ANILLOS Y MÓDULOS SEMISIMPLES

ANDREA SOLOTAR - MARIANO SUÁREZ-ALVAREZ

RESUMEN. Este curso tratará del estudio de un tipo de anillos para los que hay una descripción completa de la categoría de módulos: los anillos semisimples.

Nos ocuparemos en particular del caso de representaciones de grupos finitos sobre k-espacios vectoriales, cuando la característica de k no divide al orden del grupo.

ÍNDICE

INTRODUCCIÓN

Los anillos semisimples tienen categorías de módulos muy sencillas: todos los módulos son proyectivos e inyectivos. Los anillos semisimples son hereditarios. En general, la dimensión global de un anillo A mide cuan lejos está A de ser semisimple.

Para un anillo conmutativo, ser semisimple es equivalente a ser un producto finito de cuerpos. En el caso no conmutativo, el teorema de Wedderburn dice que todo anillo semisimple es un producto finito de anillos de matrices sobre anillos de división.

Date: 09/07/2012.

1991 *Mathematics Subject Classification.* 16D60.

El objetivo de este curso es caracterizar los anillos y los módulos semisimples y demostrar sus propiedades más importantes.

1. Módulos simples y semisimples

1.1. Módulos simples. Sea A un anillo. Trabajaremos en general con A-módulos a izquierda.

Nos interesa describir propiedades de A que hagan que todo A-módulo sea proyectivo, o inyectivo, o libre.

Por ejemplo, para que todo A-módulo sea proyectivo se necesita que todo A-módulo sea sumando directo de un libre. En particular, todo ideal de A debe ser un sumando directo de A.

Definición 1.1. Decimos que un A-módulo S es *simple* si es no nulo y no posee submódulos propios no triviales.

Ejemplo 1.2. Si $A = k$ es un cuerpo o, más generalmente, un álgebra de división, entonces un A-módulo es simple sii tiene dimensión 1.

Ejemplo 1.3. Si $A = \mathbb{Z}$, entonces un A-módulo, es decir un grupo abeliano, es simple sii es finito de orden primo.

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

Lema 1.4. *Sea A un anillo.*

- *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 $\mathsf{ann}(m)$ es un ideal a izquierda 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 a izquierda 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 a izquierda maximal. □

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 a izquierda maximal de A y estos forman un conjunto.

Lema 1.5. *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. □

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.

Lema 1.6. *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 $\mathcal{S}_A$ y $\mathcal{S}_B$ conjuntos completos de representantes de las clases de isomorfismo de los A- y B-módulos simples, respectivamente. Entonces*

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

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 $\mathcal{S}$, entonces, alcanza con mostrar que S_1 es simple, pero esto es inmediato, ya que todo A-submódulo propio no trivial de S_1 es un $A \times B$-submódulo propio no trivial de S.

Para terminar, tenemos que ver que los elementos de $\mathcal{S}$ son no isomorfos dos a dos. Consideremos primero un par de A-módulos simples S, $T \in \mathcal{S}_A$ 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, $T \in \mathcal{S}_B$ 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 $e_1\pi_2^*(T) = 0$. □

Proposición 1.7. (Schur, 1905) *Sean S y S' dos A-módulos simples y M un A-módulo cualquiera.*

- *Si $f : S \to M$ es un morfismo no nulo, entonces f es inyectivo.*
- *Si $g : M \to S$ es un morfismo no nulo, entonces g es sobreyectivo.*
- *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. □

Proposición 1.8. *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 1.7. □

1.2. Módulos semisimples. Si N y S son submódulos de un A-módulo M, se dice que S es un complemento de N si $S \cap N = 0$ y $S + N = M$. Es claro que se trata de una relación simétrica, que el complemento cuando existe no es único y que hay anillos A con A-módulos M con submódulos que no tienen complemento. Veremos en esta sección que la existencia de complemento para todo submódulo es una característica de los módulos semisimples.

Definición 1.9. Un A-módulo M es *semisimple* si M es suma de submódulos simples. El anillo A es *semisimple* si A, considerado como A-módulo a izquierda, es semisimple.

Ejemplos 1.10.

- Todo módulo simple es semisimple. En particular, el módulo $\{0\}$ es semisimple.
- Si k es un cuerpo, todo k-espacio vectorial es k-módulo semisimple.
- Si k es un cuerpo y $A = k \times \cdots \times k$ (n-factores), entonces A es un anillo semisimple.
- $\mathbb{Z}$ no es un $\mathbb{Z}$-módulo semisimple pues los ideales de $\mathbb{Z}$ no son sumandos directos de $\mathbb{Z}$.
- Un grupo abeliano G es simple si y sólo si $G \cong \mathbb{Z}_p$ para algún número primo p. G es semisimple si y sólo si

$$G \cong \bigoplus_{p \text{ primo}} \mathbb{Z}_p^{(I_p)}$$

para ciertos conjuntos I_p.
- Si k es un cuerpo, G es un grupo finito y la característica de k divide a $|G|$, entonces kG no es kG-módulo semisimple.

