ANILLOS 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 generado por cualquiera de sus elementos no nulos.

1.5. Lema. *Sea A un anillo.*

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

Demostración. La primera afirmación es clara. La existencia de módulo simples es consecuencia de ella y de la existencia de ideales izquierdos maximales. Si S es un módulo simple y $m \in S \setminus 0$, entonces el morfismo $a \in A \mapsto am \in S$ es sobreyectivo, así que $S \cong A/\mathsf{ann}(m)$ y, por la primera parte, $\mathsf{ann}(m)$ es un ideal izquierdo maximal. □

1.6. La segunda afirmación de este lema implica que la colección de las clases de isomorfismo de A-módulos simples es un conjunto: en efecto, cada una de esas clases posee un representante que es un ideal izquierdo maximal de A y estos forman un conjunto.

1.7. 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. □

Fecha: 11 de junio, 2007; compilado: 14 de mayo de 2015.

1.8. 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.

1.9. 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 $M_1 = e_1M$ y $M_2 = e_2M$ 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

$$m \in M \mapsto (e_1m, e_2m) \in \pi_1^*(M_1) \oplus \pi_2^*(M_2)$$

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 $e_1\pi_2^*(T) = 0$. □

1.10. 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. □

1.11. 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 **1.10**. □

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 $\mathfrak{a} \supset \mathsf{ann}(m)$. 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 implicación $(a) \Rightarrow (c)$ 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. □

2.11. Considerando el caso de los espacios vectoriales, es claro que la escritura de un módulo semisimple como suma directa de submódulos simples no es, en general, única. Tenemos, sin embargo, el siguiente resultado:

Proposición. *Sea M un A-módulo. Para cada A-módulo simple S, sea*

$$M_S = \sum_{f\in \mathsf{hom}_A(S,M)} \mathsf{im}\, f.$$

Entonces M_S es un sub-A-módulo de M y depende únicamente de la clase de isomorfismo de S, de manera que si c es la clase de isomorfismo de S, podemos escribir $M_c = M_S$. Además, si M es semisimple, existe un conjunto $\mathscr{S}_M$ de clases de isomorfismo de A-módulos simples tal que $M_c \neq 0$ para todo $c \in \mathscr{S}_M$ y

$$M = \bigoplus_{c\in\mathscr{S}_M} M_c.$$

Demostración. Que para todo A-módulo simple M_S es un sub-A-módulo de M y que depende solamente de la clase de isomorfismo de S es claro. Supongamos entonces que M es semisimple y verifiquemos la última afirmación.

Sea $M = \bigoplus_{i\in I} S_i$ una descomposición de M como suma de A-módulos simples y sea $\mathscr{S}$ el conjunto de las clases de isomorfismo de A-módulos simples.

Para cada $c \in \mathscr{S}$, consideremos un A-módulo simple S_c tal que $S_c \in c$ y pongamos $I_c = \{i \in I : S_i \cong S_c\}$. Es claro que si $\mathscr{S}_M = \{c \in \mathscr{S} : I_c \neq \varnothing\}$, obtenemos una partición $\{I_c : c \in \mathscr{S}_M\}$ de I. Además, si $M'_c = \bigoplus_{i\in I_c} S_i$ para cada $c \in \mathscr{S}_M$, es

$$M = \bigoplus_{c\in\mathscr{S}_M} M'_c.$$

Para terminar, mostraremos que $M_c = M'_c$ para cada $c \in \mathscr{S}_M$.

Sean c, $c' \in \mathscr{S}_M$, $f : S_c \to M$ un morfismo de A-módulos y supongamos que existe $m \in \operatorname{im} f \cap \bigoplus_{i\in I_{c'}} S_i$ tal que $m \neq 0$. Entonces **1.10** implica que f es inyectivo, que $S_c \cong \operatorname{im} f \subset \bigoplus_{i\in I_{c'}} S_i$ y entonces, como el módulo de la izquierda es semisimple, que existe $i \in I_{c'}$ tal que $S_c \cong S_i$. La elección de I_c implica entonces que $c = c'$. Esto nos dice que $M_c \subset M'_c$. Como la inclusión recíproca es evidente, esto termina prueba la proposición. □

2.12. Si c es una clase de isomorfismo de A-módulos simples y M un A-módulo, el submódulo M_c de M construido en **2.11** es la *componente isotípica de M de tipo c*.

3. Anillos semisimples

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

3.2. Por ejemplo, es claro que un anillo de división es semisimple.

3.3. Lema. *Sea A un anillo semisimple. Si S es un A-módulo simple, entonces existe un ideal minimal $\mathfrak{a} \lhd_l A$ tal que $S \cong \mathfrak{a}$.*

Demostración. Si $m \in S \setminus 0$, entonces $S \cong A/\operatorname{ann}(m)$ y $\operatorname{ann}(m)$ es un ideal izquierdo maximal. Como A es semisimple, $\operatorname{ann}(m)$ es un sumando directo de A y existe un ideal $\mathfrak{a} \lhd_l A$ tal que $A = \operatorname{ann}(m) \oplus \mathfrak{a}$.

Observemos que $\mathfrak{a}$ es un A-módulo semisimple. En efecto, supongamos que posee un submódulo propio no nulo $\mathfrak{b} \subset \mathfrak{a}$. Entonces $\mathfrak{b}$ posee un complemento $\mathfrak{b}' \subset \mathfrak{a}$ tal que $\mathfrak{a} = \mathfrak{b} \oplus \mathfrak{b}'$ y $\operatorname{ann}(a) \subsetneq \operatorname{ann}(a) \oplus \mathfrak{b} \subsetneq A$. Esto contradice la maximalidad de $\operatorname{ann}(a)$. Vemos así que $\mathfrak{a}$ es un ideal izquierdo minimal.

