UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

TEORÍA Y CONCEPTOS PRECURSORES DE LOS ANILLOS SEMIPERFECTOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
ALEJANDRO ARGUDÍN MONROY

DIRECTOR DE TESIS:
M. en C. CLOTILDE GARCÍA VILLA

2014

1. Datos del alumno	
Apellido paterno	Argudín
Apellido materno	Monroy
Nombre	Alejandro
Teléfono	4171 1121
Universidad Nacional Autónoma de México	Universidad Nacional Autónoma de México
Facultad de Ciencias	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	305152581
2. Datos del tutor	
Grado	M. en C.
Nombre	Clotilde
Apellido paterno	García
Apellido materno	Villa
3. Datos del sinodal 1	
Grado	Dr.
Nombre	Octavio
Apellido paterno	Mendoza
Apellido materno	Hernández
4. Datos del sinodal 2	
Grado	Dr.
Nombre	Christof
Apellido paterno	Geiss
Apellido materno	Hahn
5. Datos del sinodal 3	
Grado	Dra.
Nombre	Edith Corina
Apellido paterno	Sáenz
Apellido materno	Valadez
6. Datos del sinodal 4	
Grado	Dr.
Nombre	Daniel
Apellido paterno	Labardini
Apellido materno	Fragoso
7.Datos del Trabajo escrito	
Título	Teoría y conceptos precursores de los anillos semiperfectos
Número de páginas	204
Año	2014

Índice general

Agradecimientos

Para empezar quisiera agradecer a mi familia y amigos por alentarme y apoyarme durante la realización de este trabajo.

Un agradecimiento singular debo a mi asesora Clotilde García por todo el tiempo y paciencia que invirtió en este tesis. A Zdenek Palecek por sus consejos sobre la elaboración del texto. Y a mis sinodales cuyas contribuciones y correcciones enriquecieron este trabajo.

También quisiera agradecer a todos los profesores que me han influenciado por mi paso en la carrera. En particular, a Antonio Carrillo por mostrarme las matemáticas, a Javier Elizondo por sus consejos, a Angel Manuel Carrillo, cuyas clases me ayudaron a madurar matemáticamente, y a Francisco Raggi por todas sus enseñanzas y por la beca que me brindó por medio del Conacyt. Así como a los profesores Javier y Coty, que depositaron su confianza en mí para ser ayudante, trabajo que me ha ayudado tanto económicamente, como en la maduración de algunas ideas de esta tesis.

En general a todos los archivos, bibliotecas y bases de datos en los que me apoyé para realizar este trabajo.

A la UNAM y la Facultad de Ciencias por acogerme durante mi educación y todo el tiempo en que se elaboró esta tesis.

Por último, debo un especial agradecimiento a los técnicos que arreglaron mi computadora sin borrar la tesis.

Introducción

El siglo veinte fue testigo del nacimiento del álgebra homológica, la cual llevó al descubrimiento de la subclase de los anillos semiperfectos, que son el objeto de estudio de esta tesis.

Para la década de 1950 la teoría de anillos junto a la de módulos se había desarrollado desde su nacimiento a pasos agigantados. Entre los que se pueden destacar: la generalización del teorema de Wedderburn sobre la clasificación de álgebras semisimples de dimensión finita a anillos no conmutativos; el desarrollo de lo que hoy en día se conoce como el teorema de Krull-Schmidt sobre la descomposición de un módulo de longitud finita en suma directa de módulos inescindibles; y la introducción de la teoría de categorías a manos de Saunders Mac Lane y Samuel Eilenberg.

En cambio, el desarrollo del álgebra homológica, como explica Charles A. Weibel en [Wei99], había permanecido casi nulo desde su nacimiento a mediados del siglo XIX hasta la década de 1940, a partir de la cual, se empezaron a utilizar métodos basados en técnicas topológicas para explorar y definir diversos objetos algebráicos.

Fue entonces hasta 1956 cuando sucedió lo que llama Weibel como la revolución de Cartan-Eilenberg, que inició con la publicación del libro *Homological Algebra* de Henri Cartan y Samuel Eilenberg [CE56]. En tal libro se unificaban todos los métodos homológicos antes usados y se les daba el nombre de álgebra homológica. Sería demasiado largo enumerar todas las innovaciones que ofreció este libro, pero cabe señalar que por primera vez se presentó el concepto de módulo proyectivo y se definieron los conceptos de resolución proyectiva e inyectiva, así como de dimensión proyectiva e inyectiva de un módulo y de dimensión global de un anillo.

Una resolución proyectiva de un módulo M es una sucesión exacta

$$... \to P_n \to ... \to P_1 \to P_0 \to M \to 0$$

donde P_i es proyectivo para todo $i \geq 0$, y se dice que la longitud de la resolución es k si $P_m = 0$ para todo $m > k$. La dimensión proyectiva de M es el mínimo entero k tal que existe una resolución de longitud k. En caso de no existir tal resolución se define entonces la dimensión proyectiva de M como infinito. De manera análoga se define el concepto de resolución inyectiva, así como dimensión inyectiva. Y se prueba que el supremo de las dimensiones proyectivas de los módulos derechos sobre un anillo es igual al supremo de las dimensiones inyectivas de los módulos derechos sobre el mismo anillo, a tal número se le llama dimensión global derecha del anillo, y de manera análoga se define la dimensión global izquierda.

Estos conceptos le dieron un nuevo impulso al desarrollo de la teoría de anillos. Lo que llevo a la búsqueda de métodos sencillos para calcular la dimensión de un módulo. El más común es encontrar una resolución de longitud mínima, ya que en caso de encontrar tal sucesión, claramente su longitud es la dimensión del módulo.

En el caso inyectivo, tal resolución se puede construir gracias a la envolvente inyectiva, la cual se conocía su existencia desde 1953 gracias a Eckmann y Schopf [ES53]. Esto llevó a que Eilenberg estudiara el concepto dual en su artículo *Homological Dimension and syzygies* [Eil56], que tiempo después fue bautizado como cubierta proyectiva por Hyman Bass en [Bas60]. Sin embargo, la importancia de estos artículos va más allá del estudio de un concepto dual.

En su artículo, Eilenberg trabaja sobre anillos que cumplen ciertas propiedades dando cinco axiomas necesarios para que una subcategoría de la categoría de módulos cumpla que todo elemento tenga cubierta proyectiva. Y termina enunciando un sexto axioma más que permite la construcción de una resolución proyectiva de longitud mínima.

Por su parte, Bass bautiza a los anillos que utilizó Eilenberg en su artículo como anillos semiperfectos, y los caracteriza como los anillos en los que todo módulo finitamente generado tiene cubierta proyectiva, y caracteriza los anillos que cumplen que todo módulo tenga cubierta proyectiva y los llama anillos perfectos.

El objetivo de esta tesis es brindar una exposición autocontenida sobre la teoría de anillos semiperfectos, así como de los resultados necesarios para una caracterización completa de éstos. Además, se incluye una exposición sobre el comportamiento de los módulos sobre tales anillos, abastecida de una cantidad suficiente de ejemplos y contraejemplos, sin la necesidad de recurrir al álgebra homológica. Con el fin de ofrecer al lector el conocimiento suficiente para iniciar estudios en áreas más sofisticadas como la teoría de representaciones, así como dar una motivación al estudio del álgebra homológica.

Ahora, a pesar de que el objetivo de la tesis es presentar una exposición autocontenida, los resultados básicos sobre teoría de anillos y teoría de módulos se consideran conocidos, y sólo se mencionan en el capítulo 1. Dicho capítulo termina con algunas construcciones de álgebras y anillos que se usarán a lo largo de la tesis.

El capítulo 2 contiene resultados básicos sobre la descomposición de un anillo. Inicia exponiendo propiedades básicas sobre los idempotentes de un anillo, para despueś presentar la descomposición de Peirce de un anillo y la representación matricial de un anillo. Se finaliza con el teorema de descomposición en bloques de un anillo.

Utilizando los resultados del capítulo 2, en el capítulo 3 se prueba el teorema de Wedderburn-Artin junto con propiedades de los módulos semisimples y se concluye dando una caracterización los anillos simples que son semisimples.

Con los resultados anteriores en el capítulo 4 se exponen propiedades sobre los módulos de longitud finita; empezando con módulos artinianos y noetherianos, continuando con anillos artinianos y noetherianos, y teminando con series de composición y el teorema Jordan-Hölder.

En el capítulo 5 se definen y exponen las propiedades importantes sobre el radical y el soclo de un módulo, en particular se exponen propiedades sobre el soclo de un módulo finitamente cogenerado, el radical de un módulo finitamente generado, el radical de un módulo proyectivo finitamente generado, el radical de Jacobson, el radical de Jacobson de un anillo artiniano y se finaliza con el teorema de Hopkins-Levitzki.

Con las propiedades expuestas sobre el soclo y el radical, se da una motivación natural para la definición de la envolvente inyectiva y la cubierta proyectiva en el capítulo 6. En éste, se exponen propiedades sobre estos conceptos y se muestra que no siempre existe la cubierta proyectiva.

Basándose en lo anterior y con el objetivo de caracterizar a los anillos en los que todo módulo tiene cubierta proyectiva, en el capítulo 7 se exponen las propiedades necesarias para ello sobre los anillos locales y semilocales, incluyendo el teorema de Krull-Schmidt-Azumaya.

Finalmente, el capítulo 8 caracteriza a los anillos semiperfectos, iniciando con una exposición sobre el levantamiento de idempotentes, y continuando con un estudio sobre el comportamiento de los módulos sobre un anillo semiperfecto. Dicho capítulo termina con una breve exposición sobre anillos básicos.

Por último, se anexa un apéndice con las definiciones elementales de la teoría de categorías y se da una prueba sobre el teorema de Morita.

1. Preliminares

1.1. Anillos

Definición 1.1. Un anillo con elemento unitario A es una terna $(A, +, \cdot)$, donde $(A, +)$ es un grupo abeliano y $(A, \cdot)$ es un monoide con elemento neutro 1_A, tal que el producto $\cdot$ distribuye por derecha e izquierda a la suma de $(A, +)$.

Como ejemplo de un anillo se puede tomar $\mathrm{End}(M)$, el anillo de endomorfismos de un grupo abeliano M, donde la suma es la operación heredada de M y el producto es la composición de funciones. Otros ejemplos más comunes son los números enteros $\mathbb{Z}$, los números racionales $\mathbb{Q}$, los números complejos $\mathbb{C}$, los enteros módulo un entero n $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, anillos de matrices y anillos de polinomios.

Por otro lado, dado un anillo $(A, +, \cdot)$ es natural pensar en el anillo $(A, +, \star)$, donde $a \star b = b \cdot a$, llamado el anillo opuesto de A que se suele denotar como A^{op}.

Ahora, dado un anillo $A = (A, +, \cdot)$, si S es un subgrupo de A tal que $(S, +, \cdot)$ es un anillo, entonces se dice que S es un subanillo de A si $1_S = 1_A$. Si I es un subgrupo de A tal que $xa \in I$ para todo $x \in I$ y $a \in A$, entonces se dice que I es un ideal derecho de A. Análogamente, un subgrupo I es un ideal izquierdo si $ax \in I$ para todo $a \in A$ y $x \in I$, y un subgrupo I recibe el nombre de ideal bilateral ó ideal si $ax, xa \in I$ para todo $a \in A$ y $x \in I$.

Por último, un morfismo de anillos es una función $f : A \to B$ tal que $f(1_A) = 1_B$, $f(ab) = f(a)f(b)$ y $f(a + b) = f(a) + f(b)$ para todo $a, b \in A$.

1.2. Módulos

Definición 1.2. Sea M un grupo abeliano aditivo y A un anillo, se dice que M es un A-módulo derecho si y sólo si existe una función $\mu : M \times A \to M$, escrita como $\mu(m, a) = ma$, tal que

(a) $(x + y)a = xa + ya$

(b) $x(a + b) = xa + xb$

(c) $x(ab) = (xa)b$

(d) $x1 = x$

para cualesquiera x, $y \in M$ y a, $b \in A$. Por otro lado, se dice que M es un A-módulo izquierdo si existe una función $A \times M \to M$, que cumple los siguientes puntos

(a) $a(x + y) = ax + ay$

(b) $(a + b)x = ax + bx$

(c) $(ab)x = a(bx)$

(d) $1x = x$

para cualesquiera x, $y \in M$ y a, $b \in A$.

Si M es un A-módulo derecho se le denota como M_A, si es un módulo izquierdo se le denota como ${}_AM$.

Si un grupo abeliano M es un módulo derecho sobre un anillo A y un módulo izquierdo sobre un anillo B, de tal manera que $b(ma) = (bm)a$ para todo $m \in M$, $a \in A$ y $b \in B$, entonces se dice que M es un B-A bimódulo.

Naturalmente todo anillo A es un A-módulo derecho y un A-módulo izquierdo, así como un bimódulo bajo el producto del anillo. Estos módulos reciben el nombre de A-módulo regular derecho, izquierdo y bilateral respectivamente, y se les denota A_A, ${}_AA$ y ${}_AA_A$.

1.2.1. Representación asociada a un módulo

El lema siguiente da una caracterización de los módulos sobre un anillo.

Lema 1.3. *Sean A un anillo y M un grupo abeliano.*

(a) *M es un A-módulo derecho si y sólo si existe un morfismo de anillos*

$$\phi : A \to \mathrm{End}(M)^{op},$$

llamado representación de A asociada a M.

(b) *M es un A-módulo izquierdo si y sólo si existe un morfismo de anillos*

$$\phi : A \to \mathrm{End}(M),$$

llamado representación de A asociada a M.

Demostración. La demostración se puede consultar en [Pas04]. □

Observación 1.4. Sean A y B anillos. Es sencillo probar que existe un morfismo de anillos $\psi : A \to B^{op}$ si y sólo si existe un morfismo de anillos $\phi : A^{op} \to B$. Por lo tanto, si M es grupo abeliano, entonces existe un morfismo de anillos $\psi : A \to \mathrm{End}(M)^{op}$ si y sólo si existe un morfismo de anillos $\phi : A^{op} \to \mathrm{End}(M)$. Lo que implica que M es un A-módulo derecho si y sólo si es un A^{op}-módulo izquierdo.

De ahora en adelante en el texto se trabaja con módulos derechos y por ello se les llamará módulos sin especificar que son módulos derechos, a menos que sea necesario señalarlo. Sin embargo, recuérdese que para todo resultado sobre módulos derechos existe otro análogo para módulos izquierdos.

1.2.2. Submódulos

Definición 1.5. Dado un módulo derecho M sobre un anillo A, un submódulo N de M es un subgrupo tal que para cualquier $n \in N$ y $a \in A$ se tiene que $na \in N$. Análogamente, si M es un A-módulo izquierdo, entonces un subgrupo N se le llama submódulo si para cualquier $n \in N$ y $a \in A$ se tiene que $an \in N$. Por último, si M es un A-B bimódulo, entonces un subgrupo N se le llama submódulo de M si es un submódulo de ${}_AM$ y un submódulo de M_B.

Observación 1.6. Los submódulos de A_A son los ideales derechos, los de ${}_AA$ reciben el nombre de ideales izquierdos y los de ${}_AA_A$ reciben el nombre de ideales bilaterales ó simplemente ideales.

Ahora, si N es un submódulo, entonces es un módulo, por lo que existe una representación $\phi : A \to \mathrm{End}(N)^{op}$, y si $\psi : A \to \mathrm{End}(M)^{op}$ es la representación de A asociada a M y $a \in A$, como $na \in N$ para cualquier $n \in N$, se tiene que $\psi(a)$ restringida a N es igual a $\phi(a)$, por lo que si se le llama $\rho : \mathrm{Im}(\psi) \to \mathrm{End}(N)^{op}$ al morfismo que restringe a N, se tiene que $\rho\psi = \phi$ y $\rho\psi(a)(n) = \psi(a)(n)$ para cualquier $n \in N$.

Recíprocamente, si N es un subgrupo de M y existen representaciones

$$\phi : A \to \mathrm{End}(N)^{op} \text{ y } \psi : A \to \mathrm{End}(M)^{op}$$

tales que existe un morfismo $\rho : \mathrm{Im}(\psi) \to \mathrm{End}(N)^{op}$ con el que

$$\rho\psi = \phi \text{ y } \rho\psi(a)(n) = \psi(a)(n)$$

para cualquier $n \in N$, y si $\cdot$ es el producto del módulo M y $\star$ es el producto del módulo N, inducidos por sus respectivas respresentaciones, dados $n \in N$ y $a \in A$,

$$n \cdot a = \psi(a)(n) = \rho\psi(a)(n) = \phi(a)(n) = n \star a,$$

por lo que N es submódulo de M.

Proposición 1.7. *Sea A un anillo. Si M es un grupo abeliano, N es un subgrupo de M y existen $\psi : A \to \mathrm{End}(M)^{op}$ y $\phi : A \to \mathrm{End}(N)^{op}$ representaciones de A, entonces N es un submódulo de M si y sólo si existe un morfismo de anillos $\rho : \mathrm{Im}(\psi) \to \mathrm{End}(N)^{op}$ tal que $\rho\psi = \phi$ y $\rho\psi(a)(n) = \psi(a)(n)$ para cualquier $n \in N$.*

Luego, si se tiene un morfismo de anillos $f : R \to A$ y una representación

$$\psi : A \to \mathrm{End}(M)^{op},$$

la composición $\psi f : R \to \mathrm{End}(M)^{op}$ es una representación, por lo que ahora M es un R-módulo, y además todo submódulo N_A de M_A es un submódulo N_R de M_R, pues si se tiene que existe $\rho : \mathrm{Im}(\psi) \to \mathrm{End}(N)^{op}$ tal que $\rho\psi = \phi$ y $\rho\psi(a)(n) = \psi(a)(n)$ para cualquier $n \in N$, entonces $\rho\psi f = \phi f$ y $\rho\psi f(a)(n) = \psi f(a)(n)$ para cualquier $n \in N$, por lo que todo submódulo de M_A es un submódulo de M_R.

Proposición 1.8. *Si existe un morfismo de anillos $f : R \to A$ y un A-módulo M, entonces M es un R-módulo y todo submódulo de M_A es un submódulo de M_R.*

Cuando se tiene dicho morfismo, en general no hay forma de relacionar los R-módulos con los A-módulos. Sin embargo, dada una representación $\psi : A \to \mathrm{End}(M)$, si se tiene un ideal bilateral $I \subseteq \mathrm{Ker}(\psi)$, entonces existe un morfismo $\psi' : A/I \to \mathrm{End}(M)$ tal que $\psi = \psi'\pi$, donde $\pi : A \to A/I$ es la proyección canónica. Por lo que ψ' induce que M sea un A/I-módulo.

Además si N es un submódulo de un A-módulo derecho M, entonces existe un morfismo de anillos $\rho : \mathrm{Im}(\psi) \to \mathrm{End}(N)^{op}$ tal que $\rho\psi = \phi$ y $\rho\psi(a)(n) = \psi(a)(n)$ para cualquier $n \in N$, donde $\phi : A \to \mathrm{End}(N)^{op}$, pero como $\psi = \psi'\pi$ se tiene que $\rho\psi'\pi = \phi$ y $\rho\psi'\pi(a)(n) = \psi'\pi(a)(n)$ para cualquier $n \in N$. Lo que implica que si

$$\phi' = \rho\psi' : A/I \to \mathrm{End}(N),$$

se tiene que $\rho\psi' = \phi'$ y $\rho\psi'(a)(n) = \psi'(a)(n)$ para cualquier $n \in N$ y $a \in A/I$. Por lo tanto N es un submódulo de $M_{A/I}$.

$$\begin{tikzcd}
& A/I \arrow[dr, "\psi'"] & \\
A \arrow[ur, "\pi"] \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & \mathrm{Im}(\psi) \arrow[dl, "\rho"] \\
& \mathrm{End}(N)^{op} &
\end{tikzcd}$$

Proposición 1.9. *Si M es un A-módulo derecho e I es un ideal bilateral de A tal que $MI = 0$, entonces M es un A/I-módulo y N es submódulo de M_A si y sólo si es submódulo de $M_{A/I}$.*

Demostración. Basta notar que si $\psi : A \to \mathrm{End}(M)^{op}$ es la representación inducida por M_A, entonces $MI = 0$ si y sólo si $I \subseteq \mathrm{Ker}(\psi)$. Por ello el resultado se sigue de la argumentación anterior. $\square$

1.3. Morfismos de módulos

Sean A y B anillos. Dados M y N A-módulos, un morfismo de grupos $f : M \to N$ tal que $f(ma) = f(m)a$ para todo $m \in M$ y $a \in A$, se llama morfismo de módulos.

Al conjunto de todos los morfismos con dominio M y codominio N se le denota $\mathrm{Hom}_A(M, N)$. Siendo N un grupo abeliano, $\mathrm{Hom}_A(M, N)$ hereda una estructura de grupo abeliano con la operación $(f + g)(x) = f(x) + g(x)$.

Más aún, si N es un B-A bimódulo, entonces se puede definir una operación

$$B \times Hom_A(M, N) \to Hom_A(M, N)$$

que a cada pareja (σ, f) le asigna el morfismo σf definido como $(\sigma f)(x) = \sigma f(x)$ para toda $x \in M$. Tal operación cumple que

(a) $\sigma(f + g)(x) = \sigma(f(x) + g(x)) = \sigma f(x) + \sigma g(x)$,

(b) $(\sigma_1 + \sigma_2)f(x) = \sigma_1 f(x) + \sigma_2 f(x)$,

(c) $(\sigma_1\sigma_2)f(x) = \sigma_1(\sigma_2 f(x)) = \sigma_1(\sigma_2 f)(x)$,

(d) $1_S f(x) = f(x)$,

para cualesquiera $f, g \in \mathrm{Hom}_A(M, N)$ y $\sigma_1, \sigma_2 \in B$. Por lo tanto, $\mathrm{Hom}_A(M, N)$ es un B-módulo izquierdo.

Análogamente se tiene el siguiente resultado.

Proposición 1.10. *Sean A y B anillos.*

(a) *Si M es un B-A bimódulo y N es un A-módulo derecho, entonces* $\mathrm{Hom}_A(M, N)$ *es un B-módulo derecho con el producto $(f\sigma)(x) = f(\sigma x)$.*

(b) *Si M es un A-módulo derecho y N es un B-A bimódulo, entonces* $\mathrm{Hom}_A(M, N)$ *es un B-módulo izquierdo con el producto $(\sigma f)(x) = \sigma(f(x))$.*

(c) *Si M es un B-A bimódulo y N es un B-módulo izquierdo, entonces* $\mathrm{Hom}_B(M, N)$ *es un A-módulo izquierdo con el producto $af(x) = f(xa)$.*

(d) *Si M es un B-módulo izquierdo y N es un B-A bimódulo, entonces* $\mathrm{Hom}_B(M, N)$ *es un A-módulo derecho con el producto $(fa)(x) = f(x)a$.*

1.3.1. Monomofismos, Epimorfismos e Isomorfismos

Definición 1.11. Sea $f : M \to N$ un morfismo de módulos.

- Se dice que f es monomorfismo si para cualquier par de morfismos $\alpha : K \to M$ y $\beta : K \to M$ tales que $f\alpha = f\beta$, se tiene que $\alpha = \beta$; ó equivalentemente si f es inyectiva.
- Se dice que f es epimorfismo si para cualquier par de morfismos $\alpha : N \to K$ y $\beta : N \to K$ tales que $\alpha f = \beta f$, se tiene que $\alpha = \beta$; ó equivalentemente si f es suprayectiva.
- Se dice que f es isomorfismo si existe un morfismo $g : N \to M$ tal que $fg = 1_N$ y $gf = 1_M$, ó equivalentemente si f es biyectiva. En caso de existir un isomorfismo entre M y N se dice que M y N son isomorfos, y se denota $M \cong N$.

Ahora, dado un morfismo $f : M \to N$ es sencillo probar que

$$\operatorname{Ker}(f) = \{x \in M \mid f(x) = 0\}$$

es un submódulo de M, y

$$\operatorname{Im}(f) = \{f(x) \in N \mid x \in M\}$$

es un submódulo de N. Tales submódulos reciben los nombres de núcleo e imagen de f. Por lo que f es monomorfismo si y sólo si $\operatorname{Ker}(f) = 0$ y f es epimorfismo si y sólo si $\operatorname{Im}(f) = M$.

Por otro lado, es importante mencionar que si K es un submódulo de M, entonces M/K es un módulo. Es claro entonces que la proyección natural $\pi : M \to M/K$ es un morfismo de módulos.

Utilizando tal morfismo, el siguiente resultado muestra que todo morfismo $f : M \to N$ se factoriza a través de M/K si $K \subseteq \operatorname{Ker}(f)$.

Proposición 1.12. *Si $f : M \to N$ es un morfismo de módulos y K es un submódulo de M contenido en $\operatorname{Ker}(f)$, entonces existe un único morfismo $f' : M/K \to N$ tal que $f = f'\pi$, donde $\pi : M \to M/K$ es la proyección natural.*

De donde se siguen los 3 teoremas de isomorfismos.

Teorema 1.13. *Sea $f : M \to N$ un morfismo de módulos. Existe un único ismorfismo $g : M/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ tal que $f = g\pi$, donde $\pi : M \to M/\operatorname{Ker}(f)$ es la proyección natural.*

Teorema 1.14. *Si K y N son submódulos de M, entonces $(K+N)/K \cong N/(K\cap N)$.*

Teorema 1.15. *Si K y N son submódulos de M tales que $K \subseteq N$, entonces*

$$(M/N)/(N/K) \cong M/K.$$

1.3.2. Sucesiones exactas cortas

Definición 1.16. Una sucesión de morfismos

$$... \to M_{i-1} \stackrel{f_{i-1}}{\to} M_i \stackrel{f_i}{\to} M_{i+1} \to ...$$

se dice que es exacta si $\mathrm{Im}(f_{i-1}) = \mathrm{Ker}(f_i)$ para toda i. Luego una sucesión

$$M \stackrel{f}{\to} N \to 0$$

es exacta si y sólo si f es epimorfismo; una sucesión

$$0 \to M \stackrel{f}{\to} N$$

es exacta si y sólo si f es monomorfismo; y una sucesión

$$0 \to M \stackrel{f}{\to} N \stackrel{g}{\to} K \to 0$$

es exacta si y sólo si f es monomorfismo, g es epimorfismo y

$$\mathrm{Im}(f) = \mathrm{Ker}(g).$$

Una sucesión como la anterior se le llama sucesión exacta corta.

Más adelante se expondrán algunas propiedades de las sucesiones exactas cortas, pero antes es necesaria la definición de los siguientes objetos.

1.4. Producto y Coproducto de Módulos

Definición 1.17. Dada una familia de módulos $\{M_i\}_{i\in X}$ se definen los siguientes objetos.

- El producto de la familia consiste de un módulo P junto con una familia de morfismos $\{\pi_i : P \to M_i\}_{i\in X}$, tal que para todo módulo Y y toda familia de morfismos $\{p_i : Y \to M_i\}_{i\in X}$ existe un único morfismo $f : Y \to P$ tal que $\pi_i f = p_i$ para todo $i \in X$.
- El coproducto ó suma directa de la familia consiste de un módulo C con una familia de morfismos $\{\eta_i : M_i \to C\}_{i\in X}$, tal que para todo módulo Y y toda familia de morfismos $\{h_i : M_i \to Y\}_{i\in X}$ existe un único morfismo $f : C \to Y$ tal que $f\eta_i = h_i$ para todo $i \in X$.

Claramente en caso de existir tales objetos son únicos salvo isomorfismo. Más aún, es sencillo probar que para cualquier familia $\{M_i\}_{i\in X}$ el producto y la suma directa existen. Explícitamente, el producto es el módulo

$$P = \prod_{i\in X} M_i = \{(m_i)_{i\in X} \mid m_i \in M_i \text{ para toda } i \in X\}$$

junto con los morfismos $\{\pi_i : P \to M_i\}_{i\in X}$ definidos como $\pi_j(m_i)_{i\in X} = m_j$ para toda $j \in X$; y el coproducto es el módulo

$$C = \bigoplus_{i\in X} M_i = \sum_{i\in X} N_i$$

donde $N_j = \{(m_i)_{i\in X} \in P \mid m_k = 0 \text{ para toda } k \neq j\}$, junto con la familia de morfismos $\{\eta_i : M_i \to C\}_{i\in X}$ definidos como $\eta_j(m) = (m_i)_{i\in X}$ donde $m_j = m$ y $m_i = 0$ para toda $i \neq j$.

Observación 1.18. Si $\{M_i\}_{i\in X}$ es una familia finita de módulos, entonces el producto es isomorfo al coproducto.

Cabe observar que si M tiene una familia de submódulos $\{M_i\}_{i\in X}$ tales que

$$M = \sum_{i\in X} M_i \text{ y } \left(\sum_{i\neq j} M_i\right) \cap M_j = 0 \text{ para toda } j \in X,$$

entonces $M \cong \bigoplus_{i\in X} M_i$. De hecho, $\{N_i\}_{i\in X}$ es una familia de submódulos de C tales que $N_i \cong M_i$ para todo $i \in X$, $C = \sum_{i\in X} N_i$ y $(\sum_{i\neq j} N_i) \cap N_j = 0$. Por esta razón en general cada módulo M_i se identifica con N_i y recibe el nombre de sumando directo de C, y C se considera como el módulo $\sum_{i\in X} M_i$.

Si se tiene una familia de módulos $\{M_i\}_{i\in X}$ con $M_i = M$ para todo $i \in X$ entonces el producto se denota como M^X y el coproducto como $M^{(X)}$.

Por último, por medio del coproducto se define la siguiente clase de módulos.

Definición 1.19. Un A-módulo M es libre si existe un conjunto X tal que

$$M \cong \bigoplus_{i\in X} A = A^{(X)}.$$

1.4.1. Sucesiones que se escinden

Continuando con la exposición de propiedades de la sucesiones exactas cortas, se definen a continuación las sucesiones que se escinden.

Definición 1.20. Se dice que una sucesión exacta corta

$$0 \to M \xrightarrow{f} N \xrightarrow{g} K \to 0$$

se escinde si existe un morfismo $h : K \to N$ tal que $gh = 1_K$, ó equivalentemente si existe un morfismo $s : N \to M$ tal que $sf = 1_M$. Si f es un morfismo tal que

$$0 \to M \xrightarrow{f} N \to N/\operatorname{Im}(f) \to 0$$

es una sucesión que se escinde, entonces se dice que f es monomorfismo que se escinde. Si g es un morfismo tal que

$$0 \to \operatorname{Ker}(g) \to N \xrightarrow{g} K \to 0$$

es una sucesión que se escinde, entonces se dice que g es un epimorfismo que se escinde.

Se cumple la siguiente proposición.

Proposición 1.21. *Si* $0 \to M \xrightarrow{f} N \xrightarrow{g} K \to 0$ *es una sucesión exacta, entonces* f *se escinde si, y sólo si,* g *se escinde si, y sólo si,* $\operatorname{Im}(f)$ *es sumando directo de* N *si, y sólo si,* $\operatorname{Ker}(g)$ *es sumando directo de* N*. En tal caso* $N \cong K \oplus M$*, y más aún, si* $f' : N \to M$ *y* $g' : K \to N$ *son morfismos tales que* $f'f = 1_M$ *y* $gg' = 1_K$*, entonces*

$$N = \operatorname{Im}(f) \oplus \operatorname{Ker}(f') = \operatorname{Im}(g') \oplus \operatorname{Ker}(g).$$

Demostración. Se puede consultar en [Pas04]. □

1.5. Módulos proyectivos y módulos inyectivos

Definición 1.22. Sea P un módulo.

$$\begin{tikzcd}
& P \arrow[dl, dashed, "h"'] \arrow[d, "g"] \arrow[dl, phantom, "\circlearrowleft", shift left=3ex] & \\
M \arrow[r, "f"'] & N \arrow[r] & 0
\end{tikzcd}$$

Se dice que P es proyectivo si para todo epimorfismo $f : M \to N$ y todo morfismo $g : P \to N$, existe un morfismo $h : P \to M$ tal que $fh = g$, ó equivalentemente que toda sucesión exacta corta

$$0 \to K \to M \to P \to 0$$

se escinda.

Se prueba que dada una familia de módulos $\{P_i\}_{i\in X}$, la suma directa $\bigoplus_{i\in X} P_i$ es un módulo proyectivo si y sólo si P_i es proyectivo para todo $i \in X$. Más aún, si M es un sumando directo de un módulo proyectivo, entonces M es también proyectivo.

Proposición 1.23. *Si $\{P_i\}_{i\in X}$ una familia de módulos, entonces $\bigoplus_{i\in X} P_i$ es un módulo proyectivo si y sólo si P_i es proyectivo para todo $i \in X$.*

Proposición 1.24. *Si P es un módulo proyectivo, entonces todo sumando directo de P es un módulo proyectivo.*

Luego, es sencillo probar que todo módulo libre es proyectivo, lo que implica que todo módulo proyectivo es sumando directo de un módulo libre, ya que existe un epimorfismo $f : A^{(P)} \to P$ definido como $f(a_x)_{x\in P} = \sum_{x\in P} a_x x$.

Proposición 1.25. *P es un módulo proyectivo si y sólo si P es sumando directo de un módulo libre.*

Definición 1.26. Sea I un módulo.

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[rr, "f"] \arrow[dr, "g"'] & \arrow[d, phantom, "\circlearrowright"] & M \arrow[dl, dashed, "h"] \\ & & I & \end{tikzcd}$$

Se dice que I es un módulo inyectivo si para todo monomorfismo $f : N \to M$ y todo morfismo $g : N \to I$, existe un morfismo $h : M \to I$ tal que $hf = g$, ó equivalentemente que toda sucesión exacta

$$0 \to I \to X \to Y \to 0$$

se escinda.

De la definición es evidente que un módulo Q es inyectivo si y sólo si es un sumando directo de todo módulo que lo contenga como submódulo. Con lo que se prueba que dada una familia de módulos inyectivos $\{Q_i\}_{i\in X}$, el producto $\prod_{i\in X} Q_i$ es un módulo inyectivo.

Proposición 1.27. *Un módulo Q es inyectivo si y sólo si Q es sumando directo de todo módulo que lo contenga.*

Proposición 1.28. *Si $\{Q_i\}_{i\in X}$ es una familia de módulos , entonces $\prod_{i\in X} Q_i$ es un módulo inyectivo si y solo si Q_i es un módulo inyectivo para todo $i \in X$.*

1.6. Módulos finitamente generados y cogenerados

A continuación se definen dos clases de módulos importantes y se exponen algunas propiedades.

Definición 1.29. Un módulo M es finitamente generado si para toda familia $\mathcal{F}$ de submódulos de M tal que $\sum_{N\in\mathcal{F}} N = M$, existe una subfamilia finita no vacia $\mathcal{F}'$ de $\mathcal{F}$, tal que $\sum_{N\in\mathcal{F}'} N = M$.

Se tienen las siguientes equivalencias del concepto.

Proposición 1.30. *Sea A un anillo y M un A-módulo, los siguientes enunciados son equivalentes:*

(a) *M es finitamente generado.*

(b) *Dada una familia X de morfismos con contradominio M, si $\sum_{f\in X} \mathrm{Im}(f) = M$, entonces existe una subfamilia finita X' de X tal que $\sum_{f\in X'} \mathrm{Im}(f) = M$.*

(c) *Dada una familia de módulos X, si existe un epimorfismo $f : \bigoplus_{N\in X} N \to M$, entonces existe una familia finita $X' \subseteq X$ y un epimorfismo $g : \bigoplus_{N\in X'} N \to M$, tal que g es igual a f restringido a $\bigoplus_{N\in X'} N$.*

(d) *M es generado por un número finito de elementos, llamados generadores de M.*

(e) *Si $\{N_i\}_{i\in I}$ es una cadena de submódulos tal que $N_i \neq M$ para todo $i \in I$ se tiene que $\sum_{i\in I} N_i \neq M$.*

Demostración. ($a \Rightarrow e$) Sea $\{N_i\}_{i\in I}$ una cadena de submódulos de M tal que $N_i \neq M$ para toda $i \in I$. Si se supone que $\sum_{i\in I} N_i = M$, entonces debido a que M es finitamente generado existe un subconjunto finito $I' \subseteq I$ tal que $\sum_{i\in I'} N_i = M$, lo que implica que $I_m = M$ donde m es el máximo de I', lo cual es una contradicción. Por lo tanto, para toda cadena de submódulos $\{N_i\}_{i\in I}$ tal que $N_i \neq M$ se tiene que $\sum_{i\in I} N_i \neq M$.

($e \Rightarrow a$) Si M no es finitamente generado, entonces existe una familia de submódulos X tal que

$$\sum_{N\in X} N = M \ \text{ pero } \ \sum_{N\in F} N \neq M$$

para toda subfamilia finita $F \subseteq X$. Sin pérdida de generalidad se puede suponer que $0 \in X$. Por lo que si se considera el conjunto

$$S = \left\{ \sum_{N\in Y} N \mid Y \subseteq X \ \text{ y } \ M \neq \sum_{N\in Y} N + \sum_{N\in F} N \text{ para toda subfamilia finita } F \subseteq X \right\},$$

se tiene que S no es vacío ya que $0 \in S$. Luego, si $\{K_i\}_{i\in I}$ es una cadena en $(S, \subseteq)$, entonces $T = \sum_{i\in I} K_i$ es una cota superior de la cadena en S. En efecto, es claro que

$K_j \subseteq T$ para toda $j \in I$, y si se supone que $T \notin S$, entonces existen $N_1, ..., N_n \in X$ tales que $M = T + N_1 + ... + N_n$; pero entonces la cadena

$$\{K_i + N_1 + ... + N_n\}_{i \in I}$$

contradice el punto (e) ya que

$$\sum_{i \in I} K_i + N_1 + ... + N_n = T + N_1 + ... + N_n = M.$$

Por lo tanto, T es una cota superior de la cadena. Por lo que se sigue del lema de Zorn que existe un elemento maximal K de $(S, \subseteq)$. Ahora, debido a que $K \in S$, existe una subfamilia $Y \subseteq X$ tal que $K = \sum_{N \in Y} N$ y se cumple que $K + \sum_{N \in F} N \neq M$ para toda subfamilia finita $F \subseteq X$. Pero $M = \sum_{N \in X} N$, lo que implica que existe $N \in X \backslash Y$, y entonces $K + N \supsetneq K$, lo que implica que $K + N \notin S$ por la maximalidad de K; pero entonces existen $N_1, ..., N_n \in X$ tales que

$$K + N + N_1 + ... + N_n = M,$$

lo cual contradice el hecho de que $K \in S$ ya que $N \in X$. Por lo tanto M es finitamente generado.

La demostración de la equivalencia entre (a),(b),(c) y (d) se puede consultar en [AF04]. $\square$

El concepto dual de ser finitamente generado es ser finitamente cogenerado.

Definición 1.31. Un módulo M es finitamente cogenerado si para toda familia $\mathcal{F}$ de submódulos de M tal que $\bigcap_{N \in \mathcal{F}} N = 0$ se tiene que existe una subfamilia finita no vacia $\mathcal{F}'$ de $\mathcal{F}$, tal que $\bigcap_{N \in \mathcal{F}'} N = 0$.

Se tienen las siguientes equivalencias del concepto.

Proposición 1.32. *Sea A un anillo y M un A-módulo, los siguientes enunciados son equivalentes:*

(a) *M es finitamente cogenerado.*

(b) *Dada una familia X de morfismos con dominio M, si $\bigcap_{f \in X} \mathrm{Ker}(f) = 0$, entonces existe una subfamilia finita X' de X tal que $\bigcap_{f \in X'} \mathrm{Ker}(f) = 0$.*

(c) *Dada una familia de módulos X. Si existe un monomorfismo $f : M \to \Pi_{N \in X} N$, entonces existe una familia finita $X' \subseteq X$ y un monomorfismo $g : M \to \Pi_{N \in X'} N$, tal que g es igual a $\pi_{X'} f$, donde $\pi_{X'} : \Pi_{N \in X} N \to \Pi_{N \in X'} N$ es la proyeccion natural.*

(d) *Dado un A-módulo N y un conjunto X, si existe un monomorfismo $f : M \to N^X$, entonces existe un subconjunto finito X' de X tal que $\pi_{X'} f : M \to N^{X'}$ es monomorfismo, donde $N^X = \Pi_X N$ y $\pi_{X'} : N^X \to N^{X'}$ es la proyección canónica.*

(e) *Para toda cadena de submódulos* $\{N_i\}_{i\in I}$ *tal que* $N_i \neq 0$ *para todo* $i \in I$ *se tiene que* $\bigcap_{i\in I} N_i \neq 0$.

Demostración. $(a \Rightarrow e)$ Sea $\{N_i\}_{i\in I}$ una cadena de submódulos de M tal que $N_i \neq 0$ para toda $i \in I$. Si se supone que $\bigcap_{i\in I} N_i = 0$, entonces debido a que M es finitamente cogenerado existe un subconjunto finito $I' \subseteq I$ tal que $\bigcap_{i\in I'} N_i = 0$, lo que implica que $I_m = 0$ donde m es el mínimo de I', lo cual es una contradicción. Por lo tanto, para toda cadena de submódulos $\{N_i\}_{i\in I}$ tal que $N_i \neq 0$ se tiene que $\bigcap_{i\in I} N_i \neq 0$.

$(e \Rightarrow a)$ Si M no es finitamente cogenerado, entonces existe una familia de submódulos X tal que

$$\bigcap_{N\in X} N = 0 \text{ pero } \bigcap_{N\in F} N \neq 0$$

para toda subfamilia finita $F \subseteq X$. Sin pérdida de generalidad se puede suponer que $M \in X$. Por lo que si se considera el conjunto

$$S = \left\{ \bigcap_{N\in Y} N \mid Y \subseteq X \text{ y } 0 \neq \left(\bigcap_{N\in Y} N\right) \cap \left(\bigcap_{N\in F} N\right) \text{ para toda subfamilia finita } F \subseteq X \right\},$$

se tiene que S no es vacío ya que $M \in S$. Luego, si $\{K_i\}_{i\in I}$ es una cadena en $(S, \supseteq)$, entonces $T = \bigcap_{i\in I} K_i$ es una cota superior de la cadena en S. En efecto, es claro que $K_j \supseteq T$ para toda $j \in I$, y si se supone que $T \notin S$, entonces existen $N_1, ..., N_n \in X$ tales que $0 = T \cap N_1 \cap ... \cap N_n$; pero entonces la cadena

$$\{K_i \cap N_1 \cap ... \cap N_n\}_{i\in I}$$

contradice el punto (e) ya que $\bigcap_{i\in I} K_i \cap N_1 \cap ... \cap N_n = T \cap N_1 \cap ... \cap N_n = 0$. Por lo tanto, T es una cota superior de la cadena. Por lo que se sigue del lema de Zorn que existe un elemento maximal K de $(S, \supseteq)$. Ahora, debido a que $K \in S$, existe una subfamilia $Y \subseteq X$ tal que $K = \bigcap_{N\in Y} N$ y se cumple que $K \cap (\bigcap_{N\in F} N) \neq 0$ para toda subfamilia finita $F \subseteq X$. Pero $0 = \bigcap_{N\in X} N$, lo que implica que existe $N \in X \backslash Y$, y entonces $K \cap N \subsetneq K$, lo que implica que $K \cap N \notin S$ por la maximalidad de K; pero entonces existen $N_1, ..., N_n \in X$ tales que

$$K \cap N \cap N_1 \cap ... \cap N_n = 0,$$

lo cual contradice el hecho de que $K \in S$ ya que $N \in X$. Por lo tanto M es finitamente cogenerado.

La demostración de la equivalencia entre (a),(b),(c) y (d) se puede consultar en [AF04]. □

Nótese que si M es un módulo finitamente generado, entonces tiene un conjunto finito de generadores $\{m_1, ..., m_k\}$, lo que implica que dado cualquier submódulo N de M, el cociente M/N también tiene un conjunto finito de generadores $\{m_1 + N, ..., m_k + N\}$, por lo tanto cualquier cociente de M es finitamente generado. Recíprocamente si todo cociente de M es finitamente generado, entonces en particular $M \cong M/0$ es finitamente generado.

De igual manera, si M es un módulo finitamente cogenerado, y N es un submódulo de M, entonces N también es finitamente cogenerado, en efecto si X es una familia de submódulos de N tal que $\bigcap_{V \in X} V = 0$, entonces como X también es una familia de submódulos de M, existe una subafamilia finita X' de X tal que $\bigcap_{V \in X'} V = 0$. Por lo tanto todo submódulo es finitamente cogenerado. Reciprocamente, si todo submódulo de M es finitamente cogenerado, entonces en particular M es finitamente generado.

Se ha probado la siguiente proposición.

Proposición 1.33. *Dado M un módulo se cumple lo siguiente:*

(a) *M es finitamente generado si y sólo si todo cociente de M también lo es.*

(b) *M es finitamente cogenerado si y solo si todo submódulo de M también lo es.*

Ejemplo 1.34. El módulo $\mathbb{Z}$ es finitamente generado pero no finitamente cogenerado. En efecto, es finitamente generado ya que 1 lo genera, y no es finitamente generado ya que si

$$X = \{p \in \mathbb{Z} \mid p \text{ es primo}\},$$

entonces $\bigcap_{p \in X} p\mathbb{Z} = 0$, pero $\bigcap_{p \in F} p\mathbb{Z} = m\mathbb{Z} \neq 0$ donde $m = \prod_{p \in F} p$ para todo subconjunto finito $F \subseteq X$.

Ejemplo 1.35. El módulo $M = \mathbb{Z}_{p^\infty} = \left\langle \frac{\bar{1}}{p^k} \in \mathbb{Q}/\mathbb{Z} \mid k \in \mathbb{N} \right\rangle$ es finitamente cogenerado pero no finitamente generado. En efecto, todo submódulo es de la forma $\left\langle \frac{\bar{1}}{p^n} \right\rangle$para algún $n \in \mathbb{N}$, lo que implica que $\left\langle \frac{\bar{1}}{p} \right\rangle$ está contenido en todo submódulo no nulo, por lo que si X es una familia de submódulos tal que $\bigcap_{N \in X} N = 0$, se tiene que $0 \in X$, lo que implica que existe una subfamilia finita $\{0\}$ cuya intersección es igual a 0, y entonces M es finitamente cogenerado. Luego, M no es finitamente generado, ya que $M = \sum_{k \in \mathbb{N}} \frac{\bar{1}}{p^k}\mathbb{Z}$, pero si se toma un conjunto finito de naturales F es sencillo probar que

$$\frac{\bar{1}}{p^k} \notin \left\langle \frac{\bar{1}}{p^n} \right\rangle_{n \in F}$$

para todo $k > \sum_{n \in F} n$.

Ejemplo 1.36. Dado un campo k. Un espacio vectorial V es finitamente generado si y sólo si V es de dimensión finita si y sólo si V es finitamente cogenerado. En efecto, si V es finitamente generado, entonces tiene un conjunto finito de generadores; pero entonces tal conjunto contiene una base, lo que implica que V es de dimensión finita. Recíprocamente si V es de dimensión finita, entonces V tiene un conjunto finito de generadores, por lo que V es finitamente generado. Por otro lado, si se supone que existe una base infinita β de V, entonces tomando una sucesión $\{\alpha_i\}_{i\in\mathbb{N}}$ se construye una cadena de submódulos $\{V_i\}_{i\in\mathbb{N}}$, donde

$$V_n = \langle \alpha \in \beta \mid \alpha \notin \{\alpha_1, ..., \alpha_n\}\rangle ,$$

es claro entonces que $\bigcap_{i\in I} V_i = 0$ pero $\bigcap_{i\in F} V_i \neq 0$ para toda fubfamilia finita $F \subseteq \mathbb{N}$, lo que implica que V no es finitamente cogenerado. Recíprocamente, si V es de dimensión n, toda cadena de subespacios $\{W_i\}_{i\in\mathbb{N}}$ tal que $W_i \neq 0$ para toda $i \in I$, induce una sucesión de enteros

$$n \geq \dim_k V_1 \geq \dim_k V_2 \geq ... \geq \dim_k V_m \geq ...$$

pero $\dim_k V_m > 0$ para toda $m \in \mathbb{N}$, lo que implica que existe un número natural M tal que $\dim_k V_m = \dim_k V_M$ para todo $m \geq M$; pero entonces $\bigcap_{i\in\mathbb{N}} V_i = V_M$.

Ejemplo 1.37. $\mathbb{Q}/\mathbb{Z}$ no es finitamente generado ni finitamente cogenerado. En efecto, es sencillo probar que

$$\mathbb{Q}/\mathbb{Z} = \bigoplus_{p\in X} \mathbb{Z}_{p^\infty}$$

donde X es el conjunto de todos los primos. Por lo que es claro que $\sum_{p\in X} \mathbb{Z}_{p^\infty} = \mathbb{Q}/\mathbb{Z}$ pero $\sum_{p\in F} \mathbb{Z}_{p^\infty} \neq \mathbb{Q}/\mathbb{Z}$ para toda subfamilia finita $F \subseteq X$, por lo que no es finitamente generado. Por otro lado, tomando una sucesión $\{p_i\}_{i\in\mathbb{N}}$ en X se construye la familia

$$\left\{ N_n = \sum_{i\in\mathbb{N}-\{1,...,n\}} \mathbb{Z}_{p_i^\infty} \right\}_{n\in\mathbb{N}},$$

que claramente cumple que $\bigcap_{i\in\mathbb{N}} N_i$ pero $\bigcap_{F\subseteq\mathbb{N}} N_i \neq 0$ para toda fubfamilia finita F.

1.7. Ejemplos y construcciones usuales de anillos

En esta sección se verán ejemplos y construcciones de anillos que se utilizarán más adelante.

1.7.1. Álgebras

Definición 1.38. Sea A un anillo conmutativo. Si B es un anillo tal que existe un morfismo de anillos $\phi : A \to B$ con $\phi(a)x = x\phi(a)$ para todo $a \in A$ y $b \in B$, entonces se dice que B es un A-álgebra, y que ϕ es la representación asociada al álgebra B.

Ahora, más adelante se probará que todo anillo R es isomorfo al anillo de endomorfismos $\mathrm{Hom}_R(R,R) = \mathrm{End}_R(R) \subseteq \mathrm{End}(R)$. Por lo que es inmediato del Lema 1.3 que un anillo B es un A-álgebra si y sólo si B es un A módulo izquierdo.

Pero además A es un anillo conmutativo y $\phi(a)x = x\phi(a)$ para todo $a \in A$ y $b \in B$, lo que implica que B es un A-álgebra si y sólo si B es un A-módulo izquierdo, si y sólo si B es un A-módulo derecho, si y sólo si B es un A-bimódulo.

Ahora, si B es un A-álgebra, M un B-módulo y $\psi : B \to \mathrm{End}(M)^{op}$ la representación asociada a M, entonces la composición de representaciones $\psi\phi : A \to \mathrm{End}(M)^{op}$ induce una estructura de A-módulo a M. Por lo tanto todo B-módulo es un A-módulo.

Proposición 1.39. *Si B un A-álgebra, entonces todo B-módulo es un A-módulo.*

Este hecho es de relevancia debido a que bajo determinadas hipótesis algunas propiedades de los A-módulos se heredan a los B-módulos. Un ejemplo de este fenómeno es la siguiente proposición.

Proposición 1.40. *Sea B un A-álgebra tal que B_A es finitamente generado. Si M un B-módulo derecho, entonces M es un A-módulo finitamente generado si y sólo si es un B-módulo finitamente generado.*

Demostración. Si M es un A-módulo finitamente generado, entonces existe un conjunto finito de generadores $\{m_1, ..., m_n\}$ de M sobre A; pero en tal caso para todo $m \in M$ existen $a_1, ..., a_n \in A$ tales que

$$m = \sum_{i=1}^{n} m_i a_i = \sum_{i=1}^{n} m_i \left(1_B a_i\right),$$

donde $1_B a_i \in B$ para todo $i \in \{1, ..., n\}$, lo que implica que M_B es finitamente generado.

Si M es un B-módulo finitamente generado, entonces existe un conjunto finito de generadores $\{m_1, ..., m_n\}$ de M sobre B. Por otro lado, B_A es finitamente generado, lo que implica que existe un conjunto de generadores $\{b_1, ..., b_k\} \subseteq B$ sobre A, lo que implica que

$$X = \{m_i b_j \mid i \in \{1, ..., n\}, j \in \{1, ..., k\}\}$$

es un conjunto finito de generadores de M sobre A. En efecto, para todo $m \in M$ existen $x_1, ..., x_n \in B$ tales que $m = \sum_{i=1}^{n} m_i x_i$, pero para cada x_j existen $y_1^{(j)}, ..., y_k^{(j)} \in A$ tales que $x_j = \sum_{i=1}^{k} b_i y_i^{(j)}$, lo que implica que

$$m = \sum_{j=1}^{k} \sum_{i=1}^{n} m_i b_j y_j^{(i)},$$

y entonces X es un conjunto de generadores. □

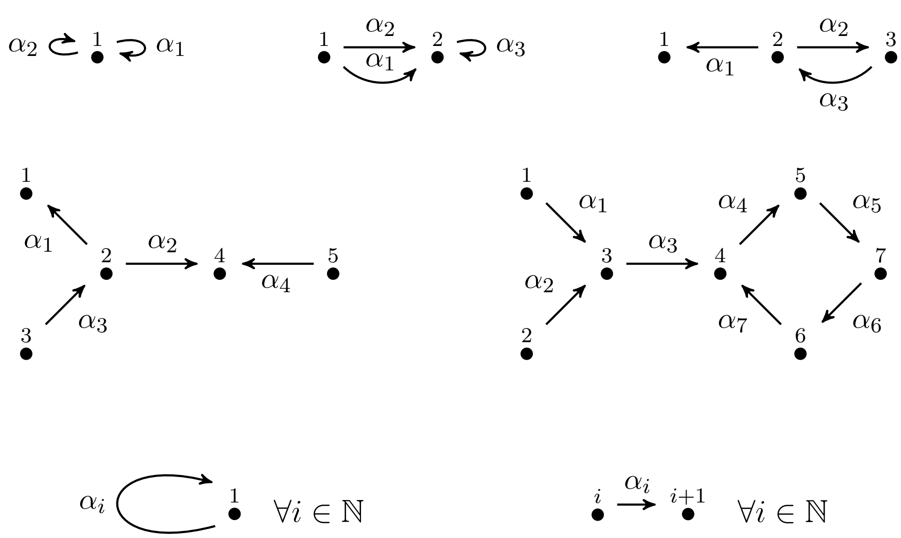
Un caso importante a considerar es cuando el anillo A es un campo. En tal caso se puede considerar la dimensión del álgebra B como espacio vectorial, así como la dimensión de los B-módulos. Se tiene entonces el siguiente corolario de la proposición anterior.