Lema 1.11. *Sea $M = \sum_{i\in I} S_i$ un A-módulo 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 $\mathcal{J} = \{J \subset I : \text{la suma } N + \sum_{i\in J} S_i \text{ es directa}\}$. Claramente $\varnothing \in \mathcal{J}$ así que $\mathcal{J} \neq \varnothing$. Si $C = \{J_\lambda\}_{\lambda\in\Lambda}$ es una cadena en $\mathcal{J}$, pongamos $J_C = \bigcup_{\lambda\in\Lambda} J_\lambda$. Veamos que $J_C \in \mathcal{J}$:
- 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 $\mathcal{J}$ 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, $J \cup \{i_0\} \in \mathcal{J}$. Esto contradice la elección de J, así que nuestra suposición debe ser falsa, esto es, debe ser $S_{i_0} \subset M'$. □

Lema 1.12. *Sea M un A-módulo tal que todo submódulo de M es un sumando directo. Entonces todo submódulo de M posee un submódulo simple.*

Demostración. Basta probar 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 a izquierda 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. □

Teorema 1.13. *Sea M un A-módulo. Las siguientes condiciones son equivalentes:*
1. *M es semisimple;*
2. *M es suma directa de submódulos simples;*
3. *todo submódulo de M es un sumando directo.*

Demostración. Para ver que la primera afirmación implica la segunda, basta tomar $N = 0$ en 1.11. Es inmediato que la segunda implica la primera, y es consecuencia directa de 1.11 que la primera implica la tercera.

Veamos, para terminar, que 3) implica 1). Sea M un A-módulo 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 1.12, existe un submódulo $S \subset N$ simple. Como $S \cap M' = 0$, esto contradice la elección de M'. $\square$

Corolario 1.14. *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 1.11 nos da un conjunto $J \subset I$ tal que $M = \bigoplus_{i \in J} S_i \oplus P$. Luego $N \cong M/P \cong \bigoplus_{i \in J} S_i$. $\square$

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 $\{S_i : i \in I\}$.

Corolario 1.15. *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 1.14. $\square$

Observación 1.16. Si M es un A-módulo con un submódulo semisimple N tal que además M/N es semisimple, no es cierto en general que M sea semisimple. Un (contra)ejemplo de esta situación es la extensión

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

Proposición 1.17. *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. □

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 1.18. *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 A-submódulo 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 $\mathcal{S}_M$ de clases de isomorfismo de A-módulos simples tal que $M_c \neq 0$ para todo $c \in \mathcal{S}_M$ y

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

Demostración. Que para todo A-módulo simple M_S es un A-submódulo 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 $\mathcal{S}$ el conjunto de las clases de isomorfismo de A-módulos simples.

Para cada $c \in \mathcal{S}$, 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 $\mathcal{S}_M = \{c \in \mathcal{S} : I_c \neq \varnothing\}$, obtenemos una partición $\{I_c : c \in \mathcal{S}_M\}$ de I. Además, si $M'_c = \bigoplus_{i \in I_c} S_i$ para cada $c \in \mathcal{S}_M$, es

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

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

Sean c, $c' \in \mathcal{S}_M$, $f : S_c \to M$ un morfismo de A-módulos y supongamos que existe $m \in \mathsf{im}\, f \cap \bigoplus_{i \in I_{c'}} S_i$ tal que $m \neq 0$. Entonces 1.7 implica que f es inyectivo, que $S_c \cong \mathsf{im}\, f \subset \bigoplus_{i \in I_{c'}} S_i$ 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 la prueba de la proposición. □

Si c es una clase de isomorfismo de A-módulos simples y M un A-módulo, el submódulo M_c de M construido en 1.18 es la *componente isotípica de M de tipo c.*

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

$$\operatorname{rad} M = \bigcap_{\substack{h:M\to S \\ S \text{ simple}}} \ker h. \tag{1.1}$$

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

Lema 1.19. *Sea A un anillo y M un A-módulo no nulo finitamente generado. Entonces $\operatorname{rad} M$ es un submódulo propio de M.*

Demostración. Sea $\mathcal{M}$ el conjunto de todos los submódulos propios de M y $\{x_1, \dots, x_n\}$ un subconjunto de M tal que $M = \sum_{i=1}^n Ax_i$. Claramente $\mathcal{M} \neq \varnothing$. Veamos que se trata de un conjunto inductivo.

Si $\{M_\lambda\}_{\lambda\in\Lambda} \subset \mathcal{M}$ es una cadena en $\mathcal{M}$, 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 $N \in \mathcal{M}$ y vemos que cada cadena en $\mathcal{M}$ 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. □

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.

Lema 1.20. *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 (1.1) implica que $h(f(m)) = 0$. Usando (1.1) 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 $(\operatorname{rad} M)/N = \pi(\operatorname{rad} M) \subset \operatorname{rad}(M/N)$. Recíprocamente, supongamos que $m \in$

$M \setminus \mathsf{rad}\, M$. Entonces existe un morfismo $h : M \to S$ con S simple y $h(m) \neq 0$. Como $N \subset \mathsf{rad}\, M \subset \ker h$, 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 $\pi(m) \notin \mathsf{rad}(M/N)$.

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

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

Proposición 1.21. *Sea A un anillo y M un A-módulo.*

(a) Si M es semisimple, entonces $\mathsf{rad}\, M = 0$.
(b) Las siguientes afirmaciones son equivalentes:
  (i) *M es artiniano y* $\mathsf{rad}\, M = 0$.
  (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 $\mathsf{rad}\, M \subset \bigcap_{i \in I} \ker \pi_i = 0$. Esto prueba *(a)*. Veamos *(b)*.

Probemos que (i) implica (ii): Sea $\mathcal{M}$ el conjunto de los submódulos maximales de M y sea $\mathcal{I} = \{\bigcap_{N \in F} N : F \subset \mathcal{M}$ es finito$\}$. Como M es artiniano, $\mathcal{I}$ posee un elemento minimal M_0. Supongamos que $F \subset \mathcal{M}$ 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 $m \notin \mathsf{rad}\, M$, existe un submódulo $N \in \mathcal{M}$ tal que $m \notin N$. Pero entonces $M_0 \subsetneq M_0 \cap N \in \mathcal{I}$, 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 $F \subset \mathcal{M}$, 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 1.17, M es isomorfo a una suma directa finita de submódulos simples.

