ÁLGEBRAS SEMISIMPLES

MARIANO SUÁREZ-ALVAREZ

Índice

1. Módulos simples

1.1. Sea A un anillo.

1.2. Decimos que un A-módulo S es *simple* si es no nulo y no posee submódulos propios no triviales.

1.3. Si $A = k$ es un cuerpo o, más generalmente, un álgebra de división, entonces un A-módulo es simple sii tiene dimensión 1. Si $A = \mathbb{Z}$, entonces un A-módulo es simple sii es finito de orden primo.

1.4. Es consecuencia directa de la definición que un módulo no nulo es simple si está generad por cualquiera de sus elementos no nulos.

1.5. Lema. *Si $\mathfrak{a} \lhd_l A$, entonces $A/\mathfrak{a}$ es simple sii $\mathfrak{a}$ es un ideal izquierdo maximal. En particular, existen siempre módulos simples.*

Si S es un módulo simple y $m \in S \setminus 0$, entonces $\operatorname{ann}(m)$ es un ideal izquierdo maximal en A y $S \cong A/\operatorname{ann}(m)$.

Demostración. Todas las afirmaciones son claras. La existencia de módulo simples es consencuencia de la primera parte y de la existencia de ideales izquierdos maximales. □

1.6. Lema. *Sea $\phi : A \to B$ un morfismo de anillos sobreyectivo y sea S un B-módulo simple. Entonces el A-módulo $\phi^*(S)$ obtenido de S por restricción de escalares a lo largo de ϕ es simple.*

Demostración. Como ϕ es sobreyectivo, el grupo abeliano subyacente de un A-submódulo propio no trivial de $\phi^*(S)$ determina un B-submódulo propio no trivial de S. □

1.7. Notemos que sin la condición de que el morfismo ϕ sea sobreyectivo la conclusión del lema no es necesariamente válida. Por ejemplo, si $\phi : \mathbb{Z} \to \mathbb{Q}$ es la inclusión, entonces el $\mathbb{Z}$-módulo $\phi^*(\mathbb{Q})$, obtenido del $\mathbb{Q}$-módulo simple $\mathbb{Q}$, no es simple.

Date: 11 de junio, 2007.

1.8. Lema. *Sean A y B anillos y sean $\pi_1 : A \times B \to A$ y $\pi_2 : A \times B \to B$ las proyecciones canónicas. Sean $\mathscr{S}_A$ y $\mathscr{S}_B$ conjuntos completos de representantes de las clases de isomorfismo de los A- y B-módulos simples, respectivamente. Entonces*

$$\mathscr{S} = \{\pi_1^*(S) : S \in \mathscr{S}_A\} \cup \{\pi_2^*(S) : S \in \mathscr{S}_B\}$$

es un conjunto completo de representantes de las clases de isomorfismo de los $A \times B$-módulos simples.

Demostración. Sean $e_1 = (1_A, 0), e_2 = (0, 1_B) \in A \times B$. Para cada $A \times B$-módulo M, consideramos los subgrupos abelianos $M_1 = e_1 M$ y $M_2 = e_2 M$ de M. Definimos una acción de A sobre M_1 poniendo

$$a \cdot m = (a, 0)m, \qquad \forall a \in A,\ m \in M_1.$$

Notemos que esto tiene sentido porque $(a, 0)m = e_1(a, 0)m \in M_1$ si $a \in A$ y $m \in M_1$. Es fácil ver que, dotado de esta acción, M_1 resulta un A-módulo. De manera similar hacemos de M_2 un B-módulo. Calculando directamente, se ve que la aplicación

$$m \in M \mapsto (e_1 m, e_2 m) \in \pi_1^*(M_1) \oplus \pi_2^*(M_2)$$

es un isomorfismo de $A \times B$-módulos.

Sea S un $A \times B$-módulo simple. Las observaciones recién hechas implican que hay un isomorfismo de $A \times B$-módulos $S \cong \pi_1^*(S_1) \oplus \pi_2^*(S_2)$. Como S es simple, necesariamente o bien $S_1 = 0$ o bien $S_2 = 0$. Supongamos, por ejemplo, que es $S_2 = 0$. Para ver que S es isomorfo a un elemento de $\mathscr{S}$, entonces, alcanza con mostrar que S_1 es simple, pero esto es inmediato, ya que todo sub-A-módulo propio no trivial de S_1 es un sub-$A \times B$-módulo propio no trivial de S.

Para terminar, tenemos que ver que los elementos de $\mathscr{S}$ son no isomorfos dos a dos. Consideremos primero un par de A-módulos simples S, $T \in \mathscr{S}_A$ tales que existe un isomorfismo $f : \pi_1^*(S) \to \pi_1^*(T)$. Es claro que el isomorfismo de grupos abelianos $S \to T$ subyacente a f es A-lineal, así que es $S \cong T$ y, entonces, $S = T$. De la misma forma, si S, $T \in \mathscr{S}_B$ son B-módulos simples tales que $\pi_2^*(S) \cong \pi_2^*(T)$, entonces $S = T$.

Queda entonces solamente por considerar la posibilidad de que existan un A-módulo simple S y un B-módulo simple T tales que $\pi_1^*(S) \cong \pi_2^*(T)$. De hecho, esto no puede ocurrir porque $e_1 \pi_1^*(S) = \pi_1^*(S) \neq 0$ y $e_1 \pi_2^*(T) = 0$. □

1.9. Proposición. (Schur, 1905) *Sean S y S' A-módulos simples.*

(a) Si $f : S \to M$ es un morfismo no nulo, entonces f es inyectivo.
(b) Si $g : M \to S$ es un morfismo no nulo, entonces g es sobreyectivo.
(c) Todo morfismo no nulo $f : S \to S'$ es un isomorfismo.

En particular, $\mathsf{End}_A(S)$ es un anillo de división.