Corolario 1.41. *Sea k un campo y B un k-álgebra de dimensión finita. Si M es un B-módulo, entonces M es finitamente generado si y sólo si es de dimensión finita.*

1.7.2. Álgebras de caminos

Definición 1.42. Un carcaj es un una cuaterna $Q = (Q_0, Q_1, s, t)$ que consiste en un conjunto de vértices Q_0, un conjunto de flechas Q_1 y dos funciones $s : Q_1 \to Q_0$ y $t : Q_1 \to Q_0$ que a cada flecha $\alpha \in Q_1$ le asignan un vértice inicial ó vértice de partida $s(\alpha)$ y un vértice final ó vértice de destino $t(\alpha)$.

Como ejemplo se pueden considerar los siguientes carcajes.



Dado un carcaj $Q = (Q_0, Q_1, s, t)$ se dice que Q es finito si Q_0 y Q_1 son conjuntos finitos. La gráfica subyacente de Q es la gráfica que se obtiene al tomar los vértices de Q_0 y considerar las de flechas de Q_1 como aristas y se le denota $\bar{Q}$. Cuando $\bar{Q}$ es conexa se dice que el carcaj Q es conexo.

Ahora, dado un carcaj $Q = (Q_0, Q_1, s, t)$ y $n \in \mathbb{N} \backslash \{0\}$, un camino de longitud n en Q es una sucesión de flechas

$$\alpha_1, \alpha_2, ..., \alpha_n$$

tal que $t(\alpha_k) = s(\alpha_{k+1})$ para todo $k \in \{1, ..., n-1\}$ y se denota como $\alpha_1\alpha_2...\alpha_n$. Además a cada vértice $i \in Q_0$ se le asocia un camino de longitud 0 denotado como e_i.

Dado un camino $\alpha = \alpha_1 ... \alpha_n$ se define el vértice inicial de α como $s(\alpha_1)$ y se denota como $s(\alpha)$, análogamente se define el vértice final de α como $t(\alpha_n)$ y se denota como $t(\alpha)$. En caso de que α sea un camino de longitud cero e_i entonces se definen sus vertices inicial y final como $s(\alpha) = t(\alpha) = i$.

Cabe observar que si $\alpha = \alpha_1 ... \alpha_n$ y $\beta = \beta_1 ... \beta_k$ son caminos en Q tales que $t(\alpha) = s(\beta)$, entonces $\alpha_1 ... \alpha_n \beta_1 ... \beta_k$ es un camino que se denota como $\alpha\beta$.

Luego, si X es el conjunto de todos los caminos en Q y k es un campo, el álgebra de caminos en Q sobre k es el espacio vectorial

$$kQ = k^{(X)}$$

en el que se identifican sus elementos como combinaciones lineales de caminos, es decir

$$kQ = \left\{ \sum_{\alpha \in X'} a_\alpha \alpha \mid X' \text{ es un subconjunto finito de } X, a_\alpha \in k \, \forall \alpha \in X' \right\},$$

con el producto que definido en X como

$$\alpha \cdot \beta = \begin{cases} \alpha\beta & \text{si } t(\alpha) = s(\beta) \\ 0 & \text{si } t(\alpha) \neq s(\beta) \end{cases}$$

se extiende al resto de kQ lineal y distributivamente.

Cabe observar que en general kQ no es un anillo, ya que no tiene unidad a menos que Q tenga un número finito de vértices, como se muestra en la siguiente proposición.

Proposición 1.43. *Si k un campo y Q es un carcaj, entonces kQ es un anillo si y sólo si Q tiene un número finito de vértices.*

Demostración. Por construcción, para probar que AQ es anillo basta probar que tiene elemento identidad, el cual es $1_{AQ} = \sum_{i \in Q_0} e_i$. La demostración se puede consultar en [ASS06]. □

Ejemplo 1.44. Si k es un campo y Q el siguiente carcaj

$$\alpha_2 \circlearrowleft \overset{1}{\bullet} \circlearrowright \alpha_1$$

entonces $kQ \cong k\langle x, y \rangle$, donde $k\langle x, y \rangle$ denota al anillo de polinomios sobre k con variables no conmutativas x, y; y si I es el ideal de kQ generado por $\alpha_1\alpha_2 - \alpha_2\alpha_1$, entonces $kQ/I \cong k[x, y]$.

Ejemplo 1.45. Si k es un anillo conmutativo y Q es el carcaj

$$\begin{tikzcd} \overset{1}{\bullet} \arrow[r, bend left, "\alpha_1"] & \overset{2}{\bullet} \arrow[l, bend left, "\alpha_2"] \end{tikzcd}$$

entonces si I es el ideal de kQ generado por el conjunto $\{\alpha_1\alpha_2, \alpha_2\alpha_1\}$, se tiene que $kQ/I \cong \mathbb{M}_2(k)$.

1.7.3. Anillos de grupos

Definición 1.46. Sea A un anillo conmutativo y $(G, \cdot)$ un grupo con elemento neutro e. El anillo de grupo G sobre el anillo A es el A-módulo libre $AG = A^{(G)}$ en el que se identifican sus elementos como combinaciones lineales de elementos de G, es decir

$$AG = \left\{ \sum_{g\in X} a_g g \mid X \text{ es un subconjunto finito de } G,\ a_g \in A\, \forall g \in X \right\},$$

con el producto

$$\left(\sum_{g\in X} a_g g\right)\left(\sum_{h\in Y} b_h h\right) = \sum_{g\in X}\sum_{h\in Y} a_g b_h gh.$$

AG es un anillo con elemento unitario $1_A e$.

Ejemplo 1.47. Si $(G, \cdot) \cong (\mathbb{Z}_2, +)$ y k es un campo, entonces $kG \cong k[x]/\left\langle x^2\right\rangle$.

2. Descomposiciones de anillos

Si un anillo se descompone como suma directa de grupos abelianos, entonces se puede obtener información de este anillo a partir de estos sumandos directos. El objetivo de éste capítulo es presentar algunas descomposiciones clásicas que serán de utilidad más adelante.

Se inicia la discusión definiendo los elementos idempotentes y se expone la relación entre las descomposiciones de un módulo como suma directa finita de submódulos y los idempotentes de su anillo de endomorfismos.

Ya con esta herramienta, es sencillo presentar resultados clásicos en la teoría de anillos como la descomposición en bloques, que descompone un anillo como producto de anillos conexos y el teorema de Wedderburn-Artin que describe la estructura de los anillos semisimples.

2.1. Idempotentes

En 1870 se publicó la obra *"Linear associative algebra"* del matemático Benjamin Peirce, donde se aborda el estudio de las álgebras asociativas con unidad, encontrando una relación entre los elementos idempotentes de las álgebras y las descomposiciones de éstas.

En esta sección se siguen sus pasos definiendo los elementos idempotentes de un anillo y se exponen propiedades de éstos.

2.1.1. Conceptos básicos

Definición 2.1. Sea A un anillo. Se dice que $e \in A$ es idempotente si $e^2 = e$. Si además e pertenece al centro del anillo, es decir $ea = ae$ para toda $a \in A$, entonces se dice que e es un idempotente central.

Observación 2.2. Si e es un idempotente, entonces $1 - e$ también es idempotente. Más aún, si e es central, entonces $1 - e$ también lo es.

Es inmediato de la definición que todo anillo tiene elementos idempotentes, ya que 1 y 0 lo son. A un idempotente distinto de 0 y 1 se le llamará idempotente no trivial.

Si e es un idempotente distinto de 0, entonces se cumple que eAe es un anillo con las operaciones de A restringidas a eAe, con neutro aditivo $0 = e0e$ y unidad $e = e1e$.

Proposición 2.3. *Sea A un anillo. Si $e \in A$ es un idempotente distinto de 0, entonces eAe es un anillo. Y dados M un A-módulo derecho y N un A-módulo izquierdo, se tiene que Me es un eAe-módulo derecho y eN un eAe-módulo izquierdo.*

Demostración. Sea M un A-módulo derecho. Para cada $xe \in Me$, $xe(e) = xe$, y debido a que M es un A-módulo, para todo $me, ne \in Me$ y $eae, ebe \in eAe$ se cumple lo siguiente

(a) $me(eae + ebe) = meae + mebe$,

(b) $(me + ne)eae = meae + mebe$,

(c) $me(eaeebe) = (meae)ebe$.

En consecuencia Me es un eAe-módulo derecho. Análogamente se prueba eN es un eAe-módulo izquierdo. □

Si además e es un idempotente central, entonces todo grupo abeliano M admite estructura de eAe-módulo derecho si y sólo si M es un A-módulo derecho tal que $M(1-e) = 0$.

Para probar la necesidad se observa que $eAe = Ae = eA$ debido a que e es central, y se considera la función $\tau : A \to eAe$ definida como $\tau(a) = eae = ea$ para toda $a \in A$. Claramente

$$\tau(1) = e,$$
$$\tau(a + b) = eae + ebe = \tau(a) + \tau(b) \text{ y}$$
$$\tau(ab) = eabe = eeabe = eaebe = (eae)(ebe) = \tau(a)\tau(b),$$

por lo que τ es un morfismo de anillos que claramente es suprayectivo, cuyo núcleo es $\mathrm{Ker}(\tau) = (1 - e)A(1 - e)$ ya que $ex = \tau(x) = 0$ si y sólo si

$$x = ex + (1 - e)x = (1 - e)x = (1 - e)x(1 - e).$$

De manera que, si M es un grupo abeliano que admite estructura de eAe-módulo derecho, la representación asociada $\phi : eAe \to \mathrm{End}(M)$ induce un morfismo de anillos $\phi\tau : A \to \mathrm{End}(M)$ el cual confiere al grupo M una estructura de A-módulo tal que $M(1 - e) = 0$ ya que $1 - e \in \mathrm{Ker}(\tau)$.

Recíprocamente, si M es un A-módulo derecho tal que $M(1 - e) = 0$, entonces se cumple que $m = me + m(1 - e) = me$ para todo $m \in M$, es decir $M = Me$, y así M admite estructura de eAe-módulo por la Proposición 2.3.

Más aún, si M y N son grupos abelianos que admiten una estructura de eAe-módulos a la derecha, entonces también son A-módulos derechos y $\mathrm{Hom}_A(M,N) = \mathrm{Hom}_{eAe}(M,N)$. En efecto, es claro que $\mathrm{Hom}_A(M,N) \subseteq \mathrm{Hom}_{eAe}(M,N)$ y si $f \in \mathrm{Hom}_{eAe}(M,N)$, entonces para todo $a \in A$ y $m \in M$ se tiene que

$$f(ma) = f(meae) = f(m)eae = f(m)a,$$

ya que si $x(1-e) = 0$ se cunple que

$$xa = x((1-e)a + eae + ea(1-e)) = xeae,$$

por lo que $ma = meae$ y $f(m)a = f(m)eae$. Por lo tanto, $f \in \mathrm{Hom}_A(M,N)$.

Se ha probado el siguiente resultado.

Proposición 2.4. *Sea A un anillo y $e \neq 0$ un idempotente central de A. Se cumplen los siguientes condiciones.*

(a) *Existe un morfismo suprayectivo de anillos $g : A \to eAe$ cuyo núcleo es el anillo $(1-e)A(1-e)$.*

(b) *Un grupo abeliano M admite estructura de eAe-módulo derecho si y sólo si M es un A-módulo derecho tal que $M(1-e) = 0$.*

(c) *Sean M y N eAe-módulos derechos, entonces* $\mathrm{Hom}_A(M,N) = \mathrm{Hom}_{eAe}(M,N)$.

En la demostración anterior se usó implícitamente el hecho de que $1_A = e + (1-e)$ y que $e(1-e) = 0$. Dichas propiedades se pueden generalizar y se definen a continuación.

Definición 2.5. Sea A un anillo.

- Se dice que dos idempotentes e y f son ortogonales si $ef = 0 = fe$.
- Si la unidad del anillo se expresa como una suma finita de idempotentes ortogonales dos a dos, es decir, $1_A = e_1 + ... + e_n$ donde e_i es idempotente y $e_ie_j = 0 = e_je_i$ para todo $i \neq j$, entonces a dicha expresión se le llama una descomposición de la unidad.

Observación 2.6. Si e y f son idempotentes ortogonales, entonces $e+f$ es idempotente.

Ejemplo 2.7. Sea k un campo. Si $A = \mathbb{M}_n(k)$ entonces todo elemento idempotente de A es de la forma $S^{-1}DS$ donde S es una matriz invertible y $D = (a_{ij})$ es una matriz diagonal tal que $a_{ii} = 0$ ó 1 para toda $i \in \{1, ..., n\}$. En efecto, si E es una matriz idempotente se tiene que $E^2 - E = 0$, lo que implica que el polinomio $p(x) = x(x-1)$ anula a E. Esto muestra que el polinomio mínimo $m_E(x)$ de E divide a $p(x)$. Se tienen entonces 3 casos $m_E(x) = x$, $m_E(x) = x - 1$ ó $m_E(x) = p(x)$. Si $m_E(x) = x$, se sigue que $E = 0$. Si $m_E(x) = x - 1$, se tiene que $E = 1_A$. Y si $m_E(x) = x(x-1)$, entonces E

es diagonalizable y sus valores propios son 0 y 1, lo que implica que existe una matriz invertible S tal que $S^{-1}ES = D$ es una matriz diagonal cuyas entradas en la diagonal son iguales a 0 ó 1.

Ejemplo 2.8. Sea $A = \mathbb{M}_2(\mathbb{Z})$.

$$1_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

es una descomposición de la unidad.

Ejemplo 2.9. Sea $A = \mathbb{M}_3(\mathbb{Z})$. Si

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ f = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ y } g = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

entonces e y g son idempotentes ortogonales, pero f y g son idempotentes no ortogonales.

Ejemplo 2.10. Dado un carcaj $Q = (Q_0, Q_1, s, t)$ y un campo k. Se construye el álgebra de caminos kQ como se definió en 1.42. Los caminos triviales de kQ son idempotentes. Más aún, dados $i, j \in Q_o$ vértices distintos, los caminos triviales correspondientes e_i y e_j son ortogonales ya que $s(e_i) \neq t(e_j)$. Por lo que si Q tiene un número finito de vértices, $1 = \sum_{i \in Q_0} e_i$ es una descomposición de la unidad de kQ.

Ejemplo 2.11. Dado un campo K y $n \in \mathbb{N}$ se considera el anillo de matrices $\mathbb{M}_n(k)$. Si $E_k = (a_{ij})$ es la matriz cuyas entradas son

$$a_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 0 & \text{si } j = i \neq k \\ 1 & \text{si } j = i = k \end{cases}$$

donde $k \in \{1, ..., n\}$, entonces E_k es un idempotente no central.

Ejemplo 2.12. Sean k un campo, G un grupo y H un subgrupo finito de G. Si $\eta = \sum_{g \in H} g$, entonces

$$\eta^2 = \sum_{g \in H} \sum_{h \in H} gh = \sum_{g \in H} \sum_{t \in H} t = |H|\eta.$$

Por lo tanto, si la característica de k no divide a $|H|$, se sigue que

$$h = \frac{1}{|H|}\eta$$

es un elemento idempotente de kG. Más aún, h es central si y sólo si H es un subgrupo normal de G. En efecto, h es central si y sólo si $xh = hx$ para todo $x \in G$, lo que es equivalente a que

$$\frac{1}{|H|}\sum_{g\in H} xgx^{-1} = x(\frac{1}{|H|}\sum_{g\in H} g)x^{-1} = xhx^{-1} = h = \frac{1}{|H|}\sum_{g\in H} g$$

para todo $x \in G$, lo cual es cierto si y sólo si $xgx^{-1} \in H$ para todo $g \in H$ y $x \in G$, es decir $H \trianglelefteq G$. En particular, tomando G como el grupo dihédrico

$$D_{2n} = \left\langle r, s \mid r^n = s^2 = 1,\, rs = sr^{-1} \right\rangle,$$

se tiene que el elemento $\frac{1}{n}\sum_{i=1}^{n} r^i$ es un idempotente central de kG siempre y cuando n sea distinto de 0 en k.

Las descomposiciones de la unidad son importantes ya que permiten descomponer un módulo como una suma directa finita de grupos abelianos. Dicho procedimiento se expone en la siguiente sección. Pero antes de abordarlo es necesaria una ligera discusión sobre el grupo de morfismos de ciertos módulos.

2.1.2. Idempotentes y grupos de morfismos

Se sabe que dados M y N A-módulos, el conjunto $\mathrm{Hom}_A(M, N)$ es un grupo abeliano. En esta subsección se dan algunas condiciones sobre M y N de manera que $\mathrm{Hom}_A(M, N)$ admita estructura de módulo.

Para cada A-módulo derecho M y cada idempotente $e \in A$, se tiene que los elementos de $\mathrm{Hom}_A(eA, M)$ están determinados de manera única por su imagen en e. En efecto, se tiene que para todo $ea \in eA$ y $f \in \mathrm{Hom}_A(eA, M)$, $f(ea) = f(e)a$, por lo que f está determinado por $f(e)$. Ahora, si $m = f(e)$ se tiene que

$$m = f(e) = f(ee) = f(e)e = me,$$

por lo que $f(e) \in Me$. Esto define una función $\psi : \mathrm{Hom}_A(eA, M) \to Me$ dada por $\psi(f) = f(e)$ que claramente es un morfismo de grupos.

Además, $f(e) = \psi(f) = 0$ si y sólo si $f = 0$, por lo que ψ es inyectiva; y dado $me \in Me$ se tiene que la función definida como $f(ea) = mea$ es un elemento de $\mathrm{Hom}_A(eA, M)$ ya que

$$f(ea + eb) = m(ea + eb) = f(ea) + f(eb),$$

por lo que se tiene un elemento $f \in \mathrm{Hom}_A(eA, M)$ tal que $\psi(f) = me$. Por lo tanto, ψ es un isomorfismo de grupos.

Más aún, considerando la estructura de A-módulo izquierdo de A, se tiene por la Proposición 2.3 que eA es un eAe-módulo izquierdo. De manera que la Proposición 1.10 implica que $\mathrm{Hom}_A(eA, M)$ es un eAe-módulo derecho al igual que Me. De manera que ψ es un isomorfismo de eAe-módulos derechos, ya que

$$\psi(feae) = (feae)(e) = f(eae) = f(e)eae = \psi(f)eae$$

para todo $f \in \mathrm{Hom}_A(eA, M)$ y $eae \in eAe$.

En particular, si se toma $M = eA$, por la discusión anterior se tiene que existe un isomorfismo de módulos $\psi : \mathrm{End}_A(eA) \to eAe$, que además cumple

$$\psi(fg) = fg(e) = f(eg(e)) = f(e)g(e) = \psi(f)\psi(g),$$

$$\psi(1) = 1(e) = e = 1_{eAe}.$$

Por lo que ψ es un morfismo de anillos.

Proposición 2.13. *Sean A un anillo, M un A-módulo derecho y e un idempotente de A. Existe un isomorfismo de eAe-módulos derechos* $\mathrm{Hom}_A(eA, M) \cong Me$, *y un isomorfismo de anillos* $\mathrm{End}_A(eA) \cong eAe$.

En particular, si en el resultado anterior se toma $e = 1$ se obtiene el siguiente corolario.

Corolario 2.14. *Sea A un anillo. Existe un isomorfismo de A-módulos derechos* $\mathrm{Hom}_A(A, M) \cong M$ *y un isomorfismo de anillos* $\mathrm{End}_A(A) \cong A$.

Ahora, si se tiene un A-módulo izquierdo N, entonces de la misma manera se puede definir un morfismo $\phi : \mathrm{Hom}_A(Ae, N) \to eN$ definido como $\phi(f) = f(e)$, que resulta ser un isomorfismo de eAe-módulos izquierdos. Y más aún, se puede probar análogamente que si se toma $N = Ae$, entonces $\phi : \mathrm{End}_A(Ae)^{op} \to eAe$ es un isomorfismo de anillos.

Se tienen entonces los siguientes resultados.

Proposición 2.15. *Sean A un anillo, N un A-módulo izquierdo y e un idempotente de A. Existe un isomorfismo de eAe-módulos izquierdos* $\mathrm{Hom}_A(Ae, N) \cong eN$, *y un isomorfismo de anillos* $\mathrm{End}_A({}_AAe) \cong eAe$. *En particular, tomando $e = 1$ se tiene que existe un isomorfismo de A-módulos izquierdos* $\mathrm{Hom}_A({}_AA, {}_AN) \cong_A N$ *y un isomorfismo de anillos* $\mathrm{End}_A({}_AA) \cong A^{op}$.

Los resultados anteriores se pueden generalizar considerando el grupo de morfismos entre dos módulos de tal manera que uno admita una estructura de bimódulo. La siguiente proposición contiene el estudio de dichos casos.

Teorema 2.16. *Sean A, B y C anillos. Si $e \in A$ y $f \in B$ son elementos idempotentes se cumplen los siguientes enunciados.*

(a) *Si M es un A-C bimódulo y N es un C módulo derecho, entonces existe un isomorfismo* $\mathrm{Hom}_C(eM,N) \cong \mathrm{Hom}_C(M,N)e$ *de B-eAe bimódulos.*

(b) *Si M es un C módulo derecho y N es un B-C bimódulo, entonces existe un isomorfismo* $\mathrm{Hom}_C(M,fN) \cong f\,\mathrm{Hom}_C(M,N)$ *de fBf-A bimódulos.*

(c) *Si M es un A-C bimódulo y N es un B-C bimódulo, entonces existe un isomorfismo* $\mathrm{Hom}_C(eM,fN) \cong f\,\mathrm{Hom}_C(M,N)e$ *de fBf-eAe bimódulos.*

(d) *Si M es un C-A bimódulo y N es un C módulo izquierdo, entonces existe un isomorfismo* $\mathrm{Hom}_C(Me,N) \cong e\,\mathrm{Hom}_C(M,N)$ *de eAe-B bimódulos.*

(e) *Si M es un C-módulo izquierdo y N es un C-B bimódulo, entonces existe un isomorfismo* $\mathrm{Hom}_C(M,Nf) \cong \mathrm{Hom}_C(M,N)f$ *de A-fBf bimódulos.*

(f) *Si M es un C-A bimódulo y N es un C-B bimódulo, entonces existe un isomorfismo* $\mathrm{Hom}_C(Me,Nf) \cong e\,\mathrm{Hom}_C(M,N)f$ *de eAe-fBf bimódulos.*

Demostración. Se probarán los puntos (a), (b) y (c). La prueba de (d), (e) y (f) es análoga.

(a) Si M es un A-C bimódulo y N es un C módulo derecho, entonces por las Proposiciones 1.10 y 2.3 se tiene que $\mathrm{Hom}_C(eM,N)$ y $\mathrm{Hom}_C(M,N)e$ son B-eAe bimódulos. Luego, se considera la función $\phi : \mathrm{Hom}_C(M,N)e \to \mathrm{Hom}_C(eM,N)$ que a cada $he \in \mathrm{Hom}_C(M,N)e$ le asigna la restricción $he|_{eM}$, es decir
$$\phi(he)(x) = he(ex) = h(ex).$$
Se tiene entonces que

- $\phi(he+ge)(x) = h(ex) + g(ex) = \phi(h)(x) + \phi(g)(x)$,
- $\phi(b(he)eae)(x) = (b(he)eae)(ex) = eaeh(ex)b = (eae\phi(h)b)(x)$,
- $\phi(1_B he)(x) = h(ex) = \phi(he)(x)$,
- $\phi(he1_{eAe}) = h(ex) = \phi(he)(x)$.

Por lo tanto, ϕ es un morfismo de bimódulos. Y además $h(ex) = \phi(he)(x) = 0$ para toda $x \in M$ si y sólo si $he = 0$, por lo que ϕ es monomorfismo. Y dado $g \in \mathrm{Hom}_C(eM,N)$ se tiene que $\phi(h) = g$, donde $h(x) = g(xe)$. Por lo que ϕ es un isomorfismo.

(b) Si M es un C-módulo derecho y N es un B-C bimódulo, entonces por las Proposiciones 1.10 y 2.3 se tiene que $\mathrm{Hom}_C(M,fN)$ y $f\,\mathrm{Hom}_C(M,N)$ son fBf-A bimódulos. Luego, notando que para todo $fh \in f\,\mathrm{Hom}_C(M,N)$ el contradominio de fh está contenido en fN, se sigue que la función
$$\phi : f\,\mathrm{Hom}_C(M,N) \to \mathrm{Hom}_C(M,fN)$$

definida como $\phi(fh)(x) = fh(x)$ es un morfismo de bimódulos. Además es claro que ϕ es monomorfismo. Y dado $g \in \mathrm{Hom}_C(M, fN)$ se tiene que $\phi(h) = g$, donde $h(x) = g(x)$. Por lo que ϕ es un isomorfismo.

(c) Se sigue de los incisos anteriores.

□

2.2. La descomposición de Peirce

En esta sección se prueba que cada descomposición de la unidad del anillo induce una descomposición del anillo como suma directa de ideales derechos y como suma directa de ideales izquierdos, y recíprocamente si el anillo se descompone como una suma directa de ideales, entonces dicha descomposición induce una descomposición de la unidad. Dichas descomposiciones se les llamarán descomposiciones de Peirce, las cuales jugarán un papel importante en los siguientes capítulos.

2.2.1. Descomposición de Peirce de un anillo

Un primer paso para llegar a las descomposiciones de un anillo es considerar las descomposiciones de un módulo. Esta sección expone la relación entre las descomposiciones de un módulo y las descomposiciones de la unidad del anillo de endomorfismos del módulo.

Sea M un A-módulo derecho que se descompone como suma directa finita de submódulos $M = M_1 \oplus ... \oplus M_n$. Cada $m \in M$ se expresa de manera única como una suma $m = \sum m_i$, con $m_i \in M_i$. Considérense las proyecciones e inclusiones naturales $\pi_i : M \to M_i$ y $\eta_i : M_i \to M$ respectivamente; entonces $\rho_i = \eta_i \pi_i \in \mathrm{End}_A(M)$ para toda $i \in \{1, ..., n\}$.

Para cada $i \in \{1, ..., n\}$ se tiene que $\rho_i(m) = m_i$, donde $m = \sum m_i$ es un elemento arbitrario de M. Así, para toda pareja $i, j \in \{1, ..., n\}$ con $i \neq j$ se tiene que

$$\rho_i \rho_j(m) = \rho_i(m_j) = 0 = \rho_j(m_i) = \rho_j \rho_i(m),$$

$$\rho_i^2(m) = \rho_i(\rho_i(m)) = \rho_i(m_i) = m_i = \rho_i(m) \text{ y}$$

$$m = m_1 + ... + m_n = \rho_1(m) + ... + \rho_n(m)$$

para toda $m \in M$, por lo que $\rho_i^2 = \rho_i$, $\rho_i \rho_j = 0$ y $1_M = \rho_1 + ... + \rho_n$.

Se ha probado entonces que una descomposición de un módulo M como suma directa finita de submódulos induce una descomposición de la unidad de su anillo de endomorfismos. Recíprocamente, si existe una descomposición $1 = e_1 + ... + e_n$, donde 1 es la unidad de $\mathrm{End}_A(M)$, se tiene que

$$M = 1M = (e_1 + ... + e_n)M = M_1 + ... + M_n$$

donde $M_i = \mathrm{Im}(e_i)$. Y si $x \in M_i \cap \sum_{j\neq i} M_j$, entonces $x = e_i(m) = \sum_{j\neq i} e_j(m_j)$, por lo que

$$x = e_i(m) = e_i^2(m) = e_i \sum_{j\neq i} e_j(m_j) = \sum_{j\neq i} e_i e_j(m_j) = 0.$$

Por lo tanto, se ha obtenido una descomposición $M = M_1 \oplus ... \oplus M_n$.

Se ha probado el siguiente resultado.

Proposición 2.17. *Sea A un anillo. Dado M un A-módulo derecho, existe una biyección entre las descomposiciones de M como suma directa finita de submódulos y las descomposiciones de la unidad de* $\mathrm{End}_A(M)$.

Observación 2.18. Nótese que la discusión anterior también es válida para módulos izquierdos.

Ahora, sean M un A-módulo y $B = \mathrm{End}_A(M)$. Debido a que B es un subanillo de $\mathrm{End}(M)$, existe una inclusión de anillos $\phi : B \to \mathrm{End}(M)$, lo que implica que M es un B-módulo izquierdo por el lema 1.3.

A continuación se busca aprovechar el resultado anterior para encontrar una descomposición de la unidad de $\mathrm{End}_B({}_BM)$ que induzca una descomposición útil de M como B-módulo izquierdo. Para ello, se observa que si a es un elemento de A, entonces la función $f_a : M \to M$ definida como $f(m) = ma$ es un endomorfismo de grupos abelianos, y más aún, es un morfismo de B-módulos izquierdos. En efecto, si $g \in B$ y $m \in M$

$$f_a(gm) = g(m)a = g(ma) = g(f_a(m)),$$

por lo que $f_a \in \mathrm{End}_B(M)$ para todo $a \in A$. Además, dados $a, b \in A$ se tiene que $f_b + f_a = f_{a+b}$ y $f_b f_a = f_{ab}$. Por lo que si a es idempotente, f_a también lo es, y si a y b son idempotentes ortogonales, entonces f_a y f_b también lo son.

En consecuencia, una descomposición de la unidad $1_A = e_1 + e_2 + ... + e_s$ induce una descomposición $1_M = f_1 = f_{e_1} + ... + f_{e_s}$ de la unidad de $\mathrm{End}_B(M)$, lo que induce a su vez una descomposición de M como suma directa de B-submódulos izquierdos

$${}_BM = f_{e_1}M \oplus ... \oplus f_{e_s}M = Me_1 \oplus Me_2 \oplus ... \oplus Me_s.$$

Esta descomposición recibe el nombre de descomposición de Peirce por la derecha de M.

Análogamente, si M es un A-módulo izquierdo, entonces es un módulo izquierdo sobre $C = \mathrm{End}_A({}_AM)$ y se le puede descomponer como

$${}_CM = e_1M \oplus ... \oplus e_sM.$$

Proposición 2.19. *Sea A un anillo y $1_A = e_1 + ... + e_n$ una descomposición de la unidad.*

- *Todo módulo derecho M se descompone como suma directa de grupos abelianos $M = Me_1 \oplus ... \oplus Me_n$ y cada grupo Me_i es un módulo izquierdo sobre* $\mathrm{End}_A(M)$.
- *Todo módulo izquierdo M se descompone como suma directa de grupos abelianos $M = e_1M \oplus ... \oplus e_nM$ y cada grupo e_iM es un módulo derecho sobre* $\mathrm{End}_A(M)^{op}$.

Ahora, si se consideran A_A y ${}_AA$, los A-módulos regulares derecho e izquierdo del anillo, de la Proposición 2.19 se obtienen las siguientes descomposiciones.

Definición 2.20. Sea A un anillo con una descomposición de la unidad $1 = e_1 + ... + e_n$.

- La descomposición $A = e_1A \oplus ... \oplus e_nA$ recibe el nombre de descomposición de Peirce a la izquierda.
- La descomposición $A = Ae_1 \oplus ... \oplus Ae_n$recibe el nombre de descomposición de Peirce a la derecha.

Por lo tanto, una descomposición de la unidad del anillo induce una descomposición de éste como suma directa finita de ideales derechos y también como una suma directa finita de ideales izquierdos.

Recíprocamente, cada descomposición del anillo como suma directa finita de ideales derechos ó izquierdos induce una descomposición de la unidad. Más aún, siempre que se tenga una descomposición $A_A = \bigoplus_{i \in X} J_i$ con $J_i \neq 0$ para toda $i \in X$, se tiene que X es finito y esta descomposición induce una descomposición de la unidad $1 = \sum_{i \in X} e_i$ tal que $J_i = e_iA$ para toda $i \in X$.

En efecto, $1 \in A$ por lo que existe una expresión única $1 = \sum_{i \in Y} \alpha_i$ con $Y \subseteq X$ finito y $\alpha_i \in J_i \backslash \{0\}$ para toda $i \in Y$. Y para toda $j \in Y$ se tiene que

$$\alpha_j = (\sum_{i \in Y} \alpha_i)\alpha_j = \sum_{i \in Y} \alpha_i \alpha_j,$$

lo que implica que $\alpha_j^2 = \alpha_j$ para toda $j \in Y$ y $\alpha_i \alpha_j = 0$ para toda $i \neq j$ en Y. Por lo tanto, $1 = \sum_{i \in Y} \alpha_i$ es una descomposición de la unidad. Luego, si se supone que $X \backslash Y$ no es vacío, existe $x \in J_k$ para algún $k \in X \backslash Y$; pero en tal caso

$$x = (\sum_{i \in Y} \alpha_i)x = \sum_{i \in Y} \alpha_i x = 0$$

ya que $\alpha_i x \in J_i$, lo que implica que $J_k = 0$ lo cual es una contradicción. Por lo tanto $X = Y$.

Por último si $x \in J_i$, entonces $x = \sum_{i \in X} \alpha_i x$, por lo que $x = \alpha_i x$ ya que $\alpha_j x \in J_j$. Lo que implica que $J_i = \alpha_i A$ para toda $i \in X$.

Se tiene entonces el siguiente resultado.

Proposición 2.21. *Sea A un anillo. Si $A_A = \bigoplus_{i \in X} J_i$, entonces X es finito y la expresión única $1_A = \sum e_i$ con $e_i \in J_i$ es una descomposición de la unidad tal que $J_i = e_i A$.*

Es sencillo entonces deducir lo siguiente.

Proposición 2.22. *Sea A un anillo. Existe una biyección entre*

(a) *las descomposiciones de la unidad de A,*

(b) *las descomposiciones de la unidad de* $\mathrm{End}_A(A)$,

(c) *las descomposiciones de A como suma directa de ideales derechos y*

(d) *las descomposiciones de A como suma directa de ideales izquierdos.*

Demostración. Notando que una descomposición de la unidad de A es una descomposición de la unidad de A^{op} se tiene por las Proposiciones 2.21 y 2.17 que las descomposiciones de A como suma directa de ideales derechos ó izquierdos están en correspondencia biyectiva con las descomposiciones de la unidad de $\mathrm{End}_A(A)$. A su vez, las descomposiciones de la unidad de $\mathrm{End}_A(A)$ están en correspondencia biyectiva con las descomposiciones de la unidad de A por la Proposición 2.14. □

Ahora, dada una descomposición de la unidad $1_A = e_1 + ... + e_n$, cada sumando $e_i A$ de la descomposición de Peirce a la derecha inducida es un A-módulo derecho, por lo que la descomposición de la unidad induce una descomposición de grupos abelianos por la Proposición 2.19.

$$e_i A = e_i A e_1 \oplus ... \oplus e_i A e_n$$

Procediendo de la misma manera con cada sumando de la descomposición de Peirce a la derecha, se llega a que una descomposición de la unidad $1 = e_1 + ... + e_n$ de A induce una descomposición de grupos abelianos

$$A = \bigoplus_{i=1}^{n} (\bigoplus_{j=1}^{n} e_i A e_j) = \bigoplus_{i,j=1}^{n} e_i A e_j.$$

Dicha expresión es conocida como la descomposición de Peirce del anillo ó descomposición de Peirce bilateral.

Teorema 2.23. *Si existe una descomposición de la unidad $1 = e_1 + ... + e_s$ de un anillo A, entonces el anillo se descompone como la suma directa de grupos abelianos $A = \bigoplus_{i,j=1}^{n} e_i A e_j$.*

Observación 2.24. Cada sumando $e_i A e_j$ admite estructura de $e_i A e_i$-$e_j A e_j$ bimódulo. En efecto, por la Proposición 2.3 $e_i A e_j$ es un grupo abeliano que admite estructura de e_iAe_i-módulo derecho y e_jAe_j-módulo izquierdo, y dados $x \in e_iAe_j$, $y \in e_iAe_i$ y $z \in e_jAe_j$ se tiene que $x(yz) = (xy)z$, por lo que e_iAe_j es un bimódulo.

Además, claramente se cumple que $(e_iAe_j)(e_jAe_k) \subseteq e_iAe_k$ para todo $i, j, k \in \{1, ..., n\}$, y $(e_iAe_j)(e_kAe_l) = 0$ para todo $j \neq k$ y $j, i, k, l \in \{1, ..., n\}$.

Las descomposiciones de Peirce son útiles para estudiar la estructura de un anillo de forma separada. Para ello se pueden relacionar los ideales del anillo eAe con los de A de la siguiente manera.

En general un ideal derecho I de eAe no es un ideal derecho de A. Pero se puede considerar el ideal

$$IA = \{\sum_{i=1}^{m} n_i a_i \mid m \in \mathbb{N},\, n_i \in I,\, a_i \in A\}.$$

Cabe notar que

$$IA = I(eAe \oplus C) = IeAe \oplus IC = I \oplus IC,$$

donde $C = eA(1-e) \oplus (1-e)Ae \oplus (1-e)A(1-e)$.

Enconsecuencia, si se tienen dos ideales derechos I y J de eAe tales que $IA = JA$, esto es $J \oplus JC = I \oplus IC$, pero $I, J \subseteq eAe$ e $IC, JC \subseteq C$, entonces como $A = eAe \oplus C$ se tiene que $I = J$ e $IC = JC$.

Proposición 2.25. *Dado A un anillo con un idempotente e, si I y J son ideales de eAe tales que $IA = JA$, entonces $I = J$.*

2.2.2. Representación matricial de un anillo

Dado un anillo A, si se tiene una descomposición de la unidad $1_A = e_1 + ... + e_n$, la descomposición de Peirce inducida permite una interpretación de A en forma matricial.

Sean a y b elementos de A. Utilizando la descomposición de Peirce se tiene que

$$a = \sum_{i,j=1}^{n} a_{ij} \text{ y } b = \sum_{i,j=1}^{n} b_{ij},$$

donde $a_{ij} = e_iae_j$ y $b_{ij} = e_ibe_j$ para toda $i, j \in \{1, ..., n\}$. Por lo que

$$a + b = \sum_{i,j=1}^{n} a_{ij} + b_{ij} \text{ y } ab = \sum_{i,j=1}^{n} \sum_{k,t=1}^{n} a_{ik}b_{tj} = \sum_{i,j=1}^{n} \sum_{k=1}^{n} a_{ik}b_{kj},$$

ya que si $k \neq t$, entonces $a_{ik}b_{tj} = e_iae_ke_tbe_j = 0$.

Por lo tanto, si se considera el conjunto

$$X = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & \ddots & \\ a_{n1} & \dots & & a_{nn} \end{pmatrix} \mid a_{ij} \in e_i A e_j \right\},$$

y se definen las operaciones

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \\ a_{n1} & & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \\ b_{n1} & & b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \vdots & \ddots & \\ a_{n1}+b_{n1} & & a_{nn}+b_{nn} \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \\ a_{n1} & & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \\ b_{n1} & & b_{nn} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n a_{1i}b_{i1} & \dots & \sum_{i=1}^n a_{1i}b_{in} \\ \vdots & \ddots & \\ \sum_{i=1}^n a_{ni}b_{i1} & & \sum_{i=1}^n a_{ni}b_{in} \end{pmatrix},$$

es sencillo probar no sólo que X es un anillo, sino que X y A son isomorfos mediante el morfismo $\phi : A \to X$ definido como

$$\phi(a) = \begin{pmatrix} e_1ae_1 & \dots & e_1ae_n \\ \vdots & \ddots & \\ e_nae_1 & & e_nae_n \end{pmatrix}.$$

Por esto en general A se identifica con el anillo X, y se suele escribir

$$A = X = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & & \vdots \\ \vdots & & \ddots & \\ A_{n1} & \dots & & A_{nn} \end{pmatrix}.$$

Este procedimiento es especialmente útil cuando se considera el anillo de endomorfismos de un módulo M cuando éste se descompone como suma directa finita de submódulos $M = M_1 \oplus ... \oplus M_n$. En tal caso por la Proposición 2.17 la descomposición de M induce una descomposición de la unidad $1_M = \rho_1 + ... + \rho_n$, con la cual

$$\mathrm{End}_A(M) = \begin{pmatrix} B_{11} & B_{12} & \dots & B_{1n} \\ B_{21} & B_{22} & & \vdots \\ \vdots & & \ddots & \\ B_{n1} & \dots & & B_{nn} \end{pmatrix},$$

donde $B = \operatorname{End}_A(M)$ y $B_{ij} = \rho_i B \rho_j$.

Ahora, recordando la Proposición 2.16, se tiene que

$$\rho_i B \rho_j = \rho_i \operatorname{End}_A(M)\rho_j \cong \operatorname{Hom}_A(\rho_j M, \rho_i M) \cong \operatorname{Hom}_A(M_j, M_i).$$

Por lo tanto, si

$$C = \begin{pmatrix} C_{11} & \dots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \dots & C_{nn} \end{pmatrix}$$

donde $C_{ij} = \operatorname{Hom}_A(M_j, M_i)$, entonces $f_{ij} f_{jk} \in \operatorname{Hom}_A(M_k, M_i)$ para todo $f_{ij} \in C_{ij}$ y $f_{jk} \in C_{jk}$, por lo que las operaciones

$$\begin{pmatrix} f_{11} & \dots & f_{1n} \\ \vdots & \ddots & \\ f_{n1} & & f_{nn} \end{pmatrix} + \begin{pmatrix} g_{11} & \dots & g_{1n} \\ \vdots & \ddots & \\ g_{n1} & & g_{nn} \end{pmatrix} = \begin{pmatrix} f_{11}+g_{11} & \dots & f_{1n}+g_{1n} \\ \vdots & \ddots & \\ f_{n1}+g_{n1} & & f_{nn}+g_{nn} \end{pmatrix},$$

$$\begin{pmatrix} f_{11} & \dots & f_{1n} \\ \vdots & \ddots & \\ f_{n1} & & f_{nn} \end{pmatrix} \begin{pmatrix} g_{11} & \dots & g_{1n} \\ \vdots & \ddots & \\ g_{n1} & & g_{nn} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n f_{1i}g_{i1} & \dots & \sum_{i=1}^n f_{1i}g_{in} \\ \vdots & \ddots & \\ \sum_{i=1}^n f_{ni}g_{i1} & & \sum_{i=1}^n f_{ni}g_{in} \end{pmatrix},$$

están bien definidas. Es entonces sencillo demostrar que con estas operaciones C es un anillo, y además que C es isomorfo a B. Por lo que en general $\operatorname{End}_A(M)$ se identifica con el anillo

$$\begin{pmatrix} \operatorname{End}_A(M_1) & \dots & \operatorname{Hom}_A(M_n, M_1) \\ \vdots & \ddots & \vdots \\ \operatorname{Hom}_A(M_1, M_n) & \dots & \operatorname{End}_A(M_n) \end{pmatrix}.$$

Se puede generalizar aún más esta idea para expresar como matrices los morfismos entre dos módulos que se descomponen como suma directa finita de submódulos.

En efecto, considérense dos módulos M y N. Es sencillo probar que $W = \operatorname{Hom}_A(N, M)$ es un $\operatorname{End}_A(M)$-$\operatorname{End}_A(N)$ bimódulo. Por lo que si

$$M = M_1 \oplus ... \oplus M_n \ \text{ y } \ N = N_1 \oplus ... \oplus N_m,$$

se tienen descomposiciones de la unidad

$$1_{\operatorname{End}_A(M)} = \rho_1 + ... + \rho_n \text{ y } 1_{\operatorname{End}_A(N)} = \tau_1 + ... + \tau_m,$$

con las que, tras hacer la descomposición de Peirce a la derecha a los sumandos de la descomposición de Peirce a la izquierda de W se obtiene la descomposición

$$\mathrm{Hom}_A(N,M)=\bigoplus_{i,j=1}^{n,m}\rho_i\,\mathrm{Hom}_A(N,M)\tau_j\cong\bigoplus_{i,j=1}^{n,m}\mathrm{Hom}_A(N_j,M_i).$$

Ya con esta última expresión se tiene que $\mathrm{Hom}_A(N,M)$ es claramente isomorfo al grupo de matrices cuyas entradas son los elementos de $\mathrm{Hom}_A(N_j,M_i)$. Explícitamente, si

$$L=\begin{pmatrix}\mathrm{Hom}_A(N_1,M_1) & \dots & \mathrm{Hom}_A(N_m,M_1)\\ \vdots & \ddots & \vdots\\ \mathrm{Hom}_A(N_1,M_n) & \dots & \mathrm{Hom}_A(N_m,M_n)\end{pmatrix},$$

existe un isomorfismo $\chi_{(N,M)}:\mathrm{Hom}_A(N,M)\to L$ definido como

$$\chi_{(N,M)}(f)=\begin{pmatrix}\pi_1 f\eta'_1 & \dots & \pi_1 f\eta'_m\\ \vdots & \ddots & \vdots\\ \pi_n f\eta'_1 & \dots & \pi_n f\eta'_m\end{pmatrix},$$

donde $\pi_i:M\to M_i$ y $\pi'_j:N\to N_j$ son las proyecciones canónicas y $\eta_i:M_i\to M$ y $\eta'_j:N_j\to N$ las inclusiones canónicas. La relevancia de este isomorfismo es que se pueden identificar los morfismos entre módulos como matrices, y como tales no solo se pueden sumar, sino además se pueden componer utilizando el producto usual de matrices.

En efecto, supónganse M y N con las descomposiciones anteriores y $H=H_1\oplus\ldots\oplus H_t$, y considérense $f\in\mathrm{Hom}_A(N,M)$ y $g\in\mathrm{Hom}_A(M,H)$, entonces

$$f=\begin{pmatrix}f_{11} & \dots & f_{m1}\\ \vdots & \ddots & \vdots\\ f_{1n} & \dots & f_{mn}\end{pmatrix},\quad g=\begin{pmatrix}g_{11} & \dots & g_{n1}\\ \vdots & \ddots & \vdots\\ g_{1t} & \dots & g_{nt}\end{pmatrix}$$

con $\pi_j f\eta'_i=f_{ij}\in\mathrm{Hom}_A(N_i,M_j)$ y $\pi''_s g\eta_k=g_{ks}\in\mathrm{Hom}_A(M_k,H_s)$ donde $\pi''_s:H\to H_s$ es la proyección canónica. Operando como matrices se tiene que

$$\begin{pmatrix}f_{11} & \dots & f_{m1}\\ \vdots & \ddots & \\ f_{1n} & \dots & f_{mn}\end{pmatrix}\begin{pmatrix}g_{11} & \dots & g_{n1}\\ \vdots & \ddots & \\ g_{1t} & \dots & g_{nt}\end{pmatrix}=\begin{pmatrix}\sum_{i=1}^n g_{i1}f_{1i} & \dots & \sum_{i=1}^n g_{i1}f_{mi}\\ \vdots & \ddots & \\ \sum_{i=1}^n g_{it}f_{1i} & \dots & \sum_{i=1}^n g_{it}f_{mi}\end{pmatrix}.$$

mientras que operando normalmente se tiene que

$$gf=(\sum_{k,s=1}^{n,t}\pi''_s g\eta_k)(\sum_{i,j=1}^{m,n}\pi_j f\eta'_i)=\sum_{s=1}^{t}\sum_{k=1}^{n}\sum_{i=1}^{m}\pi''_s g\eta_k\pi_k f\eta'_i=\sum_{k=1}^{n}\sum_{s=1}^{t}\sum_{i=1}^{m}g_{ks}f_{ik},$$

por lo tanto se tiene que $\chi_{(N,H)}(gf) = \chi_{(M,H)}(g)\chi_{(N,M)}(f)$.

De la discusión anterior se tiene el siguiente resultado.

Proposición 2.26. *Dados módulos que se descomponen como suma directa finita de submódulos, los morfismos entre éstos se pueden expresar, sumar y componer como matrices cuyas entradas son morfismos entre los sumandos de dichos módulos. En particular, si $M = M_1 \oplus ... \oplus M_n$, entonces existe un isomorfismo de anillos*

$$\mathrm{End}_A(M) \cong \begin{pmatrix} \mathrm{End}_A(M_1) & \mathrm{Hom}_A(M_2, M_1) & \dots & \mathrm{Hom}_A(M_n, M_1) \\ \mathrm{Hom}_A(M_1, M_2) & \mathrm{End}_A(M_2) & & \\ \vdots & & \ddots & \\ \mathrm{Hom}_A(M_1, M_n) & & & \mathrm{End}_A(M_n) \end{pmatrix}.$$

Gracias a lo discutido en esta subsección, de ahora en adelante se identificarán los morfismos entre dos módulos como matrices siempre que sea de utilidad dicha expresión.

Por último hace falta ver si es posible evaluar un morfismo como matriz. Si M y N se descomponen como en la discusión anterior, entonces todo $m \in M$ se expresa de manera única como

$$m = \sum_{i=1}^{n} m_i,$$

y para todo $f \in \mathrm{Hom}_A(M, N)$ se tiene que

$$f(m) = \sum_{ij=1}^{n} \rho_i f \rho_j(m) = \sum_{ij=1}^{n} \rho_i f \rho_j(m_j).$$

Ahora, identificando los elementos de M con los vectores de la forma

$$m = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix},$$

se tiene que

$$f(m) = \begin{pmatrix} f_{11} & \dots & f_{n1} \\ \vdots & \ddots & \\ f_{1m} & & f_{nm} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \sum f_{i1} m_i \\ \vdots \\ \sum f_{in} m_i \end{pmatrix}.$$

De esta manera a cada morfismo se le puede asociar una matriz y operarlo como una.

Corolario 2.27. *Si $N = M^{(n)}$, entonces* $\mathrm{End}_A(N) \cong \mathbb{M}_n(\mathrm{End}_A(M))$.

Corolario 2.28. *Dado un anillo A.* $\mathrm{End}_A(A^{(m)}) \cong \mathbb{M}_m(A)$.

2.2.3. Anillos de matrices generalizadas

En la subsección anterior se mostró cómo la descomposición de Peirce induce una representación matricial de un anillo. Dicha representación se sigue del hecho de que si se tiene una descomposición de la unidad $1 = e_1 + ... + e_n$, entonces se descompone al anillo como suma de grupos abelianos $A = \bigoplus_{i,j=1}^n M_{ij}$, donde $M_{ij} = e_iAe_j$, y tales que con el producto del anillo admiten estructura de bimódulos, que además satisfacen $M_{ij}M_{jk} \subseteq M_{ik}$ y $M_{ij}M_{kl} = 0$ si $j \neq k$ para todo $i, j, k, l \in \{1, ..., n\}$.

Esta última propiedad permite definir una función e_jAe_j-balanceada

$$\psi_{ik}^j : M_{ij} \times M_{jk} \to M_{ik}$$

como $\psi_{ik}^j(m, n) = mn$, y por la propiedad universal del producto tensorial ψ_{ik}^j induce un morfismo de grupos $\varphi_{ik}^j : M_{ij} \otimes M_{jk} \to M_{ik}$ para toda i, j y k tal que $\varphi_{ik}^j(m \otimes n) = mn$. Por lo que si se tienen $x, y \in A$, su producto es igual a

$$xy = (\sum_{k,t=1}^n x_{kt})(\sum_{i,j=1}^n y_{ij}) = \sum_{k,t=1}^n (\sum_{i,j=1}^n x_{kt}y_{ij}) = \sum_{k,t=1}^n (\sum_{j=1}^n x_{kt}y_{tj}) = \sum_{k,t=1}^n \sum_{j=1}^n \varphi_{kj}^t(x_{kt} \otimes y_{tj}),$$

donde $x_{kt} = e_kxe_t$ y $y_{ij} = e_iye_j$. Luego, como el producto de A es asociativo, para cualesquiera $i, j, k, t \in \{1, ..., n\}$, dados $x \in M_{ij}$, $y \in M_{jk}$ y $z \in M_{kt}$ se tiene que

$$\varphi_{it}^j(1 \otimes \varphi_{jt}^k)(x \otimes y \otimes z) = \varphi_{it}^j(x \otimes (\varphi_{jt}^k(y \otimes z))) = x(\varphi_{jt}^k(y \otimes z)) = x(yz) = (xy)z \text{ y}$$

$$x(yz) = (xy)z = (\varphi_{ik}^j(x \otimes y))z = \varphi_{it}^k((\varphi_{ik}^j(x \otimes y)) \otimes z) = \varphi_{it}^k(\varphi_{ik}^j \otimes 1)(x \otimes y \otimes z),$$

esto es $\varphi_{it}^j(1 \otimes \varphi_{jt}^k) = \varphi_{it}^k(\varphi_{ik}^j \otimes 1)$.

Resumiendo, si A es un anillo con una descomposición de la unidad $1 = e_1 + ... + e_n$, entonces existe una descomposición de grupos abelianos $A = \bigoplus_{i,j=1}^n M_{ij}$, tal que M_{ii} es anillo para toda $i \in \{1, ..., n\}$ y M_{ij} es un M_{ii}-M_{jj} bimódulo para cualesquiera $i, j \in \{1, ..., n\}$, junto con una familia de morfismos $\{\varphi_{ik}^j : M_{ij} \otimes M_{jk} \to M_{ik}\}_{i,j,k=1}^n$ que cumple $\varphi_{it}^j(1 \otimes \varphi_{jt}^k) = \varphi_{it}^k(\varphi_{ik}^j \otimes 1)$ para cualesquiera $i, j, k, t \in \{1, ..., n\}$.

Recíprocamente, si A es un grupo abeliano con una descomposición

$$A = \bigoplus_{i,j=1}^n M_{ij}$$

donde $M_{ii} = A_i$ es anillo para toda $i \in \{1, ..., n\}$ y M_{ij} es un A_i-A_j bimódulo para cualesquiera $i, j \in \{1, ..., n\}$, junto con una familia de morfismos

$$X = \{\varphi_{ik}^j : M_{ij} \otimes_{A_j} M_{jk} \to M_{ik} \mid i, j, k \in \{1, ..., n\}\}$$

tal que $\varphi^k_{it}(\varphi^j_{ik}\otimes 1)=\varphi^j_{it}(1\otimes\varphi^k_{jt})$ para todo $i.j.k,t\in\{1,...,n\}$, es decir que conmuta el siguiente diagrama,

$$\begin{tikzcd} M_{ij}\otimes M_{jk}\otimes M_{kt} \arrow[r, "1\otimes\varphi^k_{jt}"] \arrow[d, "\varphi^j_{ik}\otimes 1"'] \arrow[dr, phantom, "\circlearrowleft"] & M_{ij}\otimes M_{jt} \arrow[d, "\varphi^j_{it}"] \\ M_{ik}\otimes M_{kt} \arrow[r, "\varphi^k_{it}"'] & M_{it} \end{tikzcd}$$

entonces A es un anillo con el producto definido como

$$[x_{ij}][y_{ij}]=\sum_{i,j=1}^{n}\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes y_{kj})=[\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes y_{kj})]$$

para todo $[x_{ij}],[y_{ij}]\in A$, donde $[x_{ij}]$ denota un elemento arbitrario $\sum_{i,j=1}^{n}x_{ij}\in A$ con $x_{ij}\in M_{ij}$ para toda pareja (i,j).