Veamos finalmente que (ii) implica (i): Si $M = \bigoplus_{i \in I} S_i$ es una suma directa finita de submódulos simples, entonces $\mathsf{rad}\, M = 0$ por la parte *(a)* de la proposición y es artiniano en vista de 1.17. □

2. Anillos semisimples

2.1. Caracterización de anillos semisimples. Recordemos que un anillo A es *semisimple* si lo es como A-módulo a izquierda. Si bien esta definición puede parecer arbitraria, veremos en esta sección que no lo es, es decir que A es semisimple como A-módulo a izquierda sii lo es como A-módulo a derecha. Esto resulta del Teorema de Wedderburn.

Comenzaremos probando algunas propiedades de los módulos simples sobre anillos semisimples.

Lema 2.1. *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 a izquierda 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 $\operatorname{ann}(m) \subsetneq \operatorname{ann}(m) \oplus \mathfrak{b} \subsetneq A$. Esto contradice la maximalidad de $\operatorname{ann}(m)$. Vemos así que $\mathfrak{a}$ es un ideal a izquierda minimal.

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

Proposición 2.2. *Sea A un anillo semisimple y sea $\mathcal{S}$ el conjunto de las clases de isomorfismo de A-módulos simples. Para todo $c \in \mathcal{S}$, la componente isotípica $A_c \subset A$ correspondiente a c es un ideal bilátero no nulo.*

Demostración. Sea $c \in \mathcal{S}$ y sea S un A-módulo simple tal que $S \in c$. Recordemos de 1.18 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 $x = \sum_{i=1}^n f_i(a)$, de donde $xb = \sum_{i=1}^n f_i(a)b = \sum_{i=1}^n (f_i b)(a) \in A_c$. Vemos así que A_c es un ideal bilátero.

Por otro lado, 2.1 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 $A_c \neq 0$. □

Proposición 2.3. *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 1.5. □

Un argumento inductivo a partir de 2.3 prueba, más generalmente, que un producto directo finito de anillos semisimples es semisimple.

Observación 2.4. 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 2.5. *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 2.2 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 A-módulo proyectivo, concluimos que A es isomorfo a un sumando directo del módulo semisimple $\mathfrak{a}^{(X)}$. Usando 1.14, 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 1.7 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 $A \cong \mathsf{M}_n(D)^{\mathsf{op}} \cong M_n(D^{\mathsf{op}})$. □

Observación 2.6. 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.

El siguiente teorema da una caracterización de los anillos semisimples en términos de sus módulos.

Teorema 2.7. *Sea A un anillo, son equivalentes:*

1. *A es semisimple.*
2. *Todo A-módulo es semisimple.*
3. *Todo A-módulo libre es semisimple.*
4. *Todo A-módulo es proyectivo.*
5. *Toda extensión de A-módulos es trivial.*
6. *Todo A-módulo es inyectivo.*
7. *Todo ideal a izquierda de A es inyectivo.*
8. *Todo cociente de A es proyectivo.*

Demostración.

- (1) implica (2). Todo A-módulo es suma de submódulos cíclicos, así que basta ver que todo A-módulo cíclico es semisimple. Si M es cíclico, $M \cong A/I$ para algún ideal a izquierda I. Como A es semisimple, el corolario 1.15 nos dice que M es semisimple.

- (2) implica (3). Esto es inmediato.
- (3) implica (4). Sea M un A-módulo. Existe un módulo libre L y un epimorfismo $p : L \to M$. El Teorema 1.13 nos dice que $\mathsf{ker}(p)$ es un sumando directo de L, así que $L/\mathsf{ker}(p) \cong M$ también es isomorfo a un sumando directo de L. Esto muesta que M es proyectivo.
- (4) implica (5). Consideramos una extensión de A-módulos

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0.$$

  Como Z es proyectivo, esta sucesión se parte.
- (5) implica (6). Sea M un A-módulo. Como la hipótesis implica que toda sucesión exacta de la forma

$$0 \longrightarrow M \longrightarrow X \longrightarrow Y \longrightarrow 0$$

  se parte, M es inyectivo.
- (6) implica (7). Esto es inmediato.
- (7) implica (8). Sea I un ideal. Por hipótesis, I es inyectivo, así que la sucesión exacta

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

  se parte. Esto dice que A/I es isomorfo a un sumando directo de A. En particular, A/I es proyectivo.
- (8) implica (1). Por el Teorema 1.13 basta ver que todo ideal I de A es un sumando directo. Consideremos de nuevo la sucesión

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0.$$

  Como A/I es proyectivo, esta sucesión se parte. Luego I es un sumando directo.

□

2.2. Teorema de Wedderburn.

Teorema 2.8. (Wedderburn, 1908 [5]; Artin) *Sea A un anillo. Las siguientes afirmaciones son equivalentes:*

1. *A es semisimple;*
2. *todo A-módulo es semisimple;*
3. *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. Ya vimos que (1) y (2) son equivalentes.