Para terminar, notamos que $S \cong A/\operatorname{ann}(m) = (\operatorname{ann}(m) \oplus \mathfrak{a})/\operatorname{ann}(m) \cong \mathfrak{a}$. □

3.4. Proposición. *Sea A un anillo semisimple y sea $\mathscr{S}$ el conjunto de las clases de isomorfismo de A-módulos simples. Para todo $c \in \mathscr{S}$, la componente isotípica $A_c \subset A$ correspondiente a c es un ideal bilátero no nulo.*

Demostración. Sea $c \in \mathscr{S}$ y sea S un A-módulo simple tal que $S \in c$. Recordemos de **2.11** que

$$A_c = \sum_{f\in\operatorname{hom}_A(S,A)} \operatorname{im} f.$$

Sea $x \in A_c$ y $b \in A$. Entonces existe $n \in \mathbb{N}$ y morfismos $f_1, \ldots, f_n : S \to A$ tales que $x = \sum_{i=1}^n f(a)$. Entonces $xb = \sum_{i=1}^n f(a)b = \sum_{i=1}^n (fb)(a) \in A_c$. Vemos así que A_c es un ideal bilátero.

Por otro lado, **3.3** implica que existe un ideal $\mathfrak{b} \lhd_l A$ tal que $S \cong \mathfrak{b}$. Claramente, esto nos dice que $\mathfrak{b} \subset A_c$ y, entonces, que $A_c \neq 0$. □

3.5. 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 $j \in J$, y consideremos

las proyecciones canónicas $\pi_1 : A \times B \to A$ y $\pi_2 : A \times B \to B$. 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 **1.7**. □

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

3.7. Recordemos que si D es un anillo de división y $n \in \mathbb{N}$, entonces $\mathsf{M}_n(D)$ es artiniano a izquierda y 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 a izquierda y simple es semisimple y todos sus módulos simples son isomorfos. Además, si S es un A-módulo simple, entonces $D = \mathsf{End}_A(S)^{\mathsf{op}}$ 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 c la clase de isomorfismo de $\mathfrak{a}$ y A_c la componente isotípica de A correspondiente a c. Como **3.4** nos dice que A_c es un ideal bilátero no nulo y estamos suponiendo que A es simple, debe ser $A = A_c$. En consecuencia, A_c es la única componente isotípica no nula y vemos que c es la única clase de isomorfismo de A-módulos simples.

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, $\mathsf{im}\, f = A_c = A$. 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.

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 **1.10** implica que $D = \mathsf{End}_A(\mathfrak{a})$ es un anillo de división y entonces $A^{\mathsf{op}} \cong \mathsf{End}_A(A) \cong \mathsf{End}_A(\mathfrak{a}^n) = \mathsf{M}_n(D)$. Por supuesto, esto nos dice que $A \cong \mathsf{M}_n(D)^{\mathsf{op}} \cong M_n(D^{\mathsf{op}})$. □

3.8. Sea D un anillo de división, $n \in \mathbb{N}$ y sea $A = \mathsf{M}_n(D)$. 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.

3.9. Teorema. (Wedderburn, 1908 [9]; Artin) *Sea A un anillo. Las siguientes afirmaciones son equivalentes:*

(a) A es semisimple;
(b) todo A-módulo es semisimple;
(c) existen $r, n_1, \ldots, n_r \in \mathbb{N}$ y anillos de división $D_1, \ldots, D_r$ 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 **1.11**. Finalmente, la implicación restante $(c) \Rightarrow (a)$ es consecuencia inmediata de **3.5** y **3.7**. □

3.10. 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. □

3.11. 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 **3.9** 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. Corolario. *Si A es un anillo semisimple, existen finitas clases de isomorfismo de A-módulos simples.*

Demostración. En efecto, el número de clases de isomorfismo de A-módulo simples es el número r que aparece en la tercera parte de **3.9**. □

3.14. 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 **3.9** son k-álgebras y el isomorfismo allí mencionado es un isomorfismo de k-álgebras.

3.15. Cuando A es un álgebra sobre un cuerpo k algebraicamente cerrado, podemos ser más precisos en la tercera afirmación de **3.9**, ya que no hay k-álgebras de dimensión finita de división no triviales:

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 $\mathsf{ker}\, f \neq 0$ y existe $p \in k[X]$ mónico tal que $\mathsf{ker}\, f = (p)$. 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 **3.9** implica 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 $A \cong \mathsf{M}_{n_1}(k) \times \cdots \times \mathsf{M}_{n_r}(k)$.* □

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

Teorema. (Wedderburn, 1905 [8]; Dickson, 1905 [4]) *Un anillo de división finito es un cuerpo.* □

El teorema **3.9** implica, en vista de esta descripción de los anillos de división finitos, 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 $A \cong \mathsf{M}_{n_1}(k_1) \times \cdots \times \mathsf{M}_{n_r}(k_r)$.* □

3.17. 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 **3.9** y de **2.9**. □

3.18. 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 **3.8** 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. El radical

4.1. Sea A un anillo. Recordemos que si M es un A-módulo izquierdo, entonces el *radical* $\operatorname{rad} M$ de M es la intersección de sus submódulos maximales. Es claro que

$$\operatorname{rad} M = \bigcap_{\substack{h:M\to S \\ S \text{ simple}}} \ker h. \tag{1}$$

Cuando M no posee submódulos maximales, es $\operatorname{rad} M = M$.

4.2. Lema. *Sea A un anillo y M un A-módulo finitamente generado. Entonces $\operatorname{rad} M$ es un submódulo propio de M.*

Demostración. Sea $\mathscr{M}$ el conjunto de todos los submódulos propios de M y sea $\{x_1, \dots, x_n\} \subset M$ tal que $M = \sum_{i=1}^n Am$. Claramente $\mathscr{M} \neq \varnothing$. veamos que se trata de un conjunto inductivo.