Demostración. Las dos primeras afirmaciones siguen inmediatamente de la observación de que $\ker f$ e $\operatorname{im} g$ son submódulos de S. La tercera es consecuencia de las dos primeras. □

1.10. Proposición. *Sea $r \in \mathbb{N}$ y sea $\{S_i : 1 \leq i \leq r\}$ un conjunto de A-módulos simples no isomorfos dos a dos. Si $1 \leq i \leq r$, sea $n_i \in \mathbb{N}$ y pongamos, si $1 \leq j \leq n_i$, $S_{i,j} = S_i$. Sea $M = \bigoplus_{i=1}^r \bigoplus_{j=1}^{n_i} S_{i,j}$. Entonces hay un isomorfismo de anillos*

$$\mathsf{End}_A(M) \cong \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_r}(D_r)$$

con $D_i = \mathsf{End}_A(S_i)$ para cada $i \in \{1, \ldots, r\}$.

Demostración. Esto es consecuencia inmediata de la descripción de los endomorfismos de M como matrices de morfismos $S_{i,j} \to S_{i',j'}$ y la tercera parte de **1.9**. □

2. Módulos semisimples

2.1. Un A-módulo M es *semisimple* si es suma de submódulos simples.

2.2. Por ejemplo, si $A = k$ es un cuerpo, todo A-módulo es semisimple. Un $\mathbb{Z}$-módulo es semisimple sii es suma de sus subgrupos cíclicos de orden primo.

2.3. Es evidente que una suma de módulos semisimples es semisimple.

2.4. Lema. *Sea $M = \sum_{i \in I} S_i$ con S_i simple para cada $i \in I$. Si $N \subset M$ es un submódulo, entonces existe $J \subset I$ tal que $M = N \oplus \bigoplus_{i \in J} S_i$.*

Demostración. Sea $\mathscr{J} = \{J \subset I : \text{la suma } N + \sum_{i \in J} S_i \text{ es directa}\}$. Claramente $\varnothing \in \mathscr{J}$ así que $\mathscr{J} \neq \varnothing$. Si $C = \{J_\lambda\}_{\lambda \in \Lambda}$ es una cadena en $\mathscr{J}$, pongamos $J_C = \bigcup_{\lambda \in \Lambda} J_\lambda$. Veamos que $J_C \in \mathscr{J}$:

- En primer lugar, si $m \in N \cap \sum_{i \in J_C} S_i$ existe un subconjunto finito $I' \subset J_C$ tal que $m \in \sum_{i \in I'} S_i$ y, como C es una cadena, es posible encontrar $\lambda \in \Lambda$ con $I' \subset J_\lambda$, de manera que $m \in N \cap \sum_{i \in J_\lambda} S_i = 0$. Esto nos dice que $N \cap \sum_{i \in J_C} S_i = 0$.
- Por otro lado, si $i_0 \in J_C$ y $m \in S_{i_0} \cap (N + \sum_{i \in J_C \setminus \{i_0\}} S_i)$, existe un subconjunto finito $I' \subset J_C \setminus \{i_0\}$ tal que $m \in S_{i_0} \cap (N + \sum_{i \in I'} S_i)$. Si $\lambda \in \Lambda$ es tal que $I' \cup \{i_0\} \subset J_\lambda$, entonces $m \in S_{i_0} \cap (N + \sum_{i \in J_\lambda \setminus \{i_0\}} S_i) = 0$. Concluimos que $S_{i_0} \cap (N + \sum_{i \in J_C \setminus \{i_0\}} S_i) = 0$.

El lema de Zorn asegura, en estas condiciones, que $\mathscr{J}$ posee un elemento maximal J. Pongamos $M' = N + \sum_{i \in J} S_i$. La elección de J implica, por supuesto, que esta suma es directa.

Para terminar, veamos que $M' = M$. Para hacerlo, y como $M = \sum_{i \in I} S_i$, basta mostrar que para cada $i \in I$ tenemos $S_i \subset M'$. Consideremos entonces $i_0 \in I$ y supongamos que $S_{i_0} \not\subset M'$. Como S_{i_0} es simple, debe ser entonces $S_{i_0} \cap M' = 0$ y, en particular, $J \cup \{i_0\} \in \mathscr{J}$. Esto contradice la elección de J, así que nuestra suposición debe ser falsa, esto es, debe ser $S_{i_0} \subset M'$. □

2.5. Lema. *Sea M un A-módulo tal que todo submódulo de M es un sumando directo. Todo submódulo de M posee un submódulo simple.*

Demostración. Basta mostrar que todo submódulo cíclico de M posee un submódulo simple. Consideremos entonces $m \in M \setminus 0$ y $Am \subset M$ el submódulo cíclico generado por m en M. Sea $\mathfrak{a} \lhd_l A$ un ideal izquierdo maximal tal que $\mathfrak{a} \supset \operatorname{ann}(m)$. Entonces $\mathfrak{a}m$ es un submódulo maximal de Am y $Am/\mathfrak{a}m$ es simple.

Por hipótesis, existe $L \subset M$ tal que $M = \mathfrak{a}m \oplus L$. Entonces

$$Am = (\mathfrak{a}m \oplus L) \cap Am = \mathfrak{a}m \oplus (L \cap Am)$$

y vemos que $L \cap Am \cong Am/\mathfrak{a}m$ es un submódulo simple de Am. □

2.6. Teorema. *Sea M un A-módulo. Las siguientes condiciones son equivalentes:*

(a) M es semisimple;
(b) M es suma directa de submódulos simples;
(c) todo submódulo de M es un sumando directo.

Demostración. Para ver que $(a) \Rightarrow (b)$, basta tomar $N = 0$ en **2.4**. La implicación $(b) \Rightarrow (a)$ es inmediata y la implicacion $(a) \Rightarrow (c)$ es consecuencia directa de **2.4**.