Mostremos que (2) implica (3). La hipótesis nos dice que, en particular, ${}_AA$ es semisimple, así que 1.13 implica que $A \cong \bigoplus_{i\in I} S_i$ con S_i submódulo simple de A

para cada $i \in I$. Como A es finitamente generado, 1.17 implica que I es finito. La afirmación (3) sigue entonces de los isomorfismos de anillos

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

y de 1.8. Finalmente, la implicación restante es consecuencia inmediata de 2.3 y 2.4. □

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

Proposición 2.9. *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 $A \cong \mathsf{M}_{n_1}(D_1^{\mathsf{op}}) \times \cdots \times \mathsf{M}_{n_r}(D_r^{\mathsf{op}})$.*

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

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 1.9:

Corolario 2.10. *Un anillo A es semisimple sii el A-módulo a derecha A es semisimple.*

Demostración. La tercera condición de 2.8 es evidentemente simétrica con respecto a la izquierda y la derecha. □

Corolario 2.11. *Un anillo semisimple es artiniano y nötheriano.*

Demostración. Esto es consecuencia directa de 1.17. □

Corolario 2.12. *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 2.8. □

Observación 2.13. Sea k un anillo conmutativo y sea A una k-álgebra que es semisimple como anillo. Entonces los anillos de división que aparecen en la tercera afirmación de 2.8 son k-álgebras y el isomorfismo allí mencionado es un isomorfismo de k-álgebras.

Cuando A es un álgebra sobre un cuerpo k algebraicamente cerrado, podemos ser más precisos en la tercera afirmación de 2.8, ya que no hay k-álgebras de división de dimensión finita no triviales:

Lema 2.14. *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 $\mathsf{deg}\, q < \mathsf{deg}\, p$.

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

Teniendo esto en cuenta, es claro que 2.8 implica la siguiente proposición:

Proposición 2.15. *Sea k un cuerpo algebraicamente cerrado y A una k-álgebra. Entonces A es semisimple sii existen r, n_1, ..., $n_r \in \mathbb{N}$ tales que $A \cong \mathsf{M}_{n_1}(k) \times \cdots \times \mathsf{M}_{n_r}(k)$.* □

Recordemos, por otro lado, el siguiente teorema:

Teorema 2.16. (Wedderburn, 1905 [4]; Dickson, 1905 [2]) *Un anillo de división finito es un cuerpo.* □

El teorema 2.8 implica, en vista de esta descripción de los anillos de división finitos, la siguiente proposición:

Proposición 2.17. *Un anillo finito A es semisimple sii existen r, n_1, ..., $n_r \in \mathbb{N}$ y cuerpos finitos k_1, ..., k_r tales que $A \cong \mathsf{M}_{n_1}(k_1) \times \cdots \times \mathsf{M}_{n_r}(k_r)$.* □

Observación 2.18. Sean r, n_1, ..., $n_r \in \mathbb{N}$ y D_1, ..., 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, para cada i, $M_i = D_i^{n_i}$ el $\mathsf{M}_{n_i}(D_i)$-módulo simple construido en 2.6 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 $\mathsf{dim}_k S_i = n_i \,\mathsf{dim}_k D_i$ para cada $i \in \{1, \ldots, r\}$.

2.3. El radical de un anillo.

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

La segunda parte de la proposición 1.21 tiene como consecuencia inmediata el siguiente teorema:

Teorema 2.19. *Sea A un anillo artiniano. Entonces A es semisimple sii $J(A) = 0$.* □

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

Proposición 2.20. *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) $J(A) = \mathsf{rad}_A A = \mathsf{rad}\, A_A$.

Demostración. Si $b \in A$ y $f : a \in A \mapsto ab \in A$, entonces $f \in \mathsf{hom}_A(A, A)$ y 1.20 implica que $f(J(A)) \subset J(A)$. Esto dice, precisamente, que el ideal a izquierda $J(A)$ también es un ideal a derecha 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 a izquierda 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 $\mathcal{I} = \{I \lhd A : \forall x \in I,\, 1 - x \in A^\times\}$. Para ver (c) tenemos que mostrar que $J(A) \in \mathcal{I}$ y que $J(A) \subset I$ para todo $I \in \mathcal{I}$.

Veamos que $J(A) \in \mathcal{I}$. 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 $J(A) \in \mathcal{I}$, como queríamos.

Sea ahora $I \in \mathcal{I}$ 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. □

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

Proposición 2.21. *Si A es un anillo artiniano, entonces $A/J(A)$ es anillo semisimple.*

Demostración. La tercera parte de 1.20 implica que $\mathsf{rad}_A(A/J(A)) = 0$, de manera que 1.21 nos permite concluir que $A/J(A)$ es semisimple como A-módulo.

Ahora bien, un subgrupo abeliano de $A/J(A)$ es un A-submódulo sii es un $A/J(A)$-submódulo. 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. □

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 $0 = \mathsf{rad}_{A/I} A/I = \mathsf{rad}_A A/I$, de manera que $J(A) = \mathsf{rad}_A A \subset I$, como consecuencia de la segunda parte de 1.20.

Esta proposición tiene la siguiente consecuencia extremadamente útil:

Proposición 2.22. *Sea A un anillo artiniano y M un A-módulo. Entonces* $\mathsf{rad}\, M = J(A)M$.

Demostración. Pongamos $J = J(A)$. Si $m \in M$ y $f : a \in A \mapsto am \in M$, entonces 1.20*(a)* nos dice que $Jm = f(\mathsf{rad}\, A) \subset \mathsf{rad}\, M$. Como esto es cierto para todo $m \in M$, $JM \subset \mathsf{rad}\, M$. Usando ahora 1.20*(b)*, vemos que $(\mathsf{rad}\, M)/JM = \mathsf{rad}(M/JM)$. Pero M/JM es un A/J-módulo y A/J es un anillo semisimple, de modo que $\mathsf{rad}_{A/J} M/JM = 0$ en vista de 1.21*(a)*. Como un A-submódulo de M/JM es lo mismo que un A/J-submódulo, esto implica que $(\mathsf{rad}\, M)/JM = \mathsf{rad}_A M/JM = 0$ y, en definitiva, que $\mathsf{rad}\, M = JM$. □

Observación 2.23. En algunos textos, aparece la siguiente definición de anillo simple: *un anillo A se dice simple si es artiniano y no tiene ideales biláteros propios.* Notamos que la condición de artiniano es esencial si se desea que la definición de simple implique semisimple, como lo muestra el siguiente ejemplo:

Sea k un cuerpo de característica cero. El *álgebra de Weyl* $A_1(k)$ es la subálgebra de $\mathsf{End}_k(k[X])$ generada por los endomorfismos p, $q \in \mathsf{End}_k(k[X])$ tales que

$$q(f) = Xf \qquad \text{y} \qquad p(f) = \frac{\mathrm{d}}{\mathrm{d}X} f$$

para todo $f \in k[X]$.