Si $M_{\lambda\lambda\in\Lambda} \subset \mathscr{M}$ es una cadena en $\mathscr{M}$, sea $N = \bigcup_{\lambda\in\Lambda} M_\lambda$. Como la unión es creciente, si fuese $N = M$, entonces existiría $\lambda \in \Lambda$ tal que $\{x_1, \dots, x_n\} \subset M_\lambda$, esto es, tal que $M = M_\lambda$, lo que es imposible. Luego $N \in \mathscr{M}$ y vemos que cada cadena en $\mathscr{M}$ es acotada.

El lema de Zorn nos permite concluir, entonces, que existe un submódulo propio maximal $N \subsetneq M$. Como $\operatorname{rad} M \subset N$, esto prueba el lema. □

4.3. Si un módulo no es finitamente generado, puede coincidir con su radical. Por ejemplo, si $A = \mathbb{Z}$ y $M = \mathbb{Q}$, entonces $\operatorname{rad} M = M$. En efecto, M no posee submódulos maximales: si $N \subset M$ es maximal, entonces M/N es un grupo abeliano simple y existe p primo tal que $M/N \cong \mathbb{Z}_p$. Pero entonces la proyección canónica es un morfismo no nulo $\mathbb{Q} \to \mathbb{Z}_p$, lo que es imposible.

4.4. Lema. *Sea A un anillo.*

(a) Si $f : M \to N$ un morfismo de A-módulos, entonces $f(\operatorname{rad} M) \subset \operatorname{rad} N$.
(b) Si M es un A-módulo y $N \subset \operatorname{rad} M$ es un submódulo, entonces $\operatorname{rad}(M/N) = (\operatorname{rad} M)/N$.
(c) Si M es un A-módulo, $\operatorname{rad}(M/\operatorname{rad} M) = 0$.

Demostración. (a) Sea $m \in \operatorname{rad} M$ y sea $h : N \to S$ un morfismo de A-módulos con S simple. Entonces (1) implica que $h(f(m)) = 0$. Usando (1) otra vez, vemos que $f(m) \in \operatorname{rad} N$.

(b) Si $\pi : M \to M/N$ es la proyección canónica, la primera parte nos dice que $(\operatorname{rad} M)/M = \pi(\operatorname{rad} M) \subset \operatorname{rad}(M/N)$. Recíprocamente, supongamos que $m \in M \setminus \operatorname{rad} M$. Entonces existe un morfismo $h : M \to S$ con S simple y $h(m) \neq= 0$. Como $N \subset \operatorname{rad} M \subset \ker h$, h induce un morfismo $\bar{h} : M/N \to S$ tal que $\bar{h} \circ \pi = h$. Es $\bar{h}(\pi(m)) \neq 0$ y vemos que $\pi(m) \notin \operatorname{rad}(M/N)$.

(c) Esto sigue de tomar $N = \operatorname{rad} M$ en *(b)*. □

4.5. La razón por la que estamos interesados en el radical es la siguiente caracterización de la semisimplicidad:

Proposición. *Sea A un anillo y M un A-módulo.*

(a) Si M es semisimple, entonces $\operatorname{rad} M = 0$.
(b) Las siguientes afirmaciones son equivalentes:
  (i) M es artiniano y $\operatorname{rad} M = 0$.
  (ii) M es suma directa finita de submódulos simples.

Demostración. Sea M un A-módulo semisimple y sea $M = \bigoplus_{i \in I} S_i$ una descomposición de M como suma directa de A-módulos simples. Si para cada $i \in I$ notamos $\pi_i : M \to S_i$ a la proyección canónica, entonces que $\operatorname{rad} M \subset \bigcap_{i \in I} \ker \pi_i = 0$. Esto prueba *(a)*. Veamos *(b)*.

(*i*) $\Rightarrow$ (*ii*): Sea $\mathscr{M}$ el conjunto de los submódulos maximales de M y sea $\mathscr{I} = \{\bigcap_{N \in F} N : F \subset \mathscr{M} \text{ es finito}\}$. Como M es artiniano, $\mathscr{I}$ posee un elemento minimal M_0. Supongamos que $F \subset \mathscr{M}$ es una familia finita de submódulos maximales tal que $M_0 = \bigcap_{N \in F} N$. Si $m \in M_0 \setminus 0$, y como $m \notin \operatorname{rad} M$, existe un submódulo $N \in \mathcal{M}$ tal que $m \notin N$. Pero entonces $M_0 \subsetneq M_0 \cap N \in \mathscr{I}$, lo que es imposible. Vemos así que debe ser $M_0 = 0$.

Esto implica que la aplicación $M \to \bigoplus_{N \in F} M/N$, que en cada componente es una proyección canónica, es inyectiva. Notemos que, como $F \subset \mathscr{M}$, el A-módulo $\bigoplus_{N \in F} M/N$ es semisimple. Como M es isomorfo a un submódulo de esta suma directa, es él mismo semisimple. En vista de **2.10**, M es isomorfo a una suma directa finita de submódulos simples.

(*ii*) $\Rightarrow$ (*i*): Si $M = \bigoplus_{i \in I} S_i$ es una suma directa finita de submódulos simples, entonces $\operatorname{rad} M = 0$ por la parte *(a)* de la proposición y es artiniano en vista de **2.10**. □

4.6. El *radical de Jacobson* de un anillo A (o, simplemente, el *radical*) es el ideal izquierdo $J(A) = \operatorname{rad} A$.