Veamos, para terminar, que $(c) \Rightarrow (a)$. Sea M un grupo en el que todo submódulo es un sumando directo, sea M' la suma de todos los submódulos simples de M y supongamos, para llegar a una contradicción, que $M' \subsetneq M$. Por hipótesis, existe un submódulo $N \subset M$ no nulo tal que $M = M' \oplus N$ y, por **2.5**, existe un submódulo $S \subset N$ simple. Como $S \cap M' = 0$, esto contradice la elección de M'. □

2.7. Corolario. *Sea $M = \sum_{i\in I} S_i$ con S_i simple para cada $i \in I$ y sea $N \subset M$ un submódulo. Entonces existe $J \subset I$ tal que $N \cong \bigoplus_{i\in J} S_i$.*

En particular, todo submódulo de un módulo semisimple es semisimple.

Demostración. El teorema implica que N es un sumando directo de M, de manera que existe un submódulo $P \subset M$ tal que $M = N \oplus P$ y **2.4** nos da un conjunto $J \subset I$ tal que $M = \bigoplus_{i\in J} S_i \oplus P$. Luego $N \cong M/P \cong \bigoplus_{i\in J} S_i$. □

2.8. Notemos que no es cierto, en las condiciones del corolario, que exista $J \subset I$ tal que $N = \bigoplus_{i\in J} S_i$. Por ejemplo, sea $A = k$ un cuerpo, $M = k^2$, $\{e_1, e_2\}$ la base canónica de M, $I = \{1, 2\}$, $S_i = \langle e_i \rangle$ si $i \in I$ y $N = \langle e_1 + e_2 \rangle$. Entonces S_i es simple para $i \in I$ y $M = \sum_{i\in I} S_i$ es semisimple, pero claramente N no es suma de una parte de $\{S_i : i \in I\}$.

2.9. Corolario. *Si*

$$0 \longrightarrow M' \xrightarrow{f} M \longrightarrow M'' \longrightarrow 0$$

es una sucesión exacta de A-módulos y M es semisimple, entonces la sucesión se parte y tanto M' como M'' son semisimples.

Demostración. El submódulo $f(M')$ de M es un sumando directo, así que la sucesión exacta se parte y $M \cong M' \oplus M''$. Luego M' y M'' son isomorfos a submódulos de M, que son semisimples en vista de **2.7**. □

2.10. Proposición. *Sea $M = \bigoplus_{i\in I} S_i$ un A-módulo semisimple con S_i simple para cada $i \in I$. Entonces M es artiniano sii es nötheriano sii es finitamente generado sii I es finito.*

Demostración. Es claro que si I es infinito, entonces M no es ni artiniano, ni nötheriano, ni finitamente generado. Supongamos entonces que I es finito y hagamos inducción sobre $|I|$; notemos que si $|I| \leq 1$ entonces no hay nada que probar.

Ahora bien, si $i_0 \in I$, entonces hay una sucesión exacta corta

$$0 \longrightarrow \bigoplus_{i\in I\setminus i_0} S_i \longrightarrow M \longrightarrow S_{i_0} \longrightarrow 0$$

Aplicando la hipótesis de inducción, vemos que $\bigoplus_{i\in I\setminus i_0} S_i$ es artiniano y nötheriano. Como lo mismo vale para S_{i_0}, entonces M es artiniano y nötheriano, como queríamos. □

3. Anillos semisimples

3.1. Un anillo A es *semisimple* si el A-módulo izquierdo ${}_AA$ es semisimple.

3.2. Es claro que un cuerpo o, más generalmente, un anillo de división es semisimple.

3.3. Lema. *Sea A un anillo.*

(a) Un ideal $\mathfrak{a} \lhd_l A$ es simple sii es minimal.
(b) Si S es un A-módulo simple, entonces existe un ideal maximal $\mathfrak{a} \lhd_l A$ tal que $S \cong A/\mathfrak{a}$. Si A es semisimple, existe además un ideal minimal $\mathfrak{b} \lhd_l A$ tal que $S \cong \mathfrak{b}$.

Demostración. La primera parte sigue inmediatamente de la definición. Veamos la segunda. Sea S un A-módulo simple y $m \in S \setminus 0$. La simplicidad implica que $S = Am$ y entonces si $\mathfrak{a} = \mathsf{ann}(m)$, que $S \cong A/\mathfrak{a}$. Como $A/\mathfrak{a}$ no posee submódulos propios no triviales, debe ser $\mathfrak{a}$ maximal en A. Si A es semisimple, existe $\mathfrak{b} \lhd_l A$ tal que $A = \mathfrak{a} \oplus \mathfrak{b}$. Claramente, es $S \cong \mathfrak{b}$ y, por la primera parte, $\mathfrak{b}$ es minimal. □

3.4. Proposición. *Sean A y B dos anillos semisimples. Entonces $A \times B$ es semisimple.*

Demostración. Supongamos que $A = \sum_{i\in I} S_i$ y $B = \sum_{j\in J} T_j$ con S_i un A-módulo simple para cada $i \in I$ y T_j un B-módulo simple para cada $j \in J$. Sean $\pi_1 : A \times B \to A$ y $\pi_2 : A \times B \to B$ las proyecciones canónicas. Es inmediato que

$$A \times B = \sum_{i\in I} \pi_1^*(S_i) + \sum_{j\in J} \pi_2^*(T_j),$$

de manera que $A \times B$ es semisimple porque $\pi_1^*(S_i)$ y $\pi_2^*(S_j)$ son simples cualesquiera sean $i \in I$ y $j \in J$, en vista de **1.6**. □

3.5. Un argumento inductivo a partir de esta proposición prueba, más generalmente, que un producto directo finito de anillos semisimples es semisimple.

