \dots, x_m] \rightarrow B$: existe una biyección canónica $\text{Hom}_{A\text{-alg}}(A[x_1, \dots, x_m], B) \cong B^m$.

- b) Para $f \in A[x]$, verificar que dar un morfismo de A -álgebras $A[x]/\langle f \rangle \rightarrow B$ es equivalente a dar una solución $b \in B$ de la ecuación $f(x) = 0$. Generalizar al caso de varias ecuaciones en varias variables $f_1, \dots, f_r \in A[x_1, \dots, x_m]$. Reflexionar sobre los ejemplos $B = A$, $B = A[t]$, $B = A[[t]]$, $A = \mathbb{R} \subset B = \mathbb{C}$, etc.

5) *Módulos sobre $A[S]$.*

Sea A un anillo, S un semigrupo, $(M, +)$ un grupo abeliano. Es equivalente dar:

- Una estructura de $A[S]$ -módulo en M .
 - Una estructura de A -módulo en M , más un morfismo de semigrupos de S en $\text{End}_A(M)$ (endomorfismos del A -módulo M , visto como semigrupo con operación de composición).
- 6) Sea A un anillo conmutativo y $\alpha \in M(n \times m, A)$ una matriz $n \times m$ con coeficientes en A . Verificar que la aplicación $a : A^m \rightarrow A^n$ definida por $a(x) = \alpha \cdot x$ (producto de matrices, identificando A^m con $M(m \times 1, A)$) es un morfismo de A -módulos. Dar un sistema finito de generadores de $\text{im}(a)$. Probar que el conjunto $S = \{x \in A^m / \alpha \cdot x = 0\}$ de soluciones del sistema de ecuaciones lineales homogéneas definido por α , es un A -submódulo de A^m . ¿Es todo submódulo de A^m de esta forma?
- 7) Sea A un anillo conmutativo y M un A -módulo. Para los siguientes morfismos de A -módulos, calcular núcleo e imagen y determinar cuáles morfismos son monomorfismo, epimorfismo, sección, retracción, isomorfismo.

- $f : M^n \rightarrow M^2$, $f(x) = (x_1 + x_n, x_n)$
- $f : M^n \rightarrow M^n$, $f(x) = (\sum_{1 \leq i \leq j} x_i)_{1 \leq j \leq n}$
- si $n \leq m$, $f : M^n \rightarrow M^m$, $f(x) = (x_1, \dots, x_n, 0, \dots, 0)$
- si $n \leq m$, $f : M^m \rightarrow M^n$, $f(x) = (x_1, \dots, x_n)$
- si $z \in M^n$, $f : A^n \rightarrow M$, $f(x) = \sum_{1 \leq i \leq n} x_i \cdot z_i$
- si $z \in A^n$, $f : M^n \rightarrow M$, $f(x) = \sum_{1 \leq i \leq n} z_i \cdot x_i$
- para $a \in A$, $e_a : A[x] \rightarrow A$, $e_a(\sum_i a_i \cdot x^i) = \sum_i a_i \cdot a^i$
- $d : A[x] \rightarrow A[x]$, $d(\sum_i a_i \cdot x^i) = \sum_i a_i \cdot i x^{i-1}$. El morfismo d tiene las propiedades adicionales $d(p \cdot q) = d(p) \cdot q + p \cdot d(q)$ y $d(a \cdot x^0) = 0$
- $\text{tr} : M(n \times n, A) \rightarrow A$, $\text{tr}(a) = \sum_{1 \leq j \leq n} a_{jj}$ (morfismo traza)
- $\text{dg} : M(n \times n, A) \rightarrow A^n$, $\text{dg}(a) = (a_{11}, a_{22}, \dots, a_{nn})$
- $\Delta : A \rightarrow A^J$, $\Delta(a)_j = a, \forall j \in J$. (morfismo diagonal)
- si $J \subset I$, $\rho : M^I \rightarrow M^J$, $\rho(\alpha) = \alpha|_J$.

- 8) Verificar que las siguientes aplicaciones son morfismos de \mathbb{Z} -módulos. Calcular núcleo e imagen.

