Álgebra II
Primer Cuatrimestre — 2007

Práctica 7: 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 $\mathbb{Z}_p$.

Solución. Sea $D = \mathsf{End}_A(M)$. El lema de Schur nos dice que D es un anillo de división y, en particular, su centro $\mathsf{Z}(D)$ es un cuerpo. Sea k la intersección de *todos* los subcuerpos de $\mathsf{Z}(D)$. Es fácil ver que o bien $k \cong \mathbb{Q}$ o bien existe $p \in \mathbb{N}$ primo tal que $k \cong \mathbb{Z}_p$. En cualquier caso, como $k \subset D$, M es un k-espacio vectorial y el resultado del ejercicio es consecuencia de que todo k-espacio vectorial es isomorfo a una suma directa de copias de k. □

1.2. Sea A un anillo conmutativo y M y N dos A-módulos. Si alguno de M o N es semisimple, $M \otimes_A N$ es semisimple.

Solución. Supongamos que N es semisimple. Como el producto tensorial se distribuye sobre sumas directas, podemos suponer sin pérdida de generalidad que N es simple. En ese caso, existe un ideal maximal $\mathfrak{m} \lhd A$ tal que $N \cong A/\mathfrak{m}$ y $M \otimes_A N \cong M \otimes_A A/\mathfrak{m} \cong M/\mathfrak{m}M$. Como $M/\mathfrak{m}M$ es un $A/\mathfrak{m}$-módulo y $A/\mathfrak{m}$ es un cuerpo, $M/\mathfrak{m}M$ es $A/\mathfrak{m}$-semisimple. Esto implica inmediatamente que $M \otimes_A N \cong M/\mathfrak{m}M$ es A-semisimple. □

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

Solución. El cuerpo $\mathbb{Q}$ es semisimple pero $\mathbb{Z} \subset \mathbb{Q}$ no es semisimple. □

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

Solución. Sea $B = A/I$. Vía la proyección canónica $\pi : A \to B$, B resulta un A-módulo a izquierda. Como A es semisimple por hipótesis, B es un A-módulo semisimple. Ahora bien, un sub-B-módulo de A es lo mismo que un sub-A-módulo de B porque π es sobreyectiva. Luego B es semisimple como B-módulo a izquierda, esto es, B es un anillo semisimple. □

1.4. *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.

Solución. Si A es semisimple, existen r, $n_1, \ldots, n_r \in \mathbb{N}$ y anillos de división $D_1, \ldots, D_r$ tales que $A \cong \mathsf{M}_{n_1}(D_1) \times \mathsf{M}_{n_r}(D_r)$. Si $n \in \mathbb{N}$, el ejercicio anterior implica entonces que

$$\mathsf{M}_n(A) \cong \mathsf{M}_n\big(\mathsf{M}_{n_1}(D_1) \times \mathsf{M}_{n_r}(D_r)\big) \cong \mathsf{M}_{n_1 n}(D_1) \times \mathsf{M}_{n_r n}(D_r)$$

y esto es, claramente, un anillo 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. Más aún, hay un isomorfismo $Q \otimes_A P \cong \mathsf{M}_n(A)$ de $\mathsf{M}_n(A)$-bimódulos y un isomorfismo $P \otimes_{\mathsf{M}_n(A)} Q \cong A$ de A-bimódulos.

Como consecuencia de esto, si M es un A-módulo izquierdo, entonces

$$P \otimes_{\mathsf{M}_n(A)} (Q \otimes_A M) \cong M.$$

Solución. Las aplicaciones $\sigma : Q \otimes_A P \to \mathsf{M}_n(A)$ y $\tau : P \otimes_{\mathsf{M}_n(A)} Q \to A$ inducidas por la multiplicación matricial, esto es, tales que $\sigma(q \otimes p) = qp$ y $\tau(p \otimes q) = pq$ cada vez que $p \in P$ y $q \in Q$ son isomorfismos de $\mathsf{M}_n(A)$- y A-bimódulos, respectivamente.

La última afirmación sigue de considerar la composición

$$P \otimes_{\mathsf{M}_n(A)} (Q \otimes_A M) \cong M \xrightarrow{\cong} (P \otimes_{\mathsf{M}_n(A)} Q) \otimes_A M \cong M \xrightarrow{\tau \otimes \mathsf{id}_M} A \otimes_A M \longrightarrow M$$

en la que el primer morfismo es el isomorfismo que da la asociatividad del producto tensorial y el tercer morfismo el isomorfismo canónico.