4.7. La segunda parte de la proposición **4.5** tiene como consecuencia inmediata el siguiente teorema:

Teorema. *Sea A un anillo artiniano. Entonces A es semisimple sii $J(A) = 0$.* □

4.8. La siguiente proposición lista alguna de las propiedades más importantes del radical de un anillo:

Proposición. *Sea A un anillo y $J(A)$ su radical de Jacobson.*

(a) $J(A)$ es un ideal bilátero.
(b) $a \in J(A)$ sii para todo $x \in A$, $1 - xa$ es inversible a izquierda.
(c) $J(A)$ es el único elemento maximal de $\{I \lhd A : \forall x \in I, 1 - x \in A^\times\}$.
(d) $J(A) = \operatorname{rad}{}_A A = \operatorname{rad} A_A$.

Demostración. Si $b \in A$ y $f : a \in A \mapsto ab \in A$, entonces $f \in \operatorname{hom}_A(A, A)$ y **4.4** implica que $f(J(A)) \subset J(A)$. Esto dice, precisamente, que el ideal izquierdo $J(A)$ también es un ideal derecho y prueba *(a)*.

Supongamos que a, $x \in A$ son tales que $1 - xa$ no tiene inverso a izquierda. Entonces el ideal $A(1 - xa)$ es propio y existe un ideal izquierdo maximal M tal que $1 - xa \in M$. Como $J(A) \subset M$, esto implica que $a \notin J(A)$: en efecto, si $a \in J(A)$, sería $1 = (1 - xa) + xa \in M + J(A) \subset M$. Esto muestra la necesidad de la condición en *(b)*.

Para ver la suficiencia, consideremos $a \in A$ tal que $1 - xa$ es inversible a izquierdo para todo $x \in A$. Supongamos que $a \notin J(A)$, de manera que existe un ideal maximal $M \lhd_l A$ tal que $a \notin M$. Pero entonces $1 \in A = M + Aa$ y vemos que existe $x \in A$ tal que $y = 1 - xa \in M$. Esto es absurdo, porque por hipótesis y es inversible a izquierda.

Sea $\mathscr{I} = \{I \lhd A : \forall x \in I,\, 1 - x \in A^\times\}$. Para ver (c) tenemos que mostrar que $J(A) \in \mathscr{I}$ y que $J(A) \subset I$ para todo $I \in \mathscr{I}$.

Veamos que $J(A) \in \mathscr{I}$. Ya sabemos que $J(A) \lhd A$. Sea $x \in J(A)$. La parte *(b)* implica que $1 - x$ es inversible a izquierda, de manera que existe $z \in A$ tal que $z(1 - x) = 1$. Como $1 - z = -zx \in J(A)$, otra vez *(b)* nos dice que $z = 1 - (1 - z)$ es inversible a izquierda, esto es, que existe $w \in A$ tal que $wz = 1$. Como $wz = 1 = z(1 - x)$, debe ser $w = 1 - x$ y entonces $z = (1 - x)^{-1}$. Concluimos que $J(A) \in \mathscr{I}$, como queríamos.

Sea ahora $I \in \mathscr{I}$ y sea $a \in I$. Si $x \in A$, $ax \in I$ así que por hipótesis $1 - ax \in A^\times$. Usando *(b)* vemos que $a \in J(A)$. Así, $I \subset J(A)$.

Para terminar, notemos que *(d)* sigue inmediatamente del hecho de que la afirmación *(c)* es simétrica con respecto a la izquierda y la derecha. □

4.9. Sabiendo que el radical es un ideal bilátero, el siguiente enunciado tiene sentido:

Proposición. *Si A es un anillo artiniano, entonces $A/J(A)$ es semisimple.*

Demostración. La tercera parte de **4.4** implica que $\operatorname{rad}_A(A/J(A)) = 0$, de manera que **4.5** nos permite concluir que $A/J(A)$ es semisimple como A-módulo.

Ahora bien, un subgrupo abeliano de $A/J(A)$ es un sub-A-módulo sii es un sub-$A/J(A)$-módulo. Esto nos dice que $A/J(A)$ es semisimple también como $A/J(A)$-módulo, esto es, que $A/J(A)$ es semisimple como anillo. □

4.10. De hecho, dado un anillo A, el radical $J(A)$ es el menor ideal de A tal que $A/J(A)$ es semisimple. En efecto, si $I \lhd A$ es un ideal tal que A/I es semisimple, entonces $0 = \operatorname{rad}_{A/I} A/I = \operatorname{rad}_A A/I$, de manera que $J(A) = \operatorname{rad}_A A \subset I$, como consecuencia de la segunda parte de **4.4**.

4.11. Esta proposición tiene la siguiente consecuencia extremadamente útil:

Proposición. *Sea A un anillo artiniano y M un A-módulo. Entonces* $\operatorname{rad} M = J(A)M$.

Demostración. Pongamos $J = J(A)$. Si $m \in M$ y $f : a \in A \mapsto am \in M$, entonces **4.4***(a)* nos dice que $Jm = f(\operatorname{rad} A) \subset \operatorname{rad} M$. Como esto es cierto para todo $m \in M$, $JM \subset \operatorname{rad} M$. Usado ahora **4.4***(b)*, vemos que $(\operatorname{rad} M)/JM = \operatorname{rad}(M/JM)$. Pero M/JM es un A/J-módulo y A/J es un anillo semisimple, de manera que $\operatorname{rad}_{A/J} M/JM = 0$ en vista de **4.5***(a)*. Como un sub-A-módulo de M/JM es lo mismo que un sub-A/J-módulo, esto implica que $(\operatorname{rad} M)/JM = \operatorname{rad}_A M/JM = 0$ y, en definitiva, que $\operatorname{rad} M = JM$. □

4.12. Un elemento x de un anillo A es *nilpotente* si existe $n \in \mathbb{N}$ tal que $x^n = 0$. Un ideal $\mathfrak{a} \lhd A$ es *nil* si todos sus elementos son nilpotentes. Finalmente, un ideal $\mathfrak{a} \lhd A$ es *nilpotente* si existe $n \in \mathbb{N}$ tal que $\mathfrak{a}^n = 0$.