En efecto, el producto es distributivo pues dados $[x_{ij}],[y_{ij}],[z_{ij}]\in A$ arbitrarios se tiene que

$$\begin{aligned}[x_{ij}]([y_{ij}]+[z_{ij}])=[x_{ij}][y_{ij}+z_{ij}] &= [\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes(y_{kj}+z_{kj}))]\\ &= [\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes y_{kj})+\varphi^k_{ij}(x_{ik}\otimes z_{kj})]\\ &= [\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes y_{kj})]+[\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes z_{kj})]\\ &= [x_{ij}][y_{ij}]+[x_{ij}][z_{ij}],\end{aligned}$$

y análogamente

$$\begin{aligned}([x_{ij}]+[y_{ij}])[z_{ij}]=[x_{ij}+y_{ij}][z_{ij}] &= [\sum_{k=1}^{n}\varphi^k_{ij}((x_{ik}+y_{ik})\otimes z_{kj})]\\ &= [\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes z_{kj})+\varphi^k_{ij}(y_{ik}\otimes z_{kj})]\\ &= [\sum_{k=1}^{n}\varphi^k_{ij}(x_{ik}\otimes z_{kj})]+[\sum_{k=1}^{n}\varphi^k_{ij}(y_{ik}\otimes z_{kj})]\\ &= [x_{ij}][z_{ij}]+[y_{ij}][z_{ij}].\end{aligned}$$

De la misma manera el producto es asociativo pues dados $[x_{ij}],[y_{ij}],[z_{ij}]\in A$ arbitrarios utilizando la distributividad y la propiedad de los morfismos de X se tiene que

$$\begin{aligned}
[x_{ij}]([y_{ij}][z_{ij}]) = [x_{ij}][\sum_{k=1}^{n} \varphi_{ij}^{k}(y_{ik} \otimes z_{kj})] &= [x_{ij}] \sum_{k=1}^{n} [\varphi_{ij}^{k}(y_{ik} \otimes z_{kj})] \\
&= \sum_{k=1}^{n} [x_{ij}][\varphi_{ij}^{k}(y_{ik} \otimes z_{kj})] \\
&= \sum_{k=1}^{n} [\sum_{t=1}^{n} \varphi_{ij}^{t}(x_{it} \otimes \varphi_{tj}^{k}(y_{tk} \otimes z_{kj}))] \\
&= \sum_{k=1}^{n} [\sum_{t=1}^{n} \varphi_{ij}^{k}(\varphi_{ik}^{t}(x_{it} \otimes y_{tk}) \otimes z_{kj})] \\
&= ([x_{ij}][y_{ij}])[z_{ij}].
\end{aligned}$$

Finalmente, $1_{A_1} + ... + 1_{A_n} = \mathbf{1}$ claramente es la unidad del anillo pues dado $[x_{ij}] \in A$ se tiene que

$$\mathbf{1}[x_{ij}] = [\varphi_{ij}^{i}(1_{A_i} \otimes x_{ij})] = [x_{ij}] = [\varphi_{ij}^{j}(x_{ij} \otimes 1_{A_j})] = [x_{ij}]\mathbf{1}.$$

Por lo tanto, A es un anillo, y por como está definido el producto es sencillo probar que $M_{ij}M_{kt} = 0$ si $j \neq k$ y $M_{ij}M_{jk} \subseteq M_{ik}$. Se tiene entonces el siguiente teorema.

Teorema 2.29. *Un grupo abeliano $A = \bigoplus_{i,j=1}^{n} M_{ij}$ admite estructura de anillo en la cual*

$$M_{ij}M_{kt} \subseteq \begin{cases} M_{it} & si\ j = k \\ 0 & si\ j \neq k \end{cases}$$

para toda $i, j, k, t \in \{1, ..., n\}$ si, y sólo si, para toda terna $i, j, k \in \{1, ..., n\}$ existen morfismos $\varphi_{ik}^{j} : M_{ij} \otimes M_{jk} \to M_{ik}$ tales que $\varphi_{it}^{k}(\varphi_{ik}^{j} \otimes 1) = \varphi_{it}^{j}(1 \otimes \varphi_{jt}^{k})$ y que satisfacen para cada $[x_{ij}], [y_{ij}] \in A$, que el producto es igual a

$$[x_{ij}][y_{ij}] = [\sum_{k=1}^{n} \varphi_{ij}^{k}(x_{ik} \otimes y_{kj})]_{i,j=1}^{n}.$$

A un anillo que cumpla con lo anterior se le llama *anillo generalizado de matrices*, y recibe ese nombre porque se puede expresar como una matriz de n renglones y n columnas, cuyas entradas del i-ésimo renglón y j-ésima columna son elementos de M_{ij}.

Ejemplo 2.30. Dado un grupo abeliano $A = \bigoplus_{i,j=1}^{n} M_{ij}$, donde $(M_{ij})_{i,j=1}^{n}$ es una familia de subgrupos, tales que M_{ii} es un anillo A_i y M_{ij} es un A_i-A_j bimódulo. Defínanse $\varphi_{ks}^{k} : A_k \otimes M_{ks} \to M_{ks}$ y $\varphi_{sk}^{k} : M_{sk} \otimes A_k \to M_{sk}$ como el isomorfismo natural y $\varphi_{ij}^{k} : M_{ik} \otimes M_{kj} \to M_{ij}$ como el morfismo 0 si $k \neq i$ y $k \neq j$ para toda cuaterna $k, s, i, j \in \{1, ..., n\}$. De manera que para cualesquiera $i, k, s, t \in \{1, ..., n\}$ se tiene que $\varphi_{it}^{s}(\varphi_{is}^{k} \otimes 1) = \varphi_{it}^{k}(1 \otimes \varphi_{kt}^{s})$ ya que *(a)* Si $s \neq t$, entonces $1 \otimes \varphi^s_{kt} = 0$ y $\varphi^s_{it} = 0$ lo que implica que

$$\varphi^s_{it}(\varphi^k_{is} \otimes 1) = 0 = \varphi^k_{it}(1 \otimes \varphi^s_{kt}).$$

(b) Si $s \neq k$, entonces $1 \otimes \varphi^s_{kt} = 0$ y $\varphi^k_{is} \otimes 1 = 0$ lo que implica que

$$\varphi^s_{it}(\varphi^k_{is} \otimes 1) = 0 = \varphi^k_{it}(1 \otimes \varphi^s_{kt}).$$

(c) Si $i \neq k$, entonces $\varphi^k_{it} = 0$ y $\varphi^k_{is} \otimes 1 = 0$ lo que implica que

$$\varphi^s_{it}(\varphi^k_{is} \otimes 1) = 0 = \varphi^k_{it}(1 \otimes \varphi^s_{kt}).$$

(d) Si $i = k = s = t$, $\varphi^s_{it}(\varphi^k_{is} \otimes 1) = \varphi^i_{ii}(\varphi^i_{ii} \otimes 1) = \varphi^i_{ii}(1 \otimes \varphi^i_{ii}) = \varphi^k_{it}(1 \otimes \varphi^s_{kt})$.

Por lo tanto, por el teorema 2.29 los morfismos φ^k_{ij} inducen un producto con el cual A es un anillo. A dicho producto se le llamará *producto trivial de matriz generalizada*, con el cual los siguientes grupos son anillos.

$$\begin{pmatrix} k & 0 \\ k^n & k \end{pmatrix} \quad \begin{pmatrix} k & k[x] \\ 0 & k[x] \end{pmatrix} \quad \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} \quad \begin{pmatrix} \mathbb{Z} & \mathbb{Z}_n \\ \mathbb{Z}_m & \mathbb{Z} \end{pmatrix}$$

También con este producto a todo A-módulo M se le puede asociar el anillo

$$\begin{pmatrix} \mathrm{End}(M) & M \\ 0 & A \end{pmatrix},$$

y a cualesquiera ${}_AN$ y M_A se les puede asociar el anillo

$$\begin{pmatrix} A^{op} & M \\ N & A \end{pmatrix}.$$

Ejemplo 2.31. En general tomando un campo k, una k-álgebra A, un A-módulo derecho M y un A-módulo izquierdo N los grupos abelianos

$$\begin{pmatrix} A & 0 \\ M & k \end{pmatrix} \text{ y } \begin{pmatrix} A & N \\ 0 & k \end{pmatrix}$$

son anillos con el producto trivial de matriz generalizada. A estos anillos se les llama extensión por un punto de A y coextensión por un punto de A.

Ejemplo 2.32. Dado un campo k, se considera el grupo abeliano $A = \bigoplus_{i,j=1}^n M_{ij}$, con $M_{ii} = k$ y $M_{ij} = k[x]$ para toda $j \neq i$. Defínanse $\varphi^j_{ik} : M_{ij} \otimes M_{jk} \to M_{ik}$ como el isomorfismo natural si $i \neq k$, como el isomorfismo natural si $i = k = j$, y si $i = k$ pero $k \neq j$ como $\varphi^j_{ik}(p(x) \otimes q(x)) = p(0)q(0)$. Claramente $\varphi^s_{it}(\varphi^k_{is} \otimes 1) = \varphi^k_{it}(1 \otimes \varphi^s_{kt})$, por lo que los morfismos φ_{ik}^{j} inducen un producto con el cual A es un anillo generalizado de matrices.

$$\begin{pmatrix} k & k[x] & \cdots & k[x] \\ k[x] & k & & \\ \vdots & & \ddots & \\ k[x] & & & k \end{pmatrix}$$

2.3. Descomposición en bloques

En esta sección se buscan las condiciones para descomponer un anillo A como un producto finito de anillos conexos. Dicha descomposición se le conoce como descomposición en bloques.

2.3.1. Módulos inescindibles

Se ha probado que si se tiene una descomposición de la unidad del anillo de endomorfismos de un módulo, entonces ésta induce una descomposición del módulo como suma directa finita de módulos. Sin embargo dichos sumandos podrían descomponerse nuevamente. Lo que lleva a preguntarse cómo deben ser los idempotentes de dicha descomposición para que los sumandos no se puedan descomponer. El objetivo de esta subsección es responder tal pregunta.

Definición 2.33. Se dice que un módulo es inescindible si sus únicos sumandos directos son 0 y M.

Ejemplo 2.34. Si $M = \mathbb{Z}_{p^2} = \mathbb{Z}/p^2\mathbb{Z}$, entonces M es un módulo inescindible. En efecto, por el teorema de correspondencia existe una biyección entre los submódulos de M y los submódulos de $\mathbb{Z}$ que contienen a $p^2\mathbb{Z}$, pero el único submódulo que cumple esta condición es $p\mathbb{Z}$, lo que implica que el único submódulo de M es pM, y entonces M es inescindible.

Recordando la Proposición 2.17 se tiene que M es inescindible si y sólo si $\mathrm{End}_A(M)$ no tiene descomposiciones no triviales de la unidad, por lo que tampoco tiene idempotentes no triviales. Se tiene entonces el siguiente resultado.

Proposición 2.35. *Sea A un anillo y M un A-módulo. Los siguientes enunciados son equivalentes.*

(a) *M es inescindible.*

(b) *Los idempotentes de $\mathrm{End}_A(M)$ son 0 y 1.*

(c) *Si* $1_M = f+g$ *es una descomposición de la unidad de* $\mathrm{End}_A(M)$, *entonces* $1_M = g$ *ó* $1_M = f$.

Lo anterior lleva a la siguiente definición.

Definición 2.36. Sea A un anillo. Se dice que un idempotente e distinto de 0 es primitivo, si no puede ser expresado como suma de dos idempotentes no triviales ortogonales. Es decir, e es idempotente primitivo si $e = f + g$ con f y g idempotentes ortogonales implica que $g = 0$ ó $f = 0$.

Observación 2.37. Si $e = f + g$ con f y g idempotentes ortogonales, entonces $ef = f$ y $fe = f$, por lo que $f = efe$, y análogamente $g = ege$. Se tiene entonces que toda expresión $e = f + g$ es una descomposición de la unidad de eAe.

Es inmediato entonces de la Proposición 2.35 y la observación anterior que e es un idempotente primitivo si y sólo si eA es inescindible. En efecto, por la Proposición 2.13 $\mathrm{End}_A(eA) \cong eAe$, por lo que las descomposiciones de la unidad no triviales de $\mathrm{End}_A(eA)$ inducen descomposiciones de la unidad no triviales de eAe, y viceversa. Esto muestra que e se expresa como suma de idempotentes ortogonales no triviales si y sólo si eA no es inescindible. Por lo que e es primitivo si y sólo si eA es inescindible

Análogamente se puede probar que e es primitivo si y sólo si Ae es inescindible.

De manera que utilizando la Proposición 2.35 se tiene el siguiente resultado.

Proposición 2.38. *Sea A un anillo. Los siguientes enunciados son equivalentes para un idempotente $e \in A$.*

(a) *$e \in A$ es un idempotente primitivo.*

(b) *Los idempotentes de eAe son* 0 *y e.*

(c) *Ae es un A-módulo izquierdo inescindible.*

(d) *eA es un A-módulo derecho inescindible.*

Ejemplo 2.39. Sea A un anillo sin idempotentes no triviales, por la proposición anterior se tiene que A_A y ${}_AA$ son inescindibles ya que los idempotentes de $A = 1A1$ son 0 y 1.

Ejemplo 2.40. La unidad de $\mathbb{Z}$ es un idempotente primitivo, por lo que $\mathbb{Z}$ es inescindible.

Ejemplo 2.41. $\mathrm{End}_{\mathbb{Z}}(\mathbb{Q})$ no tiene idempotentes diferentes de 0 y 1, por lo que $\mathbb{Q}$ es inescindible. En efecto, todo $f \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Q})$ esta determinado por $f(1)$ ya que

$$f(\frac{1}{m})m = f(1),$$

en concesuencia $f(\frac{1}{m}) = f(1)\frac{1}{m}$ y entonces $f(\frac{n}{m}) = f(1)\frac{n}{m}$. Por lo tanto, $f \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Q})$ es idempotente si y sólo si $f(1) = 1$ ó $f(1) = 0$, por lo que $\mathrm{End}_{\mathbb{Z}}(\mathbb{Q})$ no tiene idempotentes diferentes de 0 y 1.

Ejemplo 2.42. Sea $A = \mathbb{Q}[x,y]/\langle xy\rangle$. El anillo A no tiene idempotentes distintos de 0 y 1. En efecto, los elementos de A son de la forma $xp(x) + yq(y) + \lambda$ con p, q polinomios de una variable sobre $\mathbb{Q}$ y $\lambda \in \mathbb{Q}$, por lo que si $\alpha = xp(x) + yq(y) + \lambda$ es un idempotente de A se tiene que

$$x^2p^2(x) + 2\lambda xp(x) + y^2q^2(y) + 2\lambda yq(y) + \lambda^2 = \alpha^2 = \alpha = xp(x) + yq(y) + \lambda,$$

lo que implica que $p = q = 0$ y $\lambda = 0$ ó 1. Por lo tanto, A_A es inescindible. Sin embargo, $xA \oplus yA$ es submódulo de A, por lo que existen módulos inescindibles con submódulos no inescindibles.

Ejemplo 2.43. Sean $A = \mathbb{Q}[x,y]$ y $M_A = xA + yA$. Con el fin de mostrar que M es inescindible, a continuación se prueba que $\mathrm{End}_A(M) \cong A$. En efecto, si $f \in \mathrm{End}_A(M)$, considérese $P(x,y) = f(x)$; se tiene que

$$P(x,y)y = f(x)y = f(xy) = f(y)x,$$

lo que implica que x divide a $P(x,y)$, por lo que $P(x,y) = xQ(x,y)$ para algún polinomio Q, y entonces $f(y)x = xyQ(x,y)$ lo que implica que $f(y) = yQ(x,y)$. De esta manera se tiene que

$$f(\lambda x^n y^m) = f(x)\lambda x^{n-1}y^m = Q(x,y)\lambda x^n y^m$$

$$f(\lambda x^m y^n) = f(y)\lambda x^m y^{n-1} = Q(x,y)\lambda x^m y^n$$

para todo $n > 0$, $m \geq 0$ y $\lambda \in \mathbb{Q}$, por lo que es sencillo deducir que

$$f(R(x,y)) = R(x,y)Q(x,y)$$

para todo $R(x,y) \in M$. Por lo tanto, todo endomorfismo de M está dado por la multiplicación por un elemento de A, que claramente es la restricción de un morfismo de $\mathrm{End}_A(A)$. Y debido a que A es un dominio entero esto es suficiente para concluir que

$$\mathrm{End}_A(M) \cong \mathrm{End}_A(A) \cong A.$$

Luego entonces, $A \cong \mathrm{End}_A(M)$ es un dominio entero por lo que no tiene idempotentes no triviales, lo que implica que M es inescindible. Por lo tanto, M es un módulo inescindible tal que

$$M/\langle xy\rangle = xA/\langle xy\rangle \oplus yA/\langle xy\rangle\,.$$

Es decir, este es un ejemplo de un módulo inescindible con un cociente no inescindible.

Ejemplo 2.44. Sean k un campo y G un grupo finito. Por 2.12 $\alpha = \frac{1}{|G|}\sum_{g\in G} g$ es un idempotente. Además, todo $x \in kG$ se expresa de manera única como $x = \sum_{g\in G}\lambda_g g$ donde $\lambda_g \in k$ para todo $g \in G$. Ahora,

$$\alpha x = (\frac{1}{|G|}\sum_{g\in G} g)(\sum_{h\in G}\lambda_h h) = \frac{1}{|G|}\sum_{g\in G}\sum_{h\in G}\lambda_h gh = \frac{1}{|G|}(\sum_{h\in G}\lambda_h)(\sum_{g\in G} g) = (\sum_{h\in G}\lambda_h)\alpha,$$

por lo que αA es el espacio vectorial generado por α, de manera que $\dim_k \alpha A = 1$, lo que implica que αA es inescindible ya que no se puede descomponer por ser un espacio vectorial de dimensión 1. Por lo tanto, α es un idempotente primitivo.

Ejemplo 2.45. Sean k un campo y $G = D_{2n}$. Por 2.12 los elementos $\alpha = \frac{1}{n}\sum_{i=1}^{n} r^i$ y $\beta = \frac{1}{2}\sum_{i=1}^{2} s^i$ son idempotentes centrales de kG. Así que $\alpha kG\alpha = \alpha kG$ y

$$\alpha\beta = (\frac{1}{n}\sum_{i=1}^{n} r^i)(\frac{1}{2}\sum_{i=1}^{2} s^i) = \frac{1}{2n}(\sum_{i=1}^{n} r^i + \sum_{i=1}^{n} r^i s) = \frac{1}{2n}\sum_{g\in D_{2n}} g,$$

por 2.12 $\alpha\beta$ es un idempotente de αkG distinto de 0 y α, por lo que α es un idempotente no primitivo.

Ejemplo 2.46. Sea $A = \mathbb{Z}_2^{\mathbb{N}}$. Es sencillo mostrar que todo elemento de A es un idempotente. Por otro lado, $I = \mathbb{Z}_2^{(\mathbb{N})}$ es un ideal bilateral de A, y todo elemento del anillo A/I es un idempotente no primitivo. En efecto, se identifican los elementos de A como funciones $\alpha : \mathbb{N} \to \mathbb{Z}_2$ y se considera el soporte de dichas funciones

$$supp(\alpha) = \{n \in \mathbb{N} \mid \alpha(n) \neq 0\}.$$

Si $x = \alpha + I \in A/I$ es distinto de 0, el soporte de α es infinito y numerable, por lo que existe una biyección $f : \mathbb{N} \to supp(\alpha)$. Por otro lado, $\mathbb{N}$ se puede partir en números pares e impares. Si N_1 denota a los numeros impares y N_2 a los numeros pares, se tiene que f induce una partición $supp(\alpha) = f(N_1) \cup f(N_2)$ con $f(N_1)$ y $f(N_2)$ infinitos y numerables. Con estos últimos conjuntos se define $\alpha_i : \mathbb{N} \to \mathbb{Z}_2$ mediante

$$\alpha_i(n) = \begin{cases} \alpha(n) & \text{si } n \in f(N_i) \\ 0 & \text{si } n \notin f(N_i) \end{cases}$$

para $i \in \{1, 2\}$, claramente $\alpha = \alpha_1 + \alpha_2$ y $\alpha_1, \alpha_2 \notin I$ ya que $f(N_1)$ y $f(N_2)$ son infinitos. Se ha probado entonces que todo elemento $\alpha + I$ diferente de 0 de A/I es un idempotente no primitivo, ya que $\alpha + I = (\alpha_1 + I) + (\alpha_2 + I)$ y $\alpha_i + I \neq I$. Por lo tanto, existen anillos sin idempotentes primitivos.

Ejemplo 2.47. Sea k un campo. Si $Q = (Q_0, Q_1, s, t)$ es un carcaj, entonces los caminos triviales de kQ son idempotentes primitivos de kQ. En efecto, sea $i \in Q_0$; para probar que e_i es un idempotente primitivo basta probar que los idempotentes de $e_i kQe_i$ son 0 y e_i, lo cual es inmediato, ya que si e es un elemento idempotente de e_ikQe_i, entonces $e = \lambda e_i + \omega$ donde $\lambda \in k$ y ω es una combinación lineal de caminos no triviales que inician y teminan en i, de manera que

$$\lambda^2 e_i + 2\lambda\omega + \omega^2 = e^2 = e = \lambda e_i + \omega,$$

por lo que $\omega = 2\lambda\omega + \omega^2$ y $\lambda^2 e_i = \lambda e_i$, lo que implica que $\omega = 0$ y $\lambda^2 = \lambda$ en consecuencia $\lambda = 0$ ó 1. Por lo tanto, $e = e_i$ ó $e = 0$.

Es inmediato del ejemplo anterior que si Q tiene un número finito de vértices, entonces existe una descomposición de la unidad de kQ tal que cada sumando es un idempotente primitivo. En general, dado un anillo A, si se tiene una descomposición de la unidad $1_A = e_1 + ... + e_n$ donde cada e_i es un idempotente primitivo, entonces el conjunto $\{e_1, ..., e_n\}$ se llama sistema completo de idempotentes ortogonales primitivos. La existencia de dichos conjuntos es de gran importancia como se verá mas adelante.

Ejemplo 2.48. Sean $A = k^{\mathbb{N}}$ y $1_A = e_1 + ... + e_n$ una descomposición de la unidad de A. La descomposición de Peirce de A es $e_1A \oplus ... \oplus e_nA$; luego, debido a que A es un espacio de dimensión infinita, se tiene que alguno de sus sumandos debe ser de dimensión infinita, por lo que es un anillo isomorfo a A, y como tal tiene idempotentes distintos de 0 y 1. Por lo tanto, A no tiene ningún sistema completo de idempotentes ortogonales primitivos.

2.3.2. Idempotentes centrales y descomposiciones del anillo

En esta subsección se caracterizan con ayuda de los idempotentes los anillos que se pueden expresar como un producto de anillos.

Dados A_1,...,A_n anillos, sea $A = A_1 \times ... \times A_n$. Todo elemento x de A es una n-ada ordenada $x = (a_1, ..., a_n)$ con $a_i \in A_i$. Es sencillo mostrar que A contiene un anillo B_i isomorfo a cada A_i, donde

$$B_i = \{(a_1, ..., a_n) \in A \mid a_j = 0 \text{ para toda } j \neq i\}.$$

Además es inmediato que dichos anillos son subgrupos de A tales que $A = B_1 \oplus ... \oplus B_n$. Ahora bien, con el fin de simplificar la notación se identificarán los anillos B_i con los A_i, de tal manera que al referirme del anillo A_i y sus elementos, me estaré refiriendo del anillo B_i y sus elementos. Así, un elemento $x \in A$ puede ser expresado de manera única como $x = a_1 + ... + a_n$ con $a_i \in A_i$ para toda $i \in \{1, ..., n\}$.

Es inmediato entonces que si para cada $i \in \{1, ..., n\}$ se denota la unidad de A_i como e_i, entonces cada e_i es idempotente central de A y $1_A = e_1 + ... + e_n$.

Proposición 2.49. *Si $A = A_1 \times ... \times A_n$ es un producto de anillos y e_i es la unidad de A_i en A, entonces*

(a) $1_A = e_1 + ... + e_n$ *es una descomposición de la unidad.*

(b) *Cada idempotente e_i es central.*

Cuando se tiene una descomposición de la unidad donde cada sumando es central, a ésta se le llama descomposición central de la unidad.

Teniendo una descomposición central de la unidad $1_A = e_1 + ... + e_n$ se cumple que $e_iA = Ae_i = e_iAe_i$, ya que $e_ia = ae_i = e_iae_i$ para toda $a \in A$, luego si $i \neq j$ se tiene que $e_iAe_j = 0$.

En consecuencia las decomposiciones de Peirce derecha, izquierda y bilateral coinciden y los sumandos son ideales bilaterales del anillo que son anillos por sí mismos.

$$A = e_1A \oplus ... \oplus e_nA = Ae_1 \oplus ... \oplus Ae_n = e_1Ae_1 \oplus ... \oplus e_nAe_n$$

Recíprocamente, si el anillo A se descompone como suma directa de ideales bilaterales, entonces por la Proposición 2.21 la descomposición induce una descomposición de la unidad $1 = e_1 + ... + e_n$ que además es central. En efecto, al ser bilaterales los ideales de la descomposición, se tiene que $e_iA = Ae_i$ para todo $i \in \{1, ..., n\}$. De manera que para todo $a \in A$ y todo $j \in \{1, ..., n\}$ se tiene que

$$e_ia = e_i(\sum_{j=1}^{n} ae_j) = \sum_{j=1}^{n} e_iae_j = e_iae_i = \sum_{j=1}^{n} e_jae_i = ae_i$$

ya que $e_kae_j \in e_kA \cap e_jA = 0$ para todo $i \neq j$; por lo tanto los idempotentes e_i son centrales.

Se tiene entonces el siguiente resultado.

Proposición 2.50. *Sea A un anillo. Existe una correspondencia biyectiva entre*

(a) *las descomposiciones de A como producto finito de anillos,*

(b) *las descomposiciones centrales de la unidad de A y*

(c) *las descomposiciones de A como suma directa de ideales bilaterales.*

Y recordando que el centro de A es un anillo se tiene el siguiente corolario.

Corolario 2.51. *Sea A un anillo. Existe una correspondencia biyectiva entre las descomposiciones de A como producto finito de anillos y las de su centro.*

Ejemplo 2.52. Si M es un módulo tal que $M = M_1 \oplus ... \oplus M_n$ y $\mathrm{Hom}_A(M_i, M_j) = 0$ para toda $i \neq j$, entonces $\mathrm{End}_A(M) \cong \mathrm{End}_A(M_1) \times ... \times \mathrm{End}_A(M_n)$. En efecto, por la Proposición 2.26 se tiene que el anillo $\mathrm{End}_A(M)$ se representa matricialmente como

$$\begin{pmatrix} \mathrm{End}_A(M_1) & \dots & \mathrm{Hom}_A(M_n, M_1) \\ \vdots & \ddots & \\ \mathrm{Hom}_A(M_1, M_n) & & \mathrm{End}_A(M_n) \end{pmatrix} = \begin{pmatrix} \mathrm{End}_A(M_1) & \dots & 0 \\ \vdots & \ddots & \\ 0 & & \mathrm{End}_A(M_n) \end{pmatrix},$$

que claramente es isomorfo al producto $\mathrm{End}_A(M_1) \times ... \times \mathrm{End}_A(M_n)$.

Ejemplo 2.53. Sea $A = \mathbb{Z}_2^{\mathbb{N}}$. Es sencillo mostrar que $A \cong \mathbb{Z}_2 \times \mathbb{Z}_2^{\mathbb{N}}$ y $A \cong \mathbb{Z}_2^2 \times \mathbb{Z}_2^{\mathbb{N}}$. Esto muestra que la ley de cancelación bajo isomorfismo para el producto de anillos no se cumple.

Ya caracterizados los anillos que se pueden expresar como producto de anillos se pueden caracterizar los anillos que no se pueden expresar como un producto no trivial, a dichos anillos se les llama conexos.

Definición 2.54. Se dice que un anillo A es conexo si no puede ser expresado como producto de 2 anillos.

Es inmediato de la Proposición 2.50 que es equivalente que A sea conexo a que no tenga idempotentes centrales diferentes de 0 y 1. Por lo que se tiene la siguiente caracterización.

Proposición 2.55. *Un anillo A es conexo si y sólo si no tiene idempotentes centrales no triviales.*

Ejemplo 2.56. Ningún dominio entero tiene idempotentes no triviales, por lo que todo dominio entero es conexo.

Ejemplo 2.57. Dado un campo k, sea A una k-álgebra con idempotentes no triviales. El anillo de matrices generalizadas con producto trivial

$$B = \begin{pmatrix} k & 0 \\ A & A \end{pmatrix}$$

es conexo. En efecto, si $x \in B$ es un idempotente, entonces

$$\begin{pmatrix} \lambda & 0 \\ a & b \end{pmatrix} = x = x^2 = \begin{pmatrix} \lambda^2 & 0 \\ a\lambda + ba & b^2 \end{pmatrix},$$

lo que implica que $\lambda = 0$ ó 1, $b^2 = b$ y $a\lambda + ba = a$. Si $\lambda = 1$, entonces $ba = 0$; y si $\lambda = 0$, entonces $ba = a$. Por lo tanto, los idempotentes de B son de la forma

$$\begin{pmatrix} 0 & 0 \\ ba & b \end{pmatrix} \text{ con } b \text{ un idempotente de } A \text{ y } a \in A, \text{ ó bien}$$

$$\begin{pmatrix} 1 & 0 \\ (1-b)a & b \end{pmatrix} \text{ con } b \text{ un idempotente de } A \text{ y } a \in A.$$

Con lo anterior es sencillo demostrar que B no tiene idempotentes centrales no triviales ya que si b es un idempotente no trivial, entonces

$$\begin{pmatrix} 0 & 0 \\ ba & b \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ ba+b & b \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ ba & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ ba & b \end{pmatrix} \text{ y}$$

$$\begin{pmatrix} 1 & 0 \\ ba & b \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ ba+b & b \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1+ba & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ ba & b \end{pmatrix},$$

por último se prueba análogamente que los idempotentes $\begin{pmatrix} 1 & 0 \\ a & 0 \end{pmatrix}$ y $\begin{pmatrix} 0 & 0 \\ a & 1 \end{pmatrix}$ tampoco son centrales, por lo que los únicos idempotentes centrales de B son los triviales. Por lo tanto B es conexo.

2.3.3. La descomposición en bloques

A continuación se expone el teorema central de esta sección. Muestra que todo anillo con un sistema completo de idempotentes ortogonales primitivos se puede expresar como un producto finito de anillos conexos, y cómo construir la descomposición central de la unidad que induzca tal producto.

Proposición 2.58. *Sean A un anillo y $S = \{e_1, ..., e_n\}$ un sistema completo de idempotentes ortogonales primitivos. Existe una partición de $S = E_1 \cup ... \cup E_k$ tal que si $f_i = \sum_{e\in E_i} e$ para todo $i \in \{1, ..., k\}$, entonces*

(a) *$1_A = f_1 + ... + f_k$ es una descomposición central de la unidad,*

(b) *si g es un idempotente central de f_iAf_i, entonces g es un idempotente central de A,*

(c) *si e es un idempotente primitivo de A y g un idempotente central de A, entonces $ge \neq 0$ implica que $ge = e$,*

(d) *si $e, f \in S$, tales que $e, f \in E_i$ para algún $i \in \{1, ..., k\}$, y g es un idempotente central, entonces $eg \neq 0$ si y sólo si $fg \neq 0$,*

(e) *f_iAf_i es un anillo conexo.*

Demostración. Se define la relación $\sim$ en S como $e \sim f$ si $eAf \neq 0$ ó $fAe \neq 0$. Esta es una relación reflexiva y simétrica, pues $e \in eAe$ para todo $e \in S$, lo que implica que $e \sim e$, y $eAf \neq 0$ ó $fAe \neq 0$ implica que $e \sim f$ si y sólo si $f \sim e$ para todo $e, f \in S$. Luego, se construye la relación $\approx$ en S de tal manera que $e \approx f$ si existe $\{g_1, ..., g_s\} \subseteq S$ tal que $e \sim g_1 \sim g_2 \sim ... \sim g_s \sim f$, entonces claramente esta relación es de equivalencia, por lo que induce una partición $S = E_1 \cup ... \cup E_k$. Sea $f_i = \sum_{e\in E_i} e$ para todo $i \in \{1, ..., k\}$.

(a) Si $i, j \in \{1, ..., k\}$ e i es distinto de j, entonces $f_iAf_j = 0$. En efecto,

$$f_iAf_j = \bigoplus_{e\in E_i, g\in E_j} eAg,$$

y si se supone que $eAg \neq 0$ para algún $e \in E_i$ y $g \in E_j$, entonces $e \sim g$, lo que implica que $e \approx g$, lo que es una contradicción pues $i \neq j$. De manera que

$A = \oplus_{i=1}^{n} f_i A f_i$, por lo que dado $\alpha \in A$, se le puede expresar de forma única como $\alpha = \sum_{j=1}^{k} f_i \alpha f_i$, entonces

$$f_i \alpha = \sum_{j=1}^{k} f_i f_j \alpha f_j = f_i \alpha f_i = \sum_{j=1}^{k} f_j \alpha f_j f_i = \alpha f_i.$$

Por lo tanto, $\{f_1, ..., f_k\}$ es un sistema completo de idempotentes ortogonales centrales.

(b) Si g es un idempotente central de $f_i A f_i$, entonces es idempotente en A, y se tiene que $g = f_i g f_i = g f_i = f_i g$ y que dado $\alpha \in A$ $g f_i \alpha f_i = f_i \alpha f_i g$, por ser g central; de manera que

$$g\alpha = \sum_{j=1}^{k} g f_i f_j \alpha f_j = g f_i \alpha f_i = f_i \alpha f_i g = \sum_{j=1}^{k} f_j \alpha f_j f_i g = \alpha g.$$

Por lo tanto, g es un idempotente central de A.

(c) Si g es un idempotente central y e un idempotente primitivo tales que $ge \neq 0$, entonces ge y $g(1-e)$ son idempotentes, pero $e = ge + (1-g)e$, lo que implica que $e = ge$ ó $e = (1-g)e$, pero si $e = (1-g)e$ entonces $ge = 0$, lo cual es una contradicción. Por lo tanto, $ge = e$.

(d) Si g es un idempotente central y $e \sim f$, suponiendo $eg \neq 0$ se tiene que $eAf \neq 0$ ó $fAe \neq 0$, pues $e \sim f$, lo que implica que $eAfg = geAf \neq 0$ ó $gfAe = fAeg \neq 0$, por lo que $fg \neq 0$; análogamente si $fg \neq 0$, entonces $eg \neq 0$. Por lo tanto, si $e \sim f$, se tiene que $eg \neq 0$ si y sólo si $gf \neq 0$. De modo que si $e \approx f$, se tiene que $e \sim e_{l_1} \sim ... \sim e_{l_s} \sim f$, entonces utilizando lo anterior inductivamente $eg \neq 0$ si y sólo si $gf \neq 0$.

(e) Sea g un idempotente central de $f_i A f_i$ diferente de f_i y 0, y $h = f_i - g$, siendo ambos idempotentes de $f_i A f_i$ se tiene que $f_i g = g \neq 0$ y $f_i h = h \neq 0$, lo que implica que existen d_1, $d_2 \in E_i$ tales que $d_1 g \neq 0$ y $d_2 h \neq 0$, lo que implica, por (4) y (3), que $d_1 g = d_1$, $d_2 h = d_2$, $d_2 g \neq 0$ y $d_1 h \neq 0$; pero entonces $d_2 g = d_2 h g = 0$ lo cual es una contradicción. Por lo tanto, no existen idempotentes centrales en $f_i A f_i$ diferentes de f_i y 0, por lo que $f_i A f_i$ es conexa.

□

Observación 2.59. La relación usada en la demostración surge del hecho de que un anillo A es conexo si y sólo si todo idempotente no trivial no es central, lo cual se cumple si y sólo si para todo idempotente no trivial e se cumple que $eAf \neq 0$ ó $fAe \neq 0$ para álgun idempotente ortogonal f. Por lo tanto, si A es conexo todo par de idempotentes ortogonales e y f cumplen que $eAf \neq 0$ ó $fAe \neq 0$.

Corolario 2.60. *Sea A un anillo con un sistema completo de idempotentes ortogonales primitivos $S = \{e_1, ..., e_n\}$. El anillo A es conexo si y sólo si para toda $i \in \{1, ..., n\}$ existe $j \in \{1, ..., n\}$ tal que $e_iAe_j \neq 0$ ó $e_jAe_i \neq 0$.*

Demostración. Si A es conexo y se supone que existe $e_i \in S$ tal que $e_iAe_j = 0$ y $e_jAe_i = 0$ para todo $e_j \in S$, entonces siguiendo la demostración de la proposición anterior se construye una descomposición central de la unidad no trivial, lo cual es una contradicción ya que A es conexo. Si para toda $i \in \{1, ..., n\}$ existe $j \in \{1, ..., n\}$ tal que $e_iAe_j \neq 0$ ó $e_jAe_i \neq 0$, entonces la proposición anterior implica que todo A es conexo. □

Por lo tanto, si A tiene un sistema completo de idempotentes ortogonales primitivos, entonces por la proposición anterior se puede construir una descomposición central de la unidad tal que los sumandos de la descomposición de Peirce inducida sean anillos conexos. Dicha descomposición se le llama *descomposición en bloques.*

Teorema 2.61. *Sea A un anillo. Si existe un sistema completo de idempotentes ortogonales primitivos, entonces A se descompone como un producto finito de anillos conexos.*

Ejemplo 2.62. Sea M un A-módulo derecho. Si $\mathrm{End}_A(M)$ tiene un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$, entonces la descomposición central de la unidad $1 = f_1 + ... + f_m$ construida en la Proposición 2.58, induce una descomposición

$$M = f_1(M) \oplus ... \oplus f_m(M) = M_1 \oplus ... \oplus M_m$$

tal que $\mathrm{Hom}_A(M_i, M_j) = \mathrm{Hom}_A(f_iM, f_jM) = f_j \,\mathrm{End}_A(M) f_i = 0$ para todo $i \neq j$ y M_i se descompone como una suma directa finita de submódulos inescindibles para todo $i \in \{1, ..., m\}$, pues

$$M_i = f_i(M) = (\sum_{e_j \in E_i} e_j)(M) = \bigoplus_{e_j \in E_i} e_jM$$

y cada e_jM es inescindible pues cada e_j es primitivo.

Ejemplo 2.63. Sean k un campo y Q un carcaj con un número finito de vértices. Siguiendo la demostración de la Proposición 2.58 se deduce que kQ es un producto de anillos conexos. Más aún, considerando el hecho de que dados e_i y e_j caminos triviales, $e_ikQe_j \neq 0$ ó $e_jkQe_i \neq 0$ si y sólo si existe un camino de i a j o de j a i, se deduce que kQ es un anillo conexo si y sólo si Q es conexo.

Por último, el siguiente ejemplo muestra que el recíproco del teorema es falso, es decir existen anillos conexos sin un sistema completo de idempotentes ortogonales primitivos.

Ejemplo 2.64. Sea $B = \mathbb{Z}_2^{\mathbb{N}}/\mathbb{Z}_2^{(\mathbb{N})}$, se mostró en 2.46 que todos los elementos de B son idempotentes no primitivos. Y por 2.57 el anillo de matrices generalizadas con producto trivial

$$A = \begin{pmatrix} \mathbb{Z}_2 & 0 \\ B & B \end{pmatrix}.$$

es un anillo conexo y los idempotentes de A son de la forma

$$\begin{pmatrix} 0 & 0 \\ c & b \end{pmatrix} \text{ con } b \text{ idempotente y } c \in bB \text{ ó}$$

$$\begin{pmatrix} 1 & 0 \\ c & b \end{pmatrix} \text{ con } b \text{ idempotente y } c \in (1-b)B.$$

En consecuencia, debido a que B no contiene idempotentes primitivos, los únicos idempotentes primitivos de A son

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

por lo que A no tiene sistemas completos de idempotentes ortogonales primitivos.

Ahora, en caso de que un anillo A se descomponga como un producto finito de anillos conexos, dicha descomposición es única salvo una permutación; es decir, si se tiene que

$$B_1 \times ... \times B_m = A = A_1 \times ... \times A_n$$

son descomposiciones en anillos conexos, entonces $m = n$ y existe una permutación $\sigma \in S_n$ tal que $A_i = B_{\sigma(i)}$.

En efecto, supóngase que el anillo A se descompone como producto finito de anillos conexos $A = A_1 \times ... \times A_n$ y que se tiene una descomposición $B_1 \times ... \times B_m = A$, Sean $1 = e_1 + ... + e_n$ y $1 = f_1 + ... + f_m$ las descomposiciones centrales inducidas por las descomposiciones $A = A_1 \times ... \times A_n$ y $B_1 \times ... \times B_m = A$, respectivamente. Ahora, dado $j \in \{1, ..., m\}$, para cada $i \in \{1, ..., n\}$ se tiene que $e_i f_j$ es un idempotente central de A_i, lo que implica que $e_i f_j = e_i$ ó $e_i f_j = 0$, de manera que que si

$$X_j = \{e_i \mid e_i f_j = e_i\},$$

entonces

$$f_j = (e_1 + ... + e_n) f_j = \sum_{i \in X_j} e_i,$$

por lo que $B_j = \prod_{i \in X_j} A_i$. Más aún, si $j \neq k$ entonces f_i es ortogonal a f_k, lo que implica que X_i es ajeno a X_j, y entonces $\{1, ..., n\} = X_1 \cup ... \cup X_m$.

En particular, si cada B_j es conexo, entonces cada X_j contiene un solo elemento, por lo que $m = n$ y si define $\sigma(j)$ como el subíndice de este elemento se tiene que $B_j = A_{\sigma(j)}$.

Teorema 2.65. *Sea A un anillo que se descompone como producto finito de anillos conexos $A = A_1 \times ... \times A_n$. Si $A = B_1 \times ... \times B_m$, entonces existe una partición $\{1, ..., n\} = X_1 \cup ... \cup X_m$ tal que $B_j = \prod_{i \in X_j} A_i$ para toda $j \in \{1, ..., m\}$. En particular, si $A = B_1 \times ... \times B_m$ es una descomposición en anillos conexos entonces $m = n$ y existe $\sigma \in S_n$ tal que $A_i = B_{\sigma(i)}$.*

Como corolario, se tiene que si A es un anillo que se puede descomponer como producto de anillos conexos, entonces la ley de la cancelación es válida.

Corolario 2.66. *Sea A un anillo que se descompone como producto finito de anillos conexos. Si existen isomorfismos de anillos $A_1 \times A_2 \cong A \cong B_1 \times B_2$ y $A_1 \cong B_1$, entonces $A_2 \cong B_2$.*

Por último cabe dedicar unas palabras sobre la conveniencia de presentar un anillo A como un producto de anillos. Ésta no viene sólo del hecho que el estudio del anillo se reduce al estudio de sus factores, sino también del hecho que el estudio de los módulos sobre dicho anillo se reduce al estudio de los módulos sobre los anillos en que se factoriza A.

En efecto, si $A = A_1 \times ... \times A_n$ y M es un A-módulo derecho, entonces la descomposición central de la unidad $1 = e_1 + ... + e_n$ que resulta de la descomposición de A induce una descomposición de $\mathrm{End}_A(M)$-módulos izquierdos $M = Me_1 \oplus ... \oplus Me_n$ donde cada Me_i es un A_i-módulo por la Proposición 2.19, pero por la Proposición 2.4 se tiene que cada Me_i es un A-módulo tal que $Me_i(1 - e_i) = 0$. Por lo que la descomposición $M = Me_1 \oplus ... \oplus Me_n$ es también una descomposición de A-módulos derechos. En consecuencia, todo A-módulo M se puede presentar como

$$M = \begin{pmatrix} Me_1 \\ Me_2 \\ \vdots \\ Me_n \end{pmatrix}.$$

Más aún, dados M y N A-módulos derechos se tiene por la Proposición 2.26 que

$$\mathrm{Hom}_A(M, N) = \begin{pmatrix} (Me_1, Ne_1) & 0 & \cdots & 0 \\ 0 & (Me_2, Ne_2) & & \\ \vdots & & \ddots & \\ 0 & & & (Me_n, Ne_n) \end{pmatrix}$$

donde $(Me_i, Ne_i) = \mathrm{Hom}_{A_i}(Me_i, Ne_i)$, ya que $\mathrm{Hom}_A(Me_i, Ne_i) = \mathrm{Hom}_{A_i}(Me_i, Ne_i)$ para toda $i \in \{1, ..., n\}$ por la Proposición 2.4, y para todo $f \in \mathrm{Hom}_A(Me_i, Ne_j)$ se tiene que

$$f(Me_i) = f(Me_ie_i)e_j = f(M)e_ie_j = 0$$

por lo que $\mathrm{Hom}_A(Me_i, Ne_j) = 0$. De manera que se puede hacer la identificación

$$\mathrm{Hom}_A(M, N) = \prod_{i=1}^{n} \mathrm{Hom}_{A_i}(Me_i, Ne_i).$$

.

Por lo tanto, se ha identificado a cada A-módulo con una n-ada de grupos abelianos tal que cada uno es un A_i-módulo, y a cada morfismo entre dos A-módulos se ha identificado con una n-ada de morfismos entre A_i-módulos. Proceso que es fácilmente invertible gracias a la Proposición 2.4.

Formalmente se puede enunciar lo discutido en la siguiente proposición.

Proposición 2.67. *Sea $A = A_1 \times ... \times A_n$ un producto de anillos. Existe una equivalencia de categorías $Mod_A \cong Mod_{A_1} \times ... \times Mod_{A_n}$.*

La demostración no se encuentra en esta sección, pero se puede consultar en el Apéndice.

3. Semisimples y Simples

En este capítulo se aborda el estudio de los anillos semisimples. Históricamente, matemáticos como Tsi-Yuen Lam [Lam01], Michiel Hazewinkel, Nadiya Gubareni y V. V. Kirichenko [HGK05] concuerdan en que el estudio de esta clase de anillos marcó el inicio de la teoría moderna de anillos no conmutativos con el teorema de clasificación de álgebras semisimples de dimensión finita de J.H.N. Wedderburn en 1909.

3.1. Módulos Semisimples

En el capítulo anterior se probó que existe una biyección entre las descomposiciones de un módulo como suma directa finita de submódulos y las descomposiciones de la unidad de su anillo de endomorfismos. Si M es un módulo tal que cualquier submódulo es sumando directo de M, entonces cada submódulo induce una descomposición de la unidad de $\mathrm{End}_A(M)$. A tales módulos se les llama módulos completamente reducibles ó semisimples y son el objeto de estudio de esta sección.

Definición 3.1. Sean A un anillo y M un A-módulo. Se dice que M es semisimple ó completamente reducible si todo submódulo de M es sumando directo de M.

Ejemplo 3.2. Dado un espacio vectorial, todo subespacio es un sumando directo del espacio. Por lo tanto, todo espacio vectorial es semisimple.

Ejemplo 3.3. $\mathbb{Z}_\mathbb{Z}$ no es semisimple. En efecto, los submódulos de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$ con $m \in \mathbb{Z}$, y para dos submódulos distintos de cero $m\mathbb{Z}$ y $n\mathbb{Z}$ se tiene que $mn \in m\mathbb{Z} \cap n\mathbb{Z}$, por lo que ningún submódulo distinto de cero es sumando directo de $\mathbb{Z}$.

Cabe resaltar que si M es un A-B bimódulo, puede suceder que M_B sea semisimple pero ${}_AM$ no lo sea e inversamente, como se puede ver en el siguiente ejemplo.

Ejemplo 3.4. Dado un campo k, el anillo $A = k[x]$ es un A-k bimódulo. A_k es un espacio vectorial, por lo que es un módulo semisimple sobre k. Por otro lado, debido a que A es un dominio de ideales principales, los submódulos de ${}_AA$ son de la forma $Ap(x)$ para algún polinomio $p(x)$, entonces para dos ideales distintos de cero $Ap(x)$ y $Aq(x)$ se tiene que $p(x)q(x) \in Ap(x) \cap Aq(x)$, por lo que ${}_AA$ no es semisimple.

Ahora, si M es semisimple y N_1 es un submódulo de M, entonces $M = N_1 \oplus N_2$. Así, de la Proposición 2.17 se sigue que $1_M = \rho_1 + \rho_2$, donde $\rho_i = \eta_i \pi_i$, π_i es la proyección canónica y η_i es la inclusión canónica para $i \in \{1, 2\}$. Luego, si N_3 es un submódulo de N_1, también es un submódulo de M, por lo que existe un submódulo N_4 tal que $M = N_3 \oplus N_4$, lo que implica que $1_M = \rho_3 + \rho_4$.

Por otro lado, $\rho_1\eta_1 = \eta_1\pi_1\eta_1 = 1_{N_1}$, entonces debido a que $\rho_1 + \rho_2 = \rho_3 + \rho_4$ se cumple que

$$1_{N_1} = \rho_1\eta_1 = \rho_3\eta_1 + \rho_4\eta_1 - \rho_2\eta_1 = \rho_3\eta_1 + \rho_4\eta_1$$

y además $\rho_3\eta_1\rho_4\eta_1 = 0$, $0 = \rho_4\eta_1\rho_3\eta_1$, $\rho_4\eta_1\rho_4\eta_1 = \rho_4\eta_1$ y $\rho_3\eta_1\rho_3\eta_1 = \rho_3\eta_1$. Es decir, $1_{N_1} = \rho_3\eta_1 + \rho_4\eta_1$ es una descomposición de la unidad de $\mathrm{End}_A(N_1)$, entonces por la Proposición 2.17

$$N_1 = \rho_3\eta_1(N_1) \oplus \rho_4\eta_1(N_1) = N_3 \oplus \rho_4\eta_1(N_1).$$

Por lo tanto, todo submódulo de N_1 es sumando directo de éste, es decir N_1 es semisimple.

De igual manera, M/N_1 es semisimple, pues si N'/N_1 es un submódulo de M/N_1, entonces existe un submódulo N'' tal que $M = N' \oplus N''$, y así

$$M/N_1 = N'/N_1 \oplus (N'' + N_1)/N_1.$$

Ahora, si $f : M' \to M$ es un isomorfismo, donde M es semisimple, entonces M' también lo es. En efecto, si N' es un submódulo de M', entonces es isomorfo a $N = f(N')$, y como M es semisimple existe una descomposición de la unidad de $1_M = \rho_1 + \rho_2$ tal que $\rho_1(M) = N$ y entonces se tiene una descomposición de la unidad $1_{M'} = f^{-1}\rho_1 f + f^{-1}\rho_2 f$ tal que $f^{-1}\rho_1 f(N') = N'$. Por lo tanto, todo submódulo de M' es sumando directo de éste, es decir M' es semisimple.

Además, si se tiene una sucesión exacta $0 \to N \to M \to N' \to 0$ donde M es semisimple, debido a que N es isomorfo a un submódulo de M y N' a un cociente de M, se tiene que ambos son semisimples.

Proposición 3.5. *Sea $0 \to N \to M \to N' \to 0$ una sucesión exacta de módulos. Si M es semisimple, entonces N y N' también lo son.*

Sin embargo, si se tiene una sucesión exacta $0 \to N \to M \to N' \to 0$ con N y N' semisimples, M no es semisimple forzosamente como se ve en el siguiente ejemplo.

Ejemplo 3.6. Considérese el monomorfismo $f : \mathbb{Z}_p \to \mathbb{Z}_{p^2}$ definido como $f(x) = px$. Se tiene que $\mathrm{Im}(f) = p\mathbb{Z}_{p^2}$, lo que implica que $\mathbb{Z}_{p^2}/\mathrm{Im}(f) \cong \mathbb{Z}_p$. Por lo tanto, se tiene la siguiente sucesión exacta, donde $\mathbb{Z}_{p^2}$ no es semisimple por el Ejemplo 2.34, a pesar de que $\mathbb{Z}_p$ sí lo es.

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

3.1.1. Módulos Simples

Se ha visto que todo submódulo N de un módulo semisimple M es a su vez semisimple, así que cuando N tiene un submódulo propio N' se induce una descomposición

$$M = N \oplus M_0 = N' \oplus N_0 \oplus M_0.$$

Con el fin de estudiar la estructura de M se podría seguir este proceso recursivamente tomando un submódulo de N' y considerar la descomposición inducida, pero no hay indicadores de que dicho proceso sea finito. En consecuencia cabe preguntarse en qué casos este proceso es finito.

Un caso a considerar es cuando M no tiene submódulos propios no triviales. Lo que lleva a la siguiente definición.

Definición 3.7. Si M es un módulo diferente de cero que no tiene submódulos propios distintos de cero, se dice que M es un módulo simple.

Es sencillo probar que si M es un módulo semisimple diferente de cero, entonces contiene un submódulo simple. En efecto, tomando $m \in M$ no nulo, considérese el conjunto X de submódulos de $M' = mA$ que no contienen a m. El conjunto X es no vacío pues $0 \in X$; y si se toma una cadena $(N_i)_{i \in Z}$ de elementos de X, entonces $\sum_{i \in Z} N_i$ tampoco contiene a m y es una cota superior de la cadena. Ciertamente, si se supone que $m \in \sum_{i \in Z} N_i$, entonces existe un subconjunto finito $Z' \subseteq Z$ tal que $m = \sum_{i \in Z'} n_i$ con $n_i \in N_i$; pero en tal caso $m \in N_\alpha$ donde α es el máximo de Z', lo cual es una contradicción. Por lo tanto, el lema de Zorn implica que X tiene un elemento maximal K.

Luego, como M' es semisimple existe un submódulo S tal que $M' = K \oplus S$. El submódulo S es distinto de cero ya que $m \notin K$ y no tiene submódulos propios, ya que si se supone que S' es un submódulo de S, entonces $K \oplus S'$ contiene a m por la maximalidad de K, lo que implica que $mA = M' = K \oplus S'$; pero entonces $S = S'$.

Con la argumentación anterior se tiene el siguiente resultado.

Proposición 3.8. *Todo módulo semisimple contiene un módulo simple.*

Antes de continuar, la siguiente proposición caracteriza los módulos simples.

Proposición 3.9. *Sea $S \neq 0$ un A-módulo derecho. Las siguientes afirmaciones son equivalentes:*

(a) *S es simple.*

(b) *$S = sA$ para cualquier $s \in S$, $s \neq 0$.*

(c) *Existe un submódulo derecho maximal $I \subseteq A$ tal que $S \cong A/I$.*

Demostración. $(a \Rightarrow b)$ Si $x \in S\backslash\{0\}$, entonces xA es un submódulo de S, lo que implica que $xA = S$, pues S es simple y $x \neq 0$.

