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 $j : N \to G(N)$ (ver ejercicio 1 de la práctica 2). Probar que si G es un grupo y $f : N \to G$ es un morfismo de semigrupos, entonces existe un único morfismo de grupos $\overline{f} : G(N) \to G$ tal que $f = \overline{f} \circ j$.

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 $j : A \to K(A)$ definida por $j(a) =$ clase de $(a, 1)$. Probar que j es un morfismo de anillos y que si K es un cuerpo y $f : A \to K$ es un morfismo de anillos, entonces existe un único morfismo de cuerpos $\overline{f} : K(A) \to K$ tal que $f = \overline{f} \circ j$.

3) *Observación.*

En el ejercicio 7 de la práctica 2 se definición 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 $\alpha : S \to A$ 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 $f : A[S] \to B$

ii) Un morfismo de anillos $f_A : A \to B$ y un morfismo de semigrupos $f_S : S \to B$ (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 $A \to B$ una A-álgebra conmutativa. Verificar que dar un morfismo de A-álgebras $A[x] \to B$ 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 $A[x_1, \ldots, x_m] \to B$: existe una biyección canónica $\mathrm{Hom}_{A-\mathrm{alg}}(A[x_1, \ldots, x_m], B) \cong B^m$.

b) Para $f \in A[x]$, verificar que dar un morfismo de A-álgebras $A[x]/ < f > \to B$ es equivalente a dar una solución $b \in B$ de la ecuación $f(x) = 0$. Generalizar al caso de varias ecuaciones en varias variables $f_1, \ldots, f_r \in A[x_1, \ldots, x_m]$. 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:

a) Una estructura de $A[S]$-módulo en M.

b) Una estructura de A-módulo en M, más un morfismo de semigrupos de S en $\mathrm{End}_A(M)$ (endomorfismos del A-módulo M, visto como semigrupo con operacion de composicion).

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 $a : A^m \to A^n$ definida por $a(x) = \alpha.x$ (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 $\mathrm{im}(a)$. Probar que el conjunto $S = \{x \in A^m / \alpha.x = 0\}$ 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 cuales morfismos son monomorfismo, epimorfismo, sección, retracción, isomorfismo.

a) $f : M^n \to M^2$, $f(x) = (x_1 + x_n, x_n)$

b) $f : M^n \to M^n$, $f(x) = (\sum_{1 \le i \le j} x_i)_{1 \le j \le n}$

c) si $n \le m$, $f : M^n \to M^m$, $f(x) = (x_1, \ldots, x_n, 0, \ldots, 0)$

d) si $n \le m$, $f : M^m \to M^n$, $f(x) = (x_1, \ldots, x_n)$

e) si $z \in M^n$, $f : A^n \to M$, $f(x) = \sum_{1 \le i \le n} x_i.z_i$

f) si $z \in A^n$, $f : M^n \to M$, $f(x) = \sum_{1 \le i \le n} z_i.x_i$

g) para $a \in A$, $e_a : A[x] \to A$, $e_a(\sum_i a_i.x^i) = \sum_i a_i.a^i$

h) $d : A[x] \to A[x]$, $d(\sum_i a_i.x^i) = \sum_i a_i.ix^{i-1}$. El morfismo d tiene las propiedades adicionales $d(p.q) = d(p).q + p.d(q)$ y $d(a.x^0) = 0$

i) $\mathrm{tr} : M(n \times n, A) \to A$, $\mathrm{tr}(a) = \sum_{1 \le j \le n} a_{jj}$ (morfismo traza)

j) $\mathrm{dg} : M(n \times n, A) \to A^n$, $\mathrm{dg}(a) = (a_{11}, a_{22}, \ldots, a_{nn})$

k) $\Delta : A \to A^J$, $\Delta(a)_j = a, \forall j \in J$. (morfismo diagonal)

l) si $J \subset I$, $\rho : M^I \to M^J$, $\rho(\alpha) = \alpha|_J$.