Proposición. *Sea A un anillo.*

(a) Todo ideal nil está contenido en $J(A)$.

Supongamos ahora que A es artiniano a izquierda.

(b) $J(A)$ *es el ideal bilátero nilpotente más grande.*
(c) $J(A)$ *es el único ideal nil* $\mathfrak{a}$ *de* A *tal que* $A/\mathfrak{a}$ *es semisimple.*

Demostración. (a) Sea $\mathfrak{a} \lhd A$ un ideal nil. Si $x \in A$ y $n \in \mathbb{N}$ es tal que $x^n = 0$, entonces $(1-x)\sum_{i=0}^{n-1} x^i = 1$, de manera que $1-x$ es inversible. Usando la tercera parte de **4.8**, vemos que $x \in J(A)$.

(b) Es claro que todo ideal nilpotente es nil, así que *(a)* implica que $J(A)$ contiene a todo ideal nilpotente. La afirmación *(b)* quedará probada, entonces, si mostramos que $J = J(A)$ es nilpotente.

La cadena de ideales $J \supset J^2 \supset J^3 \supset \cdots$ debe estabilizarse, así que existe $n \in \mathbb{N}$ tal que $J^n = J \cdot J^n$. Supongamos que $J^n \neq 0$. Entonces el conjunto de ideales izquierdos $\mathscr{I} = \{\mathfrak{a} \lhd_l A : \mathfrak{a} = J\mathfrak{a}\}$ es no vacío. Como A es artiniano, existe un elemento $\mathfrak{a} \in I$ minimal. Además, como $\mathfrak{a} = J\mathfrak{a} = J^2\mathfrak{a} = \cdots = J^n\mathfrak{a}$, existe $x \in \mathfrak{a}$ tal que $J^n x \neq 0$ y, entonces, $J \cdot J^n x = J^n x$. Así, $J^n x \in \mathscr{I}$. Como $J^n x \subset \mathfrak{a}$, la elección de $\mathfrak{a}$ implica que $\mathfrak{a} = J^n x$ y vemos que $\mathfrak{a}$ es finitamente generado. Pero entonces

$$\begin{aligned} \mathfrak{a} &\supsetneq \operatorname{rad}\mathfrak{a} && \text{por } \mathbf{4.2} \\ &= J\mathfrak{a} && \text{por } \mathbf{4.11} \\ &= \mathfrak{a} \end{aligned}$$

Esto es imposible y debe ser, en consecuencia, $J^n = 0$.

Finalmente, sea $\mathfrak{a} \lhd A$ un ideal nil tal que $A/\mathfrak{a}$ es semisimple. Por la parte *(a)*, $\mathfrak{a} \subset J(A)$; por otro lado, como el ideal $J(A)/\mathfrak{a} \lhd A/\mathfrak{a}$ es nilpotente, la parte *(b)* nos dice que $J(A)/\mathfrak{a} \subset \operatorname{rad}(A/\mathfrak{a})$. Como estamos suponiendo que $A/\mathfrak{a}$ es semisimple, $\operatorname{rad}(A/\mathfrak{a}) = 0$ y vemos que $J(A) = \mathfrak{a}$. Esto prueba *(c)*. □

4.13. La última parte de esta proposición puede ser usada frecuentemente para identificar el radical de un álgebra.

Por ejemplo, sea $Q = (Q_0, Q_1)$ un quiver finito, k un cuerpo y kQ la k-álgebra de caminos sobre Q. Sea $R \lhd kQ$ el ideal generado por los caminos de longitud 1 y sea $I \lhd kQ$ un ideal *admisible*, esto es, sea I un ideal tal que *(i)* $I \subset R^2$ y *(ii)* existe $n \in \mathbb{N}$ tal que $U \supset R^n$. Consideremos el álgebra $A = kQ/I$. Afirmamos que $\operatorname{rad} A = R/I$.

Notemos que A es artiniana, ya que $\dim_k A < \infty$ debido a la condición *(ii)*. Ahora bien, el cociente $A/R = (kQ/I)/(R/I) \cong kQ/R \cong k^{|Q_0|}$ es isomorfo a un producto de $|Q_0|$ copias de k, así que es semisimple, y, por otro lado, todo elemento de R/I es nilpotente en A en vista de la condición *(ii)*. Luego **4.12***(c)* implica que R/I es el radical de A.

4.14. Proposición. *Sea* A *un anillo y sea* $J(A)$ *su radical de Jacobson. Si* S *es un* A*-módulo simple, entonces* $J(A)S = 0$ *y* S *es, de manera natural, un* $A/J(A)$*-módulo simple. Recíprocamente, si* S *es un* $A/J(A)$*-módulo simple, entonces, vía restricción de escalares a lo largo de la proyección canónica* $A \to A/J(A)$*,* S *es un* A*-módulo simple.*

Demostración. Claramente alcanza con probar que si S es un A-módulo simple, entonces $J(A)S = 0$.

Sea $s \in S$. La aplicación $f : a \in A \mapsto as \in S$ es un morfismo de A-módulos no nulo, así que $J(A) \subset \ker s$. Esto significa que $J(A)s = 0$. En consecuencia $J(A)S = 0$, como queríamos ver. □

4.15. Corolario. *Sea* A *un anillo. Hay un biyección entre las clases de isomorfismo de* A*-módulos simples y las clases de isomorfismo de* $A/J(A)$*-módulos simples.*

En particular, si A *es artiniano, hay un número finito de clases de isomorfismo de* A*-módulos simples.*

Demostración. La primera afirmación es consecuencia inmediata de **4.14**. Para ver la segunda, basta observar que si A es artiniano, **4.9** nos dice que $A/J(A)$ es

semisimple y entonces **3.13** junto con la primera parte implican la finitud del conjunto de clases de isomorfismo de A-módulos simples. □

5. Álgebras de grupo

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

5.2. 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 extiende al de G.