3.6. Recordemos que si D es un anillo de división y $n \in \mathbb{N}$, entonces $\mathsf{M}_n(D)$ es artiniano simple. La siguiente proposición nos dice que obtenemos de esta forma todos los anillos artinianos simples y que éstos son semisimples:

Proposición. *Un anillo A artiniano simple es semisimple y todos sus módulos simples son isomorfos. Además, si S es un A-módulo simple, entonces $D = \mathsf{End}_A(S)$ es un anillo de división y existe $n \in \mathbb{N}$ tal que $A \cong \mathsf{M}_n(D)$.*

Demostración. Sea A un anillo artiniano simple. Como es artiniano, existe un ideal minimal $\mathfrak{a} \lhd_l A$. Sea $X = \mathsf{hom}_A(\mathfrak{a}, A)$ y consideremos el morfismo $\phi : \mathfrak{a}^{(X)} \to A$ tal que $\phi((a_f)_{f\in X}) = \sum_{f\in X} f(a_f)$. Es sobreyectivo: en efecto, si $x \in \mathsf{im}\,\phi$ y $b \in A$, entonces existe $(a_f)_{f\in X} \in \mathfrak{a}^{(X)}$ tal que $x = \sum_{f\in X} f(a_f)$ y

$$xb = \sum_{f\in X} f(a_f)b = \sum_{f\in X} (bf)(a_f) \in \mathsf{im}\,\phi,$$

así que $\mathsf{im}\,\phi$ es un ideal bilátero no nulo en A, esto es, $\mathsf{im}\,\phi = A$. Como A es proyectivo, concluimos que A es un sumando directo del módulo semisimple $\mathfrak{a}^{(X)}$. Usando **2.7**, vemos entonces que existe $X' \subset A$ tal que $A \cong \mathfrak{a}^{(X')}$; en particular, A es semisimple. Como todo A-módulo simple es isomorfo a un submódulo de A, el corolario **2.7** y la descomposición $A \cong \mathfrak{a}^{(X')}$ nos dicen que todos los módulos simples son isomorfos a $\mathfrak{a}$.

Finalmente, como A es finitamente generado, debe ser X' finito y concluimos que existe $n \in \mathbb{N}$ tal que $A \cong \mathfrak{a}^n$. El lema de Schur implica que $D = \mathsf{End}_A(\mathfrak{a})$ es un anillo de división y $A \cong \mathsf{End}_A(A) \cong \mathsf{End}_A(\mathfrak{a}^n) = \mathsf{M}_n(D)$. □

3.7. Sea D un anillo de división, $n \in \mathbb{N}$ y sea $A = \mathsf{M}_n(D)$ como en **3.6**. Sea $S = D^n$ el D-módulo de los vectores columna con coeficientes en D. Es claro que S es un A-módulo izquierdo con respecto a la multiplicación matricial. Es fácil ver, como en el caso de los espacios vectoriales, que se trata de un A-módulo simple. Obtenemos así un representante de la única clase de isomorfismo de A-módulos simples.

3.8. Teorema. (Wedderburn, 1908 [8]; Artin) *Sea A un anillo. Las siguientes afirmaciones son equivalentes:*

- *(a) A es semisimple;*
- *(b) todo A-módulo es semisimple;*
- *(c) existen $r, n_1, \dots, n_r \in \mathbb{N}$ y anillos de división $D_1, \dots, D_r$ tales que hay un isomorfismo de anillos $A \cong \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_r}(D_r)$.*

Demostración. Si A es semisimple, todo módulo libre es semisimple. Si M es un A-módulo arbitrario, entonces existe una sobreyección $L \to M$ con L libre, así que M es semisimple por **2.9**. Esto prueba que $(a) \Rightarrow (b)$.

Mostremos que $(b) \Rightarrow (c)$. La hipótesis nos dice que, en particular, ${}_AA$ es semisimple, así que **2.6** implica que $A \cong \bigoplus_{i\in I} S_i$ con $S_i \subset A$ un submódulo simple para cada $i \in I$. Como A es finitamente generado, **2.10** implica que I es finito. La afirmación *(c)* sigue entonces de los isomorfismos de anillos

$$A \cong \mathsf{End}_A(A) \cong \mathsf{End}_A(\bigoplus_{i\in I} S_i)$$

y de **1.10**. Finalmente, la implicación restante $(c) \Rightarrow (a)$ es consecuencia inmediata de **3.4** y **3.6**. □

3.9. Podemos describir los parámetros que aparecen en la tercera afirmación del teorema de la siguiente manera:

Proposición. *Sea A un anillo semisimple. Entonces hay un número finito de clases de isomorfismo de A-módulos simples. Sea $\{S_1, \dots, S_r\}$ un conjunto de representantes dos a dos no isomorfos para estas clases de isomorfismo y, para cada $i \in \{1, \dots, r\}$, pongamos $D_i = \mathsf{End}_A(S_i)$. Si $i \in \{1, \dots, r\}$, entonces $\mathsf{hom}_A(S_i, A)$ es un D_i-módulo a derecha de dimensión $n_i = \mathsf{dim}_{D_i} \mathsf{hom}_A(S_i, A)$ finita. Hay un isomorfismo de anillos $A \cong \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_r}(D_r)$.*

Demostración. Esto es consecuencia del teorema y del lema de Schur. □

3.10. Sea k un anillo conmutativo y sea A una k-álgebra que es semisimple en tanto anillo. Entonces los anillos de división que aparecen en la tercera afirmación de **3.8** son k-álgebras y el isomorfismo allí mencionado es un isomorfismo de k-álgebras.