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

a) $f : (\mathbb{R}, +) \to (\mathbb{C} - \{0\}, .)$, $f(x) = e^{2\pi i x}$

b) $f : (\mathbb{C} - \{0\}, .) \to (\mathbb{R}_{>0}, .)$, $f(x) = |x|$

c) $(n \in \mathbb{N})$, $f_n : (\mathbb{C} - \{0\}, .) \to (\mathbb{C} - \{0\}, .)$, $f_n(x) = x^n$

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 $f = \mathrm{id}_{\mathbb{Q}}$.

c) Si V y W son $\mathbb{Q}$-espacios vectoriales, una aplicación $f : V \to W$ es morfismo de $\mathbb{Q}$-espacios vectoriales si y solo si es morfismo de grupos.

10) a) Sea A un anillo y $f : M \to N$ 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 $\mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$ con la operación de composición constituye un anillo. Si M es simple entonces $\mathrm{End}_A(M)$ es un anillo de división.

c) Si I y J son conjuntos coordinables (existe una biyección $I \to J$) entonces M^I y M^J son isomorfos, para todo A-módulo M.

d) Una involución de un A-módulo M es un morfismo $f : M \to M$ tal que $f^2 = \mathrm{id}_M$. Toda involución es un automorfismo. Exhibir ejemplos de involución.

e) Un proyector de un A-módulo M es un morfismo $f : M \to M$ tal que $f^2 = f$. Probar que $M \cong \ker(f) \oplus \mathrm{im}(f)$. Probar que, reciprocamente, si A y B son submódulos de M tales que $M \cong A \oplus B$ entonces existe un único proyector $f : M \to M$ tal que $A = \ker(f)$ y $B = \mathrm{im}(f)$.

11) a) El morfismo $\mathrm{tr} : M(n \times n, A) \to A$, $\mathrm{tr}(a) = \sum_{1 \le j \le n} a_{jj}$ satisface

a) $\mathrm{tr}(e) = n$,1 (e denota la matriz identidad)

b) $\mathrm{tr}(a.b) = \mathrm{tr}(b.a)$ (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 $M(n \times n, A) \to A$ que satisface i) y ii).

c) Sea A como en b) y $n > 1$. Probar que no existe ningun epimorfismo $f : M(n \times n, A) \to A$ 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 $\mathrm{Hom}_A(A, M) \cong M$.

b) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Q}) \cong \mathbb{Q}$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) = 0$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}) \cong \mathbb{Q}$.

c) Dado un A-módulo M, se llama dual de M al A-módulo $M^* = \mathrm{Hom}_A(M,A)$. La aplicación $c_M : M \to M^{**}$ 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 $v_j = (a_{ij})_{1\le i\le n} \in A^n$ la j-esima columna de a. Demostrar:

a) $v_1, \ldots, v_n$ son linealmente independientes si y solo si $\det(a) \neq 0$.

b) $v_1, \ldots, v_n$ generan A^n si y solo si $\det(a)$ es una unidad de A.

c) dar criterios de independencia lineal y generación para $v_1, \ldots, v_m \in A^n$.
(Definición: para $a \in M(n \times n, A)$, $\det(a) = \sum_{\sigma\in\mathbb{S}_n} \mathrm{sg}(\sigma) \prod_{i=1}^n a_{i\sigma(i)}$)

15) 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) $N = M(n \times n, A)$, $S = \{x \in N / \mathrm{dg}(x) = 0\}$.

e) $N = M(n \times n, A)$, $S = \{x \in N / \mathrm{tr}(x) = 0\}$.

f) $N = M^J$, $S = \{x \in N / x_i = 0 \ \ \forall i \in I\} (I \subset J)$.

16) 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, $G_n/G_m \cong G_{m/n}$.

17) 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.

18) Sea A un anillo. Denotamos $S = \{a \in M(n \times n, A) \ / t(a) = a\}$ el submódulo de matrices simétricas ($t(a)_{ij} = a_{ji}$) y $T = \{a \in M(n \times n, A) \ / t(a) = -a\}$ el submódulo de matrices anti-simétricas. Verificar que si $2 \in A$ es una unidad entonces $M(n \times n, A) \cong S \oplus T$.

19) Sea A un anillo y M un A-módulo. Si $S \subset M$ genera M, decimos que S es un sistema de generadores minimal si ningun subconjunto propio de S genera M.

a) Probar que un módulo de tipo finito posee un sistema de generadores minimal.

b) Consideramos $\mathbb{Z}$ como $\mathbb{Z}$-módulo. Demostrar que para cada $n \in \mathbb{N}$ existe en $\mathbb{Z}$ un sistema de generadores minimal con n elementos.

c) $\mathbb{Q}$, visto como $\mathbb{Z}$-módulo, no posee un sistema de generadores minimal.

d) Si A es un cuerpo y M es un A-módulo entonces $S \subset M$ es un sistema de generadores minimal sii S es una base de M. Todo A-módulo M posee una base, y todas las bases de M tienen la misma cardinalidad.