Es fácil ver que $[p, q] = 1$ (verificarlo!). Usando esto, se puede ver que $\{p^i q^j : i, j \in \mathbb{N}_0\}$ es una base de $A_1(k)$ como k-espacio vectorial. Si $P \in A_1(k)$ se escribe de la forma $P = \sum_{i=0}^{n} f_i(q)p^i$, en donde cada f_i es un polinomio en q y $f_n \neq 0$, diremos que el *grado* de P es n y que el polinomio $f_n \in k[q]$ es el coeficiente principal de P.

Dejamos como ejercicio verificar que:

- Si $P \in A_1(k)$ es un elemento de grado n con coeficiente principal f_n, entonces $[P, q]$ es un elemento de grado $n - 1$ y su coeficiente principal es nf_n.
- Si $f \in k[q]$, entonces $[p, f] = f'$.

Usando estas dos afirmaciones, es fácil ver que $A_1(k)$ no tiene ideales biláteros propios. En efecto, supongamos que I es un ideal bilátero no nulo de $A_1(k)$.

Sea $P_0 \in I$ un elemento no nulo arbitrario y sea g el grado de P_0. Definamos inductivamente $P_{i+1} = [P_i, q]$ para cada $i \in \mathbb{N}_0$. Entonces es fácil ver, usando la primera afirmación, que P_g es un elemento no nulo de $I \cap k[q]$. Escribamos $Q_0 = P_g$ y sea d el grado de Q_0 en $k[q]$. Definamos $Q_{i+1} = [p, Q_i]$ para cada $i \in \mathbb{N}_0$. Usando ahora la segunda afirmación, vemos que Q_d es un elemento no nulo de $I \cap k$. Como es inversible, vemos que $I = A_1(k)$.

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 2.24. *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 $(1-x)\sum_{i=0}^{m-1} x^i = 1$, de manera que $1-x$ es inversible. Usando la tercera parte de 2.20, 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 a izquierda $\mathcal{I} = \{\mathfrak{a} \lhd_l A : \mathfrak{a} = J\mathfrak{a}\}$ 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, $J^n x \in \mathcal{I}$. 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

$$\begin{aligned} \mathfrak{a} &\supsetneq \operatorname{rad}\mathfrak{a} && \text{por 1.19} \\ &= J\mathfrak{a} && \text{por 2.22} \\ &= \mathfrak{a} \end{aligned}$$

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)*. □

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 $I \supset R^n$. 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 2.24*(c)* implica que R/I es el radical de A.

Proposición 2.25. *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. □

Corolario 2.26. *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 2.25. Para ver la segunda, basta observar que si A es artiniano, 2.21 nos dice que $A/J(A)$ es semisimple y entonces 2.12 junto con la primera parte implican la finitud del conjunto de clases de isomorfismo de A-módulos simples. □

2.4. Algebras de grupo.

Veremos ahora un familia importante de ejemplos de álgebra semisimple.

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

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.

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

Observación 2.27. 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.

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).

Observación 2.28. Sea M 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.

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

Teorema 2.29. (Teorema de Maschke) *Sea G un grupo finito y sea k un cuerpo en el que $|G|$ es inversible. Entonces $k[G]$ es un anillo semisimple.*

Demostración. Sea M un $k[G]$-módulo y $S \subseteq M$ un submódulo. Mostremos que S es un sumando directo. Para eso, alcanza con mostrar que existe un morfismo de $k[G]$-módulos $\phi : M \to S$ tal que $\phi|_S = \mathsf{I}_S$.

Como k es un cuerpo, existe ciertamente una transformación k-lineal $\pi : M \to S$ tal que $\pi|_S = \mathsf{I}_S$. Definamos $\phi : M \to S$ poniendo

$$\phi(m) = \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}m)$$

para todo $m \in M$. Afirmamos que ϕ es $k[G]$-lineal y que $\phi|_S = \mathsf{I}_S$.

Si $s \in S$, entonces $g^{-1}s \in S$ y $\pi(g^{-1}s) = g^{-1}s$, así que

$$\begin{aligned}\phi(s) &= \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}s) = \tfrac{1}{|G|} \sum_{g \in G} gg^{-1}s \\ &= \tfrac{1}{|G|} \sum_{g \in G} s = \tfrac{|G|}{|G|} s = s.\end{aligned}$$

Esto dice que $\phi|_S = \mathsf{I}_S$. Por otro lado, si $h \in G$ y $m \in M$, es

$$\phi(hm) = \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hm);$$

Si ponemos $g' = hg$ en la suma, esto queda

$$\begin{aligned}&= \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hm) = \tfrac{1}{|G|} \sum_{g' \in G} g'\pi((g')^{-1}hm) \\ &= \tfrac{1}{|G|} \sum_{g' \in G} hg\pi(g^{-1}h^{-1}hm) = \tfrac{1}{|G|} h\Big(\sum_{g' \in G} g\pi(g^{-1}m) \Big) \\ &= h\phi(m).\end{aligned}$$

Vemos así que ϕ es un morfismo de $k[G]$-módulos. □

Observación 2.30. 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

$$kG \cong \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_r}(D_r). \tag{2.1}$$

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

Proposición 2.31. *Es* $\sum_{i=1}^{r} n_i^2 \mathsf{dim}_k D_i = |G|$.