(d) Si M es un A-B-bimódulo y N es un B-módulo izquierdo proyectivo, entonces $M \otimes_B N$ es un A-módulo proyectivo.

Solución. Es claro que si N es un B-módulo a izquierda libre, $M \otimes_B N$ es libre como A-módulo. Si N es un B-módulo proyectivo, entonces existe otro B-módulo N' tal que $N \oplus N'$ es libre. Pero entonces $M \otimes_B (N \oplus N') \cong (M \otimes_B N) \oplus (M \otimes_B N')$ es B-libre y $M \otimes_B N$, es un sumando directo de él, es B-proyectivo. □

(e) 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.

Solución. Basta mostrar que si $\mathsf{M}_n(A)$ es semisimple, entonces todo A-módulo izquierdo es proyectivo. Sea entonces M un A-módulo. Como $\mathsf{M}_n(A)$ es semisimple, el $\mathsf{M}_n(A)$-módulo $Q \otimes_A M$ es proyectivo. Usando ahora las dos partes anteriores de este ejercicio, esto implica que $M \cong P \otimes_{\mathsf{M}_n(A)} (Q \otimes_A M)$ es A-proyectivo. □

1.5. 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 **1.4**, ya que si $M = A^n$, entonces $\mathsf{End}_n(M) \cong \mathsf{M}_n(A)$.

Solución. Como A es semisimple y M es finitamente generado, existen $k \in \mathbb{N}$, $n_1, \ldots, n_k \in \mathbb{N}$ y A-módulos simples no isomorfos $M_1, \ldots, M_k$ tales que $M = \bigoplus_{i=1}^{k} M_i^{n_i}$. Si $D_i = \mathsf{End}_A(M_i)$, entonces

$$B = \mathsf{End}_A(M) \cong \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_k}(D_k).$$

En particular, B es semisimple.

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

Solución. Sea A un anillo artiniano a izquierda sin divisores de cero. Para ver que A es un anillo de división, basta mostrar que todo elemento $a \in A$ posee un inverso a izquierda. Ahora bien, la cadena decreciente de ideales izquierdos $Aa \supset Aa^2 \supset \cdots$ debe estabilizarse, de manera que existe $k \in \mathbb{N}$ tal que $Aa^k = Aa^{k+1}$. En particular, existe $b \in A$ tal que $ba^{k+1} = a^k$, esto es, tal que $(ba - 1)a^k = 0$. Como en A no hay divisores de cero, vemos que $ba = 1$. Luego a tiene a b como inverso a izquierda. □

(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.

Solución. Si $\mathsf{M}_n(A)$ es semisimple, entonces es artiniano. Esto implica que A mismo es artiniano. Como además no ay en A divisores de cero, la parte anterior implica que 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 $kG_n \cong \bigoplus_{i=1}^{r} S_i$.

Solución. En efecto, si ese no es el caso, el álgebra de la derecha no sería conmutativa. □

[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.

Solución. Supongamos que $\mu = f_1 f_2$ con $f_1, f_2 \in k[X]$ y $(f_1, f_2) = 1$. Existen entonces $\alpha_1, \alpha_2 \in k[X]$ con $\alpha_1 f_1 + \alpha_2 f_2 = 1$. Pongamos $e_i = \alpha_i(a) f(a) \in \mathsf{End}_{kG_n}(M)$ para $i \in \{1, 2\}$. Claramente

$$e_1 e_2 = e_2 e_1 = \alpha_1(a)\alpha_2(a) f_1(a) f_2(a) = \alpha_1(a)\alpha_2(a)\mu(a) = 0,$$

así que, como $\mathsf{End}_{kG_n}(M)$ es un anillo de división, podemos suponer que $e_1 = 0$. Esto implica que $\mu = f_1 f_2 \mid \alpha_1 f_1$ y vemos que $f_2 \mid \alpha_1$. Pero entonces

$$f_2 \mid \alpha_1 f_1 + \alpha_2 f_2 = 1,$$

de manera que $f_2 \in k$. Esto muestra que μ es irreducible en $k[X]$.