$(b \Rightarrow c)$ Sea $x \in S\backslash\{0\}$. Se define el morfismo $\phi : A \to S$, como $\phi(a) = xa$. Es inmediato que ϕ es epimorfismo, ya que ϕ es distinto de 0 y debido a que S es simple $\operatorname{Im}(\phi) = S$; entonces por el primer teorema de isomorfismo $A/\operatorname{Ker}(\phi) \cong S$, y por el teorema de correspondencia y el hecho de que S es simple, se concluye que $\operatorname{Ker}(\phi)$ es maximal.

$(c \Rightarrow a)$ Como I es maximal, la correspondencia entre los submódulos de A/I y de los de A que contienen a I implican que S es simple. □

Ejemplo 3.10. Sea A un anillo conmutativo y $B = A[x]$ el anillo de polinomios sobre A de una variable. Es sencillo probar que los ideales maximales de B son los generados por los polinomios irreducibles, por lo que los módulos simples sobre B son isomorfos a los módulos $B/\langle f\rangle$, donde f es un polinomio irreducible.

Por último, esta subsección concluye con el Lema de Schur, el cual contiene información importante sobre los morfismos que tienen como dominio ó contradominio un módulo simple.

Lema 3.11. *Sea S un módulo simple. Se cumplen los siguientes enunciados:*

(a) *Si $f : S \to N$ es un morfismo de módulos, entonces f es un monomorfismo ó $f = 0$.*

(b) *Si $f : N \to S$ es un morfismo de módulos, entonces f es un epimorfismo ó $f = 0$.*

Demostración. Sea S simple.

(a) Si $f : S \to N$ es un morfismo de módulos, entonces debido a que S es simple $\operatorname{Ker}(f) = 0$ ó $\operatorname{Ker}(f) = S$, lo que implica que f es un monomorfismo ó $f = 0$.

(b) Si $f : N \to S$ es un morfismo de módulos, entonces $\operatorname{Im}(f) = 0$ ó $\operatorname{Im}(f) = S$, lo que implica que f es un epimorfismo ó $f = 0$.

□

Corolario 3.12. *Sea S un módulo simple. Se cumplen los siguientes enunciados:*

(a) *Si $f : S \to S$ es un morfismo de módulos, entonces f es un isomorfismo ó $f = 0$.*

(b) $\operatorname{End}_A(S)$ *es un anillo con división.*

(c) *S es inescindible.*

Demostración. Sea S simple.

(a) Es inmediato del lema de Schur.

(b) Al ser M simple los morfismos distintos de 0 de $\operatorname{End}_A(S)$ son isomorfismos, por lo que todo elemento no nulo tiene inverso.

(c) No existen idempotentes no triviales en $\operatorname{End}_A(S)$ por ser un anillo con división, lo que implica que S es inescindible.

□

3.1.2. Módulos Semisimples

El objetivo de esta subsección es describir los módulos semisimples.

En primer lugar cabe notar que si se tiene una sucesión exacta

$$0 \to N \xrightarrow{f} M \to N' \to 0, \tag{3.1}$$

donde M es semisimple, entonces $\operatorname{Im}(f)$ es un sumando directo de M, por lo que dicha sucesión se escinde. Recíprocamente, si se tiene un módulo M tal que toda sucesión exacta de la forma (3.1) se escinde, entonces en particular todos sus submódulos son sumandos directos de M. De esta manera se tiene la primer caracterización.

Proposición 3.13. *M es semisimple si y sólo si toda sucesión exacta de la forma $0 \to N \to M \to N' \to 0$ se escinde.*

Ahora, dado un módulo semisimple M, considérese el submódulo N igual a la suma de todos los submódulos simples de M. Debido a que M es semisimple, $M = N \oplus N'$ para algún submódulo N', pero si N' es diferente de 0, debe de contener un submódulo simple por la Proposición 3.8, lo cual es una contradicción pues N contiene todos los submódulos simples de M. Por lo tanto, $N' = 0$ y $M = N$, es decir M es la suma de sus submódulos simples.

Más aún, si M es una suma no vacía de submódulos simples $\sum_{i\in Z} S_i$, entonces existe un subconjunto $Z' \subseteq Z$ tal que $M = \bigoplus_{i\in Z'} S_i$. En efecto, se observa que el conjunto

$$T = \left\{ W \subseteq Z \mid \sum_{i\in W} S_i = \bigoplus_{i\in W} S_i \right\}$$

no es vacío ya que $\{i\} \in T$ para todo $i \in Z$; y si se toma una cadena $B = (W_i)_{i\in X}$ en T, entonces $W = \bigcup_{i\in X} W_i$ es una cota superior de la cadena, ya que si se supone que $W \notin T$, existe $i \in W$, con $i \in W_h$ para algún $h \in X$, tal que se puede encontrar

$$m \in S_i \cap \bigoplus_{j\in W\setminus\{i\}} S_j$$

no nulo, y debido a que B es una cadena existe $k \in X$ tal que $m \in \bigoplus_{j \in W_k} S_j$; pero entonces

$$S_i = mA \subseteq \bigoplus_{j \in W_k} S_j,$$

lo cual es una contradicción ya que la suma $\sum_{j \in W_m} S_j$, donde $m = max\{k, h\}$, es una suma directa que contiene como sumandos tanto a S_i como a $\bigoplus_{j \in W_k} S_j$. Se sigue entonces del lema de Zorn que T tiene un elemento maximal Z', el cual cumple que $M = \bigoplus_{i \in Z'} S_i$, ya que si se supone que $M \neq \bigoplus_{i \in Z'} S_i$, entonces existe $j \in Z$ tal que $S_j \nsubseteq \bigoplus_{i \in Z'} S_i$, pero como S_j es simple

$$S_j \cap \bigoplus_{i \in Z'} S_i = 0,$$

lo que implica que $Z' \cup \{j\} \in T$, lo cual es una contradicción. Por lo tanto $M = \bigoplus_{i \in Z'} S_i$.

Por lo tanto, todo módulo semisimple es una suma directa de módulos simples. Y recíprocamente toda suma directa de módulos simples es un módulo semisimple. En efecto, si M es una suma directa de simples $\bigoplus_{i \in Z} S_i$, entonces dado un submódulo N se considera el conjunto X de subconjuntos Y de Z tales que

$$N \cap \bigoplus_{i \in Y} S_i = 0.$$

X no es vacío pues contiene al conjunto vacío, y es un conjunto parcialmente ordenado con la contención. Además, si $(Y_{i \in E})_E$ es una cadena entonces $\Psi = \bigcup_{i \in E} Y_i$ es una cota superior de ésta. Ciertamente, $Y_i \subseteq \Psi$ para toda $j \in E$, y si $x \in N \cap \bigoplus_{i \in \Psi} S_i$, entonces existe $j \in E$ tal que $x \in N \cap \bigoplus_{i \in Y_j} S_i = 0$; por lo tanto $N \cap \bigoplus_{i \in \Psi} S_i = 0$, y entonces $\Psi \in X$. De esta manera, el lema de Zorn implica que X tiene un elemento maximal W, con el cual

$$M = N \oplus \bigoplus_{i \in W} S_i,$$

ya que si S_j no está contenido en $N \oplus \bigoplus_{i \in W} S_i$, entonces $S_j \cap N \oplus \bigoplus_{i \in W} S_i = 0$, de manera que $W \cup \{j\}$ pertenece a X, lo cual contradice la maximalidad de W. Por lo tanto $S_j \subseteq N \oplus \bigoplus_{i \in W} S_i$, y así

$$\bigoplus_{i \in Z} S_i = M = N \oplus \bigoplus_{i \in W} S_i.$$

Por lo tanto, si M es una suma directa de simples, entonces M es semisimple.

Se tiene entonces la siguiente caracterización de los módulos semisimples.

Proposición 3.14. *Sea M un A-módulo. Los siguientes enunciados son equivalentes:*

(a) *M es semisimple.*

(b) *M es igual a la suma de sus submódulos simples.*

(c) *M es igual a una suma directa de módulos simples.*

Ejemplo 3.15. Sea X el conjunto de los enteros primos. Los módulos maximales de $\mathbb{Z}$ son de la forma $p\mathbb{Z}$ con $p \in X$, por lo que los módulos simples sobre $\mathbb{Z}$ son de la forma $\mathbb{Z}_p$ con $p \in X$. Por lo tanto, los módulos semisimples sobre $\mathbb{Z}$ son de la forma

$$\bigoplus_{p \in Y} \mathbb{Z}_p^{(X_p)},$$

donde Y es un subconjunto de X y X_p es un cardinal.

Como corolario de la Proposición 3.14 se tiene que una suma directa de módulos da como resultado un módulo semisimple si y sólo si cada sumando es semisimple. En efecto, si se tiene una familia de módulos semisimples $\{M_i\}_{i \in I}$, entonces al ser cada M_i igual a una suma de submódulos simples, $\bigoplus_{i \in I} M_i$ es igual a una suma de submódulos simples. Recíprocamente, si M es semisimple, entonces todo M_i es semisimple por la Proposición 3.5.

Corolario 3.16. *Dada una familia de módulos $\{M_i\}_{i \in I}$, el módulo $\bigoplus_{i \in I} M_i$ es semisimple si y sólo si M_i es semisimple para toda $i \in \{1, ..., n\}$.*

Sin embargo, si se tiene una familia infinita de módulos semisimples, el producto no tiene que ser semisimple como muestra el siguiente ejemplo.

Ejemplo 3.17. Si X es el conjunto de todos los enteros primos, entonces $M = \prod_{p \in X} \mathbb{Z}_p$ no es semisimple. En efecto, la función $f : \mathbb{Z} \to M$ definida como $f(m) = (m + p\mathbb{Z})_{p \in X}$ es un monomorfismo, pues $f(m) = 0$ si y sólo si $m + p\mathbb{Z} = 0$ para todo $p \in X$, es decir si y sólo si todo primo divide a m, lo cual sólo ocurre si $m = 0$. De manera que si se supone M semisimple, la Proposición 3.5 implica que $\mathbb{Z}$ es semisimple, lo cual es una contradicción.

3.2. Anillos Semisimples

Si A es un anillo tal que A_A es semisimple se tiene una gran cantidad de información tanto de su estructura como de sus módulos, el siguiente teorema reúne los resultados más inmediatos sobre sus módulos.

Teorema 3.18. *Para un anillo A los siguientes enunciados son equivalentes:*

(a) *Toda sucesión exacta corta de A-módulos se escinde.*

(b) *Todo A-módulo es semisimple.*

(c) *Todo A-módulo finitamente generado es semisimple.*

(d) *Todo A-módulo cíclico es semisimple.*

(e) A_A *es semisimple.*

(f) *Todo A-módulo es inyectivo.*

(g) *Todo A-módulo es proyectivo.*

(h) *Todo A-módulo finitamente generado es proyectivo.*

(i) *Todo A-módulo cíclico es proyectivo.*

(j) *Todo ideal derecho de A es generado por un elemento idempotente.*

Demostración. $(a \Leftrightarrow b)$ Se sigue de la Proposición 3.13.

$(b \Rightarrow c \Rightarrow d \Rightarrow e)$ Es trivial.

$(e \Rightarrow b)$ Dado un A-módulo M, por la Proposición 3.5 mA es semisimple para toda $m \in M$, y entonces $M = \sum_{m \in M} mA$ es una suma de simples por la Proposición 3.14, por lo que M es semisimple.

$(a \Leftrightarrow f)$ Basta recordar que M es inyectivo si y sólo si toda sucesión de la forma $0 \to M \to N \to N' \to 0$ se escinde. Así, si toda sucesión exacta se escinde, en particular para un módulo M toda sucesión exacta $0 \to M \to N \to N' \to 0$ se escinde, lo que implica que M es inyectivo. Recíprocamente, si todo módulo es inyectivo, entonces toda sucesión exacta $0 \to M \to N \to N' \to 0$ se escinde debido a que M es inyectivo.

$(g \Rightarrow h \Rightarrow i)$ Es trivial.

$(a \Leftrightarrow g)$ Análogo a $(a \Leftrightarrow f)$.

$(i \Rightarrow d)$ Sea M cíclico, dado N un submódulo de M, M/N también es cíclico y entonces proyectivo por hipótesis, lo que implica que la sucesión $0 \to N \to M \to M/N \to 0$ se escinde. Por lo tanto todo submódulo de M es sumando directo, es decir M es semisimple.

$(e \Leftrightarrow j)$ A_A es semisimple si y sólo si todo ideal derecho de A es sumando directo de A si y sólo si todo ideal derecho es generado por un idempotente por la Proposición 2.21. □

Ejemplo 3.19. Sea $\mathcal{C}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ es continua}\}$. Es sencillo probar que $\mathcal{C}(\mathbb{R})$ es un anillo bajo la suma y producto de funciones. Se le llama el anillo de funciones continuas reales. Para probar que A_A no es semisimple hay que notar que $f \in A$ es idempotente si y sólo si $f(x) = f(x)f(x)$ lo que implica que $f(x) = 0$ ó $f(x) = 1$ para toda $x \in \mathbb{R}$, y como f es continua se tiene entonces que f es la función constante 0 ó 1, por lo que la unidad de A no tiene descomposiciones no triviales. Así, debido a que toda descomposición de A_A induce una descomposición de la unidad de A, A_A no puede ser semisimple, a menos que A_A sea simple. Pero esto último no sucede, ya que si $g(x) = x$, entonces es sencillo probar que gA es un submódulo propio de A_A. Por lo tanto A_A no es semisimple.

Ejemplo 3.20. Si D es un anillo con división y $n \in \mathbb{N}$, entonces $A = \mathbb{M}_n(D)$ es un anillo tal que A_A es semisimple. En efecto, sea e_i la matriz cuyas entradas son todas igual a cero, con excepción de la entrada de la i-ésima columna e i-ésimo renglón, la cual es igual a 1. Así, $1 = e_1 + ... + e_n$ es una descomposición de la unidad, que induce una descomposición $A_A = e_1 A \oplus ... \oplus e_n A$ donde cada $e_i A$ es simple. En efecto, sea $x \in e_i A$ diferente de 0 se tiene entonces que $xe_j \neq 0$ para algún $j \in \{1, ..., n\}$, por lo que $xe_j u e_i \alpha^{-1} = e_i$, donde u es la matriz que todas sus entradas son igual a 1_D y α es la entrada del i-ésimo renglón y j-ésima columna, la cual es diferente de 0 porque $xe_j \neq 0$. Por lo tanto, $e_i A$ es simple para todo $i \in \{1, ..., n\}$ y entonces A_A es semisimple.

Corolario 3.21. *Sea A un anillo. Si A_A es semisimple, entonces todo A-módulo simple es isomorfo a un sumando directo de A_A.*

Demostración. Sea S un A-módulo simple, por la Proposición 3.9 existe un epimorfismo $f : A \to S$ no nulo. Luego, debido a que A_A es semisimple, toda sucesión exacta corta se escinde, en particular $0 \to \mathrm{Ker}(f) \to A \to S \to 0$ se escinde, lo que implica que S es isomorfo a un sumando directo de A_A. □

Ahora, se ha visto que un módulo semisimple es suma directa de sus submódulos simples, suma que en general es infinita. Sin embargo, por la Proposición 2.21 se tiene que un anillo A tal que A_A es semisimple se descompone como una suma directa finita de módulos simples.

Proposición 3.22. *Sea A un anillo. Si A_A es semisimple, entonces es una suma directa finita de módulos simples.*

Como corolario, se tiene que si A_A es semisimple, entonces existe un número finito de clases de isomorfismo de módulos simples. Ya que si S es un A-módulo simple, entonces por el Corolario 3.21 S es isomorfo a un sumando directo de A_A, pero por la proposición anterior sólo existe un número finito de sumandos directos.

Corolario 3.23. *Sea A un anillo. Si A_A es semisimple, entonces contiene un número finito de submódulos simples. Más aún, existe un número finito de clases de isomorfismo de A-módulos simples.*

Ejemplo 3.24. Sean X el conjunto de los enteros primos, $A = \prod_{p \in X} \mathbb{Z}_p$ y $e_q = 1_{\mathbb{Z}_q}$ para todo $q \in X$. Claramente $e_q A \cong \mathbb{Z}_q$, por lo que A tiene tantos submódulos simples como primos. El resultado anterior implica que A_A no es semisimple.

Ejemplo 3.25. $\mathbb{Q}$ es un campo, por lo que toda sucesión exacta corta de $\mathbb{Q}$-módulos se escinde, por lo tanto $\mathbb{Q}_{\mathbb{Q}}$ es semisimple. Por otro lado, $\mathbb{Z}$ es subanillo de $\mathbb{Q}$, y $\mathbb{Z}_{\mathbb{Z}}$ no es semisimple pues ningún submódulo es sumando directo de éste. Esto es un ejemplo de un anillo que es un módulo semisimple con un subanillo que no lo es. Esto no debe sugerir que todo anillo es isomorfo a un subanillo de un anillo semisimple. Como contraejemplo supóngase que existe un anillo B tal que B_B es semisimple y que tiene un subanillo isomorfo a $A = \prod_{p\in X} \mathbb{Z}_p$. Procediendo análogamente al ejemplo anterior, se tiene un conjunto de idempotentes ortogonales dos a dos $\{e_p\}_{p\in X}$, con los que se construye la familia de submódulos $\{e_pB\}_{p\in X}$. Luego, debido a que los submódulos de dicha familia son todos diferentes y su intersección es 0 y a que B_B es semisimple, se concluye que todo e_pB es semisimple, y como tal contiene un submódulo simple. Por lo tanto, B_B tiene una infinidad de submódulos simples, lo cual es una contradicción por el Corolario 3.23.

Para concluir esta sección se presenta el teorema de Maschke, que caracteriza una clase de anillos semisimples.

Teorema 3.26. *Sea G un grupo finito de orden m y k un campo de característica p. El anillo de grupo $B = kG$ es un B-módulo derecho semisimple, si y sólo si p no divide a m.*

Demostración. Recuérdese que los elementos de kG son de la forma $\sum_{g\in G} g\lambda_g$, y para simplificar la notación se suprime el subíndice de la suma cuando no cause confusión, expresando a los elementos como $\sum g\lambda_g$.

Ahora, es evidente que k es un B-módulo derecho, ya que si se define la función $\phi : B \to \mathrm{End}(k)$ como $\phi(\sum g\lambda_g) = \sum \Lambda_g$, donde $\Lambda_g : k \to k$ definido como $\Lambda_g(x) = x\lambda_g$ es un endomorfismo de grupo de k. Es sencillo probar que ϕ es un morfismo de anillos, por lo que k es un B-módulo derecho gracias a la Proposición 1.3.

Luego, si B es semisimple y se supone que p divide a m, es decir $mx = 0$ para todo $x \in k$. Considérese el B-monomorfismo $f : k \to B$ definido como $f(x) = \sum gx$. Como B es semisimple, la sucesión exacta inducida se escinde, es decir existe un morfismo $h : B \to k$ tal que $hf = 1_k$. En consecuencia, para toda $x \in k$ se tiene que

$$x = hf(x) = h(\sum gx) = \sum h(gx) = \sum h(1)gx = \sum h(1)x = mx = 0,$$

lo cual es una contradicción. Por lo tanto p no divide a m.

Por otro lado, si p no divide a m, entonces para probar que B_B es semisimple basta probar que todo B-módulo es semisimple por la proposición anterior. Sea entonces M un B-módulo arbitrario y N un submódulo de éste. Debido a que B es una k-álgebra, M es un k-espacio vectorial y N es un subespacio de éste, por lo que existe un k-morfismo $f : M \to N$ tal que $f|_N = 1_N$, ya que todo espacio vectorial es semisimple.

Ahora, se define el B-morfismo $h : M \to M$ como

$$h(x) = \sum_{g\in G} f(xg)g^{-1}m^{-1}.$$

Es evidente que la imagen de este morfismo está contenida en N por cómo está definido f, y si $x \in N$ se tiene que $h(x) = \sum xgg^{-1}m^{-1} = x$. Por lo tanto $g : M \to N$ es un epimorfismo tal que $g|_N = 1_N$, lo que implica que N es un sumando directo de M. Por lo tanto todo módulo es semisimple. $\square$

Ejemplo 3.27. Para todo $n \in \mathbb{N}$ el anillo de grupo $\mathbb{Z}_2 S_n$ no es semisimple. En efecto, el orden de S_n es $n!$, por lo que la característica de $\mathbb{Z}_2$ siempre lo divide. Mas aún $\mathbb{Z}_p S_n$ es semisimple para todo primo p mayor a n, ya que de esta manera p no divide a $n!$.

3.2.1. El Teorema de Wedderburn-Artin

Supóngase que A es un anillo tal que A_A es semisimple, de manera que $A_A = \bigoplus_{S \in X} S_A$ donde X es un subconjunto del conjunto de todos los submódulos simples de A_A por la Proposición 3.14. Por la Proposición 2.21 existe una descomposición de la unidad $1_A = e_1 + ... + e_n$ donde $e_i \in S_i$ para algún $S_i \in X$, y $S_i = e_i A$. Por lo tanto $A = e_1 A \oplus ... \oplus e_n A = S_1 \oplus ... \oplus S_n$.

Luego, $X = \{e_1, ..., e_n\}$ es un sistema completo de idempotentes ortogonales primitivos, ya que $1 = e_1 + ... + e_n$ es una descomposición de la unidad y $e_i A$ es simple y en consecuencia inescindible, por lo que cada e_i es un idempotente primitivo.

De manera que por la Proposición 2.58 se puede construir una descomposición central de la unidad $1 = f_1 + ... + f_k$ tal que cada $f_i A f_i$ es un anillo conexo.

Más aún, recuérdese que dicha descomposición se construye definiendo una relación de equivalencia en X, definida como $e_i \approx e_j$ si y sólo si existe $\{g_1, ..., g_s\} \subseteq S$ tal que $e_i \sim g_1 \sim g_2 \sim ... \sim g_s \sim e_j$, donde $e \sim f$ si $eAf \neq 0$ ó $fAe \neq 0$, lo que es equivalente a que $\mathrm{Hom}_A(fA, eA) \neq 0$ ó $\mathrm{Hom}_A(eA, fA) \neq 0$, pero fA y eA son simples, por lo que el lema de Schur implica que $e_i \approx e_j$ si y sólo si $e_i A \cong e_j A$.

Además, dicha relación induce una partición $X = E_1 \cup ... \cup E_k$ y se definen $f_i = \sum_{e \in E_i} e$, por lo que $f_i A f_i \cong \mathbb{M}_{m_i}(D_i)$ por la Proposición 2.26 donde $m_i = |E_i|$ y $D_i = \mathrm{End}_A(eA)$ para algún $e \in E_i$.

En consecuencia, por la discusión anterior y por el Corolario 3.23, se tiene el teorema de Wedderburn-Artin.

Teorema 3.28. *Sea A un anillo. Si A_A es semisimple, y $S_1, ..., S_k$ son representantes de las clases de isomorfismo de los submódulos simples de A y $m_1, ..., m_k$ son sus respectivas multiplicidades como sumandos de A_A, entonces existe un isomorfismo de anillos*

$$A \cong \mathbb{M}_{m_1}(D_1) \oplus ... \oplus \mathbb{M}_{m_k}(D_k),$$

donde $D_i = \mathrm{End}_A(S_i)$.

Demostración. Tomando la descomposición central de la unidad $1_A = f_1 + ... + f_k$ se tiene que

$$A = f_1Af_1 \oplus ... \oplus f_kAf_k,$$

y para todo $i \in \{1, ..., k\}$

$$f_iAf_i = \mathrm{End}_A(f_iA) = \mathrm{End}_A(\bigoplus_{j\in E_i} e_jA) \cong \mathrm{End}_A(S_i^{m_i}) \cong \mathbb{M}_{m_i}(D_i),$$

donde $D_i = \mathrm{End}_A(S_i)$ ya que $e_jA \cong S_i$ para todo $j \in E_i$. □

Corolario 3.29. *Sea A un anillo. A_A es semisimple si y sólo si A es isomorfo a un producto de anillos de matrices sobre anillos con división.*

Demostración. Se sigue de 3.20 que un producto de anillos de matrices sobre anillos con división es un anillo semisimple. El recíproco se sigue del teorema de Wedderburn-Artin. □

Observación 3.30. Como es natural se puede puede probar de que un anillo A es isomorfo a un producto de anillos de matrices sobre anillos con división si y sólo si $_AA$ es semisimple. Esto lleva a la conclusión de que A_A es semisimple si y sólo si $_AA$ es semisimple. Por lo tanto de ahora en adelante a dichos anillos se les llamará semisimples.

Definición 3.31. Se dice que un anillo A es semisimple si A_A es semisimple, ó equivalentemente, si $_AA$ es semisimple.

Para finalizar, supóngase que e es un idempotente de un anillo semisimple A, entonces $A \cong S_1^{n_1} \oplus ... \oplus S_k^{n_k}$ con S_i simple y

$$eA \oplus (1-e)A = A \cong S_1^{n_1} \oplus ... \oplus S_k^{n_k},$$

entonces del teorema de Wedderburn-Artin se deduce que

$$eA \cong S_1^{m_1} \oplus ... \oplus S_k^{m_k}$$

con $m_i \leq n_i$ para toda i. Y análogamente a la argumentación anterior

$$eAe \cong \mathrm{End}_A(eA) \cong \bigoplus_{i,j=1}^{k} \mathrm{Hom}_A(S_i^{m_i}, S_j^{m_j}) \cong \mathbb{M}_{m_1}(D_1) \oplus ... \oplus \mathbb{M}_{m_k}(D_k),$$

donde $D_i = \mathrm{End}_A(S_i)$.

En particular, si eAe es un anillo con división, entonces eA es un sumando simple de A, ya que de suponer lo contrario, eAe debe un anillo de matrices sobre un anillo con división, ó una suma directa finita no trivial de anillos sobre matrices, en cualquier caso eAe no puede ser un anillo con división. Así, se tiene el siguiente corolario.

Corolario 3.32. *Sea A un anillo semisimple y e un idempotente de A. El anillo eAe es isomorfo a una suma finita de anillos de matrices sobre anillos con división. Más aún, si eAe es un anillo con división, entonces eA es simple.*

Ejemplo 3.33. Sea k un campo algebraicamente cerrado. Si A es una k-álgebra de dimensión finita tal que A es un anillo con división entonces $A = k$. En efecto, si $\dim_k A = n$, entonces para todo $a \in A$ se tiene que $1, a, ..., a^n$ son linealmente dependientes, por lo que existe una combinación lineal $\sum_{i=0}^{n} \lambda_i a^i = \sum_{i=0}^{m} \lambda_i a^i = 0$ con $\lambda_m \neq 0$. Pero como k es algebraicamente cerrado

$$\sum_{i=0}^{m} \lambda_i x^i = \lambda_n (x - b_1)...(x - b_m),$$

lo que implica que $0 = \lambda_m(a-b_1)...(a-b_m)$ y entonces $a-b_i = 0$ para algún i ya que A es un anillo con división. Por lo tanto $A = k$. De manera que si B es una k-álgebra de dimensión finita semisimple y k es un campo algebraicamente cerrado, B es isomorfa a un producto de anillos de matrices sobre k.

3.3. Anillos Simples

Se probó en la sección anterior que todo anillo semisimple se puede descomponer como una suma directa finita de anillos de matrices sobre anillos con división. Esta subsección estudia y caracteriza dichos anillos de matrices.

Considérese un anillo $B = \mathbb{M}_n(D)$, donde D es un anillo con división. Los ideales bilaterales de B son de la forma $\mathbb{M}_n(I)$ donde I es un ideal bilateral de D, pero como D es un anillo con división $I = D$ ó $I = 0$, por lo que B no tiene ideales bilaterales propios. Un anillo que cumpla esto se llama anillo simple.

Definición 3.34. Sea A un anillo. Se dice que un anillo es simple si no tiene ideales bilaterales diferentes de 0 y A.

Por lo tanto, se ha mostrado que un anillo A tal que A_A es semisimple se puede expresar como un producto finito de anillos simples. El recíproco es falso como se verá más adelante. Pero antes considérense los siguientes ejemplos de anillos simples.

Ejemplo 3.35. Ya se ha probado que si D es un anillo con división, entonces cualquier anillo de matrices de orden finito con coeficientes en D es un anillo simple. De la misma manera, cualquier anillo de matrices de orden finito sobre un anillo simple es simple.

Ejemplo 3.36. Si $(A_i)_{i\in\mathbb{N}}$ es una cadena ascendente de anillos con división, entonces $B = \bigcup_{i\in\mathbb{N}} A_i$ es un anillo simple. En efecto, supóngase que I es un ideal bilateral de B que contiene un elemento x distinto de 0; entonces $x \in A_n$ para algún $k \in \mathbb{N}$, pero A_n es un anillo con división, por lo que existe $y \in A_n$ tal que $xy = yx = 1$, y así $I = B$.

Ejemplo 3.37. Sea $A_0 = D$ un anillo con división. Se sabe entonces que todo anillo de matrices sobre D es un anillo simple. Considérense entonces los anillos simples $A_k = \mathbb{M}_{2^k}(D)$. Cada A_k se puede identificar con un subanillo de A_{k+1} con ayuda del monomorfismo de anillos $f_k : A_k \to A_{k+1}$ definido como

$$f_k(M) = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}.$$

De esta manera se tiene una sucesión de anillos simples $(A_i)_{i\in\mathbb{N}}$ tales que $A_k \subseteq A_{k+1}$. Así, $B = \bigcup_{i\in\mathbb{N}} A_i$ es un anillo simple.

Ejemplo 3.38. Sea $M = k^{(\mathbb{N})}$, donde k es un anillo con división. M es un espacio vectorial sobre k con base $\{e_i\}_{i\in\mathbb{N}}$. Se dice que un morfismo tiene rango finito ó infinito si la dimensión de su imagen es finita ó infinita respectivamente. Es evidente que el conjunto de todos los morfismos de rango finito es un ideal I de $\mathrm{End}_k(M)$. Y si se supone que J es un ideal bilateral que contiene un morfismo g de rango infinito, entonces $M = N \oplus \mathrm{Ker}(g)$ y $N \cong \mathrm{Im}(g)$ tiene una base $\{u_i\}_{i\in\mathbb{N}}$, defínanse entonces $f : M \to M$ y $h : M \to M$ como $h(e_i) = u_i$ y $f = f|_N + f|_{\mathrm{Ker}(g)}$ donde $f|_N(u_i) = e_i$ y $f|_{\mathrm{Ker}(g)}(x) = (x)$, entonces se tiene que $fgh = 1$, lo que implica que $J = A$. En consecuencia, A/I es un anillo simple, ya que no existen ideales bilaterales de A que contengan a I.

Como se puede observar en los ejemplos, en general la estructura de módulo de un anillo simple puede ser complicada, pero por ahora los anillos simples de interés son aquellos que son módulos semisimples, que se caracterizan de manera sencilla. Para ello considérese el siguiente teorema de M. Reiffel.

Teorema 3.39. *Sea A un anillo simple. Si I es un ideal derecho, entonces A es isomorfo a $B = \mathrm{End}_D({}_DI)$, donde $D = \mathrm{End}_A(I_A)$.*

Demostración. Sea A un anillo simple e I un ideal derecho de A. Defínase $f : A \to B$ como $f(a) = f_a$ donde $f_a(x) = xa$. f es un monomorfismo pues $\mathrm{Ker}(f)$ es un ideal bilateral, lo que implica que $\mathrm{Ker}(f) = A$ ó $\mathrm{Ker}(f) = 0$, pero f no es el morfismo 0, por lo tanto $\mathrm{Ker}(f) = 0$.

Para probar que f es epimorfismo basta mostrar que $f(A)$ es un ideal izquierdo de B ya que $f(1) = 1_B$. Para ello nótese que dado $h \in B$ y $a \in A$ se tiene que

$$hf(a)(x) = h(xa) = xh(a) = f(h(a))(x),$$

por lo tanto $Bf(A) \subseteq f(A)$. Y así, $f(A)$ es un ideal derecho. $\square$

Ya con este teorema se observa que si A es un anillo simple que es semisimple, entonces contiene un ideal derecho minimal por la Proposición 3.8. Y recíprocamente, si A es un anillo que contiene un ideal derecho minimal I, entonces por el teorema anterior $A \cong \mathrm{End}_D(I)$ con $D = \mathrm{End}_A(I)$.

Luego, como D es un anillo con división, ${}_DI$ es un espacio vectorial sobre éste. Si ${}_DI$ es de dimensión finita, $\mathrm{End}_D(I)$ es un anillo de matrices de orden finito, y por lo tanto semisimple por 3.20. Y si se tuviera el caso que ${}_DI$ es de dimensión infinita, entonces procediendo análogamente a 3.38 se tiene que $\mathrm{End}_D(I) \cong A$ tiene un ideal bilateral propio, lo cual es una contradicción. Por lo tanto A_A es semisimple.

Corolario 3.40. *Sea A un anillo simple. El módulo A_A es semisimple si y sólo si tiene un ideal derecho minimal.*

Ahora, si A es un anillo simple semisimple, entonces todos los ideales minimales derechos son isomorfos. En efecto, si se supone lo contrario el teorema de Wedderburn-Artin implica que A es isomorfo a un producto no trivial de anillos, por lo que A es una suma directa no trivial de ideales bilaterales, lo cual es una contradicción ya que A es simple.

Luego entonces el teorema de Wedderburn-Artin implica que A es isomorfo a un anillo de matrices sobre $\mathrm{End}_A(I)$, donde I es un ideal derecho mínimo de A. Por lo que se tiene el siguiente corolario.

Corolario 3.41. *Sea A un anillo simple semisimple. Se cumplen los siguientes enunciados.*

(a) *Todos los ideales minimales derechos de A son isomorfos.*

(b) $A \cong \mathbb{M}_n(\mathrm{End}_A(I))$ *donde I es un ideal minimal de A y n es el número de ideales minimales de A.*

(c) *B es un anillo simple semisimple si y sólo si B es isomorfo a un anillo de matrices de $n \times n$ sobre un anillo con división para algún $n \in \mathbb{N}$.*

4. Condiciones de Finitud

En la sección anterior se vio que un anillo simple es un módulo derecho semisimple en caso de tener un ideal minimal derecho. En esta sección se buscarán condiciones suficientes para que toda familia de ideales derechos tenga un mínimo ó un máximo.

Los anillos que cumplen dichas condiciones reciben el nombre de artinianos ó noetherianos respectivamente. Sus epónimos fueron los matemáticos Emil Artin y Emmy Noether cuyo trabajo fue fundamental en el desarrollo de dichos conceptos.

Con el objetivo de estudiar dichos anillos se inicia el capítulo definiendo los módulos artinianos y noetherianos, para después estudiar los anillos de endomorfismos sobre éstos, una vez hecho esto se definen y caracterizan los anillos noetherianos y artinianos. Se finaliza el capítulo con el estudio de módulos de longitud finita, que se caracterizan por ser módulos artinianos y noetherianos simultáneamente.

4.1. Módulos Artinianos y Noetherianos

Definición 4.1. Dado un anillo A y un A-módulo M, una cadena ascendente de M es una sucesión $(M_i)_{i\in\mathbb{N}}$ de submódulos de M, tales que $M_i \subseteq M_{i+1}$ para todo $i \in \mathbb{N}$, mientras que una cadena descendente de M es una sucesión $(M_i)_{i\in\mathbb{N}}$ de submódulos de M, tales que $M_i \supseteq M_{i+1}$ para todo natural i.

Cuando todos los elementos de una cadena son distintos se dice que la cadena es estricta. Y se dice que una cadena $(M_i)_{i\in\mathbb{N}}$ se estaciona si existe un natural m tal que $M_i = M_m$ para todo $i \geq m$.

En la teoría de módulos surgen naturalmente construcciones con cadenas de submódulos, que por lo general no se estacionan. Sin embargo, existen módulos que cumplen la condición de que todas las cadenas se estacionan, lo que implica que toda construcción hecha con cadenas sea finita, lo que hace a estos módulos más manejables. En esta sección se estudian las clases de dichos módulos y sus propiedades.

Definición 4.2. Dado A un anillo. Se dice que un A-módulo M es artiniano si toda cadena descendente de M se estaciona.

Análogamente, si toda cadena ascendente de M se estaciona se dice que M es noetheriano.

Ejemplo 4.3. Todo espacio vectorial de dimensión finita es un módulo noetheriano y artiniano. Esto se sigue del hecho de que una cadena de subespacios induce una sucesión de naturales por medio de sus dimensiones, y como dichas dimensiones están acotadas la cadena se estaciona forzosamente.

Ejemplo 4.4. Todo módulo simple no tiene mas que cadenas triviales, por lo que todo módulo simple es artiniano y noetheriano.

Las siguientes proposiciones caracterizan estos módulos.

Proposición 4.5. *Sea M un módulo. Los siguientes enunciados son equivalentes:*

(a) *M es noetheriano.*

(b) *Todo conjunto no vacío de submódulos de M tiene un elemento maximal.*

(c) *Todo submódulo es finitamente generado.*

(d) *Para toda familia X de submódulos de M existe una subfamilia finita X' de X tal que $\sum_{N\in X'} N = \sum_{N\in X} N$.*

(e) *Si $(M_i)_{i\in X}$ es una familia de submódulos tal que $M_i \subseteq M_j$ ó $M_j \subseteq M_i$ para cualesquiera $i, j \in X$, entonces existe $m \in X$ tal que $M_h \subseteq M_m$ para toda $h \in X$.*

Demostración. $(a \Rightarrow b)$ Sea X un conjunto no vacío de submódulos y supóngase que no tiene elementos maximales, entonces como X es no vacío existe un submódulo $N_1 \in X$; y debido a que N_1 no es maximal existe $N_2 \in X$ tal que $N_1 \subsetneq N_2$; procediendo recursivamente, como N_k no es maximal existe $N_{k+1} \in X$ tal que $N_k \subsetneq N_{k+1}$. De esta manera, se obtiene una cadena $(N_k)_{k\in\mathbb{N}}$ estrictamente ascendente, lo cual es una contradicción pues M es noetheriano. Por lo tanto, X tiene un elemento maximal.

$(b \Rightarrow c)$ Sea M' un submódulo de M y X una familia de submódulos de M' tal que $\sum_{N\in X} N = M'$. Considérese

$$Y = \left\{ \sum_{N\in Z} N \quad | \quad Z \subseteq X \text{ finito} \right\},$$

este es un conjunto de submódulos de M, por lo que tiene un elemento maximal $V = \sum_{N\in X'} N$ para algún $X' \subseteq X$ finito. Luego, $V \subseteq \sum_{N\in X} N = M'$, por lo que si $V \neq M'$, entonces existe $N \in X$, tal que $N + V \neq V$, pero $N + V \in Y$, lo cual es una contradicción. Por lo tanto, $V = M'$ y entonces M' es finitamente generado.

$(c \Rightarrow d)$ Dada una familia X de submódulos, el submódulo $M' = \sum_{N\in X} N$ es finitamente generado, de manera que existe una subfamilia finita X' de X tal que

$$\sum_{N\in X'} N = M' = \sum_{N\in X} N.$$

$(d \Rightarrow a)$ Dada una cadena ascendente $S = (N_i)_{i\in\mathbb{N}}$ de M, existe un conjunto finito de naturales F tal que $M' = \sum_{i\in\mathbb{N}} N_i = \sum_{i\in F} N_i$. Luego, si m es el máximo de F, entonces como S es ascendente $M' = N_m = N_k$ para cualquier $k \geq m$, ya que si $k \geq m$ se tiene que $N_m \subseteq N_k \subseteq M' = N_m$, por lo que $N_m = N_k$.

$(f \Rightarrow a)$ Es trivial.

$(b \Rightarrow f)$ Es inmediato. □

Proposición 4.6. *Sea M un módulo, los siguientes enunciados son equivalentes:*

(a) *M es artiniano.*

(b) *Todo conjunto no vacío de submódulos de M tiene un elemento minimal.*

(c) *Todo cociente de M es finitamente cogenerado.*

(d) *Para toda familia X de submódulos de M existe una subfamilia finita X' de X tal que $\bigcap_{N\in X'} N = \bigcap_{N\in X} N$.*

(e) *Si $(M_i)_{i\in X}$ es una familia de submódulos tal que $M_i \subseteq M_j$ ó $M_j \subseteq M_i$ para cualesquiera $i, j \in X$, entonces existe $m \in X$ tal que $M_m \subseteq M_h$ para toda $h \in X$.*

Demostración. $(a \Rightarrow b)$ Sea X un conjunto no vacío de submódulos, y supóngase que no tiene elementos minimales, entonces como X no es vacío existe un submódulo $N_1 \in X$, y debido a que N_1 no es minimal existe $N_2 \in X$ tal que $N_2 \subsetneq N_1$, recursivamente como N_k no es minimal existe $N_{k+1} \in X$ tal que $N_{k+1} \subsetneq N_k$ para todo $k \in \mathbb{N}$, de esta manera se obtiene una cadena estrictamente descendente $(N_k)_{k\in\mathbb{N}}$, lo cual es una contradicción pues M es artiniano.

$(b \Rightarrow c)$ Sea M' un submódulo de M, dar una familia X de submódulos de M/M' tal que $\bigcap_{N\in X} N = 0$, es equivalente a dar una familia Y de submódulos de M que contengan a M' tales que $\bigcap_{N\in Y} N = M'$. Considérese

$$Z = \left\{ \bigcap_{N\in W} N \quad | \quad W \subseteq Y \text{ finito} \right\}.$$

Por (b) Z tiene un elemento minimal $V = \bigcap_{N\in Y'} N$. Luego, si $V \neq M'$, como

$$V \supseteq \bigcap_{N\in X} N = M',$$

existe $N \in X$, tal que $N \cap V \neq V$, pero $N \cap V \in Z$ lo cual es una contradicción, pues V es un elemento minimal de Z. En consecuencia, $V = M'$ y entonces se ha encontrado una subfamilia finita X' de X tal que $\bigcap_{N\in X'} N = 0$. Por lo tanto, M/M' es finitamente cogenerado.

$(c \Rightarrow d)$ Si X es una familia de submódulos de M y $M' = \bigcap_{N \in X} N$, entonces M/M' es finitamente cogenerado, lo que implica que existe una subfamilia finita X' de X tal que $\bigcap_{N \in X'} (N + M')/M' = 0$ pues $\bigcap_{N \in X} (N + M')/M' = 0$, lo que implica que $\bigcap_{N \in X'} N = M'$.

$(d \Rightarrow a)$ Dada una cadena descendente $S = (N_i)_{i \in \mathbb{N}}$ de M. Si $M' = \bigcap_{i \in \mathbb{N}} N_i$, entonces existe un conjunto finito de naturales F tal que $M' = \bigcap_{i \in F} N_i$. Luego, si m es el máximo de F, entonces $M' = N_m = N_k$ para cualquier $k \geq m$, ya que $M' = \bigcap_{i \in F} N_i = N_m$, pues la sucesión es descendente, y si $k \geq m$ se tiene que $N_m \supseteq N_k \supseteq M' = N_m$, por lo que $N_m = N_k$. Por lo tanto, cualquier cadena descendente se estaciona.

$(f \Rightarrow a)$ Es trivial.

$(b \Rightarrow f)$ Es inmediato. □

Las proposiciones anteriores implican claramente que todo módulo noetheriano es finitamente generado y que todo módulo artiniano es finitamente cogenerado, sin embargo el recíproco es falso como se muestra en los siguientes ejemplos.

Ejemplo 4.7. Sea $A = \mathbb{Z}_2[x_i]_{i \in \mathbb{N}}$ el anillo conmutativo de polinomios con variables $\{x_i\}_{i \in \mathbb{N}}$ sobre $\mathbb{Z}_2$ e I el ideal generado por $\{x_i x_j\}_{i,j \in \mathbb{N}}$. Si $B = A/I$, entonces B_B es un módulo finitamente generado no noetheriano. En efecto, el conjunto $\{N_n\}_{n \in \mathbb{N}}$, donde

$$N_n = \langle x_1 + I, ..., x_n + I \rangle ,$$

es claramente una cadena estrictamente creciente

$$N_1 \subsetneq N_2 \subsetneq ... \subsetneq N_k \subsetneq ...$$

Por lo tanto, B_B es un módulo no noetheriano pero finitamente generado, ya que 1_B lo genera.

Ejemplo 4.8. Utilizando la notación del ejemplo anterior, considérese el grupo abeliano

$$M = \mathrm{Hom}_{\mathbb{Z}_2}(B, \mathbb{Z}_2).$$

M es un B-módulo izquierdo por la Proposición 1.10 debido a que B es un $\mathbb{Z}_2$-B bimódulo. Se prueba a continuación que M es un módulo finitamente cogenerado no artiniano. Considérese $N = \{0, f\}$, donde f está definido en la base como $f(x_i + I) = 0$ para toda $i \in \mathbb{N}$ y $f(1 + I) = 1$. Claramente N es un submódulo de M. Y si se toma $g \in M$ distinto de f y 0, se tiene que existe $j \in \mathbb{N}$ tal que $g(x_j + I) = 1$; pero entonces $(x_j + I)g = f$ ya que

$$(x_j + I)g(1) = g((x_j + I)1) = 1 \text{ y}$$
$$(x_j + I)g(x_i + I) = g((x_j + I)(x_i + I)) = g((x_j x_i + I)) = g(0) = 0$$

para todo $i \in \mathbb{N}$. Lo que implica que todo submódulo de M contiene a N. Lo que implica que M es finitamente cogenerado, ya que si se tiene una cadena de submódulos $\{N_i\}_{i\in I}$ tal que $N_i \neq 0$ para toda $i \in I$, entonces $N \subseteq N_i$ para toda $i \in I$ y entonces $\bigcap_{i\in I} N_i \neq 0$. Sin embargo, M no es artiniano, para mostrarlo considérense los morfismos f_{x_i} definidos como $f_{x_i}(x_j) = \delta_{ij}$ y $f_{x_i}(1) = 0$, análogamente a lo anterior se prueba que $pf_{x_i} = f_{x_i}$, $pf_{x_i} = 0$ ó $pf_{x_i} = f$ para todo $p \in B$. Por lo tanto, la cadena

$$\langle f_{x_i}\rangle_{i\in\mathbb{N}\setminus\{1\}} \supsetneq \langle f_{x_i}\rangle_{i\in\mathbb{N}\setminus\{1,2\}} \supsetneq \cdots \supsetneq \langle f_{x_i}\rangle_{\mathbb{N}\setminus\{1,\ldots,n\}} \supsetneq \cdots$$

es estrictamente decreciente.

Por otro lado, ser artiniano ó noetheriano es cerrado bajo extensiones. Más aún, dada una sucesión exacta corta de módulos $0 \to K \to M \to N \to 0$, M es artiniano (noetheriano) si y sólo si K y N son artinianos (noetherianos).

Proposición 4.9. *Sea $0 \to K \xrightarrow{f} M \to N \to 0$ una sucesión exacta de módulos. El módulo M es artiniano (noetheriano) si y sólo si K y N también lo son.*

Demostración. Nótese que $K \cong \mathrm{Im}(f)$ que es un submódulo de M, y que $N \cong M/K$, por lo que sin pérdida de generalidad supóngase $K \subseteq M$ y $N = M/K$.

Si M es artiniano, entonces todo submódulo es artiniano, en particular K es también es artiniano, y como $N = M/K$, dado un submódulo N'/K de N, el cociente

$$N/N' \cong (M/K)\,/\,(N'/K) \cong M/N',$$

entonces por la Proposición 4.6 todo cociente es finitamente cogenerado, por lo que N es artiniano.

Si K y N son artinianos, considérese X un conjunto de submódulos de M. Por la Proposición 4.6 existen X_1 y X_2 subconjuntos finitos de X, tales que

$$\bigcap_{\tilde{N}\in X_1} \tilde{N} \cap K = \bigcap_{\tilde{N}\in X} \tilde{N} \cap K \quad \text{y} \quad \bigcap_{\tilde{N}\in X_2} (\tilde{N}+K)/K = \bigcap_{\tilde{N}\in X} (\tilde{N}+K)/K.$$

Ahora, si $X' = X_1 \cap X_2$, entonces $\bigcap_{\tilde{N}\in X'} \tilde{N} = \bigcap_{\tilde{N}\in X} \tilde{N}$; en efecto si $x \in \bigcap_{\tilde{N}\in X} \tilde{N}$, entonces $x+K \in \bigcap_{\tilde{N}\in X}(\tilde{N}+K)/K = \bigcap_{\tilde{N}\in X_2}(\tilde{N}+K)/K$, lo que implica que $x = x_1+x_2$, donde $x_1 \in K$ y $x_2 \in \bigcap_{\tilde{N}\in X_2} \tilde{N}$; pero entonces

$$x_1 \in \bigcap_{\tilde{N}\in X} \tilde{N} \cap K = \bigcap_{\tilde{N}\in X_1} \tilde{N} \cap K \subseteq \bigcap_{\tilde{N}\in X_1} \tilde{N}.$$

Por lo tanto,

$$x = x_1 + x_2 \in \bigcap_{\tilde{N}\in X_1} \tilde{N} + \bigcap_{\tilde{N}\in X_2} \tilde{N} \subseteq \bigcap_{\tilde{N}\in X'} \tilde{N},$$

y entonces $\bigcap_{\tilde{N}\in X'} \tilde{N} = \bigcap_{\tilde{N}\in X} \tilde{N}$. Por lo tanto, M es artiniano.

La prueba cuando M es noetheriano es análoga. $\square$

En particular se tiene lo siguiente. Supóngase que M_1 y M_2 son módulos, existe una sucesión exacta

$$0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0,$$

por lo que $M_1 \oplus M_2$ es artiniano, ó noetheriano, si y sólo si M_1 y M_2 son artinianos, ó noetherianos. Luego si se tienen m módulos $M_1, ..., M_m$, la sucesión

$$0 \to M_1 \to M_1 \oplus ... \oplus M_m \to M_2 \oplus ... \oplus M_m \to 0$$

es exacta, y entonces $M_1 \oplus ... \oplus M_m$ es artiniano ó noetheriano si y sólo si M_1 y $M_2 \oplus ... \oplus M_m$ son artinianos ó noetherianos respectivamente, y por inducción éste último es artiniano ó noetheriano si y sólo si M_2,...,M_{m-1} y M_m son artinianos ó noetherianos. Se tiene el siguiente corolario.

Corolario 4.10. *Un módulo que es igual a una suma directa finita de módulos es artiniano (noetheriano) si y sólo si cada sumando es artiniano (noetheriano).*

Del resultado anterior se obtiene que si se tiene un módulo semisimple $M = \bigoplus_{S\in X} S$ con todo $S \in X$ simple, entonces como todo módulo simple es artiniano y noetheriano, M es artiniano y noetheriano si X es finito.

Recíprocamente, si $M = \bigoplus_{S\in X} S$ es artiniano y se supone que X no es finito, entonces existe una sucesión $(S_i)_{i\in\mathbb{N}}$ en X con todos sus elementos diferentes, y con ella se puede construir la sucesión $(N_i)_{i\in\mathbb{N}}$ donde

$$N_n = \bigoplus_{S\in X\setminus\{S_1,...,S_n\}} S$$

que claramente es una sucesión estrictamente descendente, lo cual contradice que M es artiniano. Por lo tanto, X es finito.

Si $M = \bigoplus_{S\in X} S$ es noetheriano, entonces es finitamente generado y por lo tanto X es finito.

Se ha probado el siguiente corolario.

Corolario 4.11. *Si M es un módulo semisimple, entonces los siguientes enunciados son equivalentes:*

(a) *M es artiniano.*

(b) *M es noetheriano.*

(c) *M es suma directa finita de módulos simples.*

Ejemplo 4.12. En el ejemplo 1.34 se mostró que ${}_{\mathbb{Z}}\mathbb{Z}$ no es finitamente cogenerado, por lo que no es artiniano. Sin embargo, dada una cadena ascendente de submódulos $\{m\mathbb{Z}\}_{m\in I}$ todo $m \in I$ es divisible por todo $n \in I$ mayor a m, pero como todo entero tiene un número finito de divisores, la cadena se estaciona. Por lo tanto, $\mathbb{Z}$ es noetheriano no artiniano.

Ejemplo 4.13. El anillo $\mathbb{Q}$ es un campo, por lo que $\mathbb{Q}_{\mathbb{Q}}$ es simple y como tal noetheriano y artiniano. Por otro lado, ${}_{\mathbb{Z}}\mathbb{Z}$ es submódulo de ${}_{\mathbb{Z}}\mathbb{Q}$, por lo que ${}_{\mathbb{Z}}\mathbb{Q}$ no es artiniano, y ${}_{\mathbb{Z}}\mathbb{Q}$ no es finitamente generado, por lo que no es noetheriano. Por lo tanto, ${}_{\mathbb{Z}}\mathbb{Q}_{\mathbb{Q}}$ es artiniano y noetheriano como $\mathbb{Q}$-módulo derecho, pero no es artiniano ni noetheriano como $\mathbb{Z}$-módulo izquierdo.

Ejemplo 4.14. El módulo $\mathbb{Z}_{p^\infty} = \{\overline{\frac{m}{p^n}} \in \mathbb{Q}/\mathbb{Z} \quad | \quad m, n \in \mathbb{N}\}$ no es finitamente generado, por lo que no es noetheriano. Además, todo submódulo de $\mathbb{Z}_{p^\infty}$ es generado por un elemento de la forma $\overline{\frac{1}{p^k}}$ para algún $k \in \mathbb{N}$, por lo que si se tiene una cadena descendente, ésta se debe estacionar ya que p^k tiene un número finito de divisores. Por lo tanto, $\mathbb{Z}_{p^\infty}$ es artiniano no noetheriano.

Ejemplo 4.15. En el Ejemplo 1.37 se mostró que $\mathbb{Q}/\mathbb{Z}$ no es finitamente cogenerado ni finitamente generado, por lo que no es artiniano ni noetheriano.

4.2. Endomorfismos de módulos artinianos y noetherianos

Dado un morfismo de módulos $f : M \to M$ es sencillo probar que todo elemento en el núcleo de f pertenece también al núcleo de f^2, de hecho todo $x \in \mathrm{Ker}(f^n)$ pertenece también a $\mathrm{Ker}(f^{n+1})$ para todo $n \in \mathbb{N}$, por lo que se tiene una cadena

$$\mathrm{Ker}(f) \subseteq \mathrm{Ker}(f^2) \subseteq ... \subseteq \mathrm{Ker}(f^n) \subseteq ...$$

De la misma manera todo $x \in \mathrm{Im}(f^n)$ pertenece también a $\mathrm{Im}(f^{n-1})$ para todo natural $n > 1$, por lo que se tiene una cadena

$$\mathrm{Im}(f) \supseteq \mathrm{Im}(f^2) \supseteq ... \supseteq \mathrm{Im}(f^n) \supseteq ...$$

Por lo que es natural preguntarse que concecuencias se tienen a partir de estas cadenas si el módulo M es artiniano ó noetheriano.

