Álgebra II
Segundo Cuatrimestre — 2009
Práctica 9: Teoremas clásicos de estructura

1. Módulos y anillos semisimples

1.1. Sea A un anillo y sea M un A-módulo simple. Entonces o bien M, considerado como grupo abeliano, es isomorfo a una suma directa de copias de $\mathbb{Q}$, o bien existe $p \in \mathbb{N}$ primo tal que M es, considerado como grupo abeliano, isomorfo a una suma directa de copias de $\mathbb{Z}_p$.

1.2. *(a)* Si A es un anillo semisimple y $B \subset A$ es un subanillo, ¿es B necesariamente semisimple?

(b) Si A es un anillo semisimple e $I \lhd A$ es un ideal bilátero, entonces A/I es semisimple.

1.3. *Anillos de matrices.*

(a) Sean A y B anillos y $n, m \in \mathbb{N}$. Entonces $\mathsf{M}_m(\mathsf{M}_n(A)) \cong \mathsf{M}_{mn}(A)$ y $\mathsf{M}_n(A \times B) \cong \mathsf{M}_n(A) \times \mathsf{M}_n(B)$.

(b) Si A es un anillo semisimple y $n \in \mathbb{N}$, entonces $\mathsf{M}_n(A)$ es semisimple.

(c) Sea A un anillo y sea $n \in \mathbb{N}$. Sea P el conjunto de vectores *fila* de n componentes en A y sea Q el conjunto de vectores *columna* de n componentes en A. Entonces P es un A-$\mathsf{M}_n(A)$-bimódulo y Q es un $\mathsf{M}_n(A)$-A-bimódulo con acciones de $\mathsf{M}_n(A)$ inducidas por el producto matricial.

(d) Sea A un anillo. Si existe $n \in \mathbb{N}$ tal que $\mathsf{M}_n(A)$ es semisimple, entonces el anillo A mismo es semisimple.

1.4. Sea A un anillo, M un A-módulo finitamente generado. Si $B = \mathsf{End}_A(M)$ y A es semisimple, entonces B es semisimple. Notemos que esto tiene como caso particular a la segunda parte del ejercicio **1.3**, ya que si $M = A^n$, entonces $\mathsf{End}_n(M) \cong \mathsf{M}_n(A)$.

1.5. *(a)* Un anillo artiniano a izquierda sin divisores de cero es un anillo de división.

(b) Si A es un anillo sin divisores de cero tal que $\mathsf{M}_n(A)$ es semisimple para algún $n \in \mathbb{N}$, entonces A es un anillo de división.

2. Álgebras de grupos cíclicos

Si $n \in \mathbb{N}$, sea G_n un grupo cíclico de orden n y sea $g_n \in G_n$ un generador.

[1] **2.1.** Sea k un cuerpo de característica cero. Si $kG_n \cong \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_r}(D_r)$ es la factorización de kG_n como k-álgebra dada por el teorema de Wedderburn, de manera que es $r \in \mathbb{N}$, $n_1, \ldots, n_r \in \mathbb{N}$ y $D_1, \ldots, D_r$ son k-álgebras de división, entonces $n_1 = n_2 = \cdots = n_r = 1$ y D_i es un cuerpo para cada $i \in \{1, \ldots, r\}$.

En particular, hay exactamente r isoclases de kG_n-módulos simples y si $S_1, \ldots, S_n$ son representantes de estas clases, hay un isomorfismo de kG_n-módulos $kG_n \cong \bigoplus_{i=1}^r S_i$.

[1] **2.2.** Sea k un cuerpo de característica cero. Sea M un kG_n-módulo simple y sea $a : m \in M \mapsto g_n m \in M$ la multiplicación por g_n. Entonces $a \in \mathsf{End}_{kG_n}(M)$ porque kG_n es un anillo conmutativo. Sea $\mu \in k[X]$ el polinomio minimal de a sobre k. Muestre que μ es irreducible en $k[X]$. Además, si $k = \mathbb{Q}$, entonces μ tiene coeficientes enteros.

2.3. *álgebras de grupos cíclicos sobre* $\mathbb{C}$. Sea $\Omega_n \subset \mathbb{C}^\times$ el subgrupo multiplicativo de $\mathbb{C}^\times$ de las raíces n-ésimas de la unidad.

[1] *(a)* La aplicación $\phi : \chi \in \hom_{\mathsf{Grp}}(G_n, \Omega_n) \mapsto \chi(g_1) \in \Omega_n$ es un isomorfismo de grupos abelianos. Esto implica que el conjunto $\hat{G}_n = \hom_{\mathsf{Grp}}(G_n, \Omega_n)$ tiene exactamente n elementos; llamemoslos $\chi_1, \dots, \chi_n$.