5.3. 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 $\rho'(g) \circ f = f \circ \rho(g)$.

5.4. Sea M un kG-módulo. Sobre el k-espacio vectorial M podemos construir 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.

5.5. 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).

5.6. 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. □

5.7. 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. Concluimos 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 $\mu_n \cong \mathbb{Z}_n$. □

5.8. 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 **5.6** y **5.7**. □

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

Teorema. (Maschke [6, 7]) *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

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

como queríamos.

Para terminar, mostremos que $\tilde{s}\circ\iota = \mathrm{id}_N$, 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 $s\circ\iota = \mathrm{id}_N$, vemos que esto es

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

Esto prueba el teorema. □

5.10. 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 $n_i = \dim_{D_i} \hom_{kG}(S_i, kG)$. Entonces, como en la sección anterior, hay un isomorfismo de anillos

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

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

5.11. Proposición. *Es* $\sum_{i=1}^{r} n_i^2 \dim_k D_i = |G|$.

Demostración. El resultado sigue de tomar dimensión sobre k en (2). □

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

(a) Si $\dim_k S_i = 1$, *entonces* $n_i = \dim_k D_i = 1$.
(b) Si k *es algebraicamente cerrado y* $n_i = 1$, *entonces* $\dim_k S_i = 1$.

Demostración. Las dos afirmaciones siguen de la igualdad $n_i \dim_k D_i = \dim_k S_i$ observada en **3.18** y del lema **3.15**. □

5.13. 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 imagen. 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 (2), vemos que hay un isomorfismo

$$\mathsf{Z}(kG) \cong \mathsf{Z}(D_1) \times \cdots \times \mathsf{Z}(D_r). \tag{3}$$

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 $i \in \{1, \dots, r\}$, 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 (3) da inmediatamente la desigualdad del enunciado.

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

5.14. Si k es algebraicamente cerrado, podemos explicitar el isomorfismo (2).

5.15. Proposición. *Sea k un cuerpo algebraicamente cerrado. Entonces si $\{S_i\}_{i=1}^r$ es un conjunto completo de representantes de clases de isomorfismo de kQ-módulos simples, hay un isomorfismo $\phi : kG \to \prod_{i=1}^r \mathsf{End}_k(S_i)$ tal que, si para cada $i \in \{1,\dots,r\}$, $\pi_r : \prod_{i=1}^r \mathsf{End}_k(S_i) \to \mathsf{End}_k(S_i)$ es la proyección k-ésima, entonces*

$$\pi_i(\phi(g)) = \rho_{S_i}(g)$$

para cada $i \in \{1,\dots,r\}$ y $g \in G$.

6. Álgebras de grupo: el caso modular

6.1. 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*.

6.2. 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 $f^G = f|_{M^G} : M^G \to M'^G$.

6.3. 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 $\mathsf{hom}_{kG}(X,-)$ 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

$$\varepsilon_* : \mathsf{hom}_{kG}(kG \otimes_{kP} k, kG) \to \mathsf{hom}_{kG}(kG \otimes_{kP} k, k)$$

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

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

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

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

$$\begin{array}{ccc} \mathsf{hom}_{kG}(kG \otimes_{kP} k, M) & \xrightarrow{f_*} & \mathsf{hom}_{kG}(kG \otimes_{kP} k, M') \\ \downarrow{\scriptstyle \alpha_M} & & \downarrow{\scriptstyle \alpha_{M'}} \\ M^P & \xrightarrow{\quad f^P \quad} & M'^P \end{array}$$

Tenemos entonces un cuadrado conmutativo

$$\begin{array}{ccc} \mathsf{hom}_{kG}(kG \otimes_{kP} k, kG) & \xrightarrow{\varepsilon_*} & \mathsf{hom}_{kG}(kG \otimes_{kP} k, k) \\ \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong} \\ (kG)^P & \xrightarrow{\quad \varepsilon^P \quad} & k^P \end{array}$$

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. □

6.4. 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 $S \cong k$. □

6.5. Cuando la característica p del cuerpo de base divide al orden de G pero G no es necesariamente un p-grupo, es posible describir precisamente el número de kG-módulos simples. Antes necesitaremos de algunos lemas.

6.6. Supongamos que k es un cuerpo de característica p y sea A una k-álgebra de dimensión finita. Si $a, b \in A$, escribimos $[a, b] = ab - ba$. Notemos $S(A)$ al subespacio vectorial de A generado linealmente por $\{[a, b] : a, b \in A\}$ y

$$T(A) = \{x \in A : \text{existe } n \in \mathbb{N} \text{ tal que } x^{p^n} \in S\}.$$

6.7. Lema. *$T(A)$ es un subespacio vectorial de A y $S(A) \subset T(A)$. Además, siempre que $a \in S(A)$ es $a^p \in S(A)$.*

Demostración. Como $ab \equiv ba \pmod{S(A)}$ cualquiera sean a y $b \in A$, es

$$(a + b)^p \equiv \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \equiv a^p + b^p \pmod{S(A)} \tag{4}$$

ya que $\binom{p}{i} = 0$ en k si $0 < i < p$.

Sean $a, b \in T(A)$ y $\alpha, \beta \in k$. Existen entonces $n, m \in \mathbb{N}$ tales que $a^{p^n}, b^{p^m} \in S(A)$ y, si $l = \max\{n, m\}$,

$$(\alpha a + \beta b)^{p^l} \equiv \alpha^{p^l} a^{p^l} + \beta^{p^l} b^{p^l} \equiv 0 \pmod{S(A)}.$$

Esto muestra que $T(A)$ es un subespacio vectorial.