Ahora bien, como $g_n^n = 1$ en G_n, $a^n = \mathsf{id}_M$. Como μ es el polinomio minimal de a, concluimos que $\mu \mid X^n - 1$. Cuando $k = \mathbb{Q}$, usando que μ es mónico vemos que 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 $\phi : \chi \in \mathsf{hom}_{\mathrm{Grp}}(G_n, \Omega_n) \mapsto \chi(g_1) \in \Omega_n$ es un isomorfismo de grupos abelianos. Esto implica que el conjunto $\hat{G}_n = \mathsf{hom}_{\mathrm{Grp}}(G_n, \Omega_n)$ tiene exactamente n elementos; llamemoslos $\chi_1, \ldots, \chi_n$.

[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 $A = \mathbb{C} \times \cdots \times \mathbb{C}$ con n factores y sean $x_1, \ldots, x_n \in A$ 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 $M \cong \phi_{k,l}^*(N)$.

Solución. Sea M como en el enunciado. Notemos $\rho : \mathbb{Q}G_n \to \mathsf{End}_{\mathbb{Q}}(M)$ al morfismo de anillos que determina la estructura de $\mathbb{Q}G_n$-módulo sobre M. Es fácil ver que alcanza con mostrar que existe $k < l$ tal que $g_{p^l}^{p^k} - 1 \in \ker \rho$, ya que en ese caso será $\ker \phi_{k,l} \subset \ker \rho$ y ρ se factorizará a lo largo de $\phi_{k,l}$.

Sea $a : m \in M \mapsto g_{p^l} m \in M$ la multiplicación por g_{p^l} y sea $\mu \in \mathbb{Q}[X]$ el polinomio minimal de a sobre $\mathbb{Q}$. Sabemos que μ es irreducible en $\mathbb{Q}[X]$. Por otro lado, como $a^{p^l} = \mathsf{id}_M$, es

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

Luego o bien $\mu = X - 1$ o bien existe $i \in \{0, \ldots, l-1\}$ tal que $\mu = \Phi_p(X^{p^i})$.

En el primer caso, vemos que $a = \mathsf{id}_M$ y M es un $\mathbb{Q}G_{p^l}$-módulo trivial. Esto dice que $g_{p^l} - 1 \in \ker \rho$ y que podemos tomar $k = 0$.

Supongamos entonces que estamos en el segundo caso, de manera que $\mu = \Phi_p(X^{p^i})$ con $0 \leq i < l$. Como

$$p^{i+1} - p^i = \deg \mu \leq \dim_{\mathbb{Q}} M < p^l - p^{l-1},$$

se tiene de hecho que $i < l - 1$. Por otro lado,

$$\mu = \Phi_p(X^{p^i}) \mid X^{p^{i+1}} - 1,$$

así que $a^{p^{i+1}} = \mathsf{id}_M$ y vemos que $g_{p^l}^{p^{i+1}} - 1 \in \ker \rho$. Concluimos que, en este caso, podemos tomar $k = i + 1$. □

[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.

Solución. Supongamos primero que $l = 1$. Sea M un $\mathbb{Q}G_p$-módulo simple no trivial y sea $\mu \in \mathbb{Q}[X]$ el polinomio minimal de la aplicación $a : m \in M \mapsto g_p m \in M$. Es $a^p = \mathsf{id}_M$, así que $\mu \mid X^p - 1 = (X-1)\Phi_p(X)$. Como μ es irreducible y 1 no puede ser un autovalor de a, esto implica que $\mu = \Phi_p(X)$.

En particular, $\dim_{\mathbb{Q}} M \geq \deg \Phi_p(X) = p - 1$. Como todo módulo simple es sumando directo de $\mathbb{Q}G_p$, $\phi_{0,1}^*(M_0) \oplus M$ es sumando directo de $\mathbb{Q}G_p$ y vemos que $\dim_{\mathbb{Q}} M \leq p - 1$. Así, debe ser $\dim_{\mathbb{Q}} M = p - 1$ y $\mathbb{Q}G_p \cong \phi_{0,1}^*(M_0) \oplus M$.

Esto nos dice que hay dos isoclases de $\mathbb{Q}G_p$-módulos simples, las de $\phi_{0,1}^*(M_0)$ y la de M. Llamando $M_1 = M$, concluimos que el enunciado es cierto cuando $l = 1$.