3.11. Todo lo que hemos hecho ha sido considerando módulos a izquierda, pero claramente podemos desarrollar una teoría simétrica con módulos a derecha. El siguiente corolario, sin embargo, justifica la asimetría de la definición **3.1**:

Corolario. *Un anillo A es semisimple sii el A-módulo a derecha A es semisimple.*

Demostración. La tercera condición de **3.8** es evidentemente simétrica con respecto a la izquierda y la derecha. □

3.12. Corolario. *Un anillo semisimple es artiniano y nötheriano.*

Demostración. Esto es consecuencia directa de **2.10**. □

3.13. Si el cuerpo de base es algebraicamente cerrado, podemos describir más precisamente las álgebras semisimples.

Lema. *Sea k un cuerpo algebraicamente cerrado. Si D es una k-álgebra de dimensión finita, entonces $D \cong k$.*

Demostración. Sea D una k-álgebra de división y supongamos que existe $a \in D$ tal que el conjunto $\{1_D, a\}$ es linealmente independiente sobre k. Consideremos el morfismo de k-álgebras $f : p \in k[X] \mapsto p(a) \in D$. Como $\mathsf{dim}_k A < \infty$, es $\ker f \neq 0$ y existe $p \in k[X]$ mónico tal que $\ker f = (p)$. Más aún, como k es algebraicamente cerrado, existe $\lambda \in k$ y $q \in k[X]$ tal que $p = (X - \lambda)q$. Esto implica que $(a - \lambda 1_D)q(a) = 0$ en D: como $a \neq \lambda 1_D$, debe ser $q(a) = 0$, lo que contradice la elección de p, ya que $\deg q < \deg p$.

Vemos así que debe ser $\mathsf{dim}_k D = 1$, esto es, $D \cong k$. □

Teniendo esto en cuenta, es claro que **3.8** implica inmediatamente la siguiente proposición:

Proposición. *Sea k un cuerpo algebraicamente cerrado y A una k-álgebra. Entonces A es semisimple sii existen r, $n_1, \dots, n_r \in \mathbb{N}$ tales que $A \cong \mathsf{M}_{n_1}(k) \times \cdots \times \mathsf{M}_{n_r}(k)$.* □

3.14. Recordemos, por otro lado, el siguiente teorema:

Teorema. (Wedderburn, 1905 [7]; Dickson, 1905 [3]) *Un anillo de división finito es un cuerpo.* □

El teorema **3.8** implica, en vista de esto, la siguiente proposición:

Proposición. *Un anillo finito A es semisimple sii existen r, $n_1, \dots, n_r \in \mathbb{N}$ y cuerpos finitos $k_1, \dots, k_r$ tales que $A \cong \mathsf{M}_{n_1}(k_1) \times \cdots \times \mathsf{M}_{n_r}(k_r)$.* □

3.15. Proposición. *Sea A un anillo. Las siguientes afirmaciones son equivalentes:*

(a) A es semisimple;
(b) toda sucesión exacta corta de A-módulos se parte;
(c) todo A-módulo es proyectivo;
(d) todo A-módulo es inyectivo.

Demostración. Esto sigue de la equivalencia de las dos primeras afirmaciones de **3.8** y de **2.9**. □

3.16. Sean $r, n_1, \dots, n_r \in \mathbb{N}$ y $D_1, \dots, D_r$ son anillos de división y consideremos el anillo $A = \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_r}(D_r)$. Si $1 \leq i \leq r$, sea $\pi_i : A \to \mathsf{M}_{n_i}(D_i)$ la proyección en el i-ésimo factor y sean $M_i = D_i^{n_i}$ el $\mathsf{M}_{n_i}(D_i)$-módulo simple construido en **3.7** y $S_i = \pi_i^*(M_i)$. Entonces $\{S_i : 1 \leq i \leq r\}$ es un conjunto completo de representantes de las clases de isomorfismo de A-módulos simples.

Notemos que si k es un cuerpo y A es una k-álgebra, entonces es claro que $\dim_k S_i = n_i \dim_k D_i$ para cada $i \in \{1, \dots, r\}$.

4. Álgebras de grupo

4.1. Fijemos un grupo G y un cuerpo k. Notamos $\mathsf{cl}(G)$ al conjunto de las clases de conjugación de G.

4.2. Recordemos que la *k-álgebra de grupo kG* es la k-álgebra que, como k-módulo, es el k-módulo libre con base G y en la que el producto es el único producto k-bilineal y asociativo que existende al de G.

4.3. Una *representación de G (sobre k)* es un par (M, ρ) formado por un k-espacio vectorial M y un homomorfismo de grupos $\rho : G \to \mathsf{GL}(M)$. En general, escribimos M en lugar de (M, ρ), cuando esto no dé lugar a confusiones.

Si (M, ρ) y (M', ρ') son dos representaciones de G, un *morfismo de representaciones de G* $f : (M, \rho) \to (M', \rho')$ es un morfismo $f : M \to M'$ de k-espacios vectoriales tal que para todo $g \in G$ se tiene que $\rho'(g) \circ f = f \circ \rho(g)$.

4.4. Sea M un kG-módulo. Sobre el k-espacio vectorial M podemos contruir una representación (M, ρ) de G definiendo $\rho : G \to \mathsf{GL}(M)$ de manera que

$$\rho(g)(m) = gm, \qquad \forall g \in G,\ m \in M.$$

Si $f : M \to M'$ es un morfismo de kG-módulos y (M, ρ) y (M', ρ') son las representaciones de G correspondientes, es claro que $f : (M, \rho) \to (M, \rho')$ es un morfismo de representaciones.

Recíprocamente, si (M, ρ) es una representación de G, podemos hacer de M un kG-módulo si definimos la acción $kG \times M \to M$ poniendo

$$x \cdot m = \sum_{g \in G} a_g \rho(g)(m), \qquad \forall x = \sum_{g \in G} a_g g \in kG,\ m \in M.$$

Como antes, si $f : (M, \rho) \to (M', \rho')$ es un morfismo de representaciones de G, entonces la aplicación k-lineal $f : M \to M$ es de hecho kG-lineal.

Vemos así que las nociones de kG-módulo y de representación de G son equivalentes.

4.5. La *representación trivial* de G es la representación (k, ρ) con $\rho : G \to \mathsf{GL}(k)$ el homomorfismo trivial. El *kG-módulo trivial k* es el kG-módulo correspondiente a (k, ρ).