Por otro lado, si $a, b \in A$, entonces

$$(ab - ba)^p \equiv a^p b^p - b^p a^p \equiv 0 \pmod{S(A)},$$

así que $S(A) \subset T(A)$.

La última afirmación del enunciado sigue de (4) y de que $[a,b]^p = [a^p, b^p]$ si $a, b \in A$. □

6.8. Lema. *Sea k un cuerpo de característica p.*

(a) Si A y B son k-álgebras, entonces $S(A \times B) = S(A) \times S(B)$ y $T(A \times B) = T(A) \times T(B)$.
(b) Si $A = \mathsf{M}_n(k)$, $S(A) = T(A)$ es el subespacio de las matrices de traza nula. En particular, la codimensión de $T(A)$ en A es 1.

Demostración. La primera parte sigue de un cálculo directo. Veamos la segunda.

Sea $A = \mathsf{M}_n(k)$ y sea $L = \{a \in A : \mathsf{tr}\, a = \}$. Como $\mathsf{tr}[a,b] = 0$ cualesquiera sean a y $b \in A$, es $S(A) \subset L$. Si $1 \leq i, j \leq n$, sea $E_{i,j}$ la matriz elemental que tiene un 1 como componente (i,j) y 0 en todas las demás componentes, entonces

$$E_{i,j} = [E_{i,j}, E_{k,j}]$$

y

$$E_{i,i} - E_{j,j} = [E_{i,j}, E_{j,i}]$$

siempre que i, j, $j \in \{1, \dots, n\}$ son distintos dos a dos. Como $\{E_{i,j} : 1 \leq i, j \leq n\}$ es una base de A, vemos que $S(A) = L$.

Sabemos que $S(A) \subset T(A) \subset A$ y, ahora, que $S(A)$ tiene codimensión 1. Para ver que $S(A) = T(A)$, entonces, alcanza con ver que $T(A) \neq A$. Pero esto sigue inmediatamente de la observación de que $E_{1,1} \notin T(A)$. □

6.9. Proposición. *Sea k un cuerpo algebraicamente cerrado de característica p y A una k-álgebra de dimensión finita. Entonces A posee exactamente $\dim_k A/T(A)$ clases de isomorfismo de módulos simples.*

Demostración. Sea J el radical de A. La segunda parte de **4.12** nos dice que J es nilpotente, así que claramente $J \subset T(A)$. Veamos que

$$T(A)/J = T(A/J). \tag{5}$$

Si $a \in A$, notamos $\bar{a}$ a la clase de a en $A/J(S)$.

Sea primero $a \in T(A)$, de manera que existe $n \in \mathbb{N}$ tal que $a^{p^n} \in S(A)$. Entonces existen $k \in \mathbb{N}$ y x_1, y_1, …, x_k, $y_k \in A$ tales que $a^{p^n} = \sum_{i=1}^k [x_i, y_i]$ y vemos que $\bar{a}^{p^n} = \sum_{i=1}^k [\bar{x}_i, \bar{y}_i] \in S(A/J)$, esto es, $\bar{a} \in T(A/J)$. Hemos mostrado que $T(A)/J \subset T(A/J)$.

Recíprocamente, si $a \in A$ es tal que $\bar{a} \in T(A/J)$, entonces existen $n \in \mathbb{N}$ y x_1, y_1, …, x_k, $y_k \in A$ tales que $\bar{a}^{p^n} = \sum_{i=1}^k [\bar{x}_i, \bar{y}_i] \in S(A/J)$. Luego existe $z \in J$ tal que

$$a^{p^n} = \sum_{i=1}^k [x_i, y_i] + z \in S(A) + J \subset T(A).$$

En particular, vemos que $a \in T(A)$. Así, tenemos que $T(A)/J \supset T(A/J)$ y, en consecuencia, probamos (5), como queríamos.

Como A/J es semisimple y el cuerpo k es algebraicamente cerrado, existen r, $n_1, \dots, n_r \in \mathbb{N}$ tales que

$$A/J \cong \mathsf{M}_{n_1}(k) \times \cdots \times \mathsf{M}_{n_r}(k).$$

Más aún, n es precisamente el número de clases de isomorfismo de A/J-módulos simples. El lema **6.8** y este isomorfismo implican que la codimensión de $T(A/J)$

en A/J es precisamente r. Teniendo en cuenta (5), vemos que

$$\begin{aligned} r &= \dim_k A/J - \dim_k T(A/J) \\ &= \dim_k A/J - \dim_k T(A)/J \\ &= \dim_k A - \dim_k T(A), \end{aligned}$$

y esto es precisamente la codimensión de $T(A)$ en A. □

6.10. Sea G un grupo finito y p un número primo. Decimos que un elemento $g \in G$ es *p-regular* si su orden es coprimo con p y que es *p-singular* si su orden es una potencia de p.

6.11. Es evidente que si $g \in G$ es un elemento p-regular (p-singular) y g' es conjugado a g, entonces g' es p-regular (p-singular, respectivamente).

Lema. *Sea G un grupo finito y p un número primo. Todo elemento $g \in G$ puede escribirse, de manera única, como un producto $g = st$ con s p-singular, t p-regular y $st = ts$.*

Si $g' \in G$ es conjugado de g y la correspondiente escritura es $g' = s't'$, entonces s es conjugado de s' y t es conjugado de t'.

Demostración. Supongamos que el orden de $g \in G$ es $p^n m$ con $p \nmid m$ y sean $a, b \in \mathbb{Z}$ tales que $ap^n + bm = 1$. Ponemos $s = g^{bm}$ y $t = g^{ap^n}$. Es fácil verificar que la escritura $g = st$ satisface las condiciones del lema.