Si M es artiniano y $f \in \mathrm{Hom}_A(M, M)$, entonces como se ha visto, la sucesión $(\mathrm{Im}(f^i))_{i\in\mathbb{N}}$ es descendente, por lo que existe m tal que $\mathrm{Im}(f^m) = \mathrm{Im}(f^k)$ para cualquier $k \geq m$, de manera que si $x \in M$ se tiene que $f^m(x) = f^{m+1}(x')$ para algún $x' \in M$. En consecuencia, si f es monomorfismo, se tiene que $x = f(x')$, lo que implica que $\mathrm{Im}(f) = M$. Por lo tanto, todo monomorfismo de M es un automorfismo.

Análogamente, si M es noetheriano y $f : M \to M$ es un epimorfismo, entonces la sucesión $(\mathrm{Ker}(f^i))_{i\in\mathbb{N}}$ es ascendente, por lo que existe un natural m tal que

$$\mathrm{Ker}(f^m) = \mathrm{Ker}(f^k)$$

para cualquier $k \geq m$; de manera que si $x \in \mathrm{Ker}(f)$, como f es epimorfismo, f^m también lo es, por lo que existe $x' \in M$ tal que $f^m(x') = x$; pero en tal caso

$$f^{m+1}(x') = f(x) = 0,$$

lo que implica que $x' \in \mathrm{Ker}(f^{m+1}) = \mathrm{Ker}(f^m)$ y entonces $x = 0$, por lo que f es un automorfismo.

Se tiene entonces el siguiente resultado.

Proposición 4.16. *Sea M un módulo y $f : M \to M$ un morfismo de módulos.*

(a) *Si M es artiniano, f es automorfismo si y sólo si f es monomorfismo.*

(b) *Si M es noetheriano, f es automorfismo si y sólo si f es epimorfismo.*

Cabe entonces preguntarse que propiedades cumplen los endomorfismos de un módulo artiniano y noetheriano, tal información se encuentra en el siguiente resultado, el Lema de Fitting.

Lema 4.17. *Si M es un módulo artiniano y noetheriano y $f : M \to M$ es un endomorfismo, entonces existe un natural m tal que $M = \mathrm{Im}(f^m) \oplus \mathrm{Ker}(f^m)$.*

Demostración. Debido a que el módulo M es artiniano y noetheriano las sucesiones $(\mathrm{Im}(f^i))_{i\in\mathbb{N}}$ y $(\mathrm{Ker}(f^i))_{i\in\mathbb{N}}$ se estacionan, por lo que existe un natural m tal que $\mathrm{Im}(f^m) = \mathrm{Im}(f^k)$ y $\mathrm{Ker}(f^m) = \mathrm{Ker}(f^k)$ para toda $k \geq m$. Ahora, si $x \in M$, nótese que $f^m(x) = f^{2m}(x')$ para alguna $x' \in M$, esto es $f^m(x - f^m(x')) = 0$; de modo que

$$x = f^m(x') + (x - f^m(x')) \in \mathrm{Im}(f^m) + \mathrm{Ker}(f^m),$$

y así $M = \mathrm{Im}(f^m) + \mathrm{Ker}(f^m)$. Además, si $x \in \mathrm{Im}(f^m) \cap \mathrm{Ker}(f^m)$, entonces $x = f^m(x')$ para alguna $x' \in M$, y $0 = f^m(x) = f^{2m}(x')$, lo que implica que

$$x' \in \mathrm{Ker}(f^{2m}) = \mathrm{Ker}(f^m),$$

Por lo tanto $x = 0$, y así $M = \mathrm{Im}(f^m) \oplus \mathrm{Ker}(f^m)$. $\square$

Ahora, si M es un módulo artiniano y noetheriano que además es inescindible, entonces el resultado anterior implica que todo endomorfismo es nilpotente ó invertible.

Corolario 4.18. *Dado A un anillo. Si M es un A-módulo artiniano, noetheriano e inescindible, entonces todo elemento de $\mathrm{End}_A(M)$ es invertible ó nilpotente.*

4.3. Anillos artinianos y noetherianos

Definición 4.19. Dado un anillo A, si A_A es noetheriano se dice que A es un anillo noetheriano a la derecha, si ${}_AA$ es noetheriano se dice que A es noetheriano a la izquierda, y si es noetheriano a la derecha y a la izquierda se dice que A es un anillo noetheriano. Análogamente se definen los anillos artinianos a la derecha, artinianos a la izquierda y artinianos.

Ejemplo 4.20. Si A es un anillo semisimple, entonces por 4.4 y 4.10 A es artiniano y noetheriano.

Ejemplo 4.21. Sea A un anillo simple. Si A tiene un ideal minimal derecho, entonces A es semisimple por el Corolario 3.40 y por ello artiniano y noetheriano. Por lo tanto, A es artiniano por la derecha si y sólo si A es artiniano y noetheriano.

Ejemplo 4.22. Dado un campo k se considera el anillo $A = \mathrm{End}_k(k^{\mathbb{N}})/I$ donde I es el ideal de endomorfismos de rango finito, es decir morfismos cuya imagen es de dimensión finita. Debido a que $\mathbb{N}$ tiene el mismo cardinal que $\mathbb{N}^2$, se puede tomar una base $\{e_{ij} \mid i \in \mathbb{N}, j \in \mathbb{N}\}$ de $k^{\mathbb{N}}$. Así, la familia $\{(I_n + I)/I\}_{n\in\mathbb{N}}$ es una cadena estrictamente ascendente de ideales izquierdos de A, donde

$$I_n = \{f \in \mathrm{End}_k(k^{\mathbb{N}}) \mid f(e_{ij}) = 0 \,\forall i \geq n,\, \forall j \in \mathbb{N}\}.$$

En efecto, para probarlo se toma $f \in I_{n+1}$ tal que $f(e_{nj}) = e_{nj}$ para toda $j \in \mathbb{N}$. Si se supone que $f + I \in (I_n + I)/I$, entonces $f = g + h$ con $g \in I_n$ y $h \in I$, lo que implica para toda $j \in \mathbb{N}$ que

$$e_{nj} = f(e_{nj}) = g(e_{nj}) + h(e_{nj}) = h(e_{nj}),$$

lo cual es una contradicción ya que h es de rango finito. Por lo tanto, $\{(I_n + I)/I\}_{n\in\mathbb{N}}$ es estrictamente ascendente, de manera que ${}_AA$ no es noetheriano. Además, por 3.38 se sabe que A es simple, lo que implica por el ejemplo anterior que ${}_AA$ no es artiniano.

Ejemplo 4.23. Si A es el anillo generalizado de matrices con producto trivial

$$\begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix},$$

entonces A es noetheriano por la derecha, no noetheriano por la izquierda y no artiniano por derecha ni izquierda. Para probarlo se caracterizan a continuación los ideales derechos de A. Sea I un ideal derecho, por el principio del buen orden existe un entero no negativo n tal que se puede encontrar una matriz $\begin{pmatrix} n & s \\ 0 & t \end{pmatrix} \in I$ para algún $s, t \in \mathbb{Q}$, y entonces el conjunto

$$I_n = \left\{ \begin{pmatrix} n & x \\ 0 & y \end{pmatrix} \in I \quad | \quad x, y \in \mathbb{Q} \right\}$$

es no vacío. Ahora, en caso de existir $\begin{pmatrix} n & s \\ 0 & t \end{pmatrix} \in I_n$ con $t \neq 0$,

$$\begin{pmatrix} n & st^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} n & s \\ 0 & t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & t^{-1} \end{pmatrix} \in I$$

lo que implica que

$$\begin{pmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} = \begin{pmatrix} n & st^{-1} \\ 0 & 1 \end{pmatrix} A \subseteq I.$$

Más aún, $\begin{pmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} = I$, ya que si se supone que existe un elemento $\begin{pmatrix} m & z \\ 0 & w \end{pmatrix}$ con $m \notin n\mathbb{Z}$, entonces

$$\begin{pmatrix} m\mathbb{Z} + n\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} \subseteq \begin{pmatrix} m\mathbb{Z} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} \subseteq \begin{pmatrix} m & z \\ 0 & w \end{pmatrix} A + \begin{pmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} \subseteq I,$$

pero $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ donde $d = (m, n)$ lo cual contradice la minimalidad de n. Ahora, en caso de que todo elemento de I_n sea de la forma $\begin{pmatrix} n & s \\ 0 & 0 \end{pmatrix}$, análogamente al caso anterior se prueba que

$$I = \begin{pmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & 0 \end{pmatrix}.$$

Por lo tanto, se ha probado que todo ideal derecho de A es de la forma

$$X_n = \begin{pmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & 1 \\ 0 & 0 \end{pmatrix} A \text{ ó } Y_n = \begin{pmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} = \begin{pmatrix} n & 1 \\ 0 & 1 \end{pmatrix} A.$$

De esta manera, es claro que A_A es noetheriano, pues todo submódulo de A_A es finitamente generado, y A_A no es artiniano ya que la sucesión

$$\begin{pmatrix} n!\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}_{n \in \mathbb{N}}$$

es estrictamente descendente. Por otro lado, la sucesión anterior es también una sucesión submódulos izquierdos, por lo que ${}_AA$ no es artiniano. Por otro lado, si P denota el conjunto de todos los enteros primos, entonces el conjunto

$$\begin{pmatrix} \mathbb{Z} & \sum_{p\in P} \mathbb{Z}\frac{1}{p} \\ 0 & 0 \end{pmatrix}$$

es un submódulo izquierdo de ${}_AA$ que no es finitamente generado, lo que implica que ${}_AA$ no es noetheriano.

Ejemplo 4.24. Sea B un anillo conmutativo con 1 y $S \subseteq B$ un conjunto cerrado bajo la multiplicación tal que $0 \notin S$. Si A es el anillo de fracciones de S respecto a B, y B es un anillo noetheriano, entonces A es un anillo noetheriano. En efecto, si $(I_n)_{n\in\mathbb{N}}$ es una cadena ascendente de ideales de A y $J_n = I_n \cap B$ para toda $n \in \mathbb{N}$, entonces $(J_n)_{n\in\mathbb{N}}$ es una cadena ascendente de ideales de B. Lo que implica que existe $m \in \mathbb{N}$ tal que $J_n = J_m$ para todo $n > m$ y entonces $I_n = I_m$ para todo $n \in \mathbb{N}$, ya que para todo $\alpha = \frac{a}{b} \in I_n \backslash I_m$ se tiene que $\alpha b \in J_n = J_m$ y así $\alpha \in I_m$. Análogamente se prueba que si B es artiniano, entonces A es artiniano.

Proposición 4.25. *Sea A un anillo. Son equivalentes los siguientes enunciados.*

(a) *A_A es noetheriano (artiniano).*

(b) *Todo A-módulo derecho finitamente generado es noetheriano (artiniano).*

Demostración. Sea A un anillo. Si M_A es finitamente generado, entonces por la Proposición 1.30 existe un epimorfismo $f : A^{(X)} \to M$ con X finito, de manera que

$$M_A \cong A^{(X)}/\operatorname{Ker}(f).$$

Por otro lado, si A_A es artiniano ó noetheriano, entonces por el Corolario 4.10 y la Proposición 4.9 cualquier cociente de $A^{(X)}$ es también artiniano ó noetheriano. En conclusión, M_A es artiniano ó noetheriano, según sea el caso. El recíproco es inmediato ya que A_A es finitamente generado. $\square$

Ejemplo 4.26. Sea k un anillo conmutativo con 1. Se dice que un anillo A es una k-álgebra de Artin si k es artiniano y A es un k-módulo finitamente generado. Se sigue de la proposición anterior que toda álgebra de Artin es un anillo artiniano. En efecto, si $(I_n)_{n\in\mathbb{N}}$ es una cadena de ideales de A, entonces también es una cadena de k-submódulos de A, pero A es artiniano por ser finitamente generado, de manera que la cadena se estaciona. Por lo tanto, A es artiniano. Ejemplos de álgebras de Artin son las k-álgebras de dimensión finita con k un campo.

Ejemplo 4.27. Análogamente, si un anillo A es una álgebra finitamente generada sobre un anillo conmutativo noetheriano, entonces A es noetheriano. En particular, las extensiones finitas del anillo de los enteros son noetherianas con este razonamiento. Por ejemplo, dado $f \in \mathbb{Q}[x]$ irreducible y L su campo de descomposición, entonces

$$\mathcal{O}_L = \{\alpha \in L \quad | \quad \alpha \text{ satisface un polinomio mónico en } \mathbb{Z}[x]\}$$

es una extensión finita de $\mathbb{Z}$.

Cabe señalar que si en la proposición anterior se sustituye finitamente generado por finitamente cogenerado se tiene una proposición falsa como muestran los siguientes ejemplos.

Ejemplo 4.28. $\mathbb{Z}$ es un anillo noetheriano y $\mathbb{Z}_{p^\infty}$ es finitamente cogenerado, sin embargo $\mathbb{Z}_{p^\infty}$ no es noetheriano.

Más adelante, usando el Ejemplo(4.34) se mostrará un anillo artiniano con un módulo finitamente cogenerado no artiniano y no finitamente generado.

Ahora, si M_A es un módulo finitamente generado sobre un anillo noetheriano por la derecha A, entonces M es noetheriano por lo que todo submódulo es finitamente generado. Análogamente, si M_A es un módulo finitamente generado sobre un anillo artiniano por la derecha A, entonces M es artiniano, de manera que todo cociente de M es finitamente cogenerado, en particular M es finitamente cogenerado. Se tiene entonces el siguiente corolario.

Corolario 4.29. *Sea A un anillo. Se cumplen los siguientes enunciados*

(a) *A_A es artiniano si y sólo si todo módulo finitamente generado es finitamente cogenerado.*

(b) *A_A es noetheriano si y sólo si todo submódulo de un módulo finitamente generado es finitamente generado.*

Finalmente el siguiente es un criterio para identificar anillos artinianos ó noetherianos.

Teorema 4.30. *Si A es un anillo con una descomposición de la unidad $1 = e_1 + ... + e_k$, entonces A_A es artiniano (noetheriano) si y sólo si e_iAe_j es un e_jAe_j-módulo derecho artiniano (noetheriano) para toda $i, j \in \{1, ..., k\}$. Equivalentemente, si se tiene un anillo de matrices generalizadas*

$$A = \begin{pmatrix} A_1 & M_{21} & \dots & M_{1n} \\ M_{21} & A_2 & & \\ \vdots & & \ddots & \\ M_{n1} & & & A_n \end{pmatrix},$$

entonces A es artiniano (noetheriano) a la derecha si y sólo si A_i es artiniano (noetheriano) por la derecha y M_{ij} es un A_j-módulo derecho artiniano (noetheriano) para toda $i, j \in \{1, ..., k\}$.

Demostración. Si A es noetheriano y se supone que e_jAe_k es un e_kAe_k-módulo no noetheriano, existe una cadena ascendente $(N_i)_{i\in\mathbb{N}}$ de e_kAe_k-submódulos de e_jAe_k que no se estaciona, entonces $(N_iA)_{i\in\mathbb{N}}$ es una cadena ascendente de A-submódulos de A que no se estaciona, lo cual contradice que A es noetheriano. Por lo tanto, e_jAe_k es un e_kAe_k-módulo noetheriano.

Recíprocamente, si e_jAe_k es un e_kAe_k-módulo noetheriano para toda $j,k \in \{1,...,s\}$, entonces e_lA es noetheriano para todo $l \in \{1,..,k\}$. En efecto, dado $l \in \{1,...,k\}$ y una familia X de A-submódulos de e_lA, se considera $X_i = \{Ne_i \quad | \quad N \in X\}$, ésta es una familia de e_iAe_i-submódulos de e_lAe_i, por lo que existe $X_i' \subseteq X$ finito tal que

$$\sum_{N\in X_i} N = \sum_{N\in X_i'} Ne_i$$

debido a que e_lAe_i es noetheriano. En consecuencia,

$$\sum_{N\in X} N = \sum_{N\in X}(Ne_1 \oplus ... \oplus Ne_k) = \bigoplus_{i=1}^{k}(\sum_{N\in X_i} N) = \bigoplus_{i=1}^{k}(\sum_{N\in X_i'} Ne_i).$$

Por lo tanto, si $X' = X_1' \cup ... \cup X_k'$ se tiene que $\sum_{N\in X} N = \sum_{N\in X'} N$, pues

$$\sum_{N\in X} N = \bigoplus_{i=1}^{k}(\sum_{N\in X_i'} Ne_i) \subseteq \bigoplus_{i=1}^{k}(\sum_{N\in X'} Ne_i) = \sum_{N\in X'}(\bigoplus_{i=1}^{k} Ne_i) = \sum_{N\in X'} N.$$

Se sigue de la Proposición 4.5 que e_lA es noetheriano para toda $l \in \{1,...,k\}$, lo que implica que $A = e_1A \oplus ... \oplus e_kA$ es noetheriano por el Corolario 4.10.

La prueba del teorema cuando A es artiniano se omite ya que es similar a la prueba de cuando A es noetheriano. □

Corolario 4.31. *Si A es un anillo artiniano (noetheriano), entonces $\mathbb{M}_n(A)$ es un anillo artiniano (noetheriano).*

Ejemplo 4.32. El anillo $\mathbb{M}_n(\mathbb{Z})$ es noetheriano ya que $\mathbb{Z}$ es noetheriano. Más aún, todo campo k es noetheriano y artiniano, por lo que $\mathbb{M}_n(k)$ es artiniano y noetheriano.

Corolario 4.33. *Sean A un anillo y $1 = e_1 + ... + e_s$ una descomposición de la unidad. El módulo A_A es noetheriano (artiniano) si y sólo si e_iAe_i es noetheriano (artiniano) por la derecha para toda $i \in \{1,...,s\}$ y e_jAe_k es un e_kAe_k-módulo derecho finitamente generado para toda $j,k \in \{1,...,s\}$.*

Demostración. Se sigue del Teorema 4.30 y las Proposiciones 4.25, 4.5 y 4.6. □

Con ayuda de los Teoremas 2.29 y 4.30 se tienen los siguientes ejemplos utilizando el producto trivial de matrices generalizadas 2.30.

Ejemplo 4.34. Sean $D = \mathbb{Z}(x, y)$ y $C = \mathbb{Z}(x)$. Si A es el anillo de matrices generalizadas

$$A = \begin{pmatrix} D & 0 \\ D & C \end{pmatrix} \text{ y } M = \begin{pmatrix} D & 0 \\ D & D \end{pmatrix},$$

entonces A_A es artiniano y M_A es un módulo finitamente cogenerado que no es finitamente generado ni artiniano. En efecto, D y C son campos, por lo que son artinianos y D_D es finitamente generado, por lo que el corolario anterior implica que A_A es artiniano. Luego, debido a que A es un subanillo de M se tiene que M es un A-módulo derecho. Para probar que M es finitamente cogenerado basta notar que todo elemento de M diferente de 0 es de la forma

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix},$$

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}, \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \text{ ó } \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

con $a, b, c \in D - \{0\}$; lo que implica que los submódulos cíclicos de M son de la forma

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} A = \begin{pmatrix} D & 0 \\ D & cC \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} A, \begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix} A = \begin{pmatrix} 0 & 0 \\ D & cC \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} A,$$

$$\begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 0 \\ D & 0 \end{pmatrix}, \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} A = \begin{pmatrix} D & 0 \\ D & 0 \end{pmatrix} \text{ ó } \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} A = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix};$$

utilizando lo anterior es sencillo deducir que todo submódulo no nulo de M contiene un submódulo de la forma

$$N_1 = \begin{pmatrix} 0 & 0 \\ D & 0 \end{pmatrix} \text{ ó } N_2 = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}.$$

De manera que si se tiene una familia X de submódulos de M se tienen 3 casos:

(a) Todo módulo de X contiene a N_1.

(b) Todo módulo de X contiene a N_2.

(c) Existe un módulo $L \in X$ que contiene a N_1 pero no a N_2, y un módulo $K \in X$ que contiene a N_2 pero no a N_1.

Por lo tanto, si además $\bigcap X = 0$ los casos (a) y (b) no son posibles, lo que implica que existen los módulos L y K del caso (c). Pero en tal caso, debido a que L no contiene a N_2 se deduce que todos los elementos de L son de la forma

$$\begin{pmatrix} 0 & 0 \\ d & e \end{pmatrix}$$

con $d, e \in D$, y análogamente se deduce que los elementos de K son de la forma

$$\begin{pmatrix} f & 0 \\ 0 & 0 \end{pmatrix}$$

con $f \in A$. Así, es inmediato que $M \cap N = 0$. Se ha probado que dada una familia X de submódulos de M tal que $\bigcap X = 0$, existe una subfamilia finita Y de X tal que $\bigcap Y = 0$, es decir M es finitamente cogenerado. Además, debido a que D_C no es finitamente generado, M_A no puede ser finitamente generado, y la cadena

$$M_n = \begin{pmatrix} 0 & 0 \\ D & y^n C \end{pmatrix}$$

es claramente estrictamente descendente. Por lo tanto M es un módulo finitamente cogenerado que no es finitamente generado ni artiniano.

Ejemplo 4.35. Dado un campo k, éste es artiniano y noetheriano por lo que para toda $n \in \mathbb{N}$ el anillo A es artiniano y noetheriano, donde

$$A = \begin{pmatrix} k & 0 \\ k^n & k \end{pmatrix}.$$

Ejemplo 4.36. $\mathbb{Z}$ es noetheriano no artiniano, por lo que A es noetheriano no artiniano para cualesquiera $n_{ij} \in \mathbb{N}$ con $i, j \in \{1, ..., k\}$, donde

$$A = \begin{pmatrix} \mathbb{Z} & \mathbb{Z}_{n_{12}} & \cdots & \mathbb{Z}_{n_{1k}} \\ \mathbb{Z}_{n_{21}} & \mathbb{Z} & & \vdots \\ \vdots & & \ddots & \\ \mathbb{Z}_{n_{k1}} & \cdots & & \mathbb{Z} \end{pmatrix}.$$

Ejemplo 4.37. Sean k un campo y $k[x]$ el anillo de polinomios sobre una variable. Se ha probado que k es artiniano y noetheriano y que ${}_k k[x]_{k[x]}$ es noetheriano por la derecha pero no finitamente generado por la izquierda, entonces A es noetheriano a la derecha, pero no a la izquierda.

$$A = \begin{pmatrix} k & k[x] \\ 0 & k[x] \end{pmatrix}$$

Ejemplo 4.38. Sean A un anillo artiniano (noetheriano) y S un A-módulo simple. El anillo

$$B = \begin{pmatrix} \mathrm{End}_A(S) & S \\ 0 & A \end{pmatrix}$$

es un anillo artiniano (noetheriano) pues S es finitamente generado y $\mathrm{End}_A(S)$ es un anillo con división debido a que S es simple.

4.4. Módulos de longitud finita

Esta sección tratará sobre los módulos que son tanto artinianos como noetherianos.

Si M es artiniano entonces el conjunto de todos sus submódulos distintos de 0 tiene un elemento minimal M_1. Recursivamente, el conjunto de todos los submódulos de M que contienen propiamente a M_n tiene un elemento minimal M_{n+1}. De esta manera se ha construido una cadena ascendente $(M_i)_{i\in\mathbb{N}}$ tal que M_{i+1}/M_i es simple; ciertamente, si M_{i+1}/M_i no fuera simple, entonces existiría un submódulo de M que contiene propiamente a M_i, pero que esta contenido propiamente en M_{i+1}, lo que contradice la minimalidad de M_{i+1}.

Si además M es noetheriano, entonces esta sucesión es finita y se llama una serie de composición de M.

Definición 4.39. Dado un módulo M. Se dice que una cadena finita de submódulos

$$X:\ 0 = M_0 \subseteq M_1 \subseteq ... \subseteq M_n = M \tag{4.1}$$

es una serie de composición de M de longitud n si los módulos M_{i+1}/M_i, llamados factores de composición, son simples.

Se probó que si un módulo es artiniano y noetheriano, entonces tiene una serie de composición. De hecho, un módulo tiene serie de composición si y sólo si es artiniano y noetheriano. En efecto, si M es un módulo con una serie de composición

$$X:\ 0 = M_0 \subseteq M_1 \subseteq ... \subseteq M_n = M,$$

entonces se prueba que M es artiniano y noetheriano por inducción sobre n. Si $n = 1$, entonces M es simple por lo que es artiniano y noetheriano. Tomando como hipótesis de inducción que todo módulo con una serie de composición de longitud k es artiniano y noetheriano, si $n = k + 1$ se tiene la sucesión exacta

$$0 \to M_k \to M \to M/M_k \to 0$$

donde M y M/M_k son artinianos y noetherianos, lo que implica que M es artiniano y noetheriano por la Proposición(4.9). Por lo tanto, M tiene serie de composición si y sólo si es artiniano y noetheriano.

Teorema 4.40. *Un módulo M tiene serie de composición si y sólo si M es artiniano y noetheriano.*

Corolario 4.41. *Sea M un módulo semisimple. M es de longitud finita, si y sólo si es finitamente generado, si y sólo si M es finitamente cogenerado.*

Demostración. Es inmediato del hecho de que un módulo artiniano es finitamente cogenerado, y de que un módulo noetheriano es finitamente generado. $\square$

Ejemplo 4.42. Sean A un anillo y S un módulo simple. El módulo S tiene una única serie de composición $X: \; 0 \subseteq S$.

Ejemplo 4.43. Sea $M_A = S_1 \oplus S_2 \oplus S_3$, donde S_1, S_2 y S_3 son A-módulos simples tales que $S_2 \cong S_3$ y $S_1 \ncong S_2$.

$$X: \; 0 \subseteq S_1 \subseteq S_1 \oplus S_2 \subseteq S_1 \oplus S_2 \oplus S_3 = M$$

$$Y: \; 0 \subseteq S_2 \subseteq S_1 \oplus S_2 \subseteq S_1 \oplus S_2 \oplus S_3 = M$$

son series de composición de M.

Ejemplo 4.44. Considérese el $\mathbb{Z}$-módulo $M = \mathbb{Z}_{p^n}$, y sea

$$X: \; 0 \subseteq p^{n-1}\mathbb{Z}_{p^n} \subseteq ... \subseteq p^2\mathbb{Z}_{p^n} \subseteq p\mathbb{Z}_{p^n} \subseteq \mathbb{Z}_{p^n}.$$

X es una serie de composición de longitud n, ya que $p^{n-i}\mathbb{Z}_{p^n}/p^{n-(i+1)}\mathbb{Z}_{p^n} \cong \mathbb{Z}_p$ para todo i.

Luego, por la Proposición(4.9) todo módulo que sea la extensión de dos módulos con serie de composición tiene también serie de composición, y todo submódulo y cociente de un módulo con serie de composición también tiene serie de composición. De hecho, existe una estrecha relación entre los factores de composición de dos módulos y los de su extensión. Para exponer dicha relación se introduce la siguiente definición.

Definición 4.45. Sean M un módulo con una serie de composición X y S un módulo simple. El número de factores de composición de X isomorfos a S recibe el nombre de multiplicidad de S respecto a la serie X y se le denota $m_S^X(M)$.

Observación 4.46. Si W es un conjunto de representantes de las clases de módulos simples bajo isomorfismo, entonces la longitud de la serie de composición X es igual a $\sum_{S\in W} m_S^X(M)$.

Ahora, si M es un módulo con una serie de composición $X: \; M_0 \subseteq ... \subseteq M_n$, y

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

es una sucesión exacta, entonces existen las sucesiones

$$X_1: \; 0 = N_0 \subseteq N_1 \subseteq ... \subseteq N_n = N$$

$$X_2: \ 0 = N'_0 \subseteq N'_1 \subseteq ... \subseteq N'_n = N'$$

donde $N_i = f^{-1}(M_i)$ y $N'_i = g(M_i)$. Así, se tiene el siguiente diagrama conmutativo con renglones y columnas exactas

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & N_i \arrow[r] \arrow[d] & M_i \arrow[r] \arrow[d] & N'_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N_{i+1} \arrow[r] \arrow[d] & M_{i+1} \arrow[r] \arrow[d] & N'_{i+1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N_{i+1}/N_i \arrow[r] \arrow[d] & M_{i+1}/M_i \arrow[r] \arrow[d] & N'_{i+1}/N'_i \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Ahora, se observa que, debido a que M_{i+1}/M_i es un módulo simple, se tiene por el lema de Schur que $M_{i+1}/M_i \cong N_{i+1}/N_i$ y $N'_{i+1}/N'_i = 0$, ó $M_{i+1}/M_i \cong N'_{i+1}/N'_i$ y $N_{i+1}/N_i = 0$.

Por lo tanto, las sucesiones X_1 y X_2 son tales que todo cociente de elementos consecutivos es simple ó cero, de manera que si se descartan los elementos de las sucesiones cuyos factores son 0 se obtienen series de composición

$$Y = \{N_k \in X_1 \quad | \quad N_k/N_{k-1} \neq 0\} \text{ y}$$
$$Z = \{N'_k \in X_2 \quad | \quad N'_k/N'_{k-1} \neq 0\}.$$

Además, como $N'_{i+1}/N'_i = 0$ si y sólo si $N_{i+1}/N_i \neq 0$, se concluye que para todo módulo simple S, se cumple que $m_X^S(M) = m_Y^S(N) + m_Z^S(N')$.

Recíprocamente, si N tiene una serie de composición $Y = (N_i)_{i=0}^m$ y N' tiene una serie de composición $Z = (N'_i)_{i=0}^k$, entonces, como $N \cong f(N)$ y $N' \cong M/N$, se puede considerar N_i como un submódulo de M y $N'_i = (\tilde{N}_i + N)/N$ donde $\tilde{N}_i$ es algún submódulo de M. De manera que se tiene una serie

$$0 = N_0 \subseteq ... \subseteq N_m = N = \tilde{N}_0 + N \subseteq ... \subseteq \tilde{N}_k + N = M$$

donde N_{i+1}/N_i y $(\tilde{N}_{i+1}+N)/(\tilde{N}_i+N) \cong N'_{i+1}/N'_i$ son simples. Por lo tanto, se ha construido una serie de composición X de M, tal que si S es un módulo simple, entonces $m_X^S(M) = m_Y^S(N) + m_Z^S(N')$.

Se ha probado el siguiente resultado.

Proposición 4.47. *Dada una sucesión exacta de módulos* $0 \to N \to M \to N' \to 0$. *Se cumple que* M *tiene una serie de composición si y sólo si* N *y* N' *tienen series de composición, tales que para cada módulo simple* S *se tiene que*

$$m_X^S(M) = m_Y^S(N) + m_Z^S(N').$$

Además, si N *es submódulo de* M, *entonces existe una serie de composición* $(M_i)_{i=0}^n$ *de* M *en la cual* $M_i = N$ *para algún* $i \in \{1, ..., n\}$.

Con esta proposición es sencillo probar el siguiente resultado, el teorema de Jordan-Hölder.

Teorema 4.48. *Si* M *tiene una serie de composición* X *de longitud* n, *entonces toda serie de composición* Y *de* M *tiene longitud* n *y* $m_X^S(M) = m_Y^S(M)$ *para cada módulo simple* S.

Demostración. Sea n la longitud de X. Si $n = 1$, entonces M es simple, por lo que sólo tiene una serie de composición. Luego, tomando como hipótesis de inducción que si M es un módulo con una serie de composición de longitud k, entonces toda serie de composición Y de M cumple que $m_X^S(M) = m_Y^S(M)$ para todo módulo simple S. Si $n = k+1$, entonces se tiene que M/N_k es simple, por lo que toda serie de composición es de longitud 1 y la multiplicidad de cualquier simple es igual a 1 ó 0, y $Y = (N_i)_{i=0}^k$ es una serie de composición de N_k de longitud k, por lo que cumple la hipótesis de inducción.

Ahora, si M tiene una serie de composición X' de longitud m, entonces N_k y M/N_k tienen series de composición Y' y Z' tales que $m_{X'}^S(M) = m_{Y'}^S(N_k) + m_{Z'}^S(M/N_k)$ para todo módulo simple S por la Proposición 4.47, y por la argumentación anterior

$$m_{X'}^S(M) = m_{Y'}^S(N_k) + m_{Z'}^S(M/N_k) = m_Y^S(N_k) + m_Z^S(M/N_k) = m_X^S(M).$$

Por lo tanto, se ha probado inductivamente que la multiplicidad de un módulo simple es la misma sin importar la serie de composición. Y como la longitud de una serie es igual a la suma de las multiplicidades de los módulos simples, la longitud de toda serie de composición de un módulo es siempre la misma. $\square$

Se ha probado que la longitud de una serie de composición así como la multiplicidades de sus factores de composición sólo dependen del módulo. Por ello se definen los siguientes conceptos.

Definición 4.49. Sea M un módulo. Se dice M es de longitud finita si M tiene serie de composición. En tal caso, todas las series de composición de M tienen la misma longitud, tal número recibe el nombre de longitud de M y se le denota $l(M)$. Y dado un módulo simple S, se llama multiplicidad de composición de S en M a la multiplicidad de S en cualquier serie de composición de M y se denota $m_S(M)$.

Es inmediato el siguiente resultado por la Proposición 4.47 y el Teorema 4.48.

Corolario 4.50. *Dada una sucesión exacta* $0 \to N \to M \to N' \to 0$. *Si* M *tiene una serie de composición, entonces* $l(M) = l(N) + l(N')$. *En particular si* $N \subseteq M$, *entonces* $l(M) = l(N) + l(M/N)$.

Se sigue que si N y N' son submódulos de M tales que $N \subsetneq N'$, $l(N) < l(N')$ pues $l(N') = l(N) + l(N'/N) \geq l(N) + 1 > l(N)$.

Corolario 4.51. *Si* M *tiene serie de composición con submódulos* N *y* N' *tales que* $N \subsetneq N' \subseteq M$, *entonces* $l(N) < l(N')$.

Por último, nótese que si M es un módulo con una cadena finita

$$0 = M_0 \subseteq M_1 \subseteq ... \subseteq M_n = M,$$

tal que cada cociente M_{i+1}/M_i tiene serie de composición, entonces M tiene serie de composición. Ciertamente, $M_1 = M_1/M_0$ tiene serie de composición, y si para dado $k \in \{1, ..., n\}$, M_k tiene serie de composición, entonces como M_{k+1}/M_k también tiene serie de composición, M_{k+1} tiene serie de composición por la Proposición 4.47. Así, inductivamente M tiene serie de composición.

Proposición 4.52. *Si* M *tiene una serie tal que cada cociente tiene serie de composición, entonces* M *tiene serie de composición.*

5. El radical y el soclo

En este capítulo se definen el radical y el soclo, dos submódulos importantes en el estudio de la estructura de un módulo.

El radical surgió como un medio para caracterizar la semisimplicidad y el soclo es el concepto dual, por lo que ambos submódulos contienen información importante sobre el comportamiento de un módulo y su relación con módulos semisimples.

El capítulo se divide en las secciones de soclo y radical. En la sección de soclo se define el concepto y se estudian propiedades que cumple el soclo de los módulos finitamente cogenerados, entre ellas la de ser un submódulo esencial. En la sección correspondiente al radical se define el radical de un módulo y se estudian propiedades que cumple el radical de los módulos finitamente generados, como la de ser un submódulo superfluo. Por último, el capítulo concluye con una subsección dedicada al radical de Jacobson de un anillo, donde se caracteriza este ideal y sus propiedades más importantes, terminando con las propiedades del radical de Jacobson de un anillo artiniano y el teorema de Akizuki-Hopkins-Levitzki.

5.1. El soclo

Sean M un módulo y S un módulo simple. Por el lema de Schur, todo morfismo $f : S \to M$ es nulo ó inyectivo. Si $f \neq 0$, entonces $f(S)$ es un submódulo simple de M. Y recíprocamente, si N es un submódulo simple de M, entonces la inclusión natural $i : N \to M$ implica que N es la imagen de un morfismo con dominio simple y codominio M.

De manera que, si X es la suma de todos los submódulos simples de M, el submódulo X es la suma de todas las imágenes de los morfismos con dominio simple y codominio M. Este submódulo recibe el nombre de soclo de M.

Definición 5.1. Sea M un módulo. Si $M \neq 0$ se define el soclo de M, denotado como $\operatorname{soc}(M)$, como el submódulo

$$\operatorname{soc}(M) = \sum\{N \subseteq M \quad | \quad N \text{ es submódulo simple de } M\}.$$

Si $M = 0$, entonces se define $\operatorname{soc}(M) = 0$.

Teorema 5.2. *Sea M un módulo. El soclo de M es igual a la suma de todas las imágenes de los morfismos con dominio simple y codominio M.*

Ejemplo 5.3. Si $M = \mathbb{Z}_{p^n}$, entonces M tiene un único submódulo minimal simple $\operatorname{soc}(M) = p^{n-1}\mathbb{Z}_{p^n} \cong \mathbb{Z}_p$.

Ejemplo 5.4. Si $M = \mathbb{Z}$, entonces $\operatorname{soc}(M) = 0$. Ciertamente, M no contiene submódulos simples, debido a que los módulos simples sobre $\mathbb{Z}$ son de la forma $\mathbb{Z}_p$ con p primo, pero M es libre de torsión. Por lo tanto, $\operatorname{soc}(M) = 0$.

Ejemplo 5.5. Sean k un campo y $D = k[x]$. El anillo de matrices generalizadas con producto trivial

$$A = \begin{pmatrix} k & 0 \\ {}_D D_k & D \end{pmatrix}$$

cumple que $\operatorname{soc}(A_A) \neq \operatorname{soc}({}_A A)$. En efecto, debido a que los módulos simples son cíclicos es sencillo deducir que los submódulos simples de A_A son de la forma

$$\begin{pmatrix} 0 & 0 \\ p(x) & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 0 \\ p(x)k & 0 \end{pmatrix} \text{ ó } \begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix} A = \begin{pmatrix} k & 0 \\ 0 & 0 \end{pmatrix},$$

de manera que $\operatorname{soc}(A_A) = \begin{pmatrix} k & 0 \\ k[x] & 0 \end{pmatrix}$. Con el mismo razonamiento, se deduce que ${}_A A$ no tiene submódulos simples, ya que todos los submódulos cíclicos son de la forma

$$A\begin{pmatrix} 0 & 0 \\ p(x) & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ k[x]p(x) & 0 \end{pmatrix},\ A\begin{pmatrix} 0 & 0 \\ 0 & p(x) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & k[x]p(x) \end{pmatrix},$$

$$A\begin{pmatrix} 0 & 0 \\ p(x) & q(x) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ k[x]p(x) & k[x]q(x) \end{pmatrix} \text{ ó } A\begin{pmatrix} \lambda & 0 \\ p(x) & q(x) \end{pmatrix} = \begin{pmatrix} k & 0 \\ k[x] & k[x]q(x) \end{pmatrix},$$

con $\lambda \in k$ distinto de 0. Por lo tanto, $\operatorname{soc}({}_A A) = 0$.

Son inmediatos de la definición los siguientes resultados.

Proposición 5.6. *Sea M un A-módulo. Se cumplen los siguientes enunciados:*

(a) *M es semisimple si y sólo si* $\operatorname{soc}(M) = M$.

(b) *Si $f : M \to N$ es un morfismo, entonces* $f(\operatorname{soc}(M)) \subseteq \operatorname{soc}(N)$.

(c) *Si $f : M \to N$ es un monomorfismo tal que* $\operatorname{soc}(N) \subseteq f(M)$, *entonces*

$$\operatorname{soc}(M) = \operatorname{soc}(N).$$

(d) *El soclo de M es un B-submódulo de ${}_B M$, donde* $B = \operatorname{End}_A(M)$.

(e) *Si K es un submódulo de M, entonces* $\operatorname{soc}(K) = K \cap \operatorname{soc}(M)$.

Demostración. Sea M un A-módulo.

(a) M es semisimple si, y sólo si, M es igual a la suma de sus submódulos simples si, y sólo si, $M = \operatorname{soc}(M)$.

(b) Si $f : M \to N$ es un morfismo, entonces el lema de Schur implica que $f(\operatorname{soc}(M))$ es una suma del submódulo 0 y de submódulos simples, lo que implica que $f(\operatorname{soc}(M)) \subseteq \operatorname{soc}(N)$.

(c) Por el punto anterior basta probar que $\operatorname{soc}(N) \subseteq f(\operatorname{soc}(M))$. Por hipótesis $\operatorname{soc}(N) \subseteq f(M)$, con lo cual $\operatorname{soc}(N) \subseteq \operatorname{soc}(f(M))$ pero debido a que f es monomorfismo $\operatorname{soc}(f(M)) = f(\operatorname{soc}(M))$. Por lo tanto, $\operatorname{soc}(N) \subseteq f(\operatorname{soc}(M))$.

(d) Debido a que M es un B-módulo, basta probar que $f(\operatorname{soc}(M)) \subseteq \operatorname{soc}(M)$ para todo $f \in B$, lo cual se sigue del punto (b).

(e) Es inmediato de la definición.

□

Corolario 5.7. *Sea M un A-módulo. Se cumplen los siguientes enunciados.*

(a) *Si N es un submódulo de M tal que* $\operatorname{soc}(M) \subseteq N$*, entonces* $\operatorname{soc}(M) = \operatorname{soc}(N)$.

(b) $\operatorname{soc}(M)$ *es el máximo submódulo N de M tal que* $\operatorname{soc}(N) = N$.

(c) $\operatorname{soc}(\bigoplus_{i\in X} M_i) = \bigoplus_{i\in X} \operatorname{soc}(M_i)$.

Demostración.

(a) Por el punto (e) de la proposición anterior

$$\operatorname{soc}(N) = N \cap \operatorname{soc}(M),$$

pero por hipótesis $soc(M) \subseteq N$, lo que implica que $\operatorname{soc}(N) = \operatorname{soc}(M)$.

(b) Del punto (a) de la proposición anterior $\operatorname{soc}(N) = N$ si, y sólo si, N es semisimple si, y sólo si, $N \subseteq \operatorname{soc}(M)$.

(c) Sea $M = \bigoplus_{i\in X} M_i$. Por el punto (e) de la proposición anterior,

$$\operatorname{soc}(M_i) = M_i \cap \operatorname{soc}(M),$$

lo que implica que

$$\bigoplus_{i\in X} \operatorname{soc}(M_i) = \bigoplus_{i\in X} M_i \cap \operatorname{soc}(M) = M \cap \operatorname{soc}(M) = \operatorname{soc}(M).$$

□

5.1.1. El soclo de un módulo finitamente cogenerado

Como ya se ha visto en los ejemplos anteriores el soclo no siempre es distinto de cero. En esta subsección se estudian los módulos que tienen un soclo diferente de cero. Para empezar se caracterizan los módulos con soclo no nulo y se prueba que los módulos finitamente cogenerados cumplen esta propiedad.

Proposición 5.8. *Sea M un módulo. Se cumplen los siguientes enunciados*

(a) $\operatorname{soc}(M) \neq 0$ *si, y sólo si, M contiene un submódulo simple.*

(b) *Si M es finitamente cogenerado, entonces todo submódulo de M contiene un submódulo simple.*

(c) *Si M es un módulo finitamente cogenerado, entonces* $\operatorname{soc}(N) \neq 0$ *para todo submódulo $N \neq 0$. En particular,* $\operatorname{soc}(M) \neq 0$ *si $M \neq 0$.*

Demostración. Sea M un módulo.

(a) Es inmediato de la definición de soclo.

(b) Sea K un submódulo de M. Considérese el conjunto X de submódulos no nulos de K. El conjunto X es no vacío ya que $K \in X$, y si se toma una cadena descendente $(N_i)_{i\in I}$ en X entonces $N = \bigcap_{i\in X} N_i$ es una cota inferior de la cadena en X. En efecto, es inmediato que $N_j \supseteq N$ para todo $j \in I$, y si se supone que $N = 0$, entonces debido a que M es finitamente cogenerado existe un subconjunto finito J de I tal que $\bigcap_{i\in J} N_i = 0$, pero esto implica que $N_m = 0$ donde m es el mínimo de J, lo cual es una contradicción pues $N_m \in X$. Por lo tanto, $N \in X$. De manera que toda cadena en X tiene una cota inferior en X, lo que implica por el lema de Zorn que X tiene un elemento mínimo, esto es un submódulo mínimo no nulo y por ello simple. Por lo tanto, K tiene un submódulo simple.

(c) Se sigue de los puntos anteriores ya que todo submódulo de M es finitamente cogenerado.

□

Ahora, si M es un módulo finitamente cogenerado, entonces es sencillo deducir que un submódulo N contiene a $\operatorname{soc}(M)$ si, y sólo si, $N \cap K \neq 0$ para todo submódulo $K \neq 0$.

En efecto, si $\operatorname{soc}(M) \subseteq N$ y K es un submódulo tal que $N \cap K = 0$, entonces $K = 0$ ya que si se supone lo contrario $\operatorname{soc}(K) \neq 0$ por la proposición anterior, lo que implica que

$$0 \neq \operatorname{soc}(K) \subseteq K \cap \operatorname{soc}(M) \subseteq K \cap N,$$

lo cual es una contradicción.

Recíprocamente, si N es un submódulo tal que $N \cap K = 0$ implica que $K = 0$ para todo submódulo K, entonces N contiene todos los submódulos simples. En efecto, si se supone que existe un submódulo simple S tal que $S \nsubseteq N$, entonces $S \cap N \neq S$ es un submódulo de S, por lo que $S \cap N = 0$ pues S es simple, lo que implica que $S = 0$, lo cual es una contradicción.

Se ha probado el siguiente resultado.

Proposición 5.9. *Sea M un módulo finitamente cogenerado. Para todo submódulo N de M se tiene que* $\operatorname{soc}(M) \subseteq N$ *si y sólo si* $N \cap K \neq 0$ *para todo submódulo* $K \neq 0$.

La proposición anterior lleva a la siguiente definición.

Definición 5.10. Sea N un submódulo de M. Se dice que N es un submódulo esencial, denotado como $N \trianglelefteq M$, si se cumple que $N \cap K \neq 0$ para todo submódulo $K \neq 0$.

Por lo tanto, se ha demostrado que si M es un módulo finitamente cogenerado, entonces $\operatorname{soc}(M)$ es un submódulo esencial, que además es finitamente cogenerado, ya que todo submódulo de un módulo finitamente cogenerado es finitamente cogenerado.

Recíprocamente, si M es un módulo tal que $\operatorname{soc}(M)$ es un submódulo esencial finitamente cogenerado, entonces M es finitamente cogenerado. En efecto, supóngase que X es una familia de submódulos de M tal que $\bigcap_{N \in X} N = 0$, de manera que

$$\bigcap_{N \in X} \operatorname{soc}(N) = \bigcap_{N \in X} (N \cap \operatorname{soc}(M)) = \left(\bigcap_{N \in X} N \right) \cap \operatorname{soc}(M) = 0,$$

lo que implica que existe una subfamilia finita Y de X tal que

$$(\bigcap_{N \in Y} N) \cap \operatorname{soc}(M) = \bigcap_{N \in Y} \operatorname{soc}(N) = 0,$$

pero $\operatorname{soc}(M)$ es esencial, por lo que $\bigcap_{N \in Y} N = 0$. Por lo tanto, M es finitamente cogenerado.

Se ha probado la siguiente caracterización de los módulos finitamente cogenerados.

Proposición 5.11. *Un módulo M es finitamente cogenerado si y sólo si* $\operatorname{soc}(M) \trianglelefteq M$ *y* $\operatorname{soc}(M)$ *es finitamente cogenerado.*

Corolario 5.12. *Un módulo M es finitamente cogenerado si y sólo si* $\operatorname{soc}(M) \trianglelefteq M$ *y* $\operatorname{soc}(M)$ *es finitamente generado.*

Demostración. Se sigue de la proposición anterior, ya que al ser $\operatorname{soc}(M)$ es semisimple, el Corolario 4.41 implica que si $\operatorname{soc}(M)$ es finitamente generado, entonces también es finitamente cogenerado. $\square$

Ejemplo 5.13. El módulo $M = \mathbb{Z}$ no es finitamente cogenerado y $\operatorname{soc}(M) = 0$, por lo que $\operatorname{soc}(M)$ es no esencial finitamente generado.

Ejemplo 5.14. Sea $M = \bigoplus_{p\in X} \mathbb{Z}_p$ donde X es el conjunto de todos los primos. El módulo M es semisimple, de manera que $\mathrm{soc}(M) = M$. Por lo tanto, $\mathrm{soc}(M) = M$ es esencial no finitamente generado.

De la demostración de la proposición anterior se puede deducir que en general el soclo de un módulo es esencial si, y sólo si, todo submódulo no nulo contiene un submódulo simple.

En efecto, si M es un módulo tal que todo submódulo no nulo contiene un submódulo simple, entonces $\mathrm{soc}(M)\cap K \neq 0$ para todo $K \neq 0$, por lo que $\mathrm{soc}(M)$ es esencial. Recíprocamente, si el soclo es esencial, entonces $\mathrm{soc}(K) = \mathrm{soc}(M)\cap K \neq 0$ para todo submódulo $K \neq 0$, lo que implica que todo submódulo no nulo contiene un submódulo simple.

Proposición 5.15. *Sea M un módulo. Todo submódulo no nulo contiene un submódulo simple si y sólo si* $\mathrm{soc}(M) \trianglelefteq M$.

Por último nótese que en la demostración de la Proposición 5.9 se probó que el soclo está contenido en todo submódulo esencial, sin importar si M es finitamente cogenerado ó no. De hecho, en general el soclo es la intersección de todos los submódulos esenciales.

En efecto, por la argumentación anterior basta probar que la intersección de todos los submódulos esenciales está contenida en $\mathrm{soc}(M)$.

Sea X dicha intersección y N un submódulo de X. Se considera el conjunto Y de todos los submódulos L de M tales que $L\cap N = 0$. El conjunto Y es no vacío, ya que contiene al 0, y si se considera una cadena ascendente $(N_i)_{i\in I}$, entonces $K = \sum_{i\in I} N_i$ es una cota superior en Y. En efecto, es claro que $N_i \subseteq K$ para toda $i \in I$, y si se toma $x \in K\cap N$, entonces $x = \sum_{i\in J} x_i$ con $x_i \in N_i$ y J un subconjunto finito de I; y así $x \in N_m \cap N = 0$ donde $m = max\{J\}$.

Ahora, $N \oplus K$ es esencial en M, pues si se tiene un submódulo W de M tal que $(N \oplus K)\cap W = 0$, entonces

$$N \cap (W + K) = N \cap W + N \cap K = N \cap W \subseteq N \cap W + K \cap W = 0,$$

lo que implica que $W = 0$ por la maximalidad de K. Asi, $N \subseteq Y \subseteq N \oplus K$, lo que implica que $N \oplus (K \cap Y) = Y$. Por lo tanto, Y es semisimple y entonces $Y \subseteq \mathrm{soc}(M)$.

Se ha obtenido la siguiente caracterización.

Proposición 5.16. *Dado un módulo M se tiene que* $\mathrm{soc}(M) = \bigcap\{N \quad | \quad N \trianglelefteq M\}$.

Ejemplo 5.17. Sea k un campo. Si A es un anillo con una descomposición de la unidad

$1 = e_1 + ... + e_n$ cuya descomposición de Peirce es de la forma

$$A = \begin{pmatrix} k & M_{12} & \dots & M_{1n} \\ M_{21} & k & & \\ \vdots & & \ddots & \\ M_{n1} & & & k \end{pmatrix}, \, M = \begin{pmatrix} 0 & M_{12} & \dots & M_{1n} \\ M_{21} & 0 & & \\ \vdots & & \ddots & \\ M_{n1} & & & 0 \end{pmatrix} \text{ y}$$

$M_{ij}M_{jk} = 0$ para toda $i \neq k \neq j$, entonces $\operatorname{soc}(A_A) = M \oplus (\bigoplus_{i \in X} e_i A)$ donde

$$X = \{i \in \{1, ..., n\} \quad | \quad M_{ij} = 0 \; \forall j \neq i\}$$

y $\operatorname{soc}({}_A A) = M \oplus (\bigoplus_{i \in Y} Ae_i)$ donde

$$Y = \{i \in \{1, ..., n\} \quad | \quad M_{ji} = 0 \; \forall j \neq i\}.$$

En efecto, $N = M \oplus (\bigoplus_{i \in X} e_i A)$ es esencial, ya que si se supone que existe un submódulo no nulo K tal que $K \cap N = 0$, entonces existe un elemento x de K tal que su entrada en la l-ésima columna y l-ésimo renglón para algún $l \notin X$ es distinto de cero. Pero entonces

$$0 = K \cap N \supseteq xA \cap N \supseteq \begin{pmatrix} 0 & \cdots & & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & & & & 0 \\ M_{j1} & \cdots & k & \cdots & M_{jn} \\ 0 & & & & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & & \cdots & 0 \end{pmatrix} \cap N \neq 0,$$

lo cual es una contradicción. Por lo tanto, N es un submódulo esencial de A, lo que implica que $\operatorname{soc}(A_A) \subseteq N$. Pero $e_i A$ es simple para todo $i \in X$, y M es semisimple ya que para todo $m \in M_{ij}$ se tiene que $\dim_k mA = 1$, por lo que mA es simple, y así

$$M = \sum_{i,j=1}^{n} \left(\sum_{m \in M_{ij}} mA \right)$$

es semisimple. Por lo tanto, N es semisimple, lo que implica que $N = \operatorname{soc}(A_A)$. Análogamente, se prueba que $\operatorname{soc}({}_A A) = M \oplus (\bigoplus_{i \in Y} Ae_i)$.

5.2. El radical

Sea M un A-módulo derecho y S un A-módulo derecho simple. Por el lema de Schur todo morfismo $f : M \to S$ es epimorfismo ó es el morfismo 0. Si $f \neq 0$ se tiene que $M/\operatorname{Ker}(f) \cong S$, lo que implica que $\operatorname{Ker}(f)$ es un submódulo maximal. En consecuencia, si M no tiene submódulos maximales entonces el único morfismo con codominio simple es el morfismo cero.

De manera que si

$$X = \bigcap \{\operatorname{Ker}(f) \quad | \quad f : M_A \to S_A, \text{ con } S_A \text{ simple}\} \text{ y}$$

$$Y = \bigcap \{N \subseteq M \quad | \quad N \text{ es un submódulo maximal de } M\}$$

con la convención de que si el conjunto de submódulos maximales es vacío entonces Y es igual a M, se tiene que $X = Y$. En efecto, si M no tiene submódulos maximales, entonces $Y = M$ y por lo discutido en el párrafo anterior no existen morfismos no nulos con dominio M y codominio simple, en conclusión $X = M = Y$. Si M tiene submódulos maximales, entonces por lo discutido, todo submódulo maximal es el núcleo de un morfismo no nulo con codominio simple, por lo que es sencillo deducir que $X = Y$.

Dicho conjunto contiene información importante sobre la estructura del módulo M y recibe el nombre de radical.

Definición 5.18. Sea $M \in Mod_A$. La intersección de los núcleos de todos los morfismos con dominio M y codominio simple recibe el nombre de radical de M, y se le denota como $\operatorname{rad}(M)$.