Supongamos ahora que $l > 1$ y consideremos un $\mathbb{Q}G_{p^l}$-módulo simple M tal que $\dim_{\mathbb{Q}} M \geq p^l - p^{l-1}$. La hipótesis inductiva nos dice que los $\mathbb{Q}G_{p^l}$-módulos

$$\phi_{l-1,l}^*(\phi_{i,l-1}^*(M_i)) = \phi_{i,l}^*(M_i), \qquad \text{con } 0 \leq i < l-1$$

y $\phi^*_{l-1,l}(M_l)$ son simples. Como tienen dimensiones distintas dos a dos, son no isomorfos dos a dos; más aún, tienen dimensión estrictamente menor que $p^l - p^{l-1}$, de manera que no son isomorfos a M. Entonces

$$U = \bigoplus_{i=0}^{l-1} \phi^*_{i,l}(M_i) \oplus M$$

es un sumando directo de $\mathbb{Q}G_{p^l}$. Calculando dimensiones, vemos que

$$p^l \leq \dim_{\mathbb{Q}} M + p^{l-1} = 1 + \sum_{i=1}^{l-1}(p^i - p^{i-1}) + \dim_{\mathbb{Q}} M \leq \dim_{\mathbb{Q}} \mathbb{Q}G_{p^l} = p^l,$$

así que $\dim_{\mathbb{Q}} M = p^l - p^{l-1}$. Además, como entonces $\dim_{\mathbb{Q}} U = \dim_{\mathbb{Q}} \mathbb{Q}G_{p^l}$, concluimos que de hecho

$$\mathbb{Q}G_{p^l} \cong \bigoplus_{i=0}^{l-1} \phi^*_{i,l}(M_i) \oplus M$$

y que todo $\mathbb{Q}G_{p^l}$-módulo simple de dimensión al menos $p^l - p^{l-1}$ es isomorfo a $M_l = M$.

Esto completa la inducción. □

[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 $\Phi_p(X^{p^l})$.

Solución. Sea $\mu \in \mathbb{Q}[X]$ el polinomio minimal de a; recordemos que es irreducible sobre $\mathbb{Q}$. Como $a^{p^l} = \mathrm{id}_M$,

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

Como $\dim_{\mathbb{Q}} M > 1$, M no es un módulo trivial, así que $\mu \neq X - 1$. Existe entonces $i \in \{0, \ldots, l-1\}$ tal que $\mu = \Phi_p(X^{p^i})$. En particular, $\deg \mu = p^{i+1} - p^i$. Si $m \in M \setminus 0$, es

$$p^l - p^{l-1} = \dim_{\mathbb{Q}} \mathbb{Q}G_{p^l} \cdot m \leq \deg \mu = p^{i+1} - p^i,$$

de manera que $i = l - 1$ y $\deg \mu = \dim_{\mathbb{Q}} M$. Esto nos dice que μ coincide con el polinomio característico de a, y un resultado conocido de álgebra lineal implica que existe una base de M con respecto a la cual la matriz de a es precisamente la matriz compañera de μ. □

[2+] *(g)* Sea $f \in \mathbb{Q}[X]$ un polinomio mónico 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 $\mathsf{C}(a) \cong \mathbb{Q}[X]/(f)$.

Solución. Como f es irreducible, todas sus raíces en $\mathbb{C}$ son simples. El teorema sobre la forma normal de Jordan nos dice, entonces, que exite una matriz $c \in \mathsf{GL}_n(\mathbb{C})$ tal que cac^{-1} es diagonal con todos sus coeficientes diagonales distintos.

Sea ahora $b \in \mathsf{C}(a)$. Es $cbc^{-1} \in \mathsf{C}(cac^{-1})$. Como cac^{-1} es diagonal con autovalores simples, existe un polinomio $q \in \mathbb{C}[X]$ tal que $q(cac^{-1}) = cbc^{-1}$. Pero entonces $q(a) = b$.