Demostración. El resultado sigue de tomar dimensión sobre k en (2.1). □

Proposición 2.32. *Sea* $i \in \{1, \dots, r\}$.

- *Si* $\mathsf{dim}_k S_i = 1$, *entonces* $n_i = \mathsf{dim}_k D_i = 1$.
- *Si* k *es algebraicamente cerrado y* $n_i = 1$, *entonces* $\mathsf{dim}_k S_i = 1$.

Demostración. Las dos afirmaciones siguen de la igualdad $n_i \operatorname{\mathsf{dim}}_k D_i = \operatorname{\mathsf{dim}}_k S_i$ observada en 2.18 y del lema 2.14. $\square$

Recordemos que si R es un anillo -cuyo centro denotaremos $\mathsf{Z}(R)$, dado $n \in \mathbb{N}$, 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 2.33. *Es $r \leq |\operatorname{\mathsf{cl}}(G)|$. Si k es algebraicamente cerrado, entonces vale la igualdad.*

Demostración. Aplicando a (2.1) las observaciones que preceden al enunciado, vemos que hay un isomorfismo

$$\mathsf{Z}(kG) \cong \mathsf{Z}(D_1) \times \cdots \times \mathsf{Z}(D_r). \tag{2.2}$$

Para cada $c \in \operatorname{\mathsf{cl}}(G)$ pongamos $z_c = \sum_{g \in c} g \in kG$. Es fácil ver que el conjunto $\{z_c : c \in \operatorname{\mathsf{cl}}(G)\}$ es una base del k-espacio vectorial $\mathsf{Z}(kG)$ así que, en particular, $\operatorname{\mathsf{dim}}_k \mathsf{Z}(kG) = |\operatorname{\mathsf{cl}}(G)|$. Por otro lado, cualquiera sea $i \in \{1, \dots, r\}$, es claro que $k1_{D_i} \subset \mathsf{Z}(D_i)$, de manera que $\operatorname{\mathsf{dim}}_k \mathsf{Z}(D_i) \geq 1$. Teniendo esto en cuenta, el isomorfismo (2.2) 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 $\operatorname{\mathsf{dim}}_k \mathsf{Z}(D_i) = 1$. Vale entonces que $r = |\operatorname{\mathsf{cl}}(G)|$ en este caso. $\square$

Si k es algebraicamente cerrado, podemos explicitar el isomorfismo (2.1).

Proposición 2.34. *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 $\phi : kG \to \prod_{i=1}^r \operatorname{\mathsf{End}}_k(S_i)$ tal que, si para cada $i \in \{1, \dots, r\}$, $\pi_r : \prod_{i=1}^r \operatorname{\mathsf{End}}_k(S_i) \to \operatorname{\mathsf{End}}_k(S_i)$ es la proyección k-ésima, entonces*

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

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

Ejercicios.

1. Descomponer a $\mathbb{R}[\mathbb{Z}_2]$, $\mathbb{R}[\mathbb{Z}_3]$ y $\mathbb{C}[\mathbb{Z}_3]$ como producto de anillos de matrices sobre álgebras de división, como en el Teorema de Wedderburn. Sugerencia: encontrar módulos simples sobre los respectivos anillos. Antes de hacer cuentas, sabiendo que las únicas álgebras de dimensión finita sobre $\mathbb{R}$ son $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$. Cuales son las posibilidades?
2. Probar que si A es anillo semisimple y L es un ideal a izquierda de A entonces:
   - existe $e \in A$ idempotente tal que $L = Ae$.
   - A no tiene ideales a izquierda nilpotentes.

- Si L es simple entonces el idempotente es primitivo, esto es, si $e = e_1 + e_2$ con $e_i^2 = e_i$ y $e_1e_2 = 0 = e_2e_1$, entonces alguno de los e_i es cero.