4.6. Sea M es un kG-módulo de dimensión 1 y sea $m \in M \setminus 0$. Si $g \in G$, entonces g es una unidad de kG y existe $\rho_M(g) \in k^\times$ tal que $gm = \rho_M(g)m$. Obtenemos así un morfismo de grupos $\rho_M : G \to k^\times$; de hecho, si identificamos a $k^\times$ con $\mathsf{GL}(M)$, (M, ρ_M) es la representación de G correspondiente al kG-módulo M. Como $k^\times$ es un grupo abeliano, el subgrupo derivado G' de G está contenido en el núcleo de ρ_M, y ρ_M induce entonces un morfismo de grupos $\bar\rho_M : G/G' \to k^\times$.

El morfismo $\bar\rho_M$ no depende de la elección del elemento $m \in M \setminus 0$. Más aún, si M' es un kG-módulo isomorfo a M, es fácil verificar que $\bar\rho_{M'} = \bar\rho_M$. Así, $\bar\rho_M$ depende solamente de la clase de isomorfismo $[M]$ de M.

Proposición. *Sea $\mathscr{S}_1$ un conjunto completo de representantes de las clases de isomorfismo de los kG-módulos de dimensión* 1*. Entonces la aplicación*

$$\Phi : [M] \in \mathscr{S}_1 \mapsto \bar\rho_M \in \mathsf{hom}_{\mathsf{Grp}}(G/G', k^\times)$$

es una biyección.

Demostración. Ya hemos mostrado que Φ está bien definida.

Si M y M' son kG-módulos de dimensión 1 y $m \in M \setminus 0$ y $m' \in M' \setminus 0$, entonces la aplicación lineal $f : M \to M'$ determinada por la condición de que $f(m) = m'$ es un isomorfismo de kG-módulos. En efecto, si $g \in G$, entones

$$f(gm) = f(\bar\rho_M(g)m) = \bar\rho_M(g)f(m) = \bar\rho_{M'}(g)f(m) = gf(m).$$

Esto muestra que Φ es inyectiva.

Sea, por otro lado, $\rho : G/G' \to k^\times$ un morfismo de grupos y consideremos sobre $M = k$ la acción de kG tal que $g \cdot m = \rho(gG')m$ si $g \in G$ y $m \in M$. Es inmediato verificar que esto define un kG-módulo y que $\bar\rho_M = \rho$. Vemos así que Φ es sobreyectiva. □

4.7. Lema. *Sea U un grupo abeliano finito y sea k un cuerpo algebraicamente cerrado de característica p. Si $p \nmid |U|$, entonces el grupo abeliano $\mathsf{hom}_{\mathsf{Grp}}(U, k^\times)$ es isomorfo a U.*

Demostración. Si $U = \bigoplus_{i \in I} U_i$ es una suma directa finita, entonces es

$$\mathsf{hom}_{\mathsf{Grp}}(U, k^\times) = \mathsf{hom}_{\mathsf{Grp}}(\bigoplus_{i \in I} U_i, k^\times) \cong \prod_{i \in I} \mathsf{hom}_{\mathsf{Grp}}(U_i, k^\times)$$

y como el producto es finito, de hecho

$$\mathsf{hom}_{\mathsf{Grp}}(U, k^\times) \cong \bigoplus_{i \in I} \mathsf{hom}_{\mathsf{Grp}}(U_i, k^\times).$$

Esto nos dice que para mostrar que la proposición vale para U basta mostrar que vale para cada uno de los sumandos U_i.

Ahora bien, todo subgrupo abeliano finito U es suma directa de subgrupos cíclicos y, más aún, si $p \nmid |U|$, entonces cada uno de estos subgrupos necesariamente tendrá orden coprimo con p. Concluímos que basta probar la proposición cuando $U = \mathbb{Z}_n$ con $p \nmid n$.

Es fácil ver que $\mathsf{hom}_{\mathsf{Grp}}(\mathbb{Z}_n, k^\times)$ es isomorfo al subgrupo $\mu_n \subset k^\times$ de las raíces n-ésimas de la unidad de k. Para terminar, recordamos que si $\operatorname{char} k \nmid n$, entonces $\mu_n \cong \mathbb{Z}_n$. □

4.8. Corolario. *Sea G un grupo finito y k un cuerpo algebraicamente cerrado de característica p. Si $p \nmid |G|$, entonces existen exactamente $|G/G'|$ clases de isomorfismo de kG-módulos de dimensión* 1*.*

Demostración. Esto es consecuencia de **4.6** y **4.7**. □

4.9. El resultado más importante sobre álgebras de grupos es el siguiente:

Teorema. (Maschke [5, 6]) *Sea G un grupo finito y k un cuerpo cuya característica no divide al orden de G. Entonces el álgebra de grupo kG es semisimple.*

Demostración. En vista de lo hecho en la sección anterior, hay que mostrar que si M es un kG-módulo y $N \subset M$ es un submódulo, entonces N posee un complemento en M. Sea $\iota : N \to M$ la inclusión y sea $s : M \to N$ un morfismo de k-espacios vectoriales tal que $s \circ \iota = \mathsf{id}_N$. Definimos una aplicación $\tilde{s} : M \to N$ poniendo

$$\tilde{s}(m) = \frac{1}{|G|} \sum_{g \in G} gs(g^{-1}m)$$

para cada $m \in M$; esto tiene sentido porque $|G|$ es inversible en k.

Afirmamos que $\tilde{s}$ es kG-lineal. Para verlo, basta mostrar que $\tilde{s}(hm) = h\tilde{s}(m)$ si $m \in M$ y $h \in G$, ya que $\tilde{s}$ es claramente k-lineal y G genera a kG como k-álgebra. Pero si $m \in M$ y $h \in G$, es

$$\begin{aligned} \tilde{s}(hm) &= \frac{1}{|G|} \sum_{g \in G} gs(g^{-1}hm) = \frac{1}{|G|} \sum_{g \in G} hgs(g^{-1}m) \\ &= h\Big(\frac{1}{|G|} \sum_{g \in G} gs(g^{-1}m)\Big) = h\tilde{s}(m), \end{aligned}$$

como queríamos.