- a) $f : (\mathbb{R}, +) \rightarrow (\mathbb{C} - \{0\}, \cdot), f(x) = e^{2\pi i x}$
- b) $f : (\mathbb{C} - \{0\}, \cdot) \rightarrow (\mathbb{R}_{>0}, \cdot), f(x) = |x|$
- c) $(n \in \mathbb{N}), f_n : (\mathbb{C} - \{0\}, \cdot) \rightarrow (\mathbb{C} - \{0\}, \cdot), f_n(x) = x^n$
- 9) a) Si f y g son endomorfismos de la estructura aditiva de \mathbb{Q} , son equivalentes las siguientes condiciones:
- b) a) $f(1) = g(1)$
- b) $f|_{\mathbb{Z}} = g|_{\mathbb{Z}}$
- c) $f = g$
- Deducir que un endomorfismo de la estructura aditiva de \mathbb{Q} satisface $f(1) = 1$ si y solo si $f = \text{id}_{\mathbb{Q}}$.
- c) Si V y W son \mathbb{Q} -espacios vectoriales, una aplicación $f : V \rightarrow W$ es morfismo de \mathbb{Q} -espacios vectoriales si y solo si es morfismo de grupos.
- 10) a) Sea A un anillo y $f : M \rightarrow N$ un morfismo de A -módulos.
- b) a) Si M es simple entonces $f = 0$ o f es un monomorfismo.
(Def.: un A -módulo M es simple si sus únicos submódulos son $\{0\}$ y M)
- b) Si N es simple entonces $f = 0$ o f es un epimorfismo.
- c) Si M y N son simples entonces $f = 0$ o f es un isomorfismo.
- d) Probar que para un A -módulo M , el grupo aditivo $\text{End}_A(M) = \text{Hom}_A(M, M)$ con la operación de composición constituye un anillo. Si M es simple entonces $\text{End}_A(M)$ es un anillo de división.
- c) Si I y J son conjuntos coordinables (existe una biyección $I \rightarrow J$) entonces M^I y M^J son isomorfos, para todo A -módulo M .
- d) Una involución de un A -módulo M es un morfismo $f : M \rightarrow M$ tal que $f^2 = \text{id}_M$. Toda involución es un automorfismo. Exhibir ejemplos de involución.
- e) Un proyector de un A -módulo M es un morfismo $f : M \rightarrow M$ tal que $f^2 = f$. Probar que $M \cong \ker(f) \oplus \text{im}(f)$. Probar que, reciprocamente, si A y B son submódulos de M tales que $M \cong A \oplus B$ entonces existe un único proyector $f : M \rightarrow M$ tal que $A = \ker(f)$ y $B = \text{im}(f)$.
- 11) a) El morfismo $\text{tr} : M(n \times n, A) \rightarrow A, \text{tr}(a) = \sum_{1 \leq j \leq n} a_{jj}$ satisface
- a) $\text{tr}(e) = n, 1$ (e denota la matriz identidad)
- b) $\text{tr}(a.b) = \text{tr}(b.a)$ (A conmutativo)
- b) Si A es un anillo conmutativo tal que $m.a = 0$ implica $a = 0$ o $m = 0$ ($a \in A, m \in \mathbb{Z}$) entonces tr es el único morfismo $M(n \times n, A) \rightarrow A$ que satisface i) y ii).
- c) Sea A como en b) y $n > 1$. Probar que no existe ningún epimorfismo $f : M(n \times n, A) \rightarrow A$ tal que $f(a.b) = f(a).f(b), \forall a, b$.
- 12) Sea A un anillo conmutativo.
- a) Para cada A -módulo M definir un isomorfismo de A -módulos $\text{Hom}_A(A, M) \cong M$.