3. Sea k un cuerpo y $T_2(k)$ el conjunto de matrices triangulares superiores de 2×2 a coeficientes en k, que no es un anillo semisimple. Calcular $\mathsf{rad}(T_2(k))$ y $T_2(k)/\mathsf{rad}(T_2(k))$.
4. Sea k un cuerpo y $A = k \times k$ con el producto coordenada a coordenada. Mostrar que A es semisimple pero no simple. Quiénes son los idempotentes ortogonales que suman uno?
5. Para que $n \in \mathbb{N}$ es $\mathbb{Z}_n$ un anillo semisimple? Para alguno que no sea semisimple, dar un ejemplo de módulo que no sea proyectivo.
6. Sea A un anillo semisimple y M un A-módulo. A partir del teorema de Wedderburn sabemos que $A \cong \prod_{i=1}^{n} M_{r_i}(D_i)$ donde cada $D_i = \mathsf{End}_A(L_i)^{\mathsf{op}}$ es el anillo de endomorfismos del ideal simple L_i, y r_i es la cantidad de veces que aparece L_i en A como sumando directo. A su vez, M se descompone en suma directa de submódulos simples, cada uno de ellos isomorfo a algún L_i (por qué?). Dar una condición necesaria y suficiente sobre la multiplicidad de cada L_i en M para decidir cuándo M es libre. Concluir que si A es semisimple, entonces A tiene noción de rango.
7. Sea $A = M_n(k)$ con k un cuerpo, ver que es un ejemplo de anillo con noción de rango pero que no existe ningún morfismo de anillos $A \to D$ con D un anillo de división.
8. Sea A un anillo y sea M un A-módulo simple. Entonces o bien M, considerado como grupo abeliano, es isomorfo a una suma directa de copias de $\mathbb{Q}$, o bien existe $p \in \mathbb{N}$ primo tal que M es, considerado como grupo abeliano, isomorfo a una suma directa de copias de $\mathbb{Z}_p$.
9. Sea A un anillo conmutativo y M y N dos A-módulos a izquierda y a derecha respectivamente. Probar que si M o N es semisimple, entonces $M \otimes_A N$ es semisimple.
10.
    - Si A es un anillo semisimple y $B \subset A$ es un subanillo, es B necesariamente semisimple?
    - Si A es un anillo semisimple e $I \lhd A$ es un ideal bilátero, probar que A/I es semisimple.
11.
    - Sean A y B anillos y n, $m \in \mathbb{N}$. Entonces $\mathsf{M}_m(\mathsf{M}_n(A)) \cong \mathsf{M}_{mn}(A)$ y $\mathsf{M}_n(A \times B) \cong \mathsf{M}_n(A) \times \mathsf{M}_n(B)$.
    - Si A es un anillo semisimple y $n \in \mathbb{N}$, entonces $\mathsf{M}_n(A)$ es semisimple.
    - Sea A un anillo y sea $n \in \mathbb{N}$. Sea P el conjunto de vectores *fila* de n componentes en A y sea Q el conjunto de vectores *columna* de n componentes en A. Entonces P es un A-$\mathsf{M}_n(A)$-bimódulo y Q es un $\mathsf{M}_n(A)$-A-bimódulo con acciones de $\mathsf{M}_n(A)$ inducidas por el producto matricial. Más aún, hay un isomorfismo $Q \otimes_A P \cong \mathsf{M}_n(A)$ de $\mathsf{M}_n(A)$-bimódulos y un isomorfismo $P \otimes_{\mathsf{M}_n(A)} Q \cong A$ de A-bimódulos.

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

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

- Si M es un A-B-bimódulo y N es un B-módulo izquierdo proyectivo, entonces $M \otimes_B N$ es un A-módulo proyectivo.
- Sea A un anillo. Si existe $n \in \mathbb{N}$ tal que $\mathsf{M}_n(A)$ es semisimple, entonces el anillo A mismo es semisimple.

12. Sea A un anillo, M un A-módulo finitamente generado. Si $B = \mathsf{End}_A(M)$ y A es semisimple, entonces B es semisimple. Notemos que esto tiene como caso particular a la segunda parte del ejercicio 11, ya que si $M = A^n$, entonces $\mathsf{End}_n(M) \cong \mathsf{M}_n(A)$.
13.
    - Un anillo artiniano a izquierda sin divisores de cero es un anillo de división.
    - Si A es un anillo sin divisores de cero tal que $\mathsf{M}_n(A)$ es semisimple para algún $n \in \mathbb{N}$, entonces A es un anillo de división.

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

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

    En particular, hay exactamente r isoclases de kG_n-módulos simples y si $S_1, \ldots, S_n$ son representantes de estas clases, hay un isomorfismo de kG_n-módulos $kG_n \cong \bigoplus_{i=1}^r S_i$.
15. Sea k un cuerpo de característica cero. Sea M un kG_n-módulo simple y sea $a : m \in M \mapsto g_n m \in M$ la multiplicación por g_n. Entonces $a \in \mathsf{End}_{kG_n}(M)$ porque kG_n es un anillo conmutativo. Sea $\mu \in k[X]$ el polinomio minimal de a sobre k. Muestre que μ es irreducible en $k[X]$. Además, si $k = \mathbb{Q}$, entonces μ tiene coeficientes enteros.
16. Sea $\Omega_n \subset \mathbb{C}^\times$ el subgrupo multiplicativo de $\mathbb{C}^\times$ de las raíces n-ésimas de la unidad.
    - La aplicación $\phi : \chi \in \mathsf{hom}_{\mathsf{Grp}}(G_n, \Omega_n) \mapsto \chi(g_1) \in \Omega_n$ es un isomorfismo de grupos abelianos. Esto implica que el conjunto $\hat{G}_n = \mathsf{hom}_{\mathsf{Grp}}(G_n, \Omega_n)$ tiene exactamente n elementos; llamemoslos $\chi_1, \ldots, \chi_n$.
    - Muestre que si χ, $\rho \in \hat{G}_n$, entonces

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

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

- Si $\chi \in \hat{G}_n$, sea $e_\chi = \frac{1}{n}\sum_{g\in G_n}\chi(g^{-1})g \in \mathbb{C}G_n$. Entonces si χ, $\rho \in \hat{G}_n$,
$$e_\chi^2 = e_\chi,$$
$$e_\chi e_\rho = 1, \qquad \text{cuando } \chi \neq \rho, \qquad \text{y} \qquad \sum_{\chi\in\hat{G}_n} e_\chi = 1.$$
- Consideremos el anillo $A = \mathbb{C}\times\cdots\times\mathbb{C}$ con n factores y sean $x_1, \ldots,$ $x_n \in A$ los elementos de la base canónica. Hay un isomorfismo de anillos $\phi : \mathbb{C}G_n \to A$ tal que $\phi(e_{\chi_i}) = x_i$ si $1 \leq i \leq n$. Describa representantes para cada isoclase de $\mathbb{C}G_n$-módulos simples.