Sea $g = s_1 t_1$ es otra factorización de g que satisface las condiciones del enunciado, esto es, tal que s_1 es p-singular, t_1 es p-regular y $s_1 t_1 = t_1 s_1$. Como s_1 y t_1 conmutan, el orden $p^n m$ de $g = s_1 t_1$ es el mínimo común múltiplo de los órdenes de s_1 y t_1, vemos que s_1 tiene necesariamente orden p^n y t_1 orden m. Es claro que g conmuta con s_1 y con t_1, así que

$$t_1 = t_1^{ap^n+bm} = t_1^{ap^n} = (xs_1^{-1})^{ap^n} = x^{ap^n} s_1^{-ap^n} = x^{ap^n} = t$$

y

$$s_1 = s_1^{ap^n+bm} = s_1^{bm} = (xt_1^{-1})^{bm} = x^{bm} t_1^{-bm} = x^{bm} = s.$$

Concluimos que la factorización encontrada es la única.

Sea ahora $g' \in G$ conjugado a g' y sea $g' = s't'$ una factorización como la obtenida en la primera parte. Si $h \in G$ es tal que $g' = hgh^{-1}$ entonces $s'' = hsh^{-1}$ y $t'' = hth^{-1}$ son un elemento p-singular y uno p-regular tales que $g' = s''t''$ y $s''t'' = t''s''$. La unicidad ya probada implica entonces que $s' = s''$ y $t' = t''$. Esto nos dice que s y s', por un lado, y t y t', por otro, son conjugados en G. □

6.12. Teorema. (Brauer, 1935 [3]) *Sea G un grupo finito y k un cuerpo algebraicamente cerrado de característica p. Entonces el número de clases de isomorfismo de kG-módulos simples es igual al número de clases de conjugación de elementos p-regulares en G.*

Demostración. Sea $A = kG$ y pongamos $S = S(A)$ y $T = T(A)$. En vista de **6.9**, basta mostrar que si $x_1, \ldots, x_r \in G$ es un sistema completo de representantes de las clases de conjugación p-regulares de G, entonces el conjunto $\mathscr{B} = \{\bar{x}_i : 1 \leq i \leq r\}$ de sus clases módulo T es una base de A/T

Que $\{\bar{x}_i : 1 \leq i \leq r\}$ genera linealmente a A/T es consecuencia de las siguientes dos observaciones:

- Primero, si $g \in G$ y $s, t \in G$ son tales que s es p-singular de orden p^n, t es p-regular, $st = ts$ y $g = st$, entonces $(st - t)^{p^n} = s^{p^n} t^{p^n} - t^{p^n} = 0$. Así, es $\bar{g} = \bar{t}$ en A/T. Esto nos dice que A/T está generado linealmente por las clases módulo T de los elementos regulares.
- Por otro lado, si $g, g' \in G$ son conjugados y $h \in G$ es tal que $g' = hgh^{-1}$, entonces $g - g' = g - hgh^{-1} = [h^{-1}, hg] \in S \subset T$, de manera que $\bar{g} = \bar{g}'$ en A/T.

Resta probar que $\{\bar{x}_i : 1 \leq i \leq r\}$ es un conjunto linealmente independiente.

Supongamos entonces que $\lambda_1, \ldots, \lambda_r \in k$ son tales que $\sum_{i=1}^r \lambda_i x_i \in T$. Entonces existe n_0 tal que si $n \geq n_0$, es

$$\Big(\sum_{i=1}^r \lambda_i x_i\Big)^{p^n} = \sum_{i=1}^r \lambda_i^{p^n} x_i^{p^n} \in S.$$

Además, como los elementos x_i son p-regulares, existe $n_1 \geq n_0$ tal que $x_i^{p^{n_1}} = x_i$ para todo $i \in \{1, \ldots, r\}$. Concluimos que

$$\sum_{i=1}^r \lambda_i^{p^{n_1}} x_i \in S \tag{6}$$

Si $c \in \mathsf{cl}(G)$ es una clase de conjugación, sea $\phi_c : A \to k$ la única aplicación k-lineal tal que para todo $g \in G$ es

$$\phi_c(g) = \begin{cases} 1, & \text{si } g \in c; \\ 0, & \text{en caso contrario.} \end{cases}$$

Entonces si $g, h \in G$ y $c \in \mathsf{cl}(G)$, es

$$\phi_c(gh - hg) = \phi_c\big(g(hg)g^{-1} - hg\big) = 0.$$

Esto nos dice, como $\{gh - hg : g, h \in G\}$ general a S linealmente, que $\phi_c|_S = 0$ cualquiera sea $c \in \mathsf{cl}(G)$.

Pero si $i \in \{1, \ldots, r\}$ y $c \in \mathsf{cl}(G)$ es la clase de conjugación de x_i, entonces esto y (6) nos dicen que

$$0 = \phi_c\Big(\sum_{i=1}^r \lambda_i^{p^{n_1}} x_i\Big) = \phi_c(\lambda_i^{p^{n_1}} x_i) = \lambda_i^{p^{n_1}}.$$

Por supuesto, esto implica que $\lambda_i = 0$ cualquiera sea $i \in \{1, \ldots, r\}$ y vemos que $\{\bar{x}_i : 1 \leq i \leq r\}$ es una base de A/T, como queríamos □

6.13. Si G es un p-grupo, entonces es claro que la única clase de conjugación de elementos p-regulares es la del elemento neutro, así que **6.4** es consecuencia de **6.12**.

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] R. Brauer, *Über die Darstellung von Gruppen in Galoisschen Feldern.*, Hermann & Cie. 15 S., Paris, 1935. ↑18

[4] L. E. Dickson, *On finite algebras.*, Gött. Nachr. (1905), 358–393. ↑7

[5] 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. ↑

[6] H. Maschke, *Über den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen.*, Math. Ann. **50** (1898), 492-498. ↑13

[7] 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. ↑13

[8] J. H. Maclagan-Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), no. 3, 349–352. MR1500717 ↑7

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

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