De la discusión anterior se tiene el siguiente resultado.

Proposición 5.19. *Sean M un módulo y*

$$Y = \bigcap \{N \subseteq M \quad | \quad N \text{ es un submódulo maximal de } M\},$$

con la convención de que si dicho conjunto es vacío, entonces $Y = M$. Se cumple que $\operatorname{rad}(M) = Y$.

Observación 5.20. Todo módulo simple tiene como submódulo maximal al submódulo 0.

Es inmediato entonces de la definición la siguiente proposición.

Proposición 5.21. *Si M es simple, entonces* $\operatorname{rad}(M) = 0$.

De hecho, si M es semisimple, entonces $\operatorname{rad}(M) = 0$. Para probar este hecho son necesarios los siguientes tres resultados.

Lema 5.22. *Si $f : M_A \to N_A$ es un morfismo de A-módulos, entonces*

$$f(\operatorname{rad}(M)) \subseteq \operatorname{rad}(N).$$

Si además $f : M \to N$ es epimorfismo y $\operatorname{Ker}(f) \subseteq \operatorname{rad}(M)$, entonces

$$f(\operatorname{rad}(M)) = \operatorname{rad}(N).$$

Demostración. Sea B submódulo maximal de N y $\pi : N \to N/B$ la proyección canónica. El módulo N/B es simple por lo que el lema de Schur implica que πf es suprayectiva ó el morfismo 0.

Si πf es el morfismo 0, entonces $f(\operatorname{rad}(M)) \subseteq \operatorname{Ker}(\pi) = B$. Si πf es suprayectiva, entonces $M/\operatorname{Ker}(\pi f) \cong N/B$ es simple, por lo que $\operatorname{Ker}(\pi f)$ es un submódulo maximal, y así $\operatorname{rad}(A) \subseteq \operatorname{Ker}(\pi f)$, lo que implica que $f(\operatorname{rad}(A)) \subseteq \operatorname{Ker}(\pi) = B$. Por lo tanto, $f(\operatorname{rad}(A))$ está contenido en todo submódulo maximal, lo que implica que

$$f(\operatorname{rad}(M)) \subseteq \operatorname{rad}(N).$$

Si además f es suprayectiva y $\operatorname{Ker}(f) \subseteq \operatorname{rad}(M)$, es inmediato que $M/\operatorname{Ker}(f) \cong N$, entonces por el teorema de correspondencia biyectiva $f(\operatorname{rad}(M))$ es la intersección de ideales maximales, es decir $f(\operatorname{rad}(M)) = \operatorname{rad}(N)$. □

Corolario 5.23. *Sea M un A-módulo. Se cumplen los siguientes enunciados.*

(a) *Para todo $N \subseteq \operatorname{rad}(M)$ se tiene que $\operatorname{rad}(M/N) = \operatorname{rad}(M)/N$.*

(b) *Para todo $N \subseteq M$ se tiene que $\operatorname{rad}(M/N) \supseteq (\operatorname{rad}(M) + N)/N$.*

(c) *$\operatorname{rad}(M)$ es el mínimo submódulo N de M tal que $\operatorname{rad}(M/N) = 0$.*

(d) *$\operatorname{rad}(M)$ es un B-submódulo izquierdo de ${}_BM$, donde $B = \operatorname{End}_A(M)$.*

Demostración.

(a) Sea N un submódulo tal que $N \subseteq \operatorname{rad}(M)$. Considerando la proyección canónica $f : M \to M/N$, se tiene por el lema anterior que $\operatorname{rad}(M)/N = \operatorname{rad}(M/N)$ ya que f es suprayectiva y $N \subseteq \operatorname{rad}(M)$.

(b) Sea $N \subseteq M$, considerando la proyección canónica $f : M \to M/N$, el lema anterior implica que $(\operatorname{rad}(M) + N)/N = f(\operatorname{rad}(M)) \subseteq \operatorname{rad}(M/N)$.

(c) Por el punto anterior $\operatorname{rad}(M/\operatorname{rad}(M)) = \operatorname{rad}(M)/\operatorname{rad}(M) = 0$. Además, si N es un submódulo de M tal que $\operatorname{rad}(M/N) = 0$ y $f : M \to M/N$ es la proyección natural,

$$f(\operatorname{rad}(M)) \subseteq \operatorname{rad}(M/N) = 0$$

por el lema anterior, por lo que $\mathrm{rad}(M) \subseteq \mathrm{Ker}(f) = N$. Por lo tanto, $\mathrm{rad}(M)$ es el menor submódulo que cumple tal propiedad.

(d) Debido a que M es un B-módulo izquierdo basta probar que se cumple que $f(\mathrm{rad}(M)) \subseteq \mathrm{rad}(M)$ para todo $f \in B$, lo cual es inmediato del lema anterior.

□

Corolario 5.24. *Dada una familia de módulos* $\{M_i\}_{i\in X}$ *se tiene que*

$$\mathrm{rad}(\bigoplus_{i\in X} M_i) = \bigoplus_{i\in X} \mathrm{rad}(M_i).$$

Demostración. Considérense las proyecciones e inclusiones canónicas $\pi_i : M \to M_i$ y $\iota_i : M_i \to M$, donde $M = \bigoplus_{i\in X} M_i$.

Sean $m_i \in \mathrm{rad}(M_i) \subseteq M$ y $g : M \to S$ un morfismo de módulos con S simple, como $\pi_i(m_i) = m_i \in \mathrm{rad}(M_i) \subseteq \mathrm{Ker}(g\iota_i)$, se tiene que $g(m_i) = g\iota_i\pi_i(m_i) = 0$. Por lo tanto, $\mathrm{rad}(M_j) \subseteq \mathrm{rad}(M)$ para cualquier $j \in X$, lo que implica que $\bigoplus_{j\in X} \mathrm{rad}(M_i)$ esta contenido en $\mathrm{rad}(\bigoplus_{i\in X} M_i)$.

Por otro lado, sea $\sum m_i = m \in \mathrm{rad}(M)$ con $m_i \in M_i$. Si $f_i : M_i \to S$ es un morfismo con S simple para toda $i \in X$ y $f = \bigoplus f_i : M \to S$, entonces $f_i(m_i) = f\iota_i\pi_i(m) = 0$ pues $m \in \mathrm{rad}(M) \subseteq \mathrm{Ker}(f\iota_i\pi_i)$, por lo que $m_i \in \mathrm{rad}(M_i)$ para toda $i \in X$; lo que implica que $m \in \bigoplus_{i\in X} \mathrm{rad}(M_i)$. Por lo tanto, $\mathrm{rad}(\bigoplus_{i\in X} M_i) = \bigoplus_{i\in X} \mathrm{rad}(M_i)$. □

Ahora, si M es semisimple, es decir $M = \bigoplus_{i\in X} S_i$ con S_i simple, entonces

$$\mathrm{rad}(M) = \bigoplus_{i\in X} \mathrm{rad}(S_i) = 0.$$

Corolario 5.25. *Si M es semisimple, entonces* $\mathrm{rad}(M) = 0$.

Nótese que el recíproco es en general falso.

Ejemplo 5.26. Considérese el $\mathbb{Z}$-módulo $M = \prod_{p\in X} \mathbb{Z}_p$. El módulo M no es semisimple por 3.17, sin embargo $\mathrm{rad}(M) = 0$, ya que los submódulos de la forma

$$M_q = \{(m_p)_{p\in X} \in M \quad | \quad m_q = 0\}$$

son claramente maximales, por lo que $\mathrm{rad}(M) \subseteq \bigcap_{q\in X} M_q = 0$. Por lo tanto, M es un submódulo no semisimple con $\mathrm{rad}(M) = 0$.

5.2.1. El radical de un módulo finitamente generado

En esta subsección se tratan las propiedades del radical de un módulo finitamente generado. Para comenzar nótese que $\mathrm{rad}(M)$ no siempre es un submódulo propio de M.

Ejemplo 5.27. Recuérdese que dado un dominio entero D, K su campo de fracciones y S un conjunto multiplicativo que no contenga al cero, es decir $0 \notin S$ y $SS \subseteq S$, entonces la localización de D en el conjunto S es el subanillo

$$S^{-1}D = \{\frac{p}{q} \in K \quad | \quad p \in R, q \in S\}$$

de K. Sea $A = S^{-1}\mathbb{Q}[x]$ la localización de $\mathbb{Q}[x]$ en el conjunto

$$S = \{p(x) \in \mathbb{Q}[x] \quad | \quad p(0) \neq 0\}.$$

A continuación se prueba que rad($\mathbb{Q}(x)_A$)= $\mathbb{Q}(x)_A$. Para ello basta probar que dado cualquier A-submódulo N el cociente $\mathbb{Q}[x]/N$ no es simple, de esta manera el primer teorema de isomorfismo implica que el único A-morfismo de $\mathbb{Q}(x)$ a un A-módulo simple es el morfismo 0 y entonces el núcleo de cualquiera de estos morfismos es $\mathbb{Q}(x)$. Ahora, dado un A-submódulo N de $\mathbb{Q}(x)$, se considera el conjunto

$$T = \left\{ n \in \mathbb{N} \quad | \quad \frac{p(x)}{x^n q(x)} \in N \, \text{para cualesquiera} \, p, q \in \mathbb{Q}[x] \, \text{con} \, p,\ q \in S \right\}.$$

Si T no tiene máximo, entonces $N = \mathbb{Q}(x)$. En efecto, dado cualquier $m \in \mathbb{N}$ existe $t \in T$ tal que $m < t$, es decir existe un elemento $\frac{p(x)}{x^t q(x)} \in N \, \text{con} \, p,\ q \in S$,

$$\text{entonces} \; \frac{1}{x^t} = \frac{p(x)}{x^t q(x)} \frac{q(x)}{p(x)} \in N \, \text{lo que implica} \; \frac{1}{x^m} = \frac{1}{x^t} x^{t-m} \in N.$$

Por otro lado, nótese que todo elemento de $\mathbb{Q}(x)$ es de la forma $p(x)/q(x)$, $p(x)x^t/q(x)$ ó $p(x)/x^t q(x)$, donde $p(x)$, $q(x) \in S$ y $t \in \mathbb{N}$; de manera que $\mathbb{Q}(x) = N$ ya que

$$\frac{p(x)}{q(x)} = \frac{1}{x^t} \frac{x^t p(x)}{q(x)} \in N, \; \frac{x^t p(x)}{q(x)} = \frac{1}{x^t} \frac{x^{2t} p(x)}{q(x)} \in N \text{ y } \frac{p(x)}{x^t q(x)} = \frac{1}{x^t} \frac{p(x)}{q(x)} \in N.$$

En el caso de que T tuviera un máximo k, entonces $(1/x^k)S = N$. Ciertamente, dado $\alpha \in N \subseteq \mathbb{Q}[x]$ es de la forma $p(x)/q(x)$, $p(x)x^t/q(x)$ ó $p(x)/x^t q(x)$, donde $p(x)$, $q(x) \in S$ y $t \in \mathbb{N}$; nótese que en el último caso $t < k$ por construcción; de manera que

$$\begin{aligned}
\alpha &= \frac{p(x)}{q(x)} = \frac{1}{x^k} \frac{x^k p(x)}{q(x)} \in \frac{1}{x^k} S, \\
\alpha &= \frac{x^t p(x)}{q(x)} = \frac{1}{x^k} \frac{x^{t+k} p(x)}{q(x)} \in \frac{1}{x^k} S, \\
\alpha &= \frac{p(x)}{x^t q(x)} = \frac{1}{x^k} \frac{x^{k-t} p(x)}{q(x)} \in \frac{1}{x^k} S;
\end{aligned}$$

y así $N = \frac{1}{x^k}S$. En consecuencia, si N es un R-submódulo de $\mathbb{Q}(x)$, se tiene que $N = \frac{1}{x^k}S$ para algún $k \in \mathbb{N}$; pero entonces $N \subsetneq \frac{1}{x^m}S \subsetneq \mathbb{Q}(x)$ para cualquier natural $m > k$. En consecuencia, por el teorema de correspondencia, $\mathbb{Q}(x)/N$ no es simple como se queria probar. Por lo tanto, $\mathrm{rad}(\mathbb{Q}(x)) = \mathbb{Q}(x)$.

Sin embargo si M es un módulo finitamente generado y distinto de 0, entonces

$$\mathrm{rad}(M) \neq M.$$

Proposición 5.28. *Sea $\{0\} \neq M_A$ un módulo finitamente generado. Se cumplen los siguientes enunciados.*

(a) *Si $N \subsetneq M$, entonces N está contenido en un submódulo maximal.*

(b) $\mathrm{rad}(M) \neq M$.

Demostración. Sea M finitamente generado.

(a) Si M tiene un submódulo propio N, y

$$X = \{L \subsetneq M \,\text{submódulo} \quad | \quad N \subseteq L\},$$

entonces $(X, \subseteq)$ es un conjunto parcialmente ordenado no vacío en el que toda cadena se estaciona. En efecto, $N \in X$, por lo que $X \neq \emptyset$ y dada una cadena ascendente $S = (L_i)_{i \in \mathbb{N}}$ en X, si se supone que $L = M$, donde $L = \sum_{i \in \mathbb{N}} L_i$, entonces existe $F \subseteq \mathbb{N}$ finito tal que $L = \sum_{i \in F} L_i$ debido a que M es finitamente generado, y entonces $M = L_m$ donde $m = max(F)$, lo cual es una contradicción pues $L_m \in X$. Por lo tanto, $L \in X$. Esto muestra que toda cadena tiene cota superior en X, lo que implica por el lema de Zorn que X tiene un elemento maximal M'. Ahora, M' es un submódulo maximal, ya que si se supone que M' está contenido en un submódulo K, se tiene que $L \subseteq M' \subseteq K$, lo que implica que $K = M$ ó $K = M'$ por la maximalidad de M'. Por lo tanto, N se encuentra contenido en un submódulo maximal M'.

(b) Si M no tiene submódulos propios, entonces M es simple, y entonces M es distinto a $\mathrm{rad}(M)$ pues $\mathrm{rad}(M) = 0$. Si M tiene un submódulo propio N, entonces éste esta contenido en un submódulo maximal H, por lo que $\mathrm{rad}(M) \subseteq H \neq M$.

□

Se tiene el siguiente resultado, conocido como el lema de Nakayama.

Lema 5.29. *Si M es un módulo finitamente generado y N un submódulo de M, entonces $N \subseteq \mathrm{rad}(M)$ si, y sólo si, para todo submódulo L de M tal que $L + N = M$ se tiene que $L = M$. En particular, si $L + \mathrm{rad}(M) = M$, entonces $L = M$.*

Demostración. Sea $N \subseteq \operatorname{rad}(M)$ y $L \subseteq M$ tal que $L+N=M$. Si $L \neq M$, por el lema anterior L está contenido en un submódulo maximal H, de manera que

$$M = L + N \subseteq H + N \subseteq M,$$

por lo que $M = H+N \subseteq H+\operatorname{rad}(M) = H$, lo cual es una contradicción. Por lo tanto, $L = M$.

Recíprocamente, si N es un submódulo de M que cumple que, para todo $L_A \subseteq M_A$ tal que $L+N=M$ se tiene que $L=M$, entonces dado H un submódulo maximal tal que $N \nsubseteq H$ se tiene que $N+H=M$, lo que implica que $H=M$, que es una contradicción. Por lo tanto, $N \subseteq H$ para cualquier H maximal, y así $N \subseteq \operatorname{rad}(M)$. □

Definición 5.30. Si N es un módulo de M tal que $N+L \neq M$ para todo $L \neq M$, se dice que N es superfluo y se denota $N \ll M$.

Se tiene entonces que si M es finitamente generado, entonces el radical es superfluo y $M/\operatorname{rad}(M)$ es finitamente generado por la Proposición 1.33.

Recíprocamente, si $M/\operatorname{rad}(M)$ es finitamente generado y $\operatorname{rad}(M)$ es superfluo, entonces M es finitamente generado. En efecto, dada X una familia de submódulos de M tal que $\sum_{N\in X} N = M$, sea $Y = \{\overline{N} \mid N \in X\}$ donde $\overline{N} = (N+\operatorname{rad}(M))/\operatorname{rad}(M)$, esta es una familia de submódulos de $M/\operatorname{rad}(M)$ tal que $\sum_{\overline{N}\in Y} \overline{N} = M/\operatorname{rad}(M)$, por lo que existe $Y' \subseteq Y$ finito tal que $\sum_{\overline{N}\in Y} \overline{N} = \sum_{\overline{N}\in Y'} \overline{N}$, esto es

$$\sum_{N\in X} \overline{N} = \sum_{N\in X'} \overline{N},$$

donde $X' = \{N \in X \mid \overline{N} \in Y'\}$. Con esto se concluye que $\sum_{N\in X} N = \sum_{N\in X'} N$, ya que la igualdad $\sum_{N\in X'} \overline{N} = M/\operatorname{rad}(M)$ implica que $\sum_{N\in X'} N + \operatorname{rad}(M) = M$, pero como $\operatorname{rad}(M)$ es superfluo, $\sum_{N\in X'} N = M$.

Se ha probado la siguiente caracterización de los módulos finitamente generados.

Proposición 5.31. *Un módulo M es finitamente generado, si y sólo si, $M/\operatorname{rad}(M)$ es finitamente generado y $\operatorname{rad}(M)$ es superfluo.*

Ejemplo 5.32. Sea $M = \prod_{p\in X} \mathbb{Z}_p$. Se ha visto que $\operatorname{rad}(M) = 0$, lo que implica que $M/\operatorname{rad}(M) \cong M$ no es finitamente generado. Por lo tanto, $\operatorname{rad}(M)$ es superfluo pero $M/\operatorname{rad}(M)$ no es finitamente generado.

Ejemplo 5.33. Sean $A = \mathbb{Q}[x]S^{-1}$ donde

$$S = \{p(x) \in \mathbb{Q}[x] \mid p(0) \neq 0\}$$

y $M = \mathbb{Q}(x)$. Se ha visto que $\operatorname{rad}(M) = M$, por lo que $\operatorname{rad}(M)$ no es superfluo. Por lo tanto, $M/\operatorname{rad}(M)$ es finitamente generado, pero $\operatorname{rad}(M)$ no es superfluo.

Por otro lado, nótese que en la demostración del Corolario 5.29 se probó que todo submódulo del radical es superfluo si el módulo es finitamente generado. De hecho si L es un submódulo superfluo de un módulo M y N es un submódulo maximal de M, entonces $L \subseteq N$. En efecto, si se supone que $L \nsubseteq N$, entonces $L + N = M$, pero como L es superfluo $M = N$ lo cual es una contradicción. Por lo tanto, el radical contiene la suma de todos los submódulos superfluos.

Recíprocamente, dado $x \in \operatorname{rad}(M)$ y N un submódulo de M tal que $xA + N = M$, entonces $N = M$ ó existe un submódulo maximal M' que contiene a N pero no a x, pero esto último no puede ocurrir debido a que $x \in \operatorname{rad}(M)$. Por lo tanto, $\operatorname{rad}(M)$ está contendido en la suma de todos los submódulos superfluos.

Proposición 5.34. *Si M es un módulo, entonces* $\operatorname{rad}(M)$ *es igual a la suma de todos los submódulos superfluos de M.*

Ejemplo 5.35. Sea k un campo. Si A es el anillo de matrices generalizadas con producto trivial 2.30

$$A = \begin{pmatrix} k & M_{12} & \dots & M_{1n} \\ M_{21} & k & & \\ \vdots & & \ddots & \\ M_{n1} & & & k \end{pmatrix} \text{ y } M = \begin{pmatrix} 0 & M_{12} & \dots & M_{1n} \\ M_{21} & 0 & & \\ \vdots & & \ddots & \\ M_{n1} & & & 0 \end{pmatrix},$$

entonces $\operatorname{rad}(A_A) = M$. En efecto, es sencillo probar que M es superfluo, pues si se supone que existe un submódulo K de A_A tal que $M + K = A$, entonces existe un elemento x de K con todas las entradas en la diagonal diferentes de 0; pero en tal caso

$$A \supseteq K \supseteq xA = A,$$

por lo que $K = A$. Por lo tanto, M es superfluo, lo que implica que $\operatorname{rad}(A_A) \subseteq M$. Además es sencillo probar que los módulos

$$\begin{pmatrix} 0 & M_{12} & \dots & M_{1n} \\ M_{21} & k & & \\ \vdots & & \ddots & \\ M_{n1} & & & k \end{pmatrix}, \begin{pmatrix} k & M_{12} & \dots & M_{1n} \\ M_{21} & 0 & & \\ \vdots & & \ddots & \\ M_{n1} & & & k \end{pmatrix}, \dots, \begin{pmatrix} k & M_{12} & \dots & M_{1n} \\ M_{21} & k & & \\ \vdots & & \ddots & \\ M_{n1} & & & 0 \end{pmatrix}$$

son maximales, por lo que M está contenido en la intersección de los submódulos maximales, por lo tanto $M = \operatorname{rad}(A_A)$.

5.2.2. El radical de Jacobson

En esta subsección se muestra que $\operatorname{rad}(A_A) = \operatorname{rad}({}_AA)$ para todo anillo A, por obvias razones este ideal bilateral es importante para estudiar la estructura del anillo y recibe el nombre de radical de Jacobson.

El siguiente lema caracteriza los elementos del radical del anillo.

Lema 5.36. *Sea A un anillo y $a \in A$. Las siguientes condiciones son equivalentes:*

(a) $a \in \operatorname{rad}(A_A)$.

(b) $\forall b \in A, 1 - ab$ *tiene un inverso derecho.*

(c) $\forall b \in A, 1 - ab$ *tiene inverso derecho e izquierdo.*

(d) $\forall b \in A, 1 - ba$ *tiene inverso derecho e izquierdo.*

(e) $\forall b \in A, 1 - ba$ *tiene inverso izquierdo.*

(f) $a \in \operatorname{rad}({}_A A)$.

Demostración. $(a \Rightarrow b)$ Sea $a \in \operatorname{rad}(A)$ y $b \in A$. Si $1 - ab$ no tiene inverso, entonces por el lema de Zorn existe $I \subsetneq A$ ideal derecho maximal tal que $1 - ab \in I$, pero como $a \in \operatorname{rad}(A) \subseteq I$ se tiene que $ab \in I$, por lo que $1 = (1 - ab) + ab \in I$, lo que implica que $I = A$, que es una contradicción. Por lo tanto, $1 - ab$ tiene inverso derecho.

$(a \Leftarrow b)$ Sea $I \subsetneq A$ un ideal derecho maximal de A. Si $a \notin I$, entonces $A = I + aA$ pues $I \subsetneq I + aA$ e I es maximal, lo que implica que $1 = x + ab$ para alguna $x \in I$ y $b \in A$, y entonces $x = 1 - ab$ que es invertible por (a), por lo que $I = A$, lo cual es una contradicción. Por lo tanto, $a \in I$. En consecuencia, a se encuentra en todos los ideales maximales, esto es $a \in \operatorname{rad}(A)$.

$(b \Rightarrow c)$ Sean $a \in \operatorname{rad}(A)$, $b \in A$ y x el inverso derecho de $1 - ab$, de manera que

$$1 = (1 - ab)x = x - abx.$$

Ahora, $x = 1 + abx = 1 - a(-bx)$, entonces x tiene un inverso derecho y por (b), esto es $1 = xy = (1 + abx)y = y + ab$, lo que implica que $y = 1 - ab$. Por lo tanto, $1 - ab$ tiene un inverso izquierdo x.

$(b \Leftarrow c)$ Trivial.

$(c \Rightarrow d)$ Sean $a \in \operatorname{rad}(A)$, $b \in A$ y x, $y \in A$ los inversos izquierdo y derecho respectivamente de $1 - ab$, entonces

$$(1-bxa)(1-ba) = 1-bxa-ba+bxaba = 1-b(x-1+xab)a = 1-b(x(1-ab)-1)a = 1.$$

Por lo tanto, $1 - bxa$ es inverso izquierdo de $1 - ba$, y análogamente $1 - bya$ es su inverso derecho.

$(d \Leftrightarrow e)$ Análogo a $(b \Leftrightarrow c)$.

$(e \Leftrightarrow f)$ Análogo a $(a \Leftrightarrow b)$. $\square$

Con esta proposición se ha probado que $\operatorname{rad}(A_A) = \operatorname{rad}({}_AA)$, es decir el radical como módulo derecho es el radical como módulo izquierdo. Lo que lleva a la siguiente definición.

Definición 5.37. Sea A un anillo. El radical de Jacobson, denotado como $\operatorname{rad}(A)$, es la intersección de todos los ideales derechos maximales, ó equivalentemente, la intersección de todos los ideales izquierdos maximales, es decir $\operatorname{rad}(A) = \operatorname{rad}({}_AA) = \operatorname{rad}(A_A)$.

Ya caracterizados los elementos es sencillo verificar las siguientes propiedades.

Corolario 5.38. *Sea A un anillo. Se cumplen los siguientes enunciados:*

(a) $\operatorname{rad}(A)$ *es la intersección de todos los ideales maximales izquierdos.*

(b) $\operatorname{rad}(A)$ *es un ideal bilateral.*

(c) *Si e un idempotente de A, entonces* $e(\operatorname{rad}(A))e = \operatorname{rad}(eAe)$.

(d) *Si e un idempotente de A y $\bar{e} = e + \operatorname{rad}(A)$, entonces $\bar{e}$ es un idempotente de $A/\operatorname{rad}(A)$ tal que $\bar{e}(A/\operatorname{rad}(A))\bar{e} \cong eAe/\operatorname{rad}(eAe)$.*

(e) *Si I es un ideal tal que todo elemento de I es nilpotente, entonces $I \subseteq \operatorname{rad}(A)$.*

(f) *Si I es un ideal bilateral nilpotente de A, entonces $I \subseteq \operatorname{rad}(A)$.*

Demostración. Sean A un anillo, e un idempotente y $f = 1 - e$.

(a) Es inmediato del punto (f) del lema anterior.

(b) Como $\operatorname{rad}(A)$ es intersección de ideales derechos, $\operatorname{rad}(A)$ es un ideal derecho; y como también es intersección de ideales izquierdos, es un ideal derecho e izquierdo, por lo que es un ideal bilateral.

(c) Se observa que dado $a = ebe \in eAe$ se cumple que $ea = ae = eae = ebe$. Luego, si $r = ere \in rad(eAe)$ para todo $a \in A$ se cumple que $e - ra$ es invertible por la derecha en eAe, es decir existe $y = eye \in eAe$ tal que $(e - ra)y = e$, por lo que dado $a \in A$

$$(1 - ra)(y + f) = (f + e - ra)(y + f) = fy + e + f = 1,$$

y así $r \in \operatorname{rad}(A)$. Por lo tanto, $\operatorname{rad}(eAe) \subseteq e(\operatorname{rad}(A))e$.
Recíprocamente, si $r = ere \in e(\operatorname{rad}(A))e \subseteq \operatorname{rad}(A)$, entonces para toda $a \in A$ existe $y \in A$ tal que $y(1 - ra) = 1$. En particular si $a = eae \in eAe$

$$e = ey(1 - ra)e = ey(e + f - ra)e = ey(e - ra) = eye(e - ra),$$

por lo que $e(\operatorname{rad}(A))e \subseteq \operatorname{rad}(eAe)$. Por lo tanto, $e(\operatorname{rad}(A))e = \operatorname{rad}(eAe)$.

(d) Se define $f : eAe \to \bar{e}(A/\operatorname{rad}(A))\bar{e}$, como $f(eae) = eae + \operatorname{rad}(A)$. Claramente f es un epimorfismo y $\operatorname{Ker}(f) = e(\operatorname{rad}(A))e$, entonces el primer teorema de isomorfismo implica el resultado.

(e) Es bien sabido que si $x \in A$ es nilpotente, entonces $1 - x$ es invertible ya que si $0 = x^m$, entonces

$$(1-x)(1+x+x^2+...+x^{m-1}) = 1 - x^m = 1.$$

Así, si se supone que J es un ideal maximal tal que $I \nsubseteq J$, se tiene que $I + J = A$ lo que implica que existen $a \in I$ y $b \in J$ tales que $1 = a + b$; pero entonces $b = 1 - a$ es invertible ya que a es nilpotente por pertenecer a I. En consecuencia $J = A$, lo cual es una contradicción.

(f) Es inmediato del punto anterior.

□

Observación 5.39. Más adelante se verán casos cuando el radical de Jacobson es nilpotente, por lo que (f) implica en tales casos que el radical es el mayor ideal nilpotente. Sin embargo en general el radical no es nilpotente como muestra el siguiente ejemplo.

Ejemplo 5.40. Sea k un campo y

$$A = k[[x]] = \{\sum_{n=0}^{\infty} a_n x^n \quad | \quad a_i \in k \, \forall i\}$$

el anillo de series formales de potencias sobre k. Es sencillo mostrar que $\sum_{n=0}^{\infty} a_n x^n \in A$ es invertible si, y sólo si, $a_0 \neq 0$. De manera que el ideal generado por x es un ideal maximal único, lo que implica que $\operatorname{rad}(A) = xA$, que claramente no es nilpotente.

Ejemplo 5.41. Si k un dominio entero y $A = k\langle x_i \rangle_{i \in X}$, el anillo asociativo no conmutativo, donde X es un conjunto arbitrario de subíndices, entonces $\operatorname{rad}(A) = 0$. En efecto, sea $p \in A$ de grado $n > 0$, es claro que p no es invertible ya que pq es de grado mayor ó igual a n para todo $q \in A$. En consecuencia, si se toma $x = x_i$ para algún $i \in X$ y $p \in \operatorname{rad}(A)$, por (5.36) se deduce que $1 - xp$ es invertible; pero entonces $1 - xp$ es de grado 0, lo que implica que $xp \in k$ y entonces $p = 0$. Por lo tanto, $\operatorname{rad}(A) = 0$. Análogamente, si $B = k\,[x_i]_{i \in X}$ se prueba que $\operatorname{rad}(B) = 0$.

Ahora, con la proposición anterior se puede utilizar la descomposición de Peirce del anillo para visualizar el radical, como muestra el siguiente teorema.

Teorema 5.42. *Si A tiene una descomposición de la unidad $1_A = e_1 + ... + e_n$, entonces $e_i \operatorname{rad}(A) e_j = e_i A e_j$ para toda $i \neq j$ y*

$$\operatorname{rad}(A) = (\bigoplus_{i=1}^{n} \operatorname{rad}(e_i A e_i)) \oplus (\bigoplus_{i,j=1}^{n} e_i A e_j)$$

si, y sólo si, $e_iAe_j \subseteq \mathrm{rad}(A)$ *para todo* $i \neq j$ *en el conjunto* $\{1, ..., n\}$.

Demostración. La necesidad de que $e_iAe_j \subseteq \mathrm{rad}(A)$ para todo $i \neq j$ es inmediata, y tal condición es suficiente ya que por la Proposición 2.19 y la proposición anterior $\mathrm{rad}(A)$ es igual a

$$(\bigoplus_{i=1}^{n} e_i \,\mathrm{rad}(A)e_i) \oplus (\bigoplus_{i\neq j=1}^{n} e_i \,\mathrm{rad}(A)e_j) = (\bigoplus_{i=1}^{n} \mathrm{rad}(e_iAe_i)) \oplus (\bigoplus_{i\neq j=1}^{n} e_i \,\mathrm{rad}(A)e_j).$$

Esto muestra que basta probar que si $i \neq j$, entonces $e_i \,\mathrm{rad}(A)e_j = e_iAe_j$, pero por hipótesis $e_iAe_j \subseteq \mathrm{rad}(A)$ lo que implica que

$$e_iAe_j = e_i^2Ae_j^2 \subseteq e_i \,\mathrm{rad}(A)e_j,$$

y es claro que $e_i \,\mathrm{rad}(A)e_j \subseteq e_iAe_j$. Por lo tanto, $e_i \,\mathrm{rad}(A)e_j = e_iAe_j$. □

Ejemplo 5.43. Si A es un anillo de matrices generalizadas de orden n tal que $M_{ij} = 0$ para todo $i > j$,

$$\begin{pmatrix} A_1 & M_{21} & \dots & M_{1n} \\ 0 & A_2 & & \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & A_n \end{pmatrix}, \text{ entonces } \mathrm{rad}(A) = \begin{pmatrix} \mathrm{rad}(A_1) & M_{21} & \dots & M_{1n} \\ 0 & \mathrm{rad}(A_2) & & \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & \mathrm{rad}(A_n) \end{pmatrix}.$$

En efecto, si $1 = e_1 + ... + e_n$ es la descomposición de la unidad inducida, para todo $i \neq j$ el ideal $M_{ij}A$ es nilpotente ya que

$$(M_{ij}A)^2 = (e_iAe_jA)^2 = e_iA(e_jAe_iA)e_jA = e_iA(M_{ji}A)e_jA = 0,$$

lo que implica que $e_iAe_j \subseteq \mathrm{rad}(A)$ para todo $i \neq j$.

Ejemplo 5.44. Se prueba análogamente al ejemplo anterior que si A es un anillo generalizado de matrices con producto trivial 2.30

$$A = \begin{pmatrix} A_1 & M_{12} & \dots & M_{1n} \\ M_{21} & A_2 & & \\ \vdots & & \ddots & \\ M_{n1} & & & A_n \end{pmatrix},$$

es decir $M_{ij}M_{jk} = 0$ para toda $i \neq j$ y $j \neq k$, entonces

$$\operatorname{rad}(A) = \begin{pmatrix} \operatorname{rad}(A_1) & M_{12} & \dots & M_{1n} \\ M_{21} & \operatorname{rad}(A_2) & & \\ \vdots & & \ddots & \\ M_{n1} & & & \operatorname{rad}(A_n) \end{pmatrix}.$$

Proposición 5.45. *Dado un módulo derecho M sobre un anillo A, se tiene que $M \operatorname{rad}(A) \subseteq \operatorname{rad}(M)$.*

Demostración. Para cada $m \in M$ existe un morfismo $f_m : A \to M$ definido como $f(x) = mx$. Luego, por el Lema 5.22 se sigue que $m \cdot \operatorname{rad}(A) \subseteq \operatorname{rad}(M)$ para todo $m \in M$. Así,

$$M \operatorname{rad}(A) = \sum_{m \in M} m \operatorname{rad}(A) \subseteq \operatorname{rad}(M).$$

□

Con esta proposición es posible demostrar el siguiente resultado, el lema de Nakayama.

Lema 5.46. *Para todo ideal derecho $I \subseteq A$, los siguientes enunciados son equivalentes:*

(a) *$I \subseteq \operatorname{rad}(A)$.*

(b) *Dado un módulo finitamente generado M. Si $MI = M$, entonces $M = 0$.*

(c) *Sea $N \subseteq M$ tal que M/N es finitamente generado. Si $N + MI = M$, entonces $M = N$.*

Demostración. ($a \Rightarrow b$) Por la Proposición 5.45 se cumple que

$$MI \subseteq M \operatorname{rad}(A) \subseteq \operatorname{rad}(M).$$

Luego, como M es finitamente generado y $0 + MI = M$, el Corolario 5.29 implica que $M = 0$.

($b \Rightarrow c$) Si $N + MI = M$, entonces $(MI + N)/N = M/N$ y M/N es finitamente generado, entonces por (b) $M/N = 0$. Por lo tanto, $M = N$.

($c \Rightarrow a$) Si se supone que existe $x \in I$ que no pertenece a $\operatorname{rad}(A)$, entonces existe un ideal maximal J tal que $x \notin J$. De esta manera, $J + AI = A$, lo que implica por (c) que $A = J$, lo cual es una contradicción. Por lo tanto, $J \subseteq \operatorname{rad}(A)$. □

5.2.2.1. El radical de un módulo proyectivo

Se ha probado que para todo A-módulo derecho $M \operatorname{rad}(A) \subseteq \operatorname{rad}(M)$, y es importante mencionar que en general $\operatorname{rad}(M) \neq M \operatorname{rad}(A)$, como es el caso de $A = \mathbb{Z}$ y $M = \mathbb{Z}_{p^2}$. Sin embargo, si M es un módulo proyectivo se cumple que $M \operatorname{rad}(A) = \operatorname{rad}(M)$ entre otras interesantes propiedades. Esta subsubsección contiene tales resultados.

Proposición 5.47. *Sea A un anillo. Se cumplen los siguientes enunciados.*

(a) $A \operatorname{rad}(A) = \operatorname{rad}(A)$ *y* $\operatorname{rad}(A) = \operatorname{rad}(A)A$.

(b) *Si P es un A-módulo derecho libre, entonces* $\operatorname{rad}(P) = P \operatorname{rad}(A)$.

(c) *Si P es un A-módulo proyectivo derecho, entonces* $\operatorname{rad}(P) = P \operatorname{rad}(A)$.

(d) *Si e es un idempotente de A, entonces* $\operatorname{rad}(eA) = e(\operatorname{rad}(A))$.

(e) *Si e es un idempotente de A, entonces*

$$(e + \operatorname{rad}(A))(A/\operatorname{rad}(A)) = eA/\operatorname{rad}(eA) = eA/e\operatorname{rad}(A).$$

Demostración. Sea A un anillo.

(a) Se sigue del hecho de que $\operatorname{rad}(A)$ es un ideal bilateral.

(b) Si P es libre, entonces existe un conjunto X tal que $P \cong A^{(X)}$, lo que implica que

$$\operatorname{rad}(P) \cong \operatorname{rad}(A^{(X)}) = \operatorname{rad}(A)^{(X)} = (A \operatorname{rad}(A))^{(X)} = A^{(X)} \operatorname{rad}(A) \cong P \operatorname{rad}(A).$$

Por lo tanto, $\operatorname{rad}(P) = P \operatorname{rad}(A)$.

(c) Si P es un módulo proyectivo, es sumando directo de un módulo libre L, entonces existe un módulo M y un conjunto X tal que $P \oplus M = L = A^{(X)}$. De tal manera que

$$\begin{aligned}
\operatorname{rad}(P) \oplus \operatorname{rad}(M) &= \operatorname{rad}(P \oplus M) \\
&= \operatorname{rad}(L) \\
&= L \operatorname{rad}(A) \\
&= (P \oplus M) \operatorname{rad}(A) \\
&= (P \operatorname{rad}(A)) \oplus (M \operatorname{rad}(A)),
\end{aligned}$$

lo que implica que $\operatorname{rad}(P) = P \operatorname{rad}(A)$.

(d) El ideal eA es un sumando directo de A, y como tal es un módulo proyectivo, entonces por el punto anterior $\operatorname{rad}(eA) = eA \operatorname{rad}(A) = e \operatorname{rad}(A)$.

(e) Es inmediato del punto anterior.

□

Por otro lado se tiene el siguiente resultado, que se puede utilizar para diferenciar módulos proyectivos.

Corolario 5.48. *Sea A un anillo y J un ideal bilateral contenido en* $\operatorname{rad}(A)$*. Si P y Q son módulos proyectivos finitamente generados, entonces $P \cong Q$ si, y sólo si, $P/PJ \cong Q/QJ$. En particular, $P \cong Q$ si, y sólo si, $P/\operatorname{rad}(P) \cong Q/\operatorname{rad}(Q)$.*

Demostración. Supóngase que existe un isomorfismo $f : P \to Q$, y considérese la proyección natural $g : Q \to Q/QJ$, entonces

$$\operatorname{Ker}(gf) = \{x \in P \quad | \quad f(x) \in QJ\} = f^{-1}(Q)J = PJ.$$

Lo que implica por el tercer teorema de isomorfismo que $P/PJ \cong Q/QJ$.

Recíprocamente, si existe un isomorfismo $f : P/PJ \to Q/QJ$, considérense las proyecciones naturales $g : Q \to Q/QJ$ y $h : P \to P/PJ$, entonces como P es proyectivo existe un morfismo $l : P \to Q$ que hace conmutar el diagrama.

$$\begin{array}{ccccc} P & \xrightarrow{h} & P/PJ & & \\ l\downarrow & & \downarrow f & & \\ Q & \xrightarrow{g} & Q/QJ & \longrightarrow & 0 \end{array}$$

Además l es un isomorfismo. Ciertamente, nótese que

$$Q/QJ = \operatorname{Im}(fh) = \operatorname{Im}(gl) = (\operatorname{Im}(l) + QJ)/QJ,$$

lo que implica que $Q = \operatorname{Im}(l) + QJ$, y debido a que Q/QJ es finitamente generado y $J \subseteq \operatorname{rad}(A)$, el lema de Nakayama 5.46 implica que $\operatorname{Im}(l) = Q$. Por lo tanto, l es epimorfismo. Para probar que tambíen es un monomorfismo, se observa que la sucesión

$$0 \to \operatorname{Ker}(l) \to P \xrightarrow{l} Q \to 0$$

se escinde debido a que Q es proyectivo. En consecuencia, $P = Q' \oplus \operatorname{Ker}(l)$ con $Q' \cong Q$. Ahora, como $fh = gl$

$$\operatorname{Ker}(l) \subseteq \operatorname{Ker}(fh) = PJ = Q'J \oplus \operatorname{Ker}(l)J \subseteq Q'J \oplus \operatorname{Ker}(l),$$

lo que implica que $\operatorname{Ker}(l) = \operatorname{Ker}(l)J$, y entonces el lema 5.46 implica que $\operatorname{Ker}(l) = 0$, pues al ser un sumando directo de P es $\operatorname{Ker}(l)$ finitamente generado. Por lo tanto, P y Q son isomorfos. □

Como corolario se tiene el siguiente resultado.

Corolario 5.49. *Si P es un A-módulo proyectivo no nulo, entonces existe un submódulo maximal de P, es decir* $\operatorname{rad}(P) \neq P$.

Demostración. Si se supone que $\operatorname{rad}(P) = P$, entonces $P/\operatorname{rad}(P) = 0$; pero en tal caso la proposición anterior implica que $P = 0$, ya que el módulo 0 es proyectivo y cumple que $0 = 0/\operatorname{rad}(0)$. □

5.2.3. El radical de Jacobson de un anillo artiniano

En esta subsección se prueba que el radical de un anillo artiniano es nilpotente y que el cociente del anillo con su radical es un anillo semisimple, así como algunas consecuencias de estas dos condiciones.

Si A_A es artiniano, entonces como la sucesión $(\operatorname{rad}(A)^i)_{i\in\mathbb{N}}$ es descendente, existe un natural m tal que $\operatorname{rad}(A)^m \operatorname{rad}(A) = \operatorname{rad}(A)^m$, lo que implica que $\operatorname{rad}(A)^m = 0$. En efecto, si se supone que $\operatorname{rad}(A)^m \neq 0$, entonces por ser A_A artiniano existe un submódulo minimal I del conjunto X de submódulos J de A_A tales que $J(\operatorname{rad}(A)^m) \neq 0$, por lo que existe $a \in I$ tal que $a(\operatorname{rad}(A)^m) \neq 0$, pero debido a que $\operatorname{rad}(A)^m \operatorname{rad}(A) = \operatorname{rad}(A)^m$, inductivamente se cumple que

$$a(\operatorname{rad}(A)^m)(\operatorname{rad}(A)^m) = a(\operatorname{rad}(A)^m) \neq 0,$$

lo que implica que $a(\operatorname{rad}(A)^m)$ es un submódulo que pertenece al conjunto X, pero por la minimalidad de I se tiene que $I = a(\operatorname{rad}(A)^m)$, lo que implica que $a = ax$ para algún $x \in \operatorname{rad}(A)$; pero entonces $0 = a(1-x)$, lo que implica que $a = 0$ ya que $1-x$ es invertible, lo cual es una contradicción. Por lo tanto, $\operatorname{rad}(A)^m = 0$.

Proposición 5.50. *Si A_A es artiniano, entonces* $\operatorname{rad}(A)$ *es nilpotente.*

Por otro lado, si A_A es artiniano y $\operatorname{rad}(A) = 0$, entonces por la Proposición 4.6 existe un conjunto finito de ideales maximales derechos F tal que $\bigcap_{N\in F} N = 0$, entonces considerando las proyecciones naturales $\pi_N : A \to A/N$, gracias a la propiedad universal del producto éstas inducen un morfismo $f : A \to \bigoplus_{N\in F} A/N$ tal que

$$\operatorname{Ker}(f) = \bigcap_{N\in F} \operatorname{Ker}(\pi_N) = \bigcap_{N\in F} N = 0,$$

que claramente es epimorfismo. Por lo tanto, $A \cong \bigoplus_{N\in F} A/N$, y en consecuencia A es semisimple.

Recíprocamente, si A es semisimple, entonces es una suma finita de simples, y como tal es artiniano y $\operatorname{rad}(A) = 0$ por el Corolario 4.11 y (5.25). Se ha probado el siguiente resultado.

Proposición 5.51. *El anillo A es semisimple si y sólo si* $\operatorname{rad}(A) = 0$ *y* A_A *es artiniano.*

Ahora, si A_A es artiniano, $A/\operatorname{rad}(A)$ también es artiniano y $\operatorname{rad}(A/\operatorname{rad}(A)) = 0$, lo que implica que $A/\operatorname{rad}(A)$ es semisimple. Por lo tanto, se ha probado que un anillo artiniano a la derecha A cumple que $\operatorname{rad}(A)$ es nilpotente y $A/\operatorname{rad}(A)$ es semisimple.

Cuando un anillo cumple estas propiedades el radical es especialmente útil, como muestra la siguiente proposición.

Proposición 5.52. *Sea A un anillo tal que* $A/\operatorname{rad}(A)$ *es un anillo semisimple, y M es un A-módulo derecho.*

(a) *Si* $M\operatorname{rad}(A) = 0$*, entonces M es semisimple.*

(b) $\operatorname{rad}(M) = M\operatorname{rad}(A)$.

(c) $\operatorname{rad}(M) = 0$ *si, y sólo si, M es semisimple.*

(d) *Los módulos simples de* $A/\operatorname{rad}(A)$ *son los módulos simples de A.*

(e) *Existe un número finito de A -módulos derechos simples no isomorfos.*

Demostración. Sea A un anillo tal que $A/\operatorname{rad}(A)$ es un anillo semisimple.

(a) Si M es un módulo con $M\operatorname{rad}(A) = 0$, entonces M es un $A/\operatorname{rad}(A)$-módulo. Además, un grupo abeliano N es un A-submódulo de M_A si, y sólo si, es un $A/\operatorname{rad}(A)$-submódulo de $M_{A/\operatorname{rad}(A)}$ por la Proposición 1.9, entonces como todo módulo sobre un anillo semisimple es semisimple, M_A es semisimple.

(b) Por la Proposición 5.45 se tiene que $M\operatorname{rad}(A) \subseteq \operatorname{rad}(M)$, por lo que basta probar que $\operatorname{rad}(M) \subseteq M\operatorname{rad}(A)$. Para ello considérese $N = M/M\operatorname{rad}(A)$, claramente $N\operatorname{rad}(A) = 0$, de manera que N es semisimple, lo que implica que

$$0 = \operatorname{rad}(N) = \operatorname{rad}(M/M\operatorname{rad}(A)) = \operatorname{rad}(M)/M\operatorname{rad}(A)$$

por el Corolario 5.23 ya que $M\operatorname{rad}(A) \subseteq \operatorname{rad}(M)$. Por lo tanto,

$$\operatorname{rad}(M) = M\operatorname{rad}(A).$$

(c) Si $rad(M) = 0$, entonces $M\operatorname{rad}(A) = \operatorname{rad}(M) = 0$, con lo que se concluye que M es semisimple. Recíprocamente, si M es semisimple ya se ha probado que $\operatorname{rad}(M) = 0$.

(d) Si S es un A-módulo simple, entonces $S\operatorname{rad}(A) = \operatorname{rad}(S) = 0$, por lo que S es un módulo semisimple sobre $A/\operatorname{rad}(A)$. Y como es simple sobre A, no es una suma directa de módulos sobre $A/\operatorname{rad}(A)$, por lo que S es un $A/\operatorname{rad}(A)$ módulo simple.

(e) Se sabe que $A/\operatorname{rad}(A)$ tiene un número finito de módulos simples no isomorfos, por lo que A también tiene un número finito de simples no isomorfos.

□

Luego, si además $\operatorname{rad}(A)$ es nilpotente, es decir existe un m tal que $\operatorname{rad}(A)^m = 0$, entonces considerando la sucesión

$$0 = \operatorname{rad}(A)^m \subseteq \operatorname{rad}(A)^{m-1} \subseteq \ldots \subseteq \operatorname{rad}(A) \subseteq A,$$

se observa que el cociente de dos módulos consecutivos es semisimple, pues

$$\operatorname{rad}(\operatorname{rad}(A)^n/\operatorname{rad}(A)^{n+1}) = (\operatorname{rad}(A)^n/\operatorname{rad}(A)^{n+1})\operatorname{rad}(A) = 0.$$

En consecuencia, si A_A es artiniano ó noetheriano, todo cociente de módulos consecutivos de la sucesión es una suma finita de simples por el Corolario 4.11, entonces cada uno de estos cocientes tienen serie de composición, lo que implica que A tiene serie de composición por la Proposición 4.52.

Lo que lleva a la sorprendente conclusión de que todo anillo artiniano es noetheriano. Este resultado es el teorema de Hopkins-Levitzki.

Teorema 5.53. *Sea A un anillo. El módulo A_A es artiniano si y sólo si A_A es noetheriano, $A/\operatorname{rad}(A)$ es semisimple y $\operatorname{rad}(A)$ es nilpotente.*

Demostración. Si A es artiniano por la derecha, se sabe que $A/\operatorname{rad}(A)$ es semisimple y $\operatorname{rad}(A)$ es nilpotente, y por la argumentación anterior es de longitud finita, por lo que es noetheriano por la derecha.

Si A_A es noetheriano, $A/\operatorname{rad}(A)$ es semisimple y $\operatorname{rad}(A)$ es nilpotente, de nuevo por la argumentación anterior A_A es de longitud finita, por lo que A_A es artiniano. □

Por último, se ha visto en la Proposición 5.52 que si $A/\operatorname{rad}(A)$ es semisimple entonces A tiene un número finito de clases de módulos simples. A continuación se prueba que, de hecho sin importar si $A/\operatorname{rad}(A)$ es semisimple ó no, A y $A/\operatorname{rad}(A)$ tienen los mismos simples y los mismos elementos invertibles. Esta última proposición relaciona A y $A/\operatorname{rad}(A)$ de esta manera.

Proposición 5.54. *Sea A un anillo, entonces A y $A/\operatorname{rad}(A)$ tienen los mismos módulos simples, y $x \in A$ tiene inverso por la derecha ó izquierda si y sólo si $x + \operatorname{rad}(A)$ tiene inverso por la derecha ó izquierda.*

Demostración. Sea S un A-módulo simple, entonces $S\operatorname{rad}(A) \subseteq \operatorname{rad}(S) = 0$ por la Proposición 5.45, por lo que S es un $A/\operatorname{rad}(A)$-módulo simple por la Proposición 1.9.

Recíprocamente, si S es un $A/\operatorname{rad}(A)$ módulo simple, entonces S es un A-módulo simple por la Proposición 1.8.

Ahora, si x tiene inverso por derecha ó izquierda, entonces claramente $x+\operatorname{rad}(A)$ tiene inverso por derecha ó izquierda. Recíprocamente, si existe $y+\operatorname{rad}(A) \in A/\operatorname{rad}(A)$ tal que $(x+\operatorname{rad}(A))(y+\operatorname{rad}(A)) = 1$, entonces $1-xy \in \operatorname{rad}(A)$, lo que implica que $xy = 1-(1-xy)$ es invertible por el Lema 5.36, por lo que x tiene un inverso a la derecha. Análogamente, si $x+\operatorname{rad}(A)$ tiene inverso a la izquierda, entonces x también. $\square$

6. La envolvente inyectiva y la cubierta proyectiva

En el capítulo anterior se probó que si I es un módulo finitamente cogenerado, entonces $\mathrm{soc}(I)$ es un submódulo esencial de I. Lo que implica que si I_1 e I_2 son módulos inyectivos finitamente cogenerados tales que $\mathrm{soc}(I_1) \cong \mathrm{soc}(I_2)$, entonces $I_1 \cong I_2$.

En efecto, si $f : \mathrm{soc}(I_1) \to \mathrm{soc}(I_2)$ es un isomorfismo y los morfismos $\eta_1 : \mathrm{soc}(I_1) \to I_1$ y $\eta_2 : \mathrm{soc}(I_2) \to I_2$ son las inclusiones naturales, entonces debido a que I_2 es inyectivo existe un morfismo $g : I_1 \to I_2$ tal que $g\eta_1 = \eta_2 f$. Ahora, se observa que

$$\mathrm{soc}(I_1) \cap \mathrm{Ker}(g) = 0$$

lo que implica que $\mathrm{Ker}(g) = 0$ debido a que $\mathrm{soc}(I_1)$ es esencial. Luego, debido a que I_1 es inyectivo, la sucesión exacta

$$0 \to I_1 \to I_2 \to I_2/\operatorname{Im}(g) \to 0$$

se escinde, lo que implica que $I_2 = \operatorname{Im}(g) \oplus K$; pero entonces $K \cap \mathrm{soc}(I_2) = 0$ ya que $\mathrm{soc}(I_2) \subseteq \operatorname{Im}(g)$, lo que implica que $K = 0$ debido a que $\mathrm{soc}(I_2)$ es esencial. Por lo tanto, g es un isomorfismo.

En general, si M es un submódulo esencial de un módulo inyectivo I, entonces se puede probar que I es isomorfo a cualquier otro módulo inyectivo que contenga a M como submódulo esencial. Tal módulo inyectivo recibe el nombre de envolvente inyectiva de M y es el tema de estudio de esta capítulo junto con el concepto dual, la cubierta proyectiva.

6.1. La envolvente inyectiva

Para empezar recuérdese que todo módulo es submódulo de un módulo inyectivo, como se puede ver en la página 35 de [HS71]. Con ello se puede probar que para todo módulo M existe un módulo inyectivo E tal que M es un submódulo esencial de E. Para probarlo se necesita el siguiente lema.

Lema 6.1. *Sea M un A-módulo. Se cumplen los siguientes enunciados.*

(a) *Si M es submódulo de N y K es un submódulo de N que es maximal en el conjunto $\{L \subseteq N \quad | \quad N \cap M = 0\}$, entonces $M \oplus K$ es un submódulo esencial de N y $(M \oplus K)/K$ es submódulo esencial de N/K.*

(b) *Si M es submódulo de N, entonces M es sumando directo de un submódulo esencial de N.*

(c) *Si M es un submódulo de N que no es un sumando directo de N, entonces M es un submódulo esencial propio de un cociente de N.*

(d) *M es inyectivo si, y sólo si, no existe un módulo $N \neq M$ tal que M sea un submódulo esencial de N.*

(e) *Si N es un módulo que contiene a M, entonces M es un submódulo esencial de N si, y sólo si, para todo $0 \neq n \in N$ existe $0 \neq a \in A$ tal que $na \in M$.*

(f) *Si $K \trianglelefteq M$ y $M \trianglelefteq N$, entonces $K \trianglelefteq N$.*

Demostración.