17.
- Sea p un número primo. Si $0 \leq k < l$, sea $\phi_{k,l} : \mathbb{Q}G_{p^l} \to \mathbb{Q}G_{p^k}$ el único morfismo de anillos tal que $\phi_{k,l}(g_{p^l}) = g_{p^k}$. Entonces $\ker\phi_{k,l} = \langle g_{p^l}^{p^k} - 1\rangle$. Además, si $0 \leq r < k < l$, es $\phi_{r,l} = \phi_{r,k}\circ\phi_{k,l}$.
- Sea p un número primo y pongamos $\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X]$. Entonces
$$X^{p^l} - 1 = (X-1)\prod_{i=0}^{l-1}\Phi_p(X^{p^i})$$
y cada uno de los factores $\Phi_p(X^{p^i})$ con $0 \leq i < l$ es irreducible en $\mathbb{Q}[X]$.
- Sea p un número primo impar. Sea $l \geq 1$ y sea M un $\mathbb{Q}G_{p^l}$-módulo simple. Si $\dim_{\mathbb{Q}} M < p^l - p^{l-1}$, entonces existe $k < l$ y un $\mathbb{Q}G_{p^k}$-módulo simple N tal que $M \cong \phi_{k,l}^*(N)$.
- Sea p un número primo impar. Notemos M_0 al único $\mathbb{Q}G_1$-módulo simple. Entonces, para todo $l \geq 1$ existe, a menos de isomorfismo, un único $\mathbb{Q}G_{p^l}$-módulo simple M_l tal que
$$\dim_{\mathbb{Q}} M_l \geq p^l - p^{l-1}.$$
Además, se tiene que
  - $\dim_{\mathbb{Q}} M_l = p^l - p^{l-1}$; y
  - $\mathbb{Q}G_{p^l} \cong \bigoplus_{l=0}^{l-1}\phi_{i,l}^*(M_i)\oplus M_l$.

  Sugerencia: Haga inducción con respecto a l.
- Enuncie y pruebe enunciados análogos a los dos últimos para $p = 2$.
- Sea $p \in \mathbb{N}$ primo, $l \geq 1$ y sea M_l un $\mathbb{Q}G_{p^l}$-módulo simple de dimensión $p^l - p^{l-1}$. Entonces M_l posee una base con respecto a la cual la matriz de la aplicación $a : m \in M \mapsto g_{p^l}m \in M$ es la matriz compañera del polinomio $\Phi_p(X^{p^l})$.
- Sea $f \in \mathbb{Q}[X]$ un polinomio mónico irreducible. Sea $a \in \mathsf{M}_n(\mathbb{Q})$ la matriz compañera de f. Entonces, si $\mathcal{C}(a) \subset \mathsf{M}_n(\mathbb{Q})$ es el centralizador de a en $\mathsf{M}_n(\mathbb{Q})$, hay un isomorfismo de anillos $\mathcal{C}(a) \cong \mathbb{Q}[X]/(f)$.
- Sea $p \in \mathbb{N}$ primo. Para cada $l \in \mathbb{N}$, sea $\zeta_l \in \mathbb{C}$ una raíz primitiva p^l-ésima de la unidad y sea $\mathbb{Q}(\zeta_l)$ el menor subcuerpo de $\mathbb{C}$ que la contiene.

Entonces hay un isomorfismo de álgebras

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

- Supongamos que n es impar y que $n = p_1^{m_1} \cdots p_r^{m_r}$ es la factorización de n como producto de potencias de primos distintos. Entonces $G_n \cong G_{p_1^{m_1}} \times \cdots \times G_{p_r^{m_r}}$.
  Si M es un $\mathbb{Q}G_n$-módulo simple, entonces existen $l_1, \ldots, l_r \in \mathbb{N}$ tales que $l_i \leq m_i$ si $i \in \{1, \ldots, r\}$ y
  $$M \cong M_{p_1,m_1,l_1} \boxtimes \cdots \boxtimes M_{p_r,m_r,l_r}.$$
  Aquí $M_{p,m,l}$ es el único $\mathbb{Q}G_{p^m}$-módulo simple de dimensión $p^l - p^{l-1}$.

18. Muestre que si $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, entonces $kS_3 \cong k \times k \times \mathsf{M}_2(k)$.
19. Encuentre la descomposición de Wedderburn para kD_4 con $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ si $D_4 = \langle s, t : s^2 = t^4 = 1,\ sts = t^{-1}\rangle$.
20. Sea $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ el grupo de los cuaterniones unitarios. Muestre que
$$\begin{aligned} \mathbb{Q}Q &\cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H}_{\mathbb{Q}}, \\ \mathbb{R}Q &\cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}_{\mathbb{R}}, \\ \text{y} \qquad \mathbb{C}Q &\cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathsf{M}_2(\mathbb{C}). \end{aligned}$$
Aquí $\mathbb{H}_{\mathbb{R}}$ es el anillo de los cuaterniones reales y $\mathbb{H}_{\mathbb{Q}}$ es el análogo definido sobre $\mathbb{Q}$.

Referencias

[1] F. Anderson y K. Fuller, Rings and categories of modules, *Graduate Texts in Mathematics* **No. 13** ,Springer-Verlag, 1992, 376 pp.

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

[3] H. Maschke, *Uber den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen*, Math. Ann. **No. 50**, 492-498 (1898).

[4] J. H. Maclagan Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. **No. 6** (3), 349–352 (1905).

[5] J. H. Maclagan Wedderburn, *On hypercomplex numbers*, London M. S. Proc. (2) **No. 6**, 77–118 (1908).

Departamento de Matemática, FCEyN, Instituto de Matemática Luis Santaló, IMAS-CONICET, Universidad de Buenos Aires. 1428, Buenos Aires,

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