Notemos que, a menos de reemplazar a q por el resto de dividirlo por f, podemos suponer que $\deg q < n$. Si $q = \sum_{i=0}^{n-1} q_i X^i$, vemos entonces que

$$q_{n-1}a^{n-1} + q_{n-2}a^{n-2} + \cdots + q_1 a + q_0 = b.$$

Tomemos ahora $n-1$ variables escalares $X_0, \ldots, X_{n-1}$ y consideremos el sistema de n^2 ecuaciones que se obtienen tomando las coordenadas de la siguiente ecuación matricial:

$$X_{n-1}a^{n-1} + X_{n-2}a^{n-2} + \cdots + X_1 a + X_0 = b.$$

Ese sistema está sobredeterminado pero claramente es compatible, ya que poniendo $X_i = q_i$ para cada $i \in \{0, \ldots, n-1\}$ obtenemos una solución. Como tiene coeficientes racionales, esto implica que tiene soluciones *racionales*. Esto nos dice exactamente que existe un polinomio $g \in \mathbb{Q}[X]$ con $\deg g < n$ tal que $g(a) = b$.

Hemos mostrado que el morfismo de anillos $\phi : h \in \mathbb{Q}[X] \mapsto h(a) \in \mathsf{C}(a)$ es sobreyectivo. Como f es el polinomio minimal de a, $\ker \phi = (f)$ y obtenemos el isomofismo $\mathsf{C}(A) \cong \mathbb{Q}[X]/(f)$ buscado. □

[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

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

Solución. Sabemos a esta altura que hay un conjunto de representantes de las isoclases de $\mathbb{Q}G_{p^l}$-módulos simples de la forma $\{M_0, \ldots, M_l\}$ tal que M_0 es trivial y para cada $i \in \{1, \ldots, l\}$, M_i posee una base en la cual la multiplicación por g_{p^l} tiene asociada la matriz compañera del polinomio $\Phi_p(X^{p^i})$. En particular,

$$\mathbb{Q}G_{p^l} \cong \mathsf{End}_{\mathbb{Q}G_{p^l}}(M_0) \times \cdots \times \mathsf{End}_{\mathbb{Q}G_{p^l}}(M_l).$$

Bastará mostrar, entonces, que $\mathsf{End}_{\mathbb{Q}G_{p^l}}(M_i) \cong \mathbb{Q}(\zeta_i)$ para cada $i \in \{0, \ldots, l\}$. Notemos que cuando $i = 0$ esto es evidente.

Sea entonces $i \in \{1, \ldots, l\}$. Si $a \in \mathsf{M}_{p^i - p^{i-1}}(\mathbb{Q})$ es la matrix compañera de $\Phi_p(X^{p^i})$, entonces es fácil ver que $\mathsf{End}_{\mathbb{Q}G_{p^l}}(M_i) \cong \mathsf{C}(a)$. Usando el ítem anterior, esto es isomorfo a $\mathbb{Q}[X]/(\Phi_p(X^{p^i}))$. El resultado seguirá si podemos mostrar que $\Phi_p(X^{p^i})$ es el polinomio minimal de ζ_i sobre $\mathbb{Q}$. Como $\Phi_p(X^{p^i})$ es irreducible sobre $\mathbb{Q}$, esto es consecuencia inmediata de que $\Phi_p(\zeta_i^{p^i}) = 0$. □

(i) Supongamos que n es impar y que $n = p_1^{m_1} \cdots p_r^{m_r}$ es la factorización de n como producto de potencias de primos distintos. Entonces $G_n \cong G_{p_1^{m_1}} \times \cdots \times G_{p_r^{m_r}}$.

Si M es un $\mathbb{Q}G_n$-módulo simple, entonces existen $l_1, \ldots, l_r \in \mathbb{N}$ tales que $l_i \leq m_i$ si $i \in \{1, \ldots, r\}$ y

$$M \cong M_{p_1,m_1,l_1} \boxtimes \cdots \boxtimes M_{p_r,m_r,l_r}.$$

Aquí $M_{p,m,l}$ es el único $\mathbb{Q}G_{p^m}$-módulo simple de dimensión $p^l - p^{l-1}$.

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 $\{g_1, \ldots, d_n\}$ 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 $[\mathbb{Z}^n : G] = |\det M|$.

Abraham Adrian Albert
1905–1972, Estados Unidos.

Albert fue uno de los pioneros en el estudio de la estructura de las álgebras de división. Su libro *Structure of Algebras* es un clásico.