(a) Si L es un submódulo de N tal que $L \cap (M \oplus K) = 0$, se tiene entonces que $L \cap M = L \cap K = 0$ lo que implica que $M \cap (L \oplus K) = 0$, pero K es un submódulo maximal tal que $M \cap K = 0$, de manera que $L = 0$. Por lo tanto, $M \oplus K$ es esencial.
Luego, si L/K es un submódulo propio de N/K, entonces L contiene propiamente a K, lo que implica que $L \cap M \neq 0$, y entonces $L \cap (M \oplus K)$ contiene propiamente a K y así

$$(L/K) \cap (M \oplus K/K) \neq 0.$$

Por lo tanto, $(M \oplus K)/K$ es un submódulo esencial de N/K.

(b) Es inmediato del punto anterior.

(c) Se sigue del punto (a) ya que $M \cong (M \oplus K)/K$.

(d) M es inyectivo si, y sólo si, es sumando directo de todo módulo que lo contenga. De manera que, si M es inyectivo es inmediato que no existe un $N \neq M$ tal que M sea un submódulo esencial de N. Por otro lado, si M no es inyectivo, entonces existe un módulo K que contiene a M y éste no es sumando directo de K; pero entonces el punto anterior implica que M es un submódulo esencial de un cociente de K.

(e) Si M es un submódulo esencial de N, entonces para todo $n \in N$ diferente de 0, el submódulo $nA \cap M$ es distintinto de 0, lo que implica que existe $a \in A$ tal que $na \in M$. Recíprocamente, si M es un submódulo tal que para todo $0 \neq n \in N$ existe $a \in A$ tal que $na \in M$, entonces en particular para todo submódulo $K \neq 0$ de N se tiene que $K \cap M \neq 0$, por lo que M es un submódulo esencial de N.

(f) Es inmediato del punto anterior.

$\square$

Ahora, si M es un módulo contenido en un módulo inyectivo I y X es el conjunto de submódulos N de I tales que $M \trianglelefteq N$, entonces X es un conjunto parcialmente ordenado con la contención tal que toda cadena tiene cota superior en X, gracias al punto (e) del lema anterior. Lo que implica, por el lema de Zorn, que existe un módulo maximal E tal que $M \trianglelefteq E$.

Dicho módulo es además inyectivo, ya que si se supone que E es submódulo esencial de un módulo D, entonces debido a que I es inyectivo existe un morfismo $f : D \to I$ tal que $fi = \mu$ donde $i : E \to D$ y $\mu : E \to I$ son las inclusiones naturales.

$$\begin{tikzcd} 0 \arrow[r] & E \arrow[rr, "i"] \arrow[dr, "\mu"'] & & D \arrow[dl, "f"] \\ & & I & \end{tikzcd}$$

Pero f es un monomorfismo ya que $\mathrm{Ker}(f) \cap E = 0$ debido a que $fi = \mu$, y así $\mathrm{Ker}(f) = 0$ debido a que E es submódulo esencial de D. Luego,

$$M \trianglelefteq E \trianglelefteq D \subseteq I,$$

lo que implica que $M \trianglelefteq D$, pero en tal caso $D = E$ ya que E es maximal en X. Por lo tanto, no existe un módulo $N \neq M$ tal que M sea un submódulo esencial de N, de manera que E es inyectivo por el punto (d) del lema anterior.

Se ha probado la siguiente proposición.

Proposición 6.2. *Si M es un módulo contenido en un módulo inyectivo I, entonces existe un submódulo E de I tal que E es inyectivo y $M \trianglelefteq E$.*

Por supuesto, debido a que todo módulo está contenido en un módulo inyectivo, la proposición anterior implica que todo módulo es submódulo esencial de un módulo inyectivo.

Ahora, cuando se dice que M está contenido en un módulo inyectivo I, esto quiere decir estrictamente que existe un monomorfismo $f : M \to I$. Y si se dice que M es un submódulo esencial de un módulo inyectivo E, esto quiere decir que existe un monomorfismo $g : M \to E$ tal que $\mathrm{Im}(g)$ es un submódulo esencial de E. Por lo tanto, se ha probado que para todo módulo M existe un monomorfismo $f : M \to E$ tal que $\mathrm{Im}(g)$ es esencial y E inyectivo. Lo que lleva a la siguiente definición.

Definición 6.3.

- Se dice que un morfismo $f : M \to N$ es esencial si f es un monomorfismo tal que $\mathrm{Im}(f) \trianglelefteq N$.

- Una pareja (E, f), donde E es un módulo inyectivo y $f : M \to E$ es un morfismo esencial, recibe el nombre de envolvente inyectiva de M.

Ejemplo 6.4. La pareja $(\mathbb{Q}, i)$ es una envolvente inyectiva de $\mathbb{Z}$, donde $i : \mathbb{Z} \to \mathbb{Q}$ es la inclusión natural. En efecto, $\mathbb{Q}$ es inyectivo al ser divisible y el monomorfismo i es esencial ya que para todo $r \in \mathbb{Q}$ existe $n \in \mathbb{Z}$ tal que $rn \in \mathbb{Z}$.

Ejemplo 6.5. Análogamente al ejemplo anterior, se prueba que para todo número primo p la pareja $(\mathbb{Z}_{p^\infty}, f)$ formada por $\mathbb{Z}_{p^\infty} = \left\langle \frac{\bar{1}}{p^n} \in \mathbb{Q}/\mathbb{Z} \quad | \quad n \in \mathbb{N} \right\rangle$ y el monomorfismo $f : \mathbb{Z}_{p^m} \to \mathbb{Z}_{p^\infty}$ dado por $f(1) = \frac{\bar{1}}{p^m}$ es una envolvente inyectiva de $\mathbb{Z}_{p^m}$.

Observación 6.6. Como se puede ver en los ejemplos anteriores, en general una envolvente inyectiva de un módulo finitamente generado no es finitamente generada. Sin embargo, una envolvente inyectiva de un módulo finitamente cogenerado es finitamente cogenerada como se muestra en la siguiente proposición.

Proposición 6.7. *Si M es un módulo finitamente cogenerado y (E, f) es una envolvente inyectiva de M, entonces E es finitamente cogenerado.*

Demostración. Si E es una envolvente inyectiva de M, entonces $M \trianglelefteq E$, lo que implica por la Proposición 5.16 que $\operatorname{soc}(E) \subseteq M$, de manera que $\operatorname{soc}(M) = \operatorname{soc}(E)$ por la Proposición 5.6. Pero además $\operatorname{soc}(M) \trianglelefteq M$ por la Proposición 5.11 debido a que M es finitamente cogenerado. En consecuencia $\operatorname{soc}(E) \trianglelefteq E$ por el Lema 6.1, y como $\operatorname{soc}(E)$ es finitamente cogenerado por ser submódulo de un módulo finitamente cogenerado, E es finitamente cogenerado por la Proposición 5.11. □

La siguiente proposición engloba diferentes caracterizaciones de una envolvente inyectiva. Pero antes es necesaria la siguiente definición.

Definición 6.8. Sea $f : M \to E$ un morfismo de módulos. Se dice que f es es minimal a la izquierda si todo $g \in \operatorname{End}_A(E)$ tal que $gf = f$ es un isomorfismo.

Proposición 6.9. *Sea $f : M \to E$ un morfismo de módulos con E inyectivo. Son equivalentes los siguientes enunciados.*

(a) *(E, f) es una envolvente inyectiva de M.*

(b) *El morfismo f es un monomorfismo minimal a la izquierda.*

(c) *El morfismo f es un monomorfismo y si $h : M \to I$ es un monomorfismo con codominio inyectivo, entonces existe un monomorfismo $g : E \to I$ tal que $h = gf$.*

(d) *El morfismo f es minimal a la izquierda y para todo módulo inyectivo I el morfismo $\operatorname{Hom}_A(f, I) : \operatorname{Hom}_A(E, I) \to \operatorname{Hom}_A(M, I)$ es suprayectivo.*

Demostración.

($a \Rightarrow b$) Si (E, f) es una envolvente inyectiva de M y $g \in \mathrm{End}_A(E)$ es un morfismo tal que $gf = f$, entonces tomando $x \in \mathrm{Ker}(g) \cap \mathrm{Im}(f)$ se observa que

$$x = f(y) = gf(y) = g(x) = 0,$$

de manera que $\mathrm{Ker}(g) = 0$ debido a que f es esencial. En consecuencia, $\mathrm{Im}(g) \cong E$ es sumando directo de E por ser inyectivo. Supóngase entonces que $E = \mathrm{Im}(g) \oplus K$, tomando $x \in K \cap \mathrm{Im}(f)$ se tiene que $x = f(y) = gf(y) = g(x)$ lo que implica que $x \in \mathrm{Im}(g) \cap K = 0$, de esta manera $K \cap \mathrm{Im}(f) = 0$, lo que implica que $K = 0$ debido a que f es esencial. Por lo tanto, g es isomorfismo.

($b \Rightarrow c$) Si $h : M \to I$ es un monomorfismo con codominio inyectivo, entonces debido a que I es inyectivo existe g tal que $gf = h$ y debido a que E es inyectivo existe g' tal que $g'h = f$, de manera que $g'gf = f$ y $g'g \in \mathrm{End}_A(E)$, entonces el punto (b) implica que $g'g$ es un isomorfismo, lo que implica que g es un monomorfismo.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "h"'] & E \arrow[d, "g"] \\ & I \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "h"] \arrow[dr, "f"'] & I \arrow[d, "g'"] \\ & E \end{tikzcd} \qquad \begin{tikzcd} & E \arrow[d, "g"] \\ M \arrow[ur, "f"] \arrow[r, "h"] \arrow[dr, "f"'] & I \arrow[d, "g'"] \\ & E \end{tikzcd}$$

($c \Rightarrow a$) Por la Proposición 6.2 existe un submódulo inyectivo I de E tal que $\mathrm{Im}(f) \trianglelefteq I$, lo que implica por el punto (c) que existe un monomorfismo $h : E \to I$ tal que $hf = f$.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "f"'] & E \arrow[d, "h"] \\ & I \end{tikzcd}$$

Por otro lado, debido a que I es inyectivo $E = I \oplus K$. Luego, si $x \in h(K) \cap \mathrm{Im}(f)$ se tiene que $x = h(k) = f(m)$ para algún $k \in K$ y $m \in M$; pero entonces

$$h(k) = x = f(m) = hf(m),$$

lo que implica que $k = f(m)$, y así $k = 0$ ya que $\mathrm{Im}(f) \cap K \subseteq I \cap K = 0$. Por lo tanto, se ha probado que $x = h(k) = 0$ para toda $x \in h(K) \cap \mathrm{Im}(f)$. Esto muestra que $h(K) = 0$ ya que $f : M \to I$ es esencial, y entonces $K = 0$ ya que h es un monomorfismo. En consecuencia $E = I$, de manera que (E, f) es una envolvente inyectiva de M.

$(b \Rightarrow d)$ Debido a que f es monomorfismo, para todo morfismo $h : M \to I$ con codominio inyectivo existe $g : E \to I$ tal que $gf = h$, es decir $\mathrm{Hom}_A(f, I)$ es suprayectivo.

$(d \Rightarrow b)$ Basta probar que f es inyectivo, para ello se considera una envolvente inyectiva (E', f') de M, por (d) existe un morfismo $h : E \to E'$ tal que $hf = f'$, lo que implica que f es monomorfismo debido a que f' es monomorfismo. □

Observación 6.10. La construcción que se usó para probar la Proposición 6.2 muestra que la envolvente inyectiva de un módulo M es el máximo de los módulos que contienen a M como submódulo esencial. Mientras que el punto (c) de la proposición anterior muestra que la envolvente inyectiva es el mínimo módulo inyectivo que contiene a M.

Ya con estas caracterizaciones se pueden probar interesantes propiedades de la envolvente como muestra la siguiente proposición.

Proposición 6.11. *Sea M un A-módulo. Se cumplen los siguientes enunciados.*

(a) *Si (E_1, f_1) y (E_2, f_2) son envolventes inyectivas de M, entonces todo morfismo $h : E_1 \to E_2$ tal que $hf_1 = f_2$ es un isomorfismo.*

(b) *Si (E_1, f_1) y (E_2, f_2) son envolventes inyectivas de M, entonces existe un isomorfismo $g : E_1 \to E_2$ tal que $gf_1 = f_2$.*

(c) *Si (E, f) es una envolvente inyectiva de M, entonces para todo monomorfismo $g : M \to K$ con codominio inyectivo existe una descomposición $K = K_1 \oplus K_2$ tal que $g(M) \cap K_1 = 0$ y la pareja $(K_2, \pi g)$ es una envolvente inyectiva, donde $\pi : K \to K_2$ es la proyección natural.*

Demostración.

(a) Sea $h : E_1 \to E_2$ un morfismo tal que $hf_1 = f_2$. Debido a que f_1 es un monomorfismo y E_2 es inyectivo, también existe un morfismo $g : E_2 \to E_1$ tal que $gf_2 = f_1$. Así, $f_1 = gf_2$ y $hf_1 = f_2$, lo que implica que $f_2 = hgf_2$ y $f_1 = ghf_1$; pero entonces hg y gh son isomorfismos por el punto (b) de la proposición anterior. En consecuencia g y h son isomorfismos.

(b) Es inmediato del punto anterior ya que debido a que f_2 es monomorfismo y E_1 inyectivo, existe un morfismo $h : E_1 \to E_2$ tal que $hf_1 = f_2$.

(c) Sea $g : M \to K$ un monomorfismo con codominio inyectivo. Debido a que g y f son monomorfismos y los módulos E y K son inyectivos existen los morfismos h_1 y h_2 tales que $h_1 g = f$ y $h_2 f = g$, entonces el morfismo $h = h_1 h_2$ cumple que $hf = f$.

$$\begin{tikzcd} & E \arrow[d, "h_2"] \\ M \arrow[ur, "f"] \arrow[dr, "g"'] & K \end{tikzcd} \qquad \begin{tikzcd} & K \arrow[d, "h_1"] \\ M \arrow[ur, "g"] \arrow[dr, "f"'] & E \end{tikzcd} \qquad \begin{tikzcd} & E \arrow[d, "h"] \\ M \arrow[ur, "f"] \arrow[dr, "f"'] & E \end{tikzcd}$$

En consecuencia, h es un isomorfismo por el punto (b) de la proposición anterior, lo que implica que $K = \mathrm{Im}(h_2) \oplus \mathrm{Ker}(h_1)$. En efecto, debido a que $h = h_1h_2$ es isomorfismo, para todo $x \in K$ existe $y \in E$ tal que $h_1(x) = h_1h_2(y)$ y entonces $x - h_2(y) \in \mathrm{Ker}(h_1)$, lo que implica que

$$K = \mathrm{Im}(h_2) + \mathrm{Ker}(h_1).$$

Además, si se toma $x \in \mathrm{Im}(h_2) \cap \mathrm{Ker}(h_1)$ se tiene que $x = h_2(y)$ para algún $y \in E$, y entonces $h_1h_2(y) = h_1(x) = 0$, lo que implica que $y = 0$ pues h_1h_2 es un isomorfismo, y así $\mathrm{Im}(h_2) \cap \mathrm{Ker}(h_1) = 0$. Por lo tanto, $K = \mathrm{Im}(h_2) \oplus \mathrm{Ker}(h_1)$. Luego, es inmediato que

$$g(M) \cap \mathrm{Ker}(h_1) = h_2f(M) \cap \mathrm{Ker}(h_1) \subseteq \mathrm{Im}(h_2) \cap \mathrm{Ker}(h_1) = 0,$$

y que $h_2 : E \to \mathrm{Im}(h_2)$ es un isomorfismo, por lo que $(\mathrm{Im}(h_2), \pi g)$ es una envolvente inyectiva.

□

Observación 6.12. Se ha visto que si (E_1, f_1) y (E_2, f_2) son envolventes inyectivas de M, entonces $E_1 \cong E_2$. Por esta razón en ocasiones se habla de un módulo inyectivo E como la envolvente inyectiva de M, si es que E es isomorfo a E_1.

Ahora, dadas dos familias de módulos $\{M_i\}_{i\in I}$ y $\{N_i\}_{i\in I}$ es sencillo probar que si $M_i \trianglelefteq N_i$ para todo $i \in I$, entonces $\bigoplus_{i\in I} M_i \trianglelefteq \bigoplus_{i\in I} N_i$. Sin embargo, en general un suma directa arbitraria de módulos inyectivos no es inyectiva. Por lo tanto, si (N_i, f_i) es la envolvente inyectiva de M_i para toda $i \in I$, entonces $(\bigoplus_{i\in I} N_i, \bigoplus_{i\in I} f_i)$ es una envolvente inyectiva de $\bigoplus_{i\in I} M_i$ si, y sólo si, $\bigoplus_{i\in I} N_i$ es inyectivo.

Proposición 6.13. *Sean $\{M_i\}_{i\in I}$ y $\{N_i\}_{i\in I}$ dos familias de módulos tales que $M_i \trianglelefteq N_i$ para todo $i \in I$. Se cumplen los siguientes enunciados.*

(a) *$\bigoplus_{i\in I} M_i$ es un submódulo esencial de $\bigoplus_{i\in I} N_i$.*

(b) *$\bigoplus_{i\in I} N_i$ es inyectivo si, y sólo si, $(\bigoplus_{i\in I} N_i, \bigoplus_{i\in I} f_{i\in I})$ es la envolvente inyectiva de $\bigoplus_{i\in I} M_i$.*

Demostración.

(a) Se sigue del punto (e) del Lema 6.1. Dado $x \in \bigoplus_{i\in I} N_i$ se tiene que $x = \sum_{i=1}^{n} n_i$ con $n_i \in N_{\sigma(i)}$ donde σ es una función inyectiva de $\{1, ..., n\}$ a I. Se prueba por inducción sobre n que existe $a \in A$ tal que $xa \in \bigoplus_{i\in I} M_i$. Si $n = 1$, entonces es inmediato del Lema 6.1. Tomando como hipótesis inductiva que si $n = k$ entonces existe $a \in A$ tal que $xa \in \bigoplus_{i\in I} M_i$ si se tiene $x = \sum_{i=1}^{k+1} n_i$, entonces por hipótesis de inducción existe $a \in A$ tal que $\sum_{i=1}^{k} n_i a \in \bigoplus_{i\in I} M_i$ y como $M_{\sigma(1)} \trianglelefteq N_{\sigma(1)}$ existe $b \in A$ tal que $n_1(ab) \in M_{\sigma(1)}$, lo que implica que $x(ab) \in \bigoplus_{i\in I} M_i$. Por lo

tanto, para todo $x \in \bigoplus_{i \in I} N_i$ existe $a \in A$ tal que $xa \in \bigoplus_{i \in I} M_i$, lo que implica que $\bigoplus_{i \in I} M_i \trianglelefteq \bigoplus_{i \in I} N_i$.

(b) Es inmediato del punto anterior.

$\square$

Ejemplo 6.14. Sea X el conjunto de los números primos. Se ha probado que $(\mathbb{Z}_{p^\infty}, f)$ es la envolvente inyectiva de $\mathbb{Z}_p$ para todo $p \in X$, lo que implica que $\mathbb{Q}/\mathbb{Z} \cong \bigoplus_{p \in X} \mathbb{Z}_{p^\infty}$ es la envolvente inyectiva de $\bigoplus_{p \in X} \mathbb{Z}_p$.

Cabe mencionar que no existe un resultado semejante al anterior para el producto de módulos como muestra el siguiente ejemplo, por lo que en general es falso que el producto de envolventes inyectivas sea envolvente inyectiva.

Ejemplo 6.15. Sea $M = \mathbb{Z}_{p^\infty} = \left\langle \overline{\frac{1}{p^n}} \in \mathbb{Q}/\mathbb{Z} \quad | \quad n \in \mathbb{N} \right\rangle$. Claramente $(\overline{\frac{1}{p}})\mathbb{Z} \trianglelefteq M$, sin embargo $\prod_{m \in \mathbb{N}} (\overline{\frac{1}{p}})\mathbb{Z}$ no es un submódulo esencial de $\prod_{m \in \mathbb{N}} M$. En efecto, si se toma $x = \left(\overline{\frac{1}{p^{m+1}}} \right)_{m \in \mathbb{N}}$, entonces $x \in \prod_{m \in \mathbb{N}} M$, pero no existe $k \in \mathbb{Z}$ tal que $xk \in \prod_{m \in \mathbb{N}} (\overline{\frac{1}{p^m}})\mathbb{Z}$. En consecuencia, el Lema 6.1 implica que $\prod_{m \in \mathbb{N}} (\overline{\frac{1}{p}})\mathbb{Z}$ no es esencial.

En algunas ocaciones se puede utilizar el resultado anterior para calcular la envolvente inyectiva con ayuda del soclo.

Proposición 6.16. *Sea M un módulo, E un módulo inyectivo, $i : N \to M$ la inclusión natural y $f : M \to E$ un monomorfismo. Si $N \trianglelefteq M$, entonces (E, f) es la envolvente inyectiva de M si, y sólo si, (E, fi) es la envolvente inyectiva de N. En particular, si* $\operatorname{soc}(M) \trianglelefteq M$ *y la suma directa de las envolventes inyectivas de los submódulos simples de M es inyectiva, entonces la envolvente inyectiva de M es la suma directa de las envolventes inyectivas de los módulos simples contenidos en M.*

Demostración. Si $N \trianglelefteq M$, entonces (E, f) es la envolvente inyectiva de M si, y sólo si, $\operatorname{Im}(f) \trianglelefteq E$. Lo que implica que $\operatorname{Im}(fi) \trianglelefteq E$ ya que

$$\operatorname{Im}(fi) \cong N \trianglelefteq M \cong \operatorname{Im}(f) \trianglelefteq E,$$

de manera que (E, fi) es la envolvente inyectiva de N. Recíprocamente, si (E, fi) es la envolvente inyectiva de N, es entonces inmediato que (E, f) es la envolvente inyectiva de M ya que $\operatorname{Im}(fi) \subseteq \operatorname{Im}(f)$, lo que implica que $\operatorname{Im}(f) \trianglelefteq E$ por que $\operatorname{Im}(fi) \trianglelefteq E$.
En particular si $\operatorname{soc}(M) \trianglelefteq M$, entonces (E, fi) es la envolvente inyectiva de $\operatorname{soc}(M)$, pero $\operatorname{soc}(M)$ es la suma directa de los módulo simples contenidos en M. De manera que E es isomorfo a la suma directa de envolventes inyectivas de los submódulos simples. $\square$

Observación 6.17. En adelante, si un submódulo N de M cumple las condiciones de la proposición se dirá que N tiene la misma envolvente inyectiva que M.

Corolario 6.18. *Se cumplen los siguientes enunciados.*

(a) *Si M es un módulo artiniano, entonces* $\mathrm{soc}(M)$ *y M tienen la misma envolvente inyectiva.*

(b) *Si A es una álgebra de dimensión finita, entonces todo módulo finitamente generado tiene la misma envolvente inyectiva que su soclo.*

Demostración. Por la proposición anterior basta probar que el soclo es un submódulo esencial.

(a) Si M es artiniano, entonces todo submódulo de M contiene un submódulo simple, lo que implica que $\mathrm{soc}(M) \trianglelefteq M$.

(b) Se sigue del punto anterior. Si A es de dimensión finita, entonces todo módulo finitamente generado es de dimensión finita y entonces artiniano.

$\square$

El siguiente es un ejemplo de un módulo M tal que la envolvente inyectiva de $\mathrm{soc}(M)$ es distinta de la envolvente de M.

Ejemplo 6.19. Sea $M = \mathbb{Z}_2 \oplus \mathbb{Z}$. Es inmediato que la envolvente inyectiva de M es $\mathbb{Z}_{2^\infty} \oplus \mathbb{Q}$ mientras que la envolvente inyectiva de su soclo es $\mathbb{Z}_{2^\infty}$.

6.2. La cubierta proyectiva

El concepto dual de la enlvolvente inyectiva es la cubierta proyectiva. A diferencia de la envolvente no todo módulo tiene cubierta proyectiva. En capítulos posteriores se verán condiciones suficientes y necesarias sobre el anillo para que todo módulo tenga cubierta proyectiva. Esta sección expone las propiedades básicas de este concepto en caso de existir.

Definición 6.20.

- Se dice que un morfismo $f : M \to N$ es superfluo si f es un epimorfismo tal que $\mathrm{Ker}(f) \ll M$.
- Una pareja (P, f), donde P es un módulo proyectivo y $f : P \to M$ es un morfismo superfluo, recibe el nombre de cubierta proyectiva de M.

Ejemplo 6.21. Si A es un anillo y $e \in A$ un idempotente, entonces (eA, π) es una cubierta proyectiva de $eA/\operatorname{rad}(eA) = e(A/\operatorname{rad}(A))$, donde π es la proyección natural. En efecto, π es un epimorfismo, $\operatorname{Ker}(\pi) = \operatorname{rad}(eA) \ll eA$ por el lema de Nakayama y eA es proyectivo ya que es sumando directo de A. Además, debido a que eA es proyectivo se tiene por la Proposición 5.47 que

$$\operatorname{rad}(eA) = eA\operatorname{rad}(A) = e(\operatorname{rad}(A)),$$

lo que implica que

$$eA/\operatorname{rad}(eA) = eA/e(\operatorname{rad}(A)) = e(A/\operatorname{rad}(A)).$$

Proposición 6.22. *Si M es un $A/\operatorname{rad}(A)$-módulo tal que $f : P_A \to M_A$ es una cubierta proyectiva, entonces M es un $A/\operatorname{rad}(A)$-módulo proyectivo.*

Demostración. Se observa que si K es un $A/\operatorname{rad}(A)$-módulo y $h : P \to K$ un morfismo de A-módulos, entonces

$$h(\operatorname{rad}(P)) = h(P\operatorname{rad}(A)) = h(P)\operatorname{rad}(A) \subseteq K\operatorname{rad}(A) = 0,$$

es decir $\operatorname{rad}(P) \subseteq \operatorname{Ker}(h)$, lo que implica que existe un morfismo $\bar{h} : P/rad(P) \to K$ definido como $\bar{h}(x + \operatorname{rad}(P)) = h(x)$. Utilizando esta observación es sencillo deducir que

$$Q = P/\operatorname{rad}(P) = P/P\operatorname{rad}(A)$$

es un $A/\operatorname{rad}(A)$-módulo proyectivo. Más aún, si $g : Q \to M$ es el. morfismo inducido por f, entonces g es epimorfismo ya que f es epimorfismo, y g es monomorfismo debido a que $\operatorname{Ker}(f) \subseteq \operatorname{rad}(P)$, lo cual ocurre en consecuencia de que al ser (P, f) cubierta proyectiva, $\operatorname{Ker}(f) \ll P$. □

La siguiente proposición engloba diferentes caracterizaciones de una cubierta proyectiva. Para ello se introduce la siguiente definición.

Definición 6.23. Sea $f : P \to M$ un morfismo de módulos. Se dice que f es minimal a la derecha si todo $g \in \operatorname{End}_A(P)$ tal que $fg = f$ es un isomorfismo.

Proposición 6.24. *Sea $f : P \to M$ un morfismo de módulos con P proyectivo. Son equivalentes los siguientes enunciados.*

(a) *(P, f) es una cubierta proyectiva de M.*

(b) *El morfismo f es un epimorfismo minimal a la derecha.*

(c) *El morfismo f es un epimorfismo y si $h : Q \to M$ es un epimorfismo con dominio proyectivo, entonces existe un epimorfismo $g : Q \to P$ tal que $h = fg$.*

(d) *El morfismo f es minimal a la derecha y para todo modulo proyectivo Q, el morfismo* $\mathrm{Hom}_A(Q, f) : \mathrm{Hom}_A(Q, P) \to \mathrm{Hom}_A(Q, M)$ *es suprayectivo.*

Demostración.

($a \Rightarrow b$) Si (P, f) es una cubierta proyectiva de M y $g \in \mathrm{End}_A(P)$ es un morfismo tal que $fg = f$, entonces para todo $x \in P$ se tiene que $x - g(x) \in \mathrm{Ker}(f)$. De manera que $\mathrm{Ker}(f) + \mathrm{Im}(g) = P$ lo que implica que $\mathrm{Im}(g) = P$ debido a que f es superfluo. Luego, debido a que P es proyectivo, $P = P' \oplus \mathrm{Ker}(g)$ con $P \cong P'$, pero en tal caso $\mathrm{Ker}(f) + P' = P$ ya que $\mathrm{Ker}(g) \subseteq \mathrm{Ker}(f)$, pero, una vez más debido a que f es superfluo, $P = P'$ y con ello $\mathrm{Ker}(g) = 0$. Por lo tanto g es un isomorfismo.

($b \Rightarrow c$) Si $h : Q \to M$ es un epimorfismo con dominio proyectivo, entonces debido a que P es proyectivo existe g tal que $fg = h$. Además, debido a que P es proyectivo existe g' tal que $hg' = f$. Por lo tanto, $fgg' = f$ y $gg' \in \mathrm{End}_A(P)$, entonces el punto (b) implica que gg' es un isomorfismo, y con ello que g es un epimorfismo.

$$\begin{tikzcd} & Q \arrow[dl, "g"'] \arrow[dr, "h"] & \\ P \arrow[rr, "f"'] & & M \end{tikzcd} \qquad \begin{tikzcd} & P \arrow[dl, "g'"'] \arrow[dr, "f"] & \\ Q \arrow[rr, "h"'] & & M \end{tikzcd}$$

($c \Rightarrow a$) Basta probar que f es superfluo. Sea K un submódulo de P tal que

$$K + \mathrm{Ker}(f) = P,$$

se tiene que $f|_K$ es un epimorfismo. Luego, se sabe que existe un epimorfismo $g : L \to K$ con L libre, entonces el punto (c) implica que existe un epimorfismo $h : L \to P$ tal que $fh = fg$. Luego, debido a que para toda $k \in K$ existe $a \in L$ tal que $g(a) = k$, y así $fh(a) = fg(a) = f(k)$, de tal manera que $k - h(a) \in \mathrm{Ker}(f)$. En consecuencia, $K = \mathrm{Ker}(f) + \mathrm{Im}(h) = P$. Por lo tanto, f es superfluo.

($b \Rightarrow d$) Debido a que f es epimorfismo, para todo morfismo $h : Q \to M$ con dominio proyectivo existe $g : Q \to P$ tal que $fg = h$, es decir $\mathrm{Hom}_A(Q, f)$ es suprayectivo.

($d \Rightarrow b$) Basta probar que f es suprayectivo, para ello se considera una cubierta proyectiva (P', f') de M. Por (d) existe un morfismo $h : P' \to P$ tal que $fh = f'$, lo que implica que f es epimorfismo debido a que f' es epimorfismo. □

Ya con las caracterizaciones de la proposición anterior se pueden probar interesantes propiedades de la cubierta como muestra la siguiente proposición.

Proposición 6.25. *Sea M un A-módulo. Se cumplen los siguientes enunciados.*

(a) *Si (P, f) es una cubierta proyectiva de M, entonces* $\mathrm{Ker}(f) \subseteq \mathrm{rad}(P)$.

(b) *Si P es un módulo proyectivo finitamente generado y $f : P \to M$ es un epimorfismo tal que* $\operatorname{Ker}(f) \subseteq \operatorname{rad}(P)$*, entonces (P, f) es una cubierta proyectiva.*

(c) *Si (P_1, f_1) y (P_2, f_2) son cubiertas proyectivas de M, entonces todo morfismo $h : P_2 \to P_1$ tal que $f_1h = f_2$ es un isomorfismo.*

(d) *Si (P_1, f_1) y (P_2, f_2) son cubiertas proyectivas de M, entonces existe un isomorfismo $g : P_2 \to P_1$ tal que $f_1g = f_2$.*

(e) *Si (P, f) es una cubierta proyectiva de M, entonces para todo epimorfismo con dominio proyectivo $g : K \to M$ existe una descomposición $K = K_1 \oplus K_2$ tal que $g(K_1) = 0$ y (K_2, gi) es una cubierta proyectiva, donde $i : K_2 \to K$ es la inclusión natural.*

(f) *Si M es un módulo finitamente generado y (P, f) es una cubierta proyectiva de M, entonces P es finitamente generado.*

Demostración.

(a) Debido a que f es superfluo $\operatorname{Ker}(f) \ll P$, lo que implica que $\operatorname{Ker}(f) \subseteq \operatorname{rad}(P)$ por la Proposición 5.34.

(b) Debido a que P es finitamente generado $\operatorname{rad}(P) \ll P$, y asi f es superfluo ya que $\operatorname{Ker}(f) \subseteq \operatorname{rad}(P)$.

(c) Sea $h : P_2 \to P_1$ un morfismo tal que $f_1h = f_2$. Debido a que f_1 es un epimorfismo y P_2 es proyectivo también existe un morfismo $g : P_1 \to P_2$ tal que $f_2g = f_1$. De manera que $f_1 = f_2g$ y $f_1h = f_2$, lo que implica que $f_2 = f_2gh$ y $f_1 = f_1hg$; pero entonces hg y gh son isomorfismos por el punto (b) de la proposición anterior, lo que implica que g y h son isomorfismos.

(d) Es inmediato del punto anterior ya que debido a que f_2 es epimorfismo y P_1 proyectivo, existe un morfismo $h : P_2 \to P_1$ tal que $f_1h = f_2$.

(e) Sea $g : K \to M$ un epimorfismo con dominio proyectivo. Debido a que g y f son epimorfismos y los módulos P y K son proyectivos existen los morfismos h_1 y h_2 tales que $gh_1 = f$ y $fh_2 = g$, entonces el morfismo $h = h_2h_1$ cumple que $fh = f$.

$$
\begin{tikzcd}
E \arrow[dr, "f"] & \\
& M \\
K \arrow[uu, "h_2"] \arrow[ur, "g"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
K \arrow[dr, "g"] & \\
& M \\
E \arrow[uu, "h_1"] \arrow[ur, "f"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
E \arrow[dr, "f"] & \\
& M \\
E \arrow[uu, "h"] \arrow[ur, "f"'] &
\end{tikzcd}
$$

Esto muestra que h es un isomorfismo por el punto (b) de la proposición anterior. En consecuencia, $K = \operatorname{Im}(h_1) \oplus \operatorname{Ker}(h_2)$. En efecto, debido a que $h = h_2h_1$ es isomorfismo, para todo $x \in K$ existe $y \in P$ tal que $h_2(x) = h_2h_1(y)$ y entonces $x - h_1(y) \in \operatorname{Ker}(h_2)$, de manera que $K = \operatorname{Im}(h_1) + \operatorname{Ker}(h_2)$. Además, si se toma

$x \in \mathrm{Im}(h_1) \cap \mathrm{Ker}(h_2)$ se tiene que $x = h_1(y)$ para algún $y \in P$, y entonces $h_2h_1(y) = h_2(x) = 0$, lo que implica que $y = 0$ pues h_2h_1 es un isomorfismo, por lo que $\mathrm{Im}(h_1) \cap \mathrm{Ker}(h_2) = 0$. Por lo tanto, $K = \mathrm{Im}(h_1) \oplus \mathrm{Ker}(h_2)$. Es entonces inmediato que

$$g(\mathrm{Ker}(h_2)) = fh_2(\mathrm{Ker}(h_2)) = 0,$$

y que $h_2|_{\mathrm{Im}(h_1)} : \mathrm{Im}(h_1) \to P$ es un isomorfismo, por lo que $(\mathrm{Im}(h_1), gi)$ es una cubierta proyectiva.

(f) Si M es finitamente generado, entonces existe un epimorfismo $g : A^n \to M$ para algún $n \in \mathbb{N}$, pero debido a que A^n es proyectivo existe un epimorfismo $h : A^n \to P$ tal que $fh = g$ por el punto (c) de la Proposición 6.24, y así P es finitamente generado.

□

Observación 6.26. Se ha visto que si (P_1, f_1) y (P_2, f_2) son cubiertas proyectivas de M, entonces $P_1 \cong P_2$. Por esta razón en ocasiones se habla de un módulo proyectivo P como la cubierta proyectiva de M, si es que P es isomorfo a P_1.

Ejemplo 6.27. El $\mathbb{Z}$-módulo $\mathbb{Z}_2$ no tiene cubierta proyectiva. En efecto, supóngase que (P, f) es una cubierta proyectiva de $\mathbb{Z}_2$. Debido a que $\mathbb{Z}$ es un dominio entero $P = \mathbb{Z}^{(X)}$ para algún conjunto X, pero $\mathrm{Ker}(f) \subseteq \mathrm{rad}(P) = \mathrm{rad}(\mathbb{Z}^{(X)}) = 0$. Lo cual es una contradicción ya que f no puede ser un isomorfismo.

Ejemplo 6.28. Si A es un anillo tal que $\mathrm{rad}(A) = 0$, entonces los únicos módulos con cubierta proyectiva son los módulos proyectivos. En efecto, si M es un módulo con una cubierta proyectiva (P, f), entonces $\mathrm{Ker}(f) \subseteq \mathrm{rad}(P) = P\,\mathrm{rad}(A) = 0$ por la Proposición 5.47, lo que implica que f es un isomorfismo y entonces M es proyectivo.

Como corolario se tienen los siguientes resultados sobre la cubierta proyectiva de un módulo simple.

Corolario 6.29. *Sea S un A-módulo simple con cubierta proyectiva.*

(a) *Si (P, f) es una cubierta proyectiva de S, entonces $\mathrm{Ker}(f) = \mathrm{rad}(P)$.*

(b) *Si (P, f) es una cubierta proyectiva de S, entonces P tiene un único submódulo maximal.*

(c) *Si $\mathrm{rad}(A) = 0$, entonces $(S, 1_S)$ es una cubierta proyectiva de S.*

Demostración.

(a) Se sabe que $\mathrm{Ker}(f) \subseteq \mathrm{rad}(P)$ y que $\mathrm{rad}(P) \neq P$ debido a que P es proyectivo. Luego, por el tercer teorema de isomorfismos $S \cong P/\mathrm{Ker}(f)$, lo que implica que $\mathrm{rad}(P)/\mathrm{Ker}(f) = 0$. Por lo tanto, $\mathrm{Ker}(f) = \mathrm{rad}(P)$.

(b) Es inmediato del punto anterior.

(c) Sea (P, f) una cubierta proyectiva de S. Por el punto (a)

$$S \cong P/\operatorname{Ker}(f) = P/\operatorname{rad}(P),$$

pero $\operatorname{rad}(P) = P\operatorname{rad}(A) = 0$, lo que implica que $S \cong P$ y entonces $(S, 1_S)$ es una cubierta proyectiva de S.

□

Ahora, dadas dos familias de módulos $\{M_i\}_{i\in I}$ y $\{N_i\}_{i\in I}$ es sencillo probar que si $M_i \ll N_i$ para todo $i \in I$, entonces $\prod_{i\in I} M_i \ll \prod_{i\in I} N_i$. Sin embargo, en general el producto arbitrario de módulos proyectivos no es proyectivo. Por lo tanto, si (N_i, f_i) es la cubierta proyectiva de M_i para toda $i \in I$, entonces $(\prod_{i\in I} N_i, \prod_{i\in I} f_i)$ es una cubierta proyectiva de $\prod_{i\in I} M_i$ si, y sólo si, $\prod_{i\in I} N_i$ es proyectivo.

Proposición 6.30. *Sean $\{M_i\}_{i\in I}$ y $\{N_i\}_{i\in I}$ dos familias de módulos tales que $M_i \ll N_i$ para todo $i \in I$. Se cumplen los siguientes enunciados.*

(a) *$\prod_{i\in I} M_i$ es un submódulo superfluo de $\prod_{i\in I} N_i$.*

(b) *Si la pareja (N_i, f_i) es una cubierta proyectiva de T_i para toda $i \in I$, entonces $(\prod_{i\in I} N_i, \prod_{i\in I} f_i)$ es una cubierta proyectiva de $\prod_{i\in I} T_i$ si, y sólo si, $\prod_{i\in I} N_i$ es proyectivo.*

Demostración.

(a) Sea K un submódulo de $\prod_{i\in I} N_i$ tal que $K + \prod_{i\in I} M_i = \prod_{i\in I} N_i$. Para toda $j \in I$ se tiene que $\pi_j(K) + M_j = N_j$ donde $\pi_j : \prod_{i\in I} N_i \to N_j$ es la proyección natural, lo que implica que $\pi_j(K) = N_j$ para toda $j \in I$ y entonces $K = \prod_{i\in I} N_i$. Por lo tanto $\prod_{i\in I} M_i \ll \prod_{i\in I} N_i$.

(b) Es inmediato del punto anterior.

□

En algunas ocaciones se puede utilizar el resultado anterior para calcular la cubierta proyectiva con ayuda del radical como se verá a continuación.

Proposición 6.31. *Sea M un módulo, N un submódulo de M, $\pi : M \to M/N$ la proyección natural y $f : P \to M$ un epimorfismo con dominio proyectivo. Si $N \ll M$, entonces (P, f) es la cubierta proyectiva de M si, y sólo si, $(P, \pi f)$ es la cubierta proyectiva de P.*

Demostración. Si $N \ll M$ y la pareja (P, f) es la cubierta proyectiva de M, entonces $\text{Ker}(f) \ll P$, lo que implica que $\text{Ker}(\pi f) \ll P$. En efecto, si K es un submódulo de P tal que $\text{Ker}(\pi f) + K = P$, entonces $M = f(P) = f(\text{Ker}(\pi f)) + f(K)$, pero $f(\text{Ker}(\pi f)) \subseteq N \ll M$ de manera que $f(K) = M$ y así $\text{Ker}(f) + K = P$. En consecuencia, $K = P$, ya que $\text{Ker}(f) \ll P$. Por lo tanto, $\text{Ker}(\pi f) \ll P$ y así $(E, \pi f)$ es la cubierta proyectiva de N.
Recíprocamente, si $(P, \pi f)$ es la cubierta proyectiva de N, es entonces inmediato que (P, f) es la cubierta proyectiva de M ya que $\text{Ker}(f) \subseteq \text{Ker}(\pi f) \ll P$, lo que implica que $\text{Ker}(f) \ll P$. □

Observación 6.32. En adelante, si un submódulo N de M cumple las condiciones de la proposición se dirá que M/N tiene la misma cubierta proyectiva que M.

En particular si $\text{rad}(M) \ll M$, entonces M y $M/\text{rad}(M)$ tienen la misma cubierta proyectiva.

Proposición 6.33. *Sea M un módulo. Si $\text{rad}(M) \ll M$, entonces M y $M/\text{rad}(M)$ tienen la misma cubierta proyectiva.*

Corolario 6.34. *Se cumplen los siguientes enunciados.*

(a) *Si M es noetheriano, entonces $M/\text{rad}(M)$ y M tienen la misma cubierta proyectiva en caso de existir.*

(b) *Si M es finitamente generado, entonces $M/\text{rad}(M)$ y M tienen la misma cubierta proyectiva en caso de existir.*

Demostración. Por la proposición anterior basta probar que el radical es un submódulo superfluo.

(a) Si se supone que existe un submódulo $K \neq M$ tal que $\text{rad}(M) + K = M$, entonces debido a que M es noetheriano existe un submódulo maximal N de M que contiene a K; y así $M = \text{rad}(M) + K = N$ lo cual es una contradicción. Por lo tanto $\text{rad}(M) \ll M$.

(b) Si M es finitamente generado, entonces $\text{rad}(M) \ll M$ por la Proposición 5.31.

□

7. Locales y Semilocales

Se mencionó en el capítulo anterior que se buscarían más adelante condiciones en el anillo para que todo módulo tenga cubierta proyectiva. Para llegar a ese objetivo se presentan en este capítulo las clases de anillos locales y semilocales, exposición que incluirá el teorema de Krull-Schmidt-Azumaya y otros resultados que serán de utilidad más adelante.

7.1. Locales

En esta sección se definen los anillos locales y se les caracteriza de diferentes maneras, terminando con varios ejemplos que surgen de manera natural como el anillo de endomorfismos de un módulo inescindible de longitud finita.

Teorema 7.1. *Sea A un anillo. Los siguientes enunciados son equivalentes.*

(a) *A tiene un único ideal maximal derecho.*

(b) *A tiene un único ideal maximal izquierdo.*

(c) $\operatorname{rad}(A)$ *es el único ideal maximal bilateral.*

(d) $A/\operatorname{rad}(A)$ *es un anillo con división.*

(e) *El conjunto de elementos no invertibles de A es un ideal.*

(f) $\operatorname{rad}(A)$ *es el conjunto de los elementos no invertibles de A.*

(g) *El conjunto de los elementos no invertibles de A es un grupo con la suma del anillo.*

(h) *Si $a+b$ es invertible, entonces a ó b es invertible.*

(i) *Si $a \in A$ entonces a ó $1-a$ es invertible.*

Demostración.

($a \Rightarrow c$) Si A tiene un único ideal derecho máximo J, entonces $\operatorname{rad}(A) = J$. De manera que si I es un ideal bilateral, I es un ideal derecho y como tal está contenido en J, ya que es el único ideal derecho maximal. Por lo tanto, $I \subseteq \operatorname{rad}(A)$, lo que implica que $\operatorname{rad}(A)$ es el único ideal bilateral.

$(b \Rightarrow c)$ Análogo a $(a \Rightarrow c)$.

$(c \Rightarrow d)$ Si $\operatorname{rad}(A)$ es un ideal maximal, entonces $A/\operatorname{rad}(A)$ no tiene ideales propios, por lo que

$$(x + \operatorname{rad}(A))(A/\operatorname{rad}(A)) = A/\operatorname{rad}(A) = (A/\operatorname{rad}(A))(x + \operatorname{rad}(A)),$$

para cualquier $x \in A$, de modo que todo elemento de $A/\operatorname{rad}(A)$ tiene inverso derecho e izquierdo. Por lo tanto, $A/\operatorname{rad}(A)$ es un anillo con división.

$(d \Rightarrow a)$ Si $A/\operatorname{rad}(A)$ es un anillo con división, entonces $A/\operatorname{rad}(A)$ es un A-módulo derecho simple por la Proposición 1.9, de ahí que $\operatorname{rad}(A)$ sea un ideal derecho maximal.

$(d \Rightarrow b)$ Análogo a $(d \Rightarrow a)$.

$(d \Rightarrow f)$ Se sabe que $1 - a$ es invertible para todo $a \in \operatorname{rad}(A)$ por el Lema 5.36. De manera que si $A/\operatorname{rad}(A)$ es un anillo con división, para todo $x \in A \setminus \operatorname{rad}(A)$ existe $y \in A \setminus \operatorname{rad}(A)$ tal que $xy = 1 - a$ donde $a \in \operatorname{rad}(A)$; y así xy es invertible, lo que implica que x también es invertible. Por lo tanto, los elementos no invertibles de A son el conjunto $\operatorname{rad}(A)$.

$(f \Rightarrow e)$, $(e \Rightarrow g)$ y $(g \Rightarrow h)$ son triviales.

$(h \Rightarrow d)$ Sea $x \in A$. Si $x \notin \operatorname{rad}(A)$, entonces $1 - bx$ no es invertible por la izquierda para algún $b \in A$ por el Lema 5.36. Pero $1 = (1 - bx) + bx$ es invertible, de modo que bx tiene un inverso por la izquierda, y entonces x tiene un inverso por la izquierda. Análogamente se prueba que x tiene inverso por la derecha. Por lo tanto, x es invertible si $x \notin \operatorname{rad}(A)$, por lo que $A/\operatorname{rad}(A)$ es un anillo con división.

$(d \Rightarrow c)$ Si $A/\operatorname{rad}(A)$ es un anillo con división, entonces es un A-módulo simple, lo que implica que $\operatorname{rad}(A)$ es un ideal maximal.

$(h \Rightarrow i)$ Para todo $a \in A$ se tiene que $1 = a + (1 - a)$, así que a ó $1 - a$ es invertible.

$(i \Rightarrow c)$ Sea $J \neq A$ un ideal que contiene a $\operatorname{rad}(A)$. Si $x \in J$, es inmediato que $xa \in J$ para todo $a \in A$, lo que implica que xa no es invertible para todo $a \in A$ ya que $J \neq A$, entonces $1 - ax$ es invertible para todo $a \in A$, de modo que $x \in \operatorname{rad}(A)$. Por lo tanto, $J = \operatorname{rad}(A)$. □

Un anillo que cumple alguno de estos enunciados se dice que es local.

Definición 7.2. Sea A un anillo. Se dice que A es local si $\operatorname{rad}(A)$ es un ideal maximal.

Observación 7.3. Del punto (h) de la proposición anterior se sigue que si un anillo A no es local, entonces existen $a, b \in A$ no invertibles tales que $c = a + b$ es invertible. De manera que existen elementos no invertibles $ac^{-1}, bc^{-1} \in A$ tales que $ac^{-1} + bc^{-1} = 1_M$.

Ejemplo 7.4. Dado un entero primo p, el anillo $\mathbb{Z}_{p^n}$ es local para todo $n \in \mathbb{N}$ ya que tiene un ideal maximal único $p^{n-1}\mathbb{Z}_{p^n}$.

Ejemplo 7.5. Dado un entero primo p, sea

$$A = \{\frac{a}{b} \in \mathbb{Q} \quad | \quad p \, \text{no divide a } b\}.$$

El anillo A tiene un único ideal maximal pA. Por lo tanto, A es un anillo local.

Ejemplo 7.6. Dado un campo k se ha visto en el Ejemplo 5.40 que el anillo de series de potencias formales $A = k[[x]]$ tiene un único ideal maximal xA. Por lo tanto, A es un anillo local.

Es inmediato el siguiente corolario.

Corolario 7.7. *Si A es un anillo local, entonces se cumplen los siguientes enunciados.*

(a) *A tiene un único ideal maximal.*

(b) *Si $a \in A$ tiene un inverso por la derecha ó izquierda, entonces a es invertible.*

(c) *A no tiene idempotentes diferentes de 0 y 1.*

Demostración. Sea A un anillo local.

(a) $\text{rad}(A)$ es un ideal maximal, lo que implica que es el único ideal maximal.

(b) Si a tiene un inverso por la derecha ó izquierda, entonces $a \notin \text{rad}(A)$, así que a es invertible por el teorema anterior.

(c) Si $x \in A$ es un idempotente, entonces x ó $1 - x$ es invertible, pero también son idempotentes, por lo que existe un idempotente invertible e igual a x ó $1 - x$. Pero

$$e = e^2 e^{-1} = ee^{-1} = 1,$$

de donde se consluye que $x = 0$ ó $x = 1$.

□

Observación 7.8. Estos 3 enunciados son condiciones necesarias para que un anillo sea local, pero no suficientes, como es el caso del siguiente ejemplo, el álgebra de Weyl.

Ejemplo 7.9. Dado un campo k de característica 0, el álgebra de Weyl es el anillo $A = k\langle x, y\rangle / I$ donde I es el ideal bilateral generado por $xy - yx - 1$. Se prueba a continuación que A es un dominio entero simple.

Para empezar se observa que, en el anillo construido, $xy - yx = 1$, lo que implica para todo $n \in \mathbb{N}$ que

$$x^{n+1}y - yx^{n+1} = x(x^n y - yx^n) + (xy - yx)x^n = x(x^n y - yx^n) + x^n,$$

con lo que se prueba por inducción que $x^{n+1}y - yx^{n+1} = (n+1)x^n$. Por lo tanto, para todo polinomio $f(x)$

$$f(x)y - yf(x) = \frac{\partial f(x)}{\partial x}, \tag{7.1}$$

y análogamente se puede probar que

$$xg(y) - g(y)x = \frac{\partial g(y)}{\partial y} \tag{7.2}$$

para todo $g(y) \in k[y]$.

Ahora, todo elemento de A es una combinación lineal de elementos de la forma $z_1....z_n$ para algún n, donde $z_i = x$ ó $z_i = y$ para toda $i \in \{1, ..., n\}$. Pero con las identidades anteriores se puede probar inductivamente que $z_1....z_n = \sum_{i=0}^{m} x^i f_i(y)$ para algún m donde $f_i(y) \in k[y]$ para todo $i \in \{1, ..., m\}$. De manera que todo elemento $\alpha \in A$ se puede expresar como

$$\alpha = \sum_{k=0}^{s} x^k f_k(y),$$

donde $f_i(y) \in k[y]$ para toda $i \in \{1, .., s\}$. Más aún, utilizando la expresión anterior y ecuaciones (7.1) y (7.2) se observa que

$$x\alpha - \alpha x = \frac{\partial(\alpha)}{\partial y} \text{ y que } \alpha y - y\alpha = \frac{\partial(\alpha)}{\partial x}.$$

Ahora, si $\alpha = \sum_{k=0}^{s} x^k f_k(y) \in A\backslash\{0\}$ y J es un ideal bilateral tal que $\alpha \in J$, entonces $y\alpha - \alpha y \in J$, lo que implica que

$$\frac{\partial(\alpha)}{\partial x} \in J \text{ e inductivamente que } \frac{\partial^n(\alpha)}{\partial x^n} \in J \text{ para todo } n \in \mathbb{N},$$

de modo que $f_k(y) = \frac{1}{k!}\frac{\partial^k(\alpha)}{\partial x^k} \in J$, y análogamente $a = \frac{\partial^k(f_k)}{\partial y^k} \in J$. Pero a es un elemento del campo distinto de 0, así que $J = A$ debido a que a es invertible. Con esto queda probado que A es un anillo simple, y como tal tiene un ideal maximal único, es decir A cumple la condición (a) del corolario anterior.

Ahora, se sabe que todo elemento $\alpha \in A$ se puede expresar como $\alpha = \sum_{k=0}^{s} x^k f_k(y)$, y con lo que se probó en el párrafo anterior se puede probar que tal expresión es única. En efecto, si se supone que existe un elemento α con dos expresiones distinitas

$$\sum_{k=0}^{s} x^k f_k(y) = \alpha = \sum_{k=0}^{t} x^k g_k(y)$$

con $s \geq t$ sin pérdida de generalidad, se obtiene una expresión

$$0 = \sum_{k=0}^{s} x^k(f_k(y) - g_k(y))$$

con $f_j(y) - g_j(y) \neq 0$ para algún $j \in \{0, ..., s\}$; pero entonces el procedimiento del párrafo anterior implica que el ideal 0 es todo A lo cual es una contradicción.

De manera que es sencillo probar que A es un dominio entero. Ciertamente, dado $\alpha = \sum_{k=0}^{s} x^k f_k(y) \in A$ gracias a la unicidad de la expresión se puede definir el grado de α como el número

$$gr(\alpha) = max\{k + s \quad | \quad x^k y^s \text{ es un sumando de } \alpha\},$$

y entonces dado $\beta = \sum_{k=0}^{t} x^k g_k(y)$ se tiene que $gr(\alpha\beta) = gr(\alpha) + gr(\beta)$. Para probarlo, se muestra inductivamente que

$$y^n x^m = x^m y^n + \gamma$$

donde $\gamma \in A$ con $gr(\gamma) < n + m$ para todo $n, m \in \mathbb{N}$, y entonces de la unicidad de la expresión de $\alpha\beta$ se deduce que $gr(\alpha\beta) = gr(\alpha) + gr(\beta)$. Luego, es inmediato que A es un dominio entero y como tal es un anillo sin idempotentes no triviales, es decir A cumple la condición (c) del corolario anterior.