20) Sea A un anillo y M un A-módulo. M se dice localmente cíclico si todo submódulo de M de tipo finito es cíclico.

a) Si M es localmente cíclico, todo submódulo de M es localmente cíclico.

b) Sea $f : M \to N$ un epimorfismo de A-módulos. Si M es localmente cíclico entonces también lo es N.

c) Si A es un dominio de ideales principales y K es el cuerpo de fracciones de A entonces K y K/A son A-módulos localmente cíclicos.

d) $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ son grupos abelianos localmente cíclicos, pero no son de tipo finito.

21) Sea G un grupo y $x \in G$. Se llama orden de x, denotado $\text{ord}(x) \in \mathbb{N} \cup \{\infty\}$, al cardinal del subgrupo generado por x.

a) Son validas las proposiciones:

i) Si x genera G entonces $\text{ord}(x) = |G|$. La recíproca vale si G es un grupo finito.

ii) Si G es un grupo finito entonces $\text{ord}(x)$ es un divisor de $|G|$.

b) Si $n \in \mathbb{N}$, son equivalentes:

i) $\text{ord}(x) = n$

ii) $< x > \cong \mathbb{Z}_n$

iii) Si $e_x : \mathbb{Z} \to G$ es la expansión asociada a x ($e_x(m) = x^m$) entonces $\ker(e_x) = n.\mathbb{Z}$.

iv) para $m \in \mathbb{Z}$, $x^m = 1$ sii n divide a m.

v) para $r, s \in \mathbb{Z}$, $x^r = x^s$ sii r y s son congruentes módulo n.

vi) $x^n = 1$ y los elementos $x^j,\ j = 0, 1, \ldots, n-1$ son distintos.

vii) $n = \min\{r \in \mathbb{N} / x^r = 1\}$

c) Son equivalentes:

i) $\text{ord}(x) = \infty$.

ii) $< x > \cong \mathbb{Z}$.

iii) Si $e_x : \mathbb{Z} \to G$ es la expansión asociada a x entonces $\ker(e_x) = 0$.

iv) para $m \in \mathbb{Z}$, $x^m = 1$ sii $m = 0$.

22) Sea G un grupo y sea $x \in G$.

a) Si G es finito de orden n entonces $x^n = 1$.

b) Si $\text{ord}(x) = n$ y $m \in \mathbb{N}$ entonces $\text{ord}(x^m) = n/(m : n)$. En particular, si m y n son coprimos, $\text{ord}(x^m) = \text{ord}(x)$.

c) Si G es cíclico de orden n y x, y son generadores de G entonces existe m coprimo con n tal que $y = x^m$.

d) Sea $\varphi : \mathbb{N} \to \mathbb{N}$ la función de Euler, definida por

$$\varphi(n) = \text{cardinal}\{m \in \mathbb{N} / \ m \leq n, (m : n) = 1\}$$

Probar que el número de generadores de un grupo cíclico de orden n es $\varphi(n)$.

23) Sea G un grupo abeliano finito. Se llama exponente de G al número natural $\exp(G)$ maximo de los ordenes de elementos de G.

a) Si $\text{ord}(x) = n$, $\text{ord}(y) = m$ y $(n : m) = 1$ entonces $\text{ord}(xy) = nm$.

b) Si $\text{ord}(x) = n$, $\text{ord}(y) = m$ entonces existe $z \in G$ tal que $\text{ord}(z) = [n : m]$.

c) Se verifica:

i) $\exp(G)$ es un divisor de $|G|$.

ii) G es cíclico sii $\exp(G) = |G|$.

iii) $\text{ord}(x)$ es un divisor de $\exp(G)$ para todo $x \in G$.

iv) Si K es un cuerpo finito entonces $G = (K - \{0\}, .)$ es un grupo cíclico. Sug.: Todo elemento de $K - \{0\}$ es raíz del polinomio $X^e - 1 \in K[X]$ con $e = \exp(G)$.