- b) $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}) \cong \mathbb{Q}$, $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$, $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}) \cong \mathbb{Q}$.
- c) Dado un A -módulo M , se llama dual de M al A -módulo $M^* = \text{Hom}_A(M, A)$. La aplicación $c_M : M \rightarrow M^{**}$ definida por $c_M(m)(f) = f(m)$ (para $m \in M, f \in M^*$) es un morfismo de A -módulos y $\ker(c_M) = \bigcap_{f \in M^*} \ker(f)$.
- 13) Sea A un dominio de integridad. Demostrar que si $A^n \cong A^m$ entonces $m = n$.
- 14) Sea A un dominio de integridad y $a \in M(n \times n, A)$. Denotemos $v_j = (a_{ij})_{1 \leq i \leq n} \in A^n$ la j -ésima columna de a . Demostrar:
- a) v_1, \dots, v_n son linealmente independientes si y solo si $\det(a) \neq 0$.
- b) v_1, \dots, v_n generan A^n si y solo si $\det(a)$ es una unidad de A .
- c) dar criterios de independencia lineal y generación para $v_1, \dots, v_m \in A^n$.
(Definición: para $a \in M(n \times n, A)$, $\det(a) = \sum_{\sigma \in \mathbb{S}_n} \text{sg}(\sigma) \prod_{i=1}^n a_{i\sigma(i)}$)
- 15) Sea M un A -módulo. Si H y K son submódulos de M , denotamos $H + K = \{h + k, h \in H, k \in K\}$. Verificar que el conjunto de submódulos de M con la operación $+$ es un semigrupo conmutativo. El único elemento inversible es $\{0\}$.
- 16) Si X e Y son conjuntos y $f : X \rightarrow Y$ es una función, el conjunto $\Gamma(f) = \{(x, f(x)), x \in X\} \subset X \times Y$ se llama el grafo de f . Supongamos que X e Y son A -módulos. Demostrar que f es un morfismo de A -módulos si y solo si $\Gamma(f) \subset X \times Y$ es un submódulo.
- 17) a) Determinar los subgrupos de \mathbb{Z} .
- b) Determinar los ideales de $K[x]$, donde K es un cuerpo.
- 18) Sea M un A -módulo. Se llama anulador del subconjunto $S \subset M$ a $\text{An}(S) = \{a \in A/a.s = 0, \forall s \in S\}$. Si $x \in M$, $\text{An}(\{x\})$ será indicado -por abuso de notación- $\text{An}(x)$.
 M se dice un A -módulo fiel si $\text{An}(M) = 0$.
- a) $\text{An}(S)$ es un ideal a izquierda de A .
- b) $\text{An}(S) = A$ sii $S \subset \{0\}$.
- c) $\text{An}(\bigcup_{j \in J} S_j) = \bigcap_{j \in J} \text{An}(S_j)$.
- d) $\text{An}(S) = \bigcap_{s \in S} \text{An}(s)$.
- e) Si $S \subset T$ entonces $\text{An}(T) \subset \text{An}(S)$.
- f) Si $S \subset M$ es A -estable entonces $\text{An}(S)$ es un ideal bilátero de A .
- g) $M(n \times n, A)$ es un A -módulo fiel. Exhibir otros ejemplos de módulo fiel.
- h) $\text{An}(M^J) = \text{An}(M^{(J)}) = \text{An}(M)$ si $J \neq \emptyset$.
- 19) Sea M un A -módulo. Si $S \subset M$ es un subconjunto y $N \subset M$ es un submódulo, se llama transportador de S en N a $(N : S) = \{a \in A/a.s \in N, \forall s \in S\}$.
Si $x \in M$, $(N : \{x\})$ será indicado -por abuso de notación- $(N : x)$.

- a) $(N : S)$ es un ideal a izquierda de A .
 - b) $(0 : S) = \text{An}(S)$.
 - c) $(N : S) = A$ sii $S \subset N$.
 - d) $(N : \bigcup_{j \in J} S_j) = \bigcap_{j \in J} (N : S_j)$.
 - e) Si $S \subset T$ entonces $(N : T) \subset (N : S)$.
 - f) $(N^J : M^J) = (N^{(J)} : M^{(J)}) = (N : M)$ si $J \neq \emptyset$.
 - g) Si $S \subset M$ es A -estable entonces $(N : S)$ es un ideal bilátero de A .
 - h) $(\bigcap_{j \in J} N_j : S) = \bigcap_{j \in J} (N_j : S)$.
 - i) si $N \subset P$ entonces $(N : S) \subset (P : S)$.
 - j) $(N : x).x = N \cap A.x$.
 - k) Si A es conmutativo y I, J son ideales de A , existe un isomorfismo natural de A -módulos $(I : J)/I \cong \text{Hom}_A(A/J, A/I)$.
- 20) Sea M un A -módulo. Caracterizar el módulo cociente N/S en cada uno de los siguientes casos:
- a) $N = M^n, n \in \mathbb{N}, S = \{x \in N / \sum_{i=1}^n x_i = 0\}$.
 - b) $N = M^n, n > 2, S = \{x \in N / x_1 = x_n, x_2 = 0\}$.
 - c) $N = A[x], S = \{x \in N / x(c) = 0\} (c \in A)$.
 - d) $N = M(n \times n, A), S = \{x \in N / \text{dg}(x) = 0\}$.
 - e) $N = M(n \times n, A), S = \{x \in N / \text{tr}(x) = 0\}$.
 - f) $N = M^J, S = \{x \in N / x_i = 0 \ \forall i \in I\} (I \subset J)$.
- 21) a) Establecer los siguientes isomorfismos de grupos:
- i) $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$.
 - ii) $\mathbb{C}^*/\mathbb{S}^1 \cong \mathbb{R}_{>0}$.
 - iii) $\mathbb{C}^*/G_n \cong \mathbb{C}^*$.
 - iv) $T^n \cong (\mathbb{S}^1)^n$ donde $T^n = \mathbb{R}^n/\mathbb{Z}^n$.
- b) $n\mathbb{Z} \subset m\mathbb{Z}$ sii m/n . En tal caso, $n\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{n/m}$.
 - c) $G_n \subset G_m$ sii n/m . En tal caso, $G_n/G_m \cong G_{m/n}$.
- 22) Sea M un A -módulo. Se dice que un submódulo $N \subset M$ tiene índice finito si el módulo cociente M/N es finito. Probar que si N_1 y N_2 tienen índice finito en M entonces $N_1 \cap N_2$ también tiene índice finito.