Para terminar, mostremos que $\tilde{s} \circ \iota = \mathsf{id}_N$, lo que implicará que N es un sumando directo de M. Si $n \in N$, entonces

$$(\tilde{s} \circ \iota)(n) = \frac{1}{|G|} \sum_{g \in G} gs(g^{-1}\iota(n)) = \frac{1}{|G|} \sum_{g \in G} g(s \circ \iota)(g^{-1}n)$$

y, recordando que $s \circ \iota = \mathsf{id}_N$, vemos que esto es

$$= \frac{1}{|G|} \sum_{g \in G} gg^{-1}n = n$$

Esto prueba el teorema. $\square$

4.10. Supongamos desde ahora que k es un cuerpo en el que $|G|$ es inversible. Sea $\{S_1, \dots, S_r\}$ un conjunto completo de representantes de las clases de isomorfismo de kG-módulos simples y para cada $i \in \{1, \dots, r\}$, sea $D_i = \mathsf{End}_{kG}(S_i)$ y sea $n_i = \mathsf{dim}_{D_i} \mathsf{hom}_{kG}(S_i, kG)$. Entonces, como en la sección anterior, hay un isomorfismo de anillos

$$kG \cong \mathsf{M}_n(D_1) \times \cdots \times \mathsf{M}_n(D_r). \tag{1}$$

Observemos que D_i es una k-álgebra de división de dimensión finita para cualquier $i \in \{1, \dots, r\}$.

4.11. Proposición. *Es $\sum_{i=1}^r n_i^2 \,\mathsf{dim}_k D_i = |G|$.*

Demostración. El resultado sigue de tomar dimensión sobre k en (1). $\square$

4.12. Proposición. *Sea $i \in \{1, \dots, r\}$.*

(a) *Si $\mathsf{dim}_k S_i = 1$, entonces $n_i = \mathsf{dim}_k D_i = 1$.*
(b) *Si k es algebraicamente cerrado y $n_i = 1$, entonces $\mathsf{dim}_k S_i = 1$.*
(c) *Además, $|\{i \in \{1, \dots, r\} : \mathsf{dim}_k S_i = 1\}| = |G/G'|$.*

Demostración. Las dos primeras afirmaciones siguen de la igualdad $n_i \,\mathsf{dim}_k D_i = \mathsf{dim}_k S_i$ observada en **3.16** y del lema **3.13**. $\square$

4.13. Recordemos que si R es un anillo y $n \in \mathbb{N}$, entonces hay un isomorfismo $\mathsf{Z}(\mathsf{M}_n(R)) \cong \mathsf{Z}(R)$; en efecto, la aplicación $r \in \mathsf{Z}(R) \mapsto r\mathsf{I} \in \mathsf{M}_n(R)$ es un morfismo de anillos inyectivo que tiene a $\mathsf{Z}(\mathsf{M}_n(R))$ como imágen. Por otro lado, si R y S son anillos, entonces hay un isomorfismo evidente $\mathsf{Z}(R \times S) \cong \mathsf{Z}(R) \times \mathsf{Z}(S)$.

Proposición. *Es $r \leq |\mathsf{cl}(G)|$. Si k es algebraicamente cerrado, entonces vale la igualdad.*

Demostración. Aplicando las observaciones que preceden al enunciado a (1), vemos que hay un isomorfismo

$$\mathsf{Z}(kG) \cong \mathsf{Z}(D_1) \times \cdots \times \mathsf{Z}(D_r). \tag{2}$$

Para cada $c \in \mathsf{cl}(G)$ pongamos $z_c = \sum_{g \in c} g \in kG$. Es fácil ver que el conjunto $\{z_c : c \in \mathsf{cl}(G)\}$ es una base del k-espacio vectorial $\mathsf{Z}(kG)$ así que, en particular, $\dim_k \mathsf{Z}(kG) = |\mathsf{cl}(G)|$. Por otro lado, cualquiera sea $i \in \{1, \ldots, r\}$, es claro que $k1_{D_i} \subset \mathsf{Z}(D_i)$, de manera que $\dim_k \mathsf{Z}(D_i) \geq 1$. Teniendo esto en cuenta, el isomorfismo (2) da inmediatamente la desigualdad del enunciado.

Si k es algebraicamente cerrado, entonces $D_i \cong k$ para todo $i \in \{1, \ldots, r\}$, así que en este caso es $\dim_k \mathsf{Z}(D_i) = 1$. Vale entonces que $r = |\mathsf{cl}(G)|$ en este caso. □

5. Álgebras de grupo: el caso modular

5.1. El objetivo de esta sección es mostrar que la condición del teorema de Maschke es necesaria para que kG sea semisimple. Cuando la característica del cuerpo de base k divide al orden de G, decimos que estamos en el *caso modular*.

5.2. Si M es un kG-módulo, escribimos

$$M^G = \{m \in M : \text{para todo } g \in G \text{ es } gm = m\}.$$

Se trata de un subespacio vectorial de M, el subespacio de *invariantes* de M

Si $f : M \to M'$ es un morfismo de kG-módulos, entonces $f(M^G) \subset M'^G$, de manera que podemos considerar la restricción $f^G = f|_{M^G} : M^G \to M'^G$.

5.3. Teorema. *Sea G un grupo finito y k un cuerpo de característica p. Si $p \mid |G|$, entonces el álgebra kG no es semisimple.*

Demostración. Sea $P \subset G$ un p-subgrupo de Sylow. Consideremos el kP-módulo trivial k y pongamos $X = kG \otimes_{kP} k$. Como kG es un kG-kP-bimódulo, X es un kG-módulo. Mostraremos que X no es proyectivo: esto implica, claramente, que kG no es semisimple.