[1] *(b)* Muestre que si $\chi, \rho \in \hat{G}_n$, entonces

$$\sum_{g \in G_n} \chi(g)\rho(g^{-1}) = \delta_{\chi,\rho}.$$

Sugerencia. Multiplique el miembro izquierdo de esta igualdad por $(1 - \chi(g_1)\rho(g_1^{-1}))$.

[1] *(c)* Si $\chi \in \hat{G}_n$, sea $e_\chi = \frac{1}{n}\sum_{g \in G_n} \chi(g^{-1})g \in \mathbb{C}G_n$. Entonces si $\chi, \rho \in \hat{G}_n$,

$$e_\chi^2 = e_\chi,$$
$$e_\chi e_\rho = 1, \qquad \text{cuando } \chi \neq \rho,$$

y

$$\sum_{\chi \in \hat{G}_n} e_\chi = 1.$$

[1] *(d)* Consideremos el anillo $A = \mathbb{C} \times \dots \times \mathbb{C}$ con n factores y sean $x_1, \dots, x_n \in A$ los elementos de la base canónica. Hay un isomorfismo de anillos $\phi : \mathbb{C}G_n \to A$ tal que $\phi(e_{\chi_i}) = x_i$ si $1 \leq i \leq n$. Describa representantes para cada isoclase de $\mathbb{C}G_n$-módulos simples.

2.4. *álgebras de grupos cíclicos sobre* $\mathbb{Q}$.

[1] *(a)* Sea p un número primo. Si $0 \leq k < l$, sea $\phi_{k,l} : \mathbb{Q}G_{p^l} \to \mathbb{Q}G_{p^k}$ el único morfismo de anillos tal que $\phi_{k,l}(g_{p^l}) = g_{p^k}$. Entonces $\ker \phi_{k,l} = \langle g_{p^l}^{p^k} - 1\rangle$. Además, si $0 \leq r < k < l$, es $\phi_{r,l} = \phi_{r,k} \circ \phi_{k,l}$.

[1] *(b)* Sea p un número primo y pongamos $\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X]$. Entonces

$$X^{p^l} - 1 = (X-1)\prod_{i=0}^{l-1} \Phi_p(X^{p^i})$$

y cada uno de los factores $\Phi_p(X^{p^i})$ con $0 \leq i < l$ es irreducible en $\mathbb{Q}[X]$.

[3] *(c)* Sea p un número primo impar. Sea $l \geq 1$ y sea M un $\mathbb{Q}G_{p^l}$-módulo simple. Si $\dim_{\mathbb{Q}} M < p^l - p^{l-1}$, entonces existe $k < l$ y un $\mathbb{Q}G_{p^k}$-módulo simple N tal que $M \cong \phi_{k,l}^*(N)$.

[3] *(d)* Sea p un número primo impar. Notemos M_0 al único $\mathbb{Q}G_1$-módulo simple. Entonces, para todo $l \geq 1$ existe, a menos de isomorfismo, un único $\mathbb{Q}G_{p^l}$-módulo simple M_l tal que $\dim_{\mathbb{Q}} M_l \geq p^l - p^{l-1}$. Además, se tiene que

- $\dim_{\mathbb{Q}} M_l = p^l - p^{l-1}$; y
- $\mathbb{Q}G_{p^l} \cong \bigoplus_{l=0}^{l-1} \phi_{i,l}^*(M_i) \oplus M_l$.

Sugerencia. Haga inducción con respecto a l.

[3] *(e)* Enuncie y pruebe enunciados análogos a los dos últimos para $p = 2$.

[1] *(f)* Sea $p \in \mathbb{N}$ primo, $l \geq 1$ y sea M_l un $\mathbb{Q}G_{p^l}$-módulo simple de dimensión $p^l - p^{l-1}$. Entonces M_l posee una base con respecto a la cual la matriz de la aplicación $a : m \in M \mapsto g_{p^l}m \in M$ es la matriz compañera del polinomio $\Phi_p(X^{p^l})$.

[2+] *(g)* Sea $f \in \mathbb{Q}[X]$ un polinomio múnico irreducible y sea $a \in \mathsf{M}_n(\mathbb{Q})$ su matriz compañera. Entonces, si $\mathsf{C}(a) \subset \mathsf{M}_n(\mathbb{Q})$ es el centralizador de a en $\mathsf{M}_n(\mathbb{Q})$, hay un isomorfismo $\mathsf{C}(a) \cong \mathbb{Q}[X]/(f)$.

[1+] *(h)* Sea $p \in \mathbb{N}$ primo. Para cada $l \in \mathbb{N}$, sea $\zeta_l \in \mathbb{C}$ una raíz primitiva p^l-ésima de la unidad y sea $\mathbb{Q}(\zeta_l)$ el menor subcuerpo de $\mathbb{C}$ que la contiene. Entonces hay un isomorfismo de álgebras

$$\mathbb{Q}G_{p^l} \cong \mathbb{Q} \times \mathbb{Q}(\zeta_1) \times \dots \times \mathbb{Q}(\zeta_l).$$

3. álgebras de grupo

3.1. Muestre que si $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, entonces $kS_3 \cong k \times k \times \mathsf{M}_2(k)$.