Para ver que X no es proyectivo basta mostrar que $\hom_{kG}(X, -)$ no preserva epimorfismos. Consideremos el morfismo de k-espacios vectoriales $\varepsilon : kG \to k$ tal que $\varepsilon(g) = 1$ para todo $g \in G$. Si dotamos a kG de su estructura de kG-módulo a izquierda y a k de su estructura de kG-módulo trivial, entonces es evidente que ε es un epimorfismo de kG-módulos. Queremos ver que la aplicación

$$\varepsilon_* : \hom_{kG}(kG \otimes_{kP} k, kG) \to \hom_{kG}(kG \otimes_{kP} k, k)$$

es nula y que $\hom_{kG}(kG \otimes_{kP} k, k) \neq 0$, de manera que, por supuesto, ε_* no es sobreyectiva.

Es fácil verificar que, para cada kG-módulo M, la aplicación

$$\alpha_M : f \in \hom_{kG}(kG \otimes_{kP} k, M) \mapsto f(1 \otimes 1) \in M^P$$

es un isomorfismo de grupos abelianos. Más aún, si $f : M \to M'$ es un morfismo de kG-módulos, entonces conmuta el siguiente cuadrado:

$$\begin{tikzcd}
\mathsf{hom}_{kG}(kG \otimes_{kP} k, M) \arrow[r, "f_*"] \arrow[d, "\alpha_M"'] & \mathsf{hom}_{kG}(kG \otimes_{kP} k, M') \arrow[d, "\alpha_{M'}"] \\
M^P \arrow[r, "f^P"] & M'^P
\end{tikzcd}$$

Tenemos entonces un cuadrado conmutativo

$$\begin{tikzcd}
\mathsf{hom}_{kG}(kG \otimes_{kP} k, kG) \arrow[r, "\varepsilon_*"] \arrow[d, "\cong"'] & \mathsf{hom}_{kG}(kG \otimes_{kP} k, k) \arrow[d, "\cong"] \\
(kG)^P \arrow[r, "\varepsilon^P"] & k^P
\end{tikzcd}$$

Es evidente que $k^P = k \neq 0$. Para terminar, y como las flechas verticales en este cuadrado son isomorfismos, solo tenemos que mostrar que $\varepsilon^P = 0$.

Sea $x = \sum_{g \in G} a_g g \in (kG)^P$. Entonces si $h \in P$, es

$$x = hx = \sum_{g \in G} a_g hg = \sum_{g \in G} a_{h^{-1}g} g.$$

Como G es una base para kG, esto nos dice que $a_g = a_{hg}$ siempre que $g \in G$ y $h \in P$.

Si $c \in G/H$, pongamos $x_c = \sum_{g \in c} g$ y $b_c = a_g$ para algún $g \in c$; notemos que esto último está bien definido porque el valor de a_g no depende del elemento g elegido en c. Es fácil verificar que $x = \sum_{c \in G/H} b_c x_c$. Vemos así que $\{x_c : c \in G/H\}$ genera a $(kG)^p$ como espacio vectorial.

Como P es un p-grupo no trivial, es $\varepsilon^P(x_c) = \sum_{g \in c} \varepsilon(g) = |P| = 0$ en k. Esto implica, por supuesto, que $\varepsilon^P = 0$ y prueba el teorema. □

5.4. Con respecto a la semisimplicidad, el 'peor caso' ocurre cuando G es un p-grupo. En efecto, en ese caso hay demasiado pocos kG-módulos simples:

Proposición. *Sea G un p-grupo finito y sea k un cuerpo de característica p. Entonces todo kG-módulo simple es isomorfo al kG-módulo trivial k.*

Demostración. Sea M un kG-módulo no nulo y sea $m \in M \setminus 0$. Consideremos el subgrupo abeliano T generado por $\{gm : g \in G\}$ en M. Como k tiene característica p, se trata de un grupo de exponente p y entonces existe $l \in \mathbb{N}$ tal que $|T| = p^l$. Notemos que G actúa sobre T. Si $t \in T$ y $o(t)$ es su G-órbita, entonces $|o(t)| = [G : \mathsf{stab}_G(t)]$. Luego si $|o(t)| \neq 1$, necesariamente $p \mid |o(t)|$. Como la órbita de $0 \in T$ tiene, por supuesto, un único elemento, vemos que debe existir $t \in T \setminus 0$ tal que $gt = t$ para todo $g \in G$. Esto nos dice que el subespacio vectorial $\langle t \rangle \subset M$ es un sub-kG-módulo.

Consideremos ahora un kG-módulo simple S. Aplicando las observaciones anteriores a S y usando la simplicidad, vemos que existe $s \in S \setminus 0$ tal que $\{s\}$ es una base de S y $gs = s$ para todo $g \in G$. Esto claramente implica que $S \cong k$. □

Referencias

[1] F. W. Anderson and K. R. Fuller, *Rings and categories of modules*, 2nd ed., Graduate Texts in Mathematics, vol. 13, Springer-Verlag, New York, 1992. ↑

[2] I. Assem, *Algèbres et modules*, Série Enseignement des Mathématiques, Presses de l'Université d'Ottawa (Ottawa) / Masson (Paris), 1997. ↑

[3] L. E. Dickson, *On finite algebras.*, Gött. Nachr. (1905), 358–393. ↑6

[4] E. Galina, *Representaciones de Grupos Finitos y Aplicaciones*, Technical Report 15/95, Trabajos de Matemática, Serie C, Universidad Nacional de Córdoba, Facultad de Matemática, Astronomía y Física, 1995. ↑

[5] H. Maschke, *Über den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen.*, Math. Ann. **50** (1898), 492-498. ↑9

[6] H. Maschke, *Beweis des Satzes, dass diejenigen endlichen linearen Substitutionsgruppen, in welchen einige durchgehends verschwindende Coefficienten auftreten, intransitiv sind*, Math. Ann. **52** (1899), 363–368. ↑9

[7] J. H. Maclagan-Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), no. 3, 349–352. MR 1500717 ↑6

[8] J. H. Maclagan Wedderburn, *On hypercomplex numbers*, London M. S. Proc. (2) **6** (1908), 77–118. ↑5

Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I, Buenos Aires (1428) Argentina.

E-mail address: `mariano@dm.uba.ar`