3.2. Encuentre la descomposición de Wedderburn para kD_4 con $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ si $D_4 = \langle s, t : s^2 = t^4 = 1,\ sts = t^{-1} \rangle$.

3.3. Sea $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ el grupo de los cuaterniones unitarios. Muestre que

$$\mathbb{Q}Q \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H}_{\mathbb{Q}},$$
$$\mathbb{R}Q \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}_{\mathbb{R}},$$

y

$$\mathbb{C}Q \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathsf{M}_2(\mathbb{C}).$$

Aquí $\mathbb{H}_{\mathbb{R}}$ es el anillo de los cuaterniones reales y $\mathbb{H}_{\mathbb{Q}}$ es el análogo definido sobre $\mathbb{Q}$.

4. Dominios de ideales principales

4.1. Mostrar que $\mathbb{Z}[\sqrt{10}]$ y $\mathbb{Z}[\sqrt{-10}]$ no son dominios de factorización única. Encontrar ideales no principales en estos anillos.

4.2. *(a)* Mostrar que $\mathbb{Z}[\sqrt{d}]$ es euclideano si $d \in \{-2, 2, 3\}$.

(b) Factorizar a $16 + 11\sqrt{2}$ como producto de elementos irreducibles del anillo $\mathbb{Z}[\sqrt{2}]$.

(c) Un número primo $p \in \mathbb{Z}$ es irreducible en $\mathbb{Z}[\sqrt{-2}]$ sii -2 es un cuadrado en $\mathbb{Z}_p$. Dé ejemplos de factorizaciones en $\mathbb{Z}[\sqrt{-2}]$ de números primos de $\mathbb{Z}$.

4.3. Sea $p \in \mathbb{N}$ un número primo, $\mathfrak{p} = (p)$ el ideal primo correspondiente y sea $\mathbb{Z}_{\mathfrak{p}}$ la localización de $\mathbb{Z}$ en $\mathfrak{p}$. Describir todos sus ideales. Mostrar que $\mathbb{Z}_{\mathfrak{p}}$ es un dominio de ideales principales con un único ideal maximal y encontrar un conjunto completo de elementos primos no asociados dos a dos.

4.4. Sea A un dominio de ideales principales y sea M un A-módulo finitamente generado. Mostrar que

(a) M es de torsión sii $\mathsf{hom}_A(M, A) = 0$; y

(b) M es indescomponible sii o bien $M \cong A$ o bien existe $p \in A$ irreducible y $n \in \mathbb{N}$ tal es que $M \cong A/(p^n)$.

¿Qué puede decir cuando M no es finitamente generado?

4.5. Sea $p \in \mathbb{N}$ un número primo. Encuentre todos los grupos abelianos de orden p^2, p^3, p^4 y p^5.

4.6. Sea G un grupo abeliano finito y sea $p \in \mathbb{N}$ un número primo tal que $p \mid |G|$. Entonces el número de elementos de orden p de G es coprimo con p.

4.7. *(a)* Para los siguientes grupos abelianos, dar la factorización del teorema de estructura:

i) $\mathbb{Z}_4 + \mathbb{Z}_6 + \mathbb{Z}_9$;

ii) $\mathbb{Z}_2 + \mathbb{Z}_2 + \mathbb{Z}_8 + \mathbb{Z}_{14}$;

iii) $\mathbb{Z}_2 + \mathbb{Z} + \mathbb{Z}_{49} + \mathbb{Z}$;

iv) $\mathbb{Z}_{12} + \mathbb{Z}_{21} + \mathbb{Z} + \mathbb{Z} + \mathbb{Z}_{20} + \mathbb{Z}_9 + \mathbb{Z}_7$.

(b) Determinar la factorización canónica de un grupo abeliano G de orden 36 que tiene exactamente 2 elementos de orden 3 y que no tiene elementos de orden 4.

(c) Determinar la factorización canónica de un grupo abeliano G de orden 225 que tiene por lo menos 40 elementos de orden 15 y tal que todo subgrupo de orden 9 es isomorfo a $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

4.8. Sea $G \subset \mathbb{Z}^n$ un subgrupo.

(a) $[\mathbb{Z}^n : G]$ es finito sii G tiene rango n.

(b) Si G tiene rango n y $\{g_1, \dots, d_n\}$ es una base de G, sea $M \in \mathsf{M}_n(\mathbb{Z})$ la matriz que tiene a los g_i como columnas. Mostrar que $[\mathbb{Z}^n : G] = |\det M|$.