Por último, para probar que A cumple la condición (b) se observa que si existen $\alpha, \beta \in A$ tales que $\alpha\beta = 1$, entonces $\beta\alpha$ es idempotente, de modo que $\beta\alpha = 1$ ó $\beta\alpha = 0$. Pero si $\beta\alpha = 0$, entonces $\beta = \beta\alpha\beta = 0$, lo cual es una contradicción. Así que $\beta\alpha = 1$.

Por lo tanto, A cumple las tres condiciones del corolario y claramente no es local, ya que xA es un ideal derecho que no esta contenido en el único ideal maximal.

Ahora, se ha visto en la Proposición 2.17 que un módulo M es inescindible si $\mathrm{End}_A(M)$ no tiene idempotentes diferentes de 0 y 1, lo que implica que todo módulo que tenga un anillo de endomorfismos local es inescindible.

Corolario 7.10. *Si M es un módulo tal que $\mathrm{End}_A(M)$ es un anillo local, entonces M es inescindible.*

Pero, como se mostró en el ejemplo anterior, el hecho de que no existan idempotentes no triviales en un anillo no implica que el anillo sea local, por lo que el recíproco del corolario anterior es en general falso como se muestra en el siguiente ejemplo.

Ejemplo 7.11. $\mathbb{Z}$ es un $\mathbb{Z}$-módulo inescindible. Pero $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ no es local, ya que $p\mathbb{Z}$ es un ideal maximal para cualquier primo p.

Sin embargo, si el módulo inescindible M es de longitud finita, entonces por el Corolario 4.18 todos los elementos de $\mathrm{End}_A(M)$ son invertibles ó nilpotentes. Esta es una condición suficiente para que el anillo sea local como se verá a continuación.

Proposición 7.12. *Si A es un anillo tal que todos sus elementos son invertibles ó nilpotentes, entonces A es local.*

Demostración. Un elemento x no puede ser invertible y nilpotente, ya que si k es el mínimo entero tal que $x^k = 0$ se tiene que $0 \neq x^{k-1} = x^k x^{-1} = 0$, lo cual es una contradicción. De modo que si existen $a, b \in A$ tales que $a + b$ es invertible pero a no es invertible, entonces b es invertible; pues si se supone que tampoco lo es a y b son nilpotentes, lo que implica que $a+b$ también es nilpotente lo cual es una contradicción por lo antes dicho. Por lo tanto, si $a + b$ es invertible, entonces a ó b es invertible. De ahí que A sea local por el Teorema 7.1. □

Ejemplo 7.13. Si k es un campo y A el conjunto de matrices triángulares superiores de orden n sobre k tales que las entradas de la diagonal son iguales

$$A = \left\{ \begin{pmatrix} x & x_{12} & \cdots & x_{1n} \\ 0 & x & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & x \end{pmatrix} \in \mathbb{M}_n(k) \right\},$$

entonces A es un anillo local. En efecto, A es un anillo ya que es un subanillo de $\mathbb{M}_n(k)$, y es local ya que los elementos con diagonal nula son nilpotentes, mientras que los elementos con diagonal distinta de cero son invertibles debido a que su determinante es distinto de cero.

Análogamente se puede probar que si B es el anillo de matrices generalizadas con producto trivial

$$B = \begin{pmatrix} k & M_{12} & \cdots & M_{1n} \\ M_{21} & k & & \vdots \\ \vdots & & \ddots & \\ M_{n1} & \cdots & & k \end{pmatrix},$$

entonces el subanillo de B formado por las matrices cuyas entradas de la diagonal son iguales es un anillo local.

Es inmediato el siguiente resultado.

Corolario 7.14. *Sea M un módulo de longitud finita. M es inescindible si, y sólo si, $\mathrm{End}_A(M)$ es local.*

Del cual resultan los siguientes corolarios.

Corolario 7.15. *Si A es un anillo artiniano, entonces A es local si, y sólo si, no tiene idempotentes diferentes de 0 y 1.*

Demostración. Si A es local, entonces no existen idempotentes distintos de 0 y 1. Recíprocamente, si no existen idempotentes diferentes de 0 y 1, entonces por la Proposición 2.17 A es inescindible, y además al ser artiniano es de longitud finita por el Corolario 5.53, lo que implica que $\mathrm{End}_A(A) \cong A$ es local. □

Corolario 7.16. *Sean M y N son módulos inescindibles de longitud finita.*

(a) *Si $f : N \to M$ es un morfismo, entonces f es un isomorfismo, ó para todo morfismo $g : M \to N$ se tiene que $fg \in \mathrm{rad}(\mathrm{End}_A(N))$ y $gf \in \mathrm{rad}(\mathrm{End}_A(M))$.*

(b) *Si $M \ncong N$, $f \in \mathrm{Hom}_A(M^m, N^n)$ y $g \in \mathrm{Hom}_A(N^n, M^m)$ con $n, m \in \mathbb{N}$, entonces $gf \in \mathrm{rad}(\mathrm{End}_A(M^m))$ y $fg \in \mathrm{rad}(\mathrm{End}_A(N^n))$.*

Demostración. .

(a) Sea $g \in \mathrm{Hom}_A(M, N)$. Debido a que M es de longitud finita, $\mathrm{End}_A(M)$ es local. En consecuencia, si $gf \notin \mathrm{rad}(\mathrm{End}_A(M))$, se tiene que gf es invertible, lo que implica que f es un monomorfismo, y entonces f es un isomorfismo por el Corolario 4.18. Análogamente, si $fg \notin \mathrm{rad}(\mathrm{End}_A(N))$, se cumple que f es un epimorfismo lo que implica que f es un isomorfismo.

(b) Por la Proposición 2.26 f y g se pueden identificar como matrices $f = (f_{ij})_{n\times m}$ y $g = (g_{ij})_{m\times n}$ con $f_{ij} \in \mathrm{Hom}_A(M, N)$ y $g_{ij} \in \mathrm{Hom}_A(N, M)$, y así

$$fg = (\sum_{k=1}^{n} f_{ik}g_{kj})_{n\times n},$$

donde $f_{ik}g_{kj} \in \mathrm{rad}(\mathrm{End}_A(M))$ por el punto anterior para todo i, k, j. Por lo tanto, $fg \in \mathrm{rad}(\mathrm{End}_A(N^n))$. Análogamente se puede probar que $gf \in \mathrm{rad}(\mathrm{End}_A(M^m))$.

□

7.2. El Teorema de Krull-Schmidt

Ya presentados los anillos locales y sus propiedades básicas se puede abordar el problema de descomponer un módulo M como suma directa de submódulos inescindibles. A dicha descomposición se le llamará una descomposición en inescindibles.

Proposición 7.17. *Si M es un módulo artiniano ó noetheriano, entonces M tiene una descomposición en inescindibles $M = M_1 \oplus ... \oplus M_n$.*

Demostración. Sea X el conjunto de submódulos de M que tienen una descomposición en inescindibles. Si $M \notin X$, entonces en particular M no es inescindible, por lo que existen submódulos propios M_1 y N_1 tales que $M = M_1 \oplus N_1$, y por lo menos uno de ellos no pertenece a X, supóngase sin pérdida de generalidad que M_1 es tal módulo, de modo que existe una descomposición no trivial $M_1 = M_2 \oplus N_2$. Procediendo recursivamente, se obtiene un módulo $M_n \notin X$ con una descomposición no trivial $M_n = M_{n+1} \oplus N_{n+1}$ donde $M_{n+1} \notin X$.

De manera que, si se consideran las sucesiones $(M_i)_{i\in\mathbb{N}}$ y $(\bigoplus_{j=1}^{i} N_j)_{i\in\mathbb{N}}$ se llega a una contradicción, ya que la primera es una cadena estrictamente descendente y la segunda es una cadena estrictamente ascendente, lo cual contradice que M es artiniano ó noetheriano.

Por lo tanto, M tiene una descomposición en inescindibles $M = \bigoplus_{i\in I} M_i$ que además es finita debido a que M es artiniano ó noetheriano. □

Ejemplo 7.18. Sean $A = \mathbb{Z}(\sqrt{-5})$, M el módulo generado por 3 y $2+\sqrt{-5}$ y N el módulo generado por 3 y $2-\sqrt{-5}$. Se mostrará que la suma directa externa $M \oplus N$ tiene dos descomposiciones en inescindibles distinitas. Para empezar, utilizando la norma definida como

$$|a + b\sqrt{-5}| = a^2 + b^2 5,$$

que cumple la propiedad de que $|zw| = |z||w|$ para todo $z, w \in A$, se puede probar que M y N no son isomorfos a A. En efecto, si se supone que $M \cong A$, entonces existe un elemento $z \in M$ que genera a M; así que existen $x, y \in A$ tales que $zx = 3$ y $zy = 2+\sqrt{-5}$, de este hecho se deduce que $|z| = 3$, pero eso es una contradicción ya que no existe $a + b\sqrt{-5}$ tal que $3 = a^2 + 5b^2$. De modo que M no es isomorfo a A, y análogamente se prueba que $N \ncong A$. Por otro lado, utilizando que $M + N = A$, se prueba que

$$M \oplus N \cong A \oplus (M \cap N),$$

y es sencillo demostrar que $M \cap N = 3A \cong A$. Por lo tanto, se ha probado que $M \oplus N \cong A \oplus A$, la cual es una descomposición en inescindibles. Y debido a que A es noetheriano por el Ejemplo 4.27, M y N son noetherianos, lo que implica que dichos módulos tienen una descomposición en inescindibles, lo que implica que $M \oplus N$ tiene una descomposición en inescindibles distinta a $A \oplus A$ ya que M y N no son isomorfos a A.

Como se puede ver en general un módulo puede tener dos descomposiciones en inescindibles con sumandos no isomorfos. Sin embargo, bajo las condiciones suficientes se pueden encontrar módulos con una descomposición en inescindibles única salvo isomorfismo como se muestra a continuación. El siguiente es el teorema de Krull-Schmidt-Azumaya para descomposiciones finitas.

Teorema 7.19. *Sea M un módulo con una descomposición en inescindibles*

$$M = M_1 \oplus ... \oplus M_n$$

tal que $\mathrm{End}_A(M_i)$ *es local para cualquier $i \in \{1, ..., n\}$. Si existe una descomposición $M = N_1 \oplus K$ tal que N_1 es un módulo inescindible, entonces $N_1 \cong M_i$ para algún $i \in \{1, ..., n\}$. Más aún, si existe una descomposición en inescindibles $M = N_1 \oplus ... \oplus N_k$, entonces $n = k$ y existe una permutación σ de $\{1, ..., n\}$ tal que $M_i \cong N_{\sigma(i)}$ para toda $i \in \{1, ..., n\}$.*

Demostración. Si $n = 1$, entonces M es inescindible, de modo que no tiene descomposiciones diferentes a $M = M_1$. Considérese como hipótesis inductiva que si B es un módulo con una descomposición en inescindibles $B = B_1 \oplus ... \oplus B_m$ tal que $\mathrm{End}_A(B_i)$ es local para cualquier $i \in \{1, ..., m\}$, entonces todo sumando directo inescindible de B es isomorfo a B_i para algún $i \in \{1, ..., n\}$ y toda descomposición en inescindibles $B = C_1 \oplus ... \oplus C_k$ cumple que $k = m$ y existe una permutación σ de $\{1, ..., m\}$ tal que $B_i \cong C_{\sigma(i)}$ para toda $i \in \{1, ..., n\}$.

Ahora, si $n = m + 1$ y

$$M = M_1 \oplus ... \oplus M_{m+1} = N_1 \oplus ... \oplus N_k$$

donde N_1 es un módulo inescindible. La unidad de $\mathrm{End}_A(M)$ se descompone como $1_M = \rho_1 + ... + \rho_n = \rho'_1 + ... + \rho'_k$ por la Proposición 2.17, donde $\rho_i = \eta_i \pi_i$ y $\rho'_i = \eta'_i \pi'_i$, con $\eta_i : M_i \to M$ y $\eta'_i : N_i \to M$ las inclusiones canónicas, y $\pi_i : M \to M_i$ y $\pi'_i : M \to N_i$ las proyecciones canónicas . Así que

$$1_{M_1} = \pi_1(\rho'_1 + ... + \rho'_k)\eta_1 = \sum_{i=1}^{k} \pi_1 \rho_1 \rho'_i \eta_1 \in \mathrm{End}_A(M_1),$$

lo que implica por el Teorema 7.1 que uno de los sumandos es invertible, supóngase sin pérdida de generalidad que $\pi_1 \rho_1 \rho'_1 \eta_1$ es tal sumando, se observa que

$$\pi_1 \rho_1 \rho'_1 \eta_1 = \pi_1 \eta_1 \pi_1 \eta'_1 \pi'_1 \eta_1 = \pi_1 \eta'_1 \pi'_1 \eta_1 = \pi_1 \rho'_1 \eta_1.$$

Luego, debido a que $\alpha = \pi_1 \rho'_1 \eta_1$ es un isomorfismo, el monomorfismo $\rho'_1 \eta_1$ se escinde, ya que $(\alpha^{-1}\pi_1)(\rho'_1 \eta_1) = 1_{M_1}$. Lo que implica que

$$M = \mathrm{Im}(\rho'_1 \eta_1) \oplus \mathrm{Ker}(\alpha^{-1}\pi_1) = \mathrm{Im}(\rho'_1 \eta_1) \oplus \mathrm{Ker}(\pi_1) = \mathrm{Im}(\rho'_1 \eta_1) \oplus M_2 \oplus ... \oplus M_n.$$

Por otro lado, $\mathrm{Im}(\rho'_1 \eta_1) \subseteq N_1 \subseteq M = \mathrm{Im}(\rho'_1 \eta_1) \oplus \mathrm{Ker}(\pi_1)$, de manera que la ley modular implica que

$$N_1 = N_1 \cap \mathrm{Im}(\rho'_1 \eta_1) + N_1 \cap \mathrm{Ker}(\pi_1) = \mathrm{Im}(\rho'_1 \eta_1) \oplus N_1 \cap \mathrm{Ker}(\pi_1),$$

pero como N_1 es inescindible y $\operatorname{Im}(\rho_1'\eta_1) \neq 0$ se tiene que $N_1 = \operatorname{Im}(\rho_1'\eta_1)$. Por lo tanto, $M = N_1 \oplus M_2 \oplus ... \oplus M_n$.

De esta manera es sencillo concluir que

$$M_2 \oplus ... \oplus M_n \cong M/N_1 \cong N_2 \oplus ... \oplus N_k,$$

lo que implica por la hipótesis de inducción que $k = n$ y existe una permutación σ de $\{2, ..., n\}$ tal que $M_i \cong N_{\sigma(i)}$ para toda $i \in \{2, ..., n\}$, la cual se puede extender a $\{1, ..., n\}$ con $M_1 \cong N_1$, lo cual prueba el teorema. □

Como corolario se tiene el teorema clásico de Krull-Schmidt.

Corolario 7.20. *Si M es un módulo de longitud finita, entonces M tiene una descomposición en inescindibles $M = M_1 \oplus ... \oplus M_n$, y además cualquier otra descomposición en inescindibles tiene el mismo número de sumandos, los cuales son únicos salvo isomorfismo y permutación.*

Demostración. Si M es de longitud finita, entonces M tiene una descomposición en inescindibles por la Proposición 7.17, y por el Corolario 7.14 los anillos de endomorfismo de los sumandos de dicha descomposición son locales, de modo que el Teorema 7.19 implica lo que se quiere probar. □

Corolario 7.21. *Si A es un anillo artiniano y M un A-módulo finitamente generado, entonces M tiene una descomposición en inescindibles $M = M_1 \oplus ... \oplus M_n$, y además cualquier otra descomposición en inescindibles tiene el mismo número de sumandos, los cuales son únicos salvo isomorfismo y permutación.*

7.3. Anillos Semilocales

Para terminar este capítulo se presenta una clase de anillos que generaliza la de locales, y se presentan algunas propiedades que se utilizarán mas adelante.

Definición 7.22. Se dice que un anillo A es semilocal si $A/\operatorname{rad}(A)$ es un anillo semisimple.

Ejemplo 7.23. Un anillo artiniano a derecha ó izquierda es semilocal por el Corolario 5.53.

Nótese que si A es local, entonces $\operatorname{rad}(A)$ es un ideal maximal derecho, y así $A/\operatorname{rad}(A)$ es simple. Lo que muestra que todo anillo local es semilocal.

De hecho, si A tiene un número finito de ideales maximales derechos $I_1, ..., I_n$, entonces $\overline{A} = A/\operatorname{rad}(A)$ es semisimple. En efecto, por el teorema de correspondencia los ideales maximales derechos de $\overline{A}$ son $J_1, ..., J_n$ donde $J_i = I_i/\operatorname{rad}(A)$, de modo que

$$\operatorname{rad}(\overline{A}) = \bigcap_{i=1}^{n} J_i = 0.$$

De manera que el morfismo $f : \overline{A} \to \overline{A}/J_1 \oplus ... \oplus \overline{A}/J_n$ definido como

$$f(x) = (x + J_1, ..., x + J_n)$$

es un monomorfismo, ya que $\operatorname{Ker}(f) = \bigcap_{i=1}^{n} J_i = 0$, pero $\overline{A}/J_1 \oplus ... \oplus \overline{A}/J_n$ es semisimple, lo que implica que $\overline{A}$ es semisimple por la Proposición 3.5. Por lo tanto, A es semilocal.

Proposición 7.24. *Sea A un anillo. Si A tiene un número finito de ideales maximales derechos, entonces A es semilocal.*

Cabe observar que el recíproco es falso como muestra el siguiente ejemplo.

Ejemplo 7.25. Dado un campo infinito k, sea $A = \mathbb{M}_2(k)$. Debido a que A es anillo de matrices sobre un campo se sigue que A es semisimple, por lo que A es semilocal. Sin embargo, A tiene un número infinito de ideales maximales derechos. En efecto, para todo $(x, y) \in k^2$ con $y \neq 0$

$$I = \begin{pmatrix} x & x \\ y & y \end{pmatrix} A = \left\{ \begin{pmatrix} x\lambda & x\mu \\ y\lambda & y\mu \end{pmatrix} \quad | \quad \lambda, \mu \in k \right\}$$

es un ideal maximal derecho, ya que si se toma un elemento $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in J \backslash I$ donde J es un ideal derecho que contiene a I, entonces (a, b) ó (c, d) es linealmente independiente de (x, y). Si (a, b) es linealmente independiente de (x, y), entonces existen $\gamma_1, \gamma_2 \in k$ tales que $(1, 0) = \gamma_1(x, y) + \gamma_2(a, b)$, y entonces se puede generar un elemento invertible

$$\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} = \begin{pmatrix} x & x \\ y & y \end{pmatrix} \begin{pmatrix} \gamma_1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} \gamma_2 & 0 \\ 0 & 0 \end{pmatrix} \in J,$$

lo que implica que $J = A$. De la misma manera se llega al mismo resultado si se supone (c, d) linealmente independiente de (x, y). Por lo tanto, I es un ideal maximal derecho para todo $(x, y) \in k^2$ con $y \neq 0$, y como existe un número infinito de vectores de esta forma, existe una infinidad de ideales maximales derechos.

Ejemplo 7.26. Dados p y q enteros primos, si

$$A = \left\{ \frac{a}{b} \quad | \quad p \,\text{y}\, q \,\text{no dividen a}\; b \right\},$$

entonces A es un anillo semilocal. En efecto, el ideal pA es maximal ya que todo elemento $\frac{a}{b} \in A \backslash pA$ cumple que p y a son primos relativos, de modo que existen x y z tales que $1 = za + px$, y así

$$1 = zb\frac{a}{b} + \frac{pxb}{b}.$$

Por lo tanto, cualquier ideal que contenga propiamente a pA es forzosamente A. En consecuencia el ideal pA es maximal, y análogamente se prueba que qA es maximal. Además, es sencillo deducir que estos son los únicos ideales maximales. Lo que implica que A es semilocal.

Ejemplo 7.27. Si $A_1, ..., A_n$ son anillos semilocales, entonces $A = A_1 \oplus ... \oplus A_n$ es un anillo semilocal. Ciertamente, tomando la descomposición central de la unidad inducida por la descomposición del anillo $1 = e_1 + ... + e_n$ se tiene que $A/\operatorname{rad}(A)$ es igual a

$$\left(\bigoplus_{i=1}^{n} e_iAe_i\right) / \left(\bigoplus_{i=1}^{n} e_i \operatorname{rad}(A)e_i\right) \cong \bigoplus_{i=1}^{n} e_iAe_i/\operatorname{rad}(e_iAe_i) \cong \bigoplus_{i=1}^{n} A_i/\operatorname{rad}(A_i),$$

de manera que $A/\operatorname{rad}(A)$ es un anillo semisimple por ser una suma directa de anillos semisimples. Por lo tanto, se ha probado que una suma directa finita de anillos semilocales es semilocal. En particular, si B es un anillo semilocal, entonces B^n es semilocal para todo $n \in \mathbb{N}$, y toda suma directa finita de anillos locales es un anillo semilocal.

Ejemplo 7.28. Si A es un anillo semilocal, entonces $B = \mathbb{M}_n(A)$ es semilocal para todo $n \in \mathbb{N}$. En efecto, es sencillo probar que

$$\operatorname{rad}(B) = \mathbb{M}_n(\operatorname{rad}(A)) \text{ y } B/\operatorname{rad}(B) \cong \mathbb{M}_n(A/\operatorname{rad}(A)).$$

Por lo tanto, deduciendo del Teorema de Wedderburn-Artin que $\mathbb{M}_n(A/\operatorname{rad}(A))$ es semisimple, se tiene que $B/\operatorname{rad}(B)$ es semismple.

Ejemplo 7.29. Si A es semilocal y e un idempotente de A, entonces eAe es semilocal. La demostración se sigue de la proposición el Corolario 5.38 que muestra un isomorfismo $\overline{e}\,(A/\operatorname{rad}(A))\,\overline{e} \cong eAe/\operatorname{rad}(eAe)$ donde $\overline{e} = e + \operatorname{rad}(A)$. En consecuencia, si A es semilocal, $A/\operatorname{rad}(A)$ es semisimple y de modo que $\overline{e}\,(A/\operatorname{rad}(A))\,\overline{e}$ también es semisimple, lo que implica que eAe es semilocal.

Ejemplo 7.30. Si M es un módulo de longitud finita, entonces $B = \operatorname{End}_A(M)$ es semilocal. En efecto, debido a que M es de longitud finita, M tiene una descomposición en inescindibles por la Proposición 7.17, y entonces se puede suponer que existe una descomposición

$$M = M_1 \oplus ... \oplus M_n$$

con $M_i = N_i^{k_i}$ y N_i inescindibles para todo $i \in \{1, ..., n\}$ tales que $N_i \ncong N_j$ si $i \neq j$. Luego, si $1 = e_1 + ... + e_n$ es la descomposición de la unidad de $\operatorname{End}_A(M)$ inducida por tal descomposición, se tiene por la Proposición 2.26 que B es isomorfo al anillo

$$\begin{pmatrix} e_1Be_1 & \dots & e_1Be_n \\ e_2Be_1 & & \\ \vdots & \ddots & \\ e_nBe_1 & & e_nBe_n \end{pmatrix} \cong \begin{pmatrix} \mathrm{End}_A(M_1) & \dots & \mathrm{Hom}_A(M_n, M_1) \\ \mathrm{Hom}_A(M_1, M_2) & & \\ \vdots & \ddots & \\ \mathrm{Hom}_A(M_1, M_n) & & \mathrm{End}_A(M_n) \end{pmatrix}.$$

Ahora, si se toma $f \in e_iBe_j$ con $i \neq j$ y a es un elemento arbitrario de B, entonces $fa = \sum_{k=1}^{n}(e_ife_j)ae_k = \sum_{k=1}^{n} fae_k$ lo que implica que $1 - fa$ se puede identificar con la matriz

$$\begin{pmatrix} 1_{E_1} & 0 & & & & 0 \\ 0 & 1_{E_2} & & & & \\ \vdots & & \ddots & & & \\ -fae_1 & -fae_2 & \cdots & (1_{E_i} - fae_i) & \cdots & -fae_n \\ & & & & \ddots & \\ \vdots & & & & & 0 \\ 0 & \cdots & & & 0 & 1_{E_n} \end{pmatrix},$$

donde $E_i = \mathrm{End}_A(M_i)$. Además, $fae_i \in \mathrm{rad}(\mathrm{End}_A(M_i))$ por el Corolario 7.16 ya que $fae_i = f(e_jae_i)$ donde $f \in \mathrm{Hom}_A(M_j, M_i)$ y $e_jae_i \in \mathrm{Hom}_A(M_j, M_i)$, lo que implica que $1_{E_i} - fae_i$ es invertible. Ahora, si $x = (1_{E_i} - fae_i)^{-1}$, es sencillo verificar que

$$\begin{pmatrix} 1_{E_1} & 0 & & & & 0 \\ 0 & 1_{E_2} & & & & \\ \vdots & & \ddots & & & \\ xfae_1 & xfae_2 & \cdots & x & \cdots & xfae_n \\ & & & & \ddots & \\ \vdots & & & & & 0 \\ 0 & \cdots & & & 0 & 1_{E_n} \end{pmatrix}$$

es un inverso izquierdo de $1 - fa$. Por lo tanto, se ha probado para todo $f \in e_iBe_j$ con $i \neq j$ que $1 - fa$ es invertible por la izquierda para todo $a \in B$, de modo que $f \in \mathrm{rad}(B)$. Es decir, $e_iBe_j \subsetneq \mathrm{rad}(B)$ para todo $i \neq j$. Lo que implica por el Teorema 5.42 que

$$\mathrm{rad}(B) = \begin{pmatrix} \mathrm{rad}(E_1) & \mathrm{Hom}_A(M_2, M_1) & \dots & \mathrm{Hom}_A(M_n, M_1) \\ \mathrm{Hom}_A(M_1, M_2) & \mathrm{rad}(E_2) & & \\ \vdots & & \ddots & \\ \mathrm{Hom}_A(M_1, M_n) & & & \mathrm{rad}(E_n) \end{pmatrix},$$

y así es inmediato que $A/\mathrm{rad}(A) \cong E_1/\mathrm{rad}(E_1) \oplus ... \oplus E_n/\mathrm{rad}(E_n)$ que es semisimple ya que E_i es local para todo $i \in \{1, ..., n\}$.

Ejemplo 7.31. Si A es semilocal y P es un A-módulo proyectivo finitamente generado, entonces $\operatorname{End}_A(P)$ es semilocal. En efecto, si P es proyectivo finitamente generado, entonces es sumando directo de un módulo libre finitamente generado, es decir existe un módulo N tal que $P \oplus N \cong A^n$ para algún $n \in \mathbb{N}$. Luego por la Proposición 2.17 se tiene una descomposición de la unidad $1 = e_1 + e_2$ de $\operatorname{End}_A(A^n)$ tal que $e_1(A^n) \cong P$, lo que implica que

$$e_1 \operatorname{End}_A(A^n) e_1 \cong \operatorname{End}_A(e_1 A^n) \cong \operatorname{End}_A(P).$$

Y entonces $\operatorname{End}_A(P)$ es semilocal ya que $\operatorname{End}_A(A^n) \cong \mathbb{M}_n(A)$ es semilocal, lo que implica que $e_1 \operatorname{End}_A(A^n) e_1$ sea semilocal también.

Otros ejemplos y caracterizaciones de los anillos semilocales se pueden encontrar en el capítulo 4 de [Fac98] como son los siguientes.

Ejemplo 7.32. Si M es un módulo artiniano, entonces $B = \operatorname{End}_A(M)$ es semilocal.

Ejemplo 7.33. Si M es uniserial, es decir para todo par de submódulos N, K de M se cumple que $N \subseteq K$ ó $K \subseteq N$, entonces $\operatorname{End}_A(M)$ es semilocal.

Ahora, si A es semilocal, entonces por el Teorema 3.28, al ser semisimple, $A/\operatorname{rad}(A)$ es isomorfo a un producto finito de anillos de matrices sobre anillos con división. De este hecho se puede obtener información sobre los elementos de A de la siguiente manera.

En un un anillo con división D, $ab = 1$ implica que $ba = 1$ para cualesquiera $a, b \in D$. De la misma manera, si B es un anillo de matrices sobre D, entonces para toda pareja de elementos $a, b \in B$ tales que $ab = 1$ se tiene también que $ba = 1$. Y de manera similar $C = A_1 \times ... \times A_n$ donde los A_i son anillos que cumplen que si $ab = 1$ entonces $ba = 1$ para todo $a, b \in A_i$, se tiene que si $c, d \in C$ cumplen que $cd = 1$, entonces $c = (a_1, ..., a_n)$ y $d = (b_1, ..., b_n)$ lo que implica que $(1, ..., 1) = 1 = cd = (a_1 b_1, ..., a_n b_n)$, pero entonces $1 = (b_1 a_1, ..., b_n a_n) = dc$. Por lo tanto, C también se C cumple que si $ab = 1$ entonces $ba = 1$ para todo $a, b \in C$.

Con esta argumentación es sencillo probar que si $a \in A$ tiene inverso por la derecha, entonces a es invertible. En efecto, si a es invertible por la derecha, entonces $a + \operatorname{rad}(A)$ también; y asi por la argumentación anterior al ser $A/\operatorname{rad}(A)$ semisimple, $a + \operatorname{rad}(A)$ es invertible, y entonces por la Proposición 5.54 a es invertible.

Se ha probado la siguiente proposición.

Proposición 7.34. *Si A es un anillo semilocal, entonces todo elemento con inverso a la derecha es invertible.*

Esta proposición se puede generalizar al siguiente resultado, el teorema de Bass.

Teorema 7.35. *Sea A un anillo semilocal, $a \in A$ y J un ideal derecho de A. Si $aA + J = A$, entonces $a + J$ contiene un elemento invertible de A.*

Demostración. Si A es semisimple, entonces todo ideal es semisimple, de modo que existe un ideal derecho I tal que $J = (aA \cap J) \oplus I$, y así

$$A = aA + J = aA + (aA \cap J) \oplus I = aA \oplus I.$$

Luego, la función $f : A \to aA$ definida como $f(x) = ax$ es un epimorfismo, de modo que la sucesión

$$0 \to \operatorname{Ker}(f) \to A \to aA \to 0$$

se escinde debido a que A es semisimple, lo que implica que $A = C \oplus \operatorname{Ker}(f)$ con $f|_C$ un isomorfismo.

Por lo tanto, $C \oplus \operatorname{Ker}(f) = A = eA \oplus I$ con $C \cong eA$, pero A es semisimple, así que de la Proposición 4.47 se deduce que existe un isomorfismo $g : \operatorname{Ker}(f) \to I$. De manera que el morfismo $\phi : C \oplus \operatorname{Ker}(f) \to eA \oplus I$ definido como $\phi(x) = ax + g\pi(x)$, donde $\pi : A \to \operatorname{Ker}(f)$ es la proyección natural, es un automorfismo de A, ya que $\phi(x) = 0$ si, y sólo si, $ax = g\pi(x) \in aA \cap I$ si, y sólo si, $x = 0$, lo que muestra que ϕ es inyectiva. Y para mostrar que es suprayectiva basta probar que para todo $y \in I$ existe $x \in A$ tal que $g\pi(x) = y$, lo cual se cumple ya que $g\pi$ es un epimorfismo. Por lo tanto, $\phi(1) = a + g\pi(1) \in a + I \subseteq a + J$ es un elemento invertible.

De esta manera se ha probado lo deseado si A es semisimple. Si A no es semisimple se denotan $a' = a + \operatorname{rad}(A)$, $A' = A/\operatorname{rad}(A)$ y $J' = (J + \operatorname{rad}(A))/\operatorname{rad}(A)$, así que A' es semisimple y $A' = a'A' + J'$ pues $A = aA + J$: Luego, por la argumentación anterior, $a' + J'$ contiene un elemento invertible de A', y entonces por la Proposición 5.54 $a + J$ contiene un elemento invertible de A. ☐

Ahora, si A es un anillo semilocal, y se tienen $a, b \in A$ tales que $aA + bA = A$, el teorema anterior indica que existe un elemento invertible $x = a + by$ para alguna $y \in A$. Esto lleva al siguiente resultado, el teorema de cancelación de Evans.

Teorema 7.36. *Sean M, N y K módulos. Si $M \oplus N \cong M \oplus K$ y $E = \operatorname{End}_A(M)$ es semilocal, entonces $N \cong K$.*

Demostración. Sea $F : M \oplus N \to M \oplus K$ un isomorfismo y $F^{-1} = G : M \oplus K \to M \oplus N$. Considerando la representación matricial de F y G, se tiene que

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \begin{pmatrix} \operatorname{End}_A(M) & \operatorname{Hom}_A(N, M) \\ \operatorname{Hom}_A(M, K) & \operatorname{Hom}_A(N, K) \end{pmatrix} \text{ y}$$

$$G = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \in \begin{pmatrix} \operatorname{End}_A(M) & \operatorname{Hom}_A(K, M) \\ \operatorname{Hom}_A(M, N) & \operatorname{Hom}_A(K, N) \end{pmatrix}.$$

De manera que

$$\begin{pmatrix} 1_M & 0 \\ 0 & 1_N \end{pmatrix} = GF = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha'\alpha + \beta'\gamma & \alpha'\beta + \beta'\delta \\ \gamma'\alpha + \delta'\gamma & \gamma'\beta + \delta'\delta \end{pmatrix},$$

y así $0 = \gamma'\alpha + \delta'\gamma$, $1_N = \gamma'\beta + \delta'\delta$ y $1_M = \alpha'\alpha + \beta'\gamma$. Luego, de la última ecuación se concluye que

$$E = \alpha'\alpha E + \beta'\gamma E \subseteq \alpha' E + \beta'\gamma E,$$

es decir $E = \alpha' E + \beta'\gamma E$, lo que implica por el teorema anterior que existe $\omega \in E$ tal que $x = \alpha' + \beta'\gamma\omega$ es un isomorfismo.

De modo que si se define

$$F' = \begin{pmatrix} 1_M & \beta \\ \gamma\omega & \delta \end{pmatrix} : M \oplus N \to M \oplus K,$$

$$GF' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \begin{pmatrix} 1_M & \beta \\ \gamma\omega & \delta \end{pmatrix} = \begin{pmatrix} x & 0 \\ \gamma' + \delta'\gamma\omega & 1_N \end{pmatrix}$$

es claramente un isomorfismo, y como G es un isomorfismo, entonces F' es un isomorfismo. Así que,

$$\begin{pmatrix} 1_M & 0 \\ -\gamma\omega & 1_K \end{pmatrix} F' \begin{pmatrix} 1_M & -\beta \\ 0 & 1_N \end{pmatrix} = \begin{pmatrix} 1_M & 0 \\ 0 & -\gamma\omega\beta + \delta \end{pmatrix}$$

es también un isomorfismo claramente, lo que implica que $-\gamma\omega\beta + \delta : N \to K$ es un isomorfismo. □

Corolario 7.37. *Dado A un anillo semilocal se cumplen los siguientes enunciados.*

(a) *Si M, N y K son A-módulos tales que M es un proyectivo finitamente generado, entonces $M \oplus N \cong M \oplus K$ implica que $N \cong K$.*

(b) *Si $A^n \cong A^m$, entonces $n = m$.*

Demostración.

(a) Es inmediato del teorema anterior ya que $\mathrm{End}_A(M)$ es semilocal como se vió en el Ejemplo 7.31.

(b) Si existen n y m números naturales tales que $A^n \cong A^m$ donde $n \leq m$, entonces por el Teorema 7.36 $A^{n-1} \cong A^{m-1}$, pues $\mathrm{End}_A(A) \cong A$ es semilocal. Inductivamente, se deduce que para todo $k \leq n$ se cumple que $A^{n-(k-1)} \cong A^{m-(k-1)}$. Por lo tanto, $0 = A^{n-n} \cong A^{m-n}$, lo que implica que $m = n$.

□

8. Anillos Semiperfectos

En este capítulo se alcanza el objetivo de caracterizar los anillos que cumplen con que todo módulo finitamente generado tenga cubierta proyectiva.

Para ello en la primera sección se considera un anillo semilocal A, es decir, un anillo A tal que $A/rad(A)$ es semisimple, y se muestra que una condición suficiente para que todo módulo finitamente generado tenga cubierta proyectiva es que se puedan levantar los idempotentes de $A/rad(A)$.

En la segunda sección se definen los anillos semiperfectos y se dan diferentes caracterizaciones de esta clase de anillos, entre las cuales se prueba que un anillo es semiperfecto si y sólo si todo módulo finitamente generado tiene cubierta proyectiva.

Por último, en la tercera sección se exponen algunas propiedades de los módulos sobre un anillo semilocal, con las que se caracterizan las cubiertas proyectivas de los módulos finitamente generados sobre un anillo semiperfecto.

8.1. Levantamiento de idempotentes

Sea A un anillo semilocal. Si M es un módulo finitamente generado sobre A, entonces por el Corolario 6.34 M y $M/rad(M)$ tienen la misma cubierta proyectiva en caso de existir. Además, $M/rad(M)$ es semisimple de longitud finita por el Corolario 4.41, lo que implica que $M/rad(M)$ tiene cubierta proyectiva si, y sólo si, cada uno de sus sumandos simples tienen cubierta proyectiva por el Corolario 6.30. Por lo tanto, basta que todo A-módulo simple tenga cubierta proyectiva para que todo módulo finitamente generado tenga cubierta proyectiva.

De modo que cabe preguntarse qué condiciones se deben imponer sobre A para que todo módulo simple tenga cubierta proyectiva.

Se observa que si existe una descomposición de la unidad $1 = e_1 + ... + e_n$ de A tal que $\overline{e_i}(A/rad(A))$ sea simple para todo $i \in \{1, ..., n\}$, donde $\overline{e_i} = e_i + rad(A)$, entonces por el Corolario 3.21 y la Proposición 5.54 el conjunto

$$\{\bar{e}_i(A/rad(A)) \quad | \quad i \in \{1, ..., n\}\}$$

contiene un sistema completo de representantes de las clases de módulos simples bajo la relación de isomorfismo. Además, por el Ejemplo 6.21, se sigue que la proyección natural $\pi_i : e_iA \to e_iA/rad(e_iA)$ es una cubierta proyectiva de $e_iA/rad(e_iA)$ para todo $i \in \{1, ..., n\}$. Por lo tanto, todo simple tiene cubierta proyectiva, y entonces la existencia de tal descomposición de la unidad es suficiente para que todo módulo finitamente generado tenga una cubierta proyectiva sobre A, y como se verá en la siguiente sección es una condición necesaria.

Ahora, debido a que A es semilocal por las Proposiciones 2.22 y 3.22 existe una descomposición de la unidad $\overline{1} = \overline{f_1} + ... + \overline{f_n}$ de $A/rad(A)$ tal que $\overline{f_i}(A/rad(A))$ es simple para todo $i \in \{1, ..., n\}$. Por lo tanto, si para cada $\overline{f_i}$ existe un idempotente $e_i \in A$ de tal manera que $1 = e_1 + ... + e_n$ sea una descomposición de la unidad y que $e_i + rad(A) = \overline{f_i}$ para todo $i \in \{1, ..., n\}$, entonces tal descomposición es la descomposición deseada. Será útil entonces la siguiente definición.

Definición 8.1. Sea A un anillo y J un ideal bilateral. Se dice que un idempotente $a + J \in A/J$ se puede levantar si existe un idempotente $e \in A$ tal que $a + J = e + J$, y en tal caso se dice que e es un levantamiento de $a + J$. Si todo idempotente de A/J se puede levantar, entonces se dice que J admite el levantamiento de idempotentes.

Con este objetivo, en esta sección se exponen algunos ideales bilaterales J tales que todo idempotente de A/J se puede levantar, y las propiedades que cumplen los idempotentes en caso de levantarse.

Una clase de ideales que permite el levantamiento de idempotentes es la siguiente.

Definición 8.2. Sea I un ideal bilateral. Se dice que I es un ideal nil si todo elemento de I es nilpotente.

Teorema 8.3. *Sea I un ideal nil de un anillo A, entonces todo idempotente de A/I se puede levantar.*

Demostración. Sea $\pi : A \to A/I$ la proyección natural. Si a es un elemento de A tal que $\pi(a) = a + I$ es idempotente, entonces $a - a^2 \in I$, y como I es nil existe un k tal que $(a - a^2)^k = 0$. Luego, notando que

$$(1 - a)^k = \sum_{i=0}^{k} \frac{n!}{i!(n-i)!}(-a)^i = 1 - a(\sum_{i=1}^{k} \frac{n!}{i!(n-i)!}(-a)^{i-1}) = 1 - ad,$$

con $da = ad$,

$$1 - \pi(ad) = \pi(1 - ad) = \pi((1 - a)^k) = \pi(1 - a)^k = (1 - \pi(a))^k = 1 - \pi(a)$$

ya que $1 - \pi(a)$ es idempotente por ser $\pi(a)$ idempotente, y por ello $\pi(ad) = \pi(a)$. Por otro lado,

$$0 = (a - a^2)^k = a^k(1 - a)^k = a^k(1 - ad)$$

lo que implica que $a^k = a^k ad$, de manera que para todo $m > 0$

$$a^k(ad)^{m-1} = a^k(ad)^m.$$

Utilizando lo anterior se prueba inductivamente que $a^k = a^k(ad)^0 = a^k(ad)^m$. En particular, $a^k = a^k(ad)^k$ y utilizando la conmutatividad entre a y d, se prueba que $a^k = a^{2k}d^k$. Por lo tanto, $((ad)^k)^2 = a^{2k}d^{2k} = a^{2k}d^kd^k = (ad)^k$. Por lo tanto, $e = (ad)^k$ es idempotente que es un levantamiento de $a + I$. □

Corolario 8.4. *Si I es nilpotente, entonces los idempotentes de A/I se pueden levantar.*

Ejemplo 8.5. Si A es un anillo artiniano, entonces $rad(A)$ es nilpotente, por lo que los idempotentes de $A/rad(A)$ se pueden levantar a A.

Cabe hacer la observación de que un ideal no necesita ser nil para que los idempotentes de A/I se puedan levantar.

Ejemplo 8.6. Dado un campo k sea $A = k[x]$. Si $I = xA$, entonces I no es nil y los idempotentes de A/I se pueden levantar. En efecto, es claro que I no es nilpotente, y si $f(x) + I \in A/I$ es idempotente, entonces

$$f(x)(1 - f(x)) = f(x) - f^2(x) \in I,$$

lo que implica que $f(0) = 1$ ó $f(0) = 0$, ya que

$$f(0)(1 - f(0)) = f(0) - f^2(0) \in 0A = \{0\},$$

y así $f(x)+I = 0+I$ ó $f(x)+I = 1+I$ debido a que $f(x)+I = f(0)+I$. De manera que todo idempotente de A/I se puede levantar claramente.

El ejemplo anterior también muestra que no hay relación con los ideales que están contenidos en el radical y los ideales que permiten levantar idempotentes. Sin embargo, un ideal contenido en el radical que permite levantar idempotentes cumple propiedades interesantes, como se muestra en la siguiente proposición.

Proposición 8.7. *Sea A un anillo con $e \in A$ un idempotente y un ideal $I \subseteq rad(A)$.*

Si los idempotentes de A/I se pueden levantar, entonces se cumplen los siguientes enunciados, donde se consideran todos los idempotentes distintos de 0.

(a) *Dados α y β idempotentes de A tales que $\alpha\beta, \beta\alpha \in I$, existe un idempotente $\beta' \in A$ ortogonal a α tal que $\beta + I = \beta' + I$.*

(b) *$e + I$ es un idempotente primitivo si, y sólo si, cualquiera de sus levantamientos es un idempotente primitivo.*

(c) *Todo conjunto finito de idempotentes ortogonales de A/I se levanta a un conjunto de idempotentes ortogonales distintos de* 0.

(d) *Todo sistema completo de idempotentes ortogonales primitivos de A/I se levanta a un sistema completo de idempotentes ortogonales primitivos de A.*

Demostración.

(a) Como $\beta\alpha \in I \subseteq rad(A)$ se tiene que $1-\beta\alpha$ es invertible, así que

$$\gamma = (1-\beta\alpha)^{-1}\beta(1-\beta\alpha)$$

es idempotente en A. Además, debido a que $1+I = (1-\beta\alpha)+I$

$$\gamma + I = (1-\beta\alpha)^{-1}\beta(1-\beta\alpha) + I = 1\beta 1 + I = \beta + I,$$

por lo que $\gamma + I = \beta + I$. Más aún, $\gamma\alpha = 0$ ya que

$$\gamma\alpha = (1-\beta\alpha)^{-1}\beta(\alpha-\beta\alpha) = (1-\beta\alpha)^{-1}(\beta\alpha-\beta\alpha) = 0.$$

De manera que $\beta' = (1-\alpha)\gamma$ es el elemento buscado ya que

$$\beta' + I = \gamma - \alpha\gamma + I = \beta - \alpha\beta + I = \beta + I,$$

es ortogonal a α por construcción, y es idempotente pues

$$\beta'^2 = (1-\alpha)\gamma(1-\alpha)\gamma = (1-\alpha)(\gamma-\gamma\alpha)\gamma = (1-\alpha)\gamma^2 = \beta'.$$

(b) Sean $e+I$ un idempotente primitivo de A/I y f un levantamiento de $e+I$. Si se supone que $f = \alpha+\beta$ con α, β idempotentes ortogonales diferentes de cero, entonces $\alpha, \beta \notin rad(A)$. En efecto, en caso de que $\alpha \in rad(A)$, se cumple que $1-\alpha$ es invertible, lo que implica que $\alpha = 0$ ya que

$$1 = (1-\alpha)(1-\alpha)^{-1} = (1-\alpha)^2(1-\alpha)^{-1} = (1-\alpha),$$

así que $\alpha = 0$, lo cual es una contradicción. De modo que

$$e + I = f + I = (\alpha + I) + (\beta + I)$$

es una descomposición no trivial, lo cual es una contradicción. Por lo tanto, f es un idempotente primitivo.
Recíprocamente, si e es un idempotente primitivo de A y se supone que existe una descomposición no trivial $e+I = (x+I)+(y+I)$, entonces por hipótesis existen α y β levantamientos de $x+I$ y $y+I$ tales que $\alpha\beta, \beta\alpha \in I$ por ser $x+I$ y $y+I$ ortogonales. De modo que existe β' idempotente ortogonal a α que también

es un levantamiento de $y+I$ por el punto anterior. En consecuencia, $e' = \alpha + \beta'$ es un levantamiento de $e+I$, lo que implica que $eA \cong e'A$ por el Corolario 5.48 pues
$$eA/eI \cong (e+I)(A/I) = (e'+I)(A/I) \cong e'A/e'I,$$
lo cual es una contradicción pues eA es inescindible debido a que e es primitivo, pero $e'A = \alpha A \oplus \beta' A$ no lo es.

(c) Se prueba por iducción que si $X = \{\overline{x}_1, ..., \overline{x}_n\}$ es un conjunto finito de idempotentes ortogonales de A/I, entonces existe un conjunto finito de idempotentes ortogonales $\{y_1, ..., y_n\}$ de A tales que y_i es levantamiento de $\overline{x}_i$ para todo $i \in \{1, ..., n\}$. Si $X = \{\overline{x}_1, \overline{x}_2\}$, existen levantamientos ortogonales por el punto (a). Luego, suponiendo válida la hipótesis de inducción para n, si se tienen $\overline{x}_1, ..., \overline{x}_{n+1}$ idempotentes ortogonales, existen $y_1, ..., y_n \in A$ levantamientos ortogonales de $\overline{x}_1, ..., \overline{x}_n$, y por el punto 1 existe y_{n+1} levantamiento de $\overline{x}_{n+1}$ ortogonal a $y_1 + ... + y_n$. De modo que para toda $i \in \{1, ..., n\}$
$$-y_{n+1}y_i = y_{n+1}y_1 + ... + y_{n+1}y_{i-1} + y_{n+1}y_{i+1} + ... + y_{n+1}y_n,$$
lo que implica que $y_{n+1}y_i = 0$, y análogamente se muestra que $y_iy_{n+1} = 0$. Por lo tanto, todo subconjunto finito de X se puede levantar a un conjunto de idempotentes ortogonales.

(d) Si $X = \{\overline{f_1}, ..., \overline{f_n}\}$ es un sistema completo de idempotentes ortogonales primitivos de A/I, por (b) y (c) este conjunto se puede levantar a un conjunto de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$. Luego, como X es un sistema completo, $x = 1 - (e_n + ... + e_n) \in I \subseteq rad(A)$, pero x es idempotente, de manera que $x = 0$ y así $1 = e_1 + ... + e_n$. Por lo tanto, $\{e_1, ..., e_n\}$ es un sistema completo de idempotentes ortogonales primitivos.

□

Para terminar esta sección se expone un resultado que muestra la relación entre un idempotente $\overline{e} \in A/rad(A)$ y su levantamiento cuando $\overline{e}(A/rad(A))$ es simple. Para ello es necesario el siguiente lema.

Lema 8.8. *Sea A un anillo y $e \in A$ un idempotente distinto de 0. Los siguientes enunciados son equivalentes.*

(a) *eA es simple.*

(b) *eA es simple y $(eA)^2 \neq 0$.*

(c) *eAe es un anillo con división, y si $et \neq 0$ para alguna $t \in A$, entonces $ete \neq 0$.*

Demostración. ($a \Rightarrow b$) Si eA es simple, entonces debido a que $(eA)^2$ es submódulo de eA se cumple que $(eA)^2 = 0$ ó $(eA)^2 = eA$, pero $e = e^2 \in (eA)^2$. Por lo tanto, eA es simple y $(eA)^2 \neq 0$.

$(b \Rightarrow c)$ Si eA es simple, entonces $eAe \cong \mathrm{End}_A(eA)$ es un anillo con división por el Lema 3.11. De manera que si $t \in A$ tal que $et \neq 0$, el morfismo $f : eA \to eA$ definido como $f(e) = et$ no es nulo por lo que tiene un inverso g. Así que $g(et) = gf(e) = e$, por lo que

$$g(ete) = g(et)e = e^2 = e \neq 0,$$

lo que implica que $ete \neq 0$ pues g es un isomorfismo.

$(c \Rightarrow a)$ Por la Proposición 3.9 basta probar que para todo $et \in eA$ distinto de 0, $etA = eA$. Si $et \in eA$ es distinto de cero, entonces por (c) $ete \neq 0$. Por otro lado, eAe es un anillo con división por lo que ete tiene un inverso $ese \in eAe$, en consecuencia $eA \supseteq etA \supseteq eteseA = eA$, de modo que $eA = etA$. Por lo tanto, eA es simple. □

Proposición 8.9. *Sea A un anillo. Si f es un elemento de A que es un levantamiento de un idempotente $\bar{e} \in A/rad(A)$, entonces los siguientes enunciados son equivalentes.*

(a) fAf *es local.*

(b) $\bar{e}(A/rad(A))$ *es simple.*

(c) $f(rad(A)) = rad(fA)$ *es el único submódulo maximal de* fA.

Demostración. $(a \Rightarrow b)$ Si fAf es local, entonces $fAf/rad(fAf)$ es anillo con divisón pero $fAf/rad(fAf) \cong \bar{e}(A/rad(A))\bar{e}$ por el Corolario 5.38, lo que implica que $\bar{e}(A/rad(A))$ es simple. En efecto, si $\bar{e}(t + rad(A)) \neq 0$ para algún $t \in A$, entonces $ft \notin rad(A)$, lo que implica que $ftf \notin rad(A)$, ya que de suponer lo contrario se llega a que $f \in rad(A)$ debido a que $rad(A)$ es un ideal primo por ser maximal, lo cual es una contradicción. Por lo tanto, $\bar{e}(A/rad(A))\bar{e}$ es un anillo con división tal que $ft + rad(A) \neq 0$ implica que $ftf + rad(A) \neq 0$. En conclusión, $\bar{e}(A/rad(A))$ es simple por el lema anterior.

$(b \Rightarrow a)$ Por el Corolario 5.38

$$fAf/rad(fAf) \cong \bar{f}(A/rad(A))\bar{f},$$

pero por la Proposición 2.13

$$\bar{f}(A/rad(A))\bar{f} \cong \mathrm{End}_A(\bar{e}(A/rad(A)))$$

que es un anillo con división por ser $\bar{e}(A/rad(A))$ simple, lo que implica que fAf es local.

$(b \Leftrightarrow c)$ Es inmediato ya que $\bar{e}(A/rad(A)) \cong fA/rad(fA) = fA/f(rad(A))$ por la Proposición 5.47. □

8.2. Anillos Semiperfectos

Definición 8.10. Se dice que A es un anillo semiperfecto si es semilocal y los idempotentes de $A/rad(A)$ se levantan.

Tales anillos se pueden caracterizar de la siguiente manera.

Proposición 8.11. *Dado un anillo A. Los siguientes enunciados son equivalentes:*

(a) *A es semiperfecto.*

(b) *Existe un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$ tal que e_iAe_i es local para toda $i \in \{1, ..., n\}$.*

(c) *Existe una descomposición $A_A = M_1 \oplus ... \oplus M_n$ tal que cada M_i tiene un único submódulo maximal.*

(d) *Todo módulo simple sobre A tiene cubierta proyectiva.*

(e) *Todo módulo finitamente generado sobre A tiene cubierta proyectiva.*

(f) *Todo módulo cíclico sobre A tiene cubierta proyectiva.*

Demostración. $(a \Rightarrow b)$ Si A es semiperfecto, entonces $A/rad(A)$ es semisimple, lo que implica que existe un sistema completo de idempotentes ortogonales primitivos $\{\overline{e_1}, ..., \overline{e_n}\}$ de $A/rad(A)$ tales que $\overline{e_i}(A/rad(A))$ es simple para todo i por la Proposición 2.17. Luego, por la Proposición 8.7 dichos idempotentes se pueden levantar a un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$, que además cumplen con que e_iAe_i es local para todo i por la Proposición 8.9.

$(b \Rightarrow c)$ Es inmediato de la Proposición 8.9.

$(c \Rightarrow d)$ Si $A_A = M_1 \oplus ... \oplus M_n$ es la descomposición referida en el punto (c), entonces por la Proposición 2.17 existe una descomposición de la unidad $1 = e_1 + ... + e_n$ tal que $e_iA = M_i$ para todo $i \in \{1, ..., n\}$. Por otro lado, si S es un módulo simple y $f : A \to S$ un epimorfismo

$$f = f|_{e_1A} \oplus ... \oplus f|_{e_nA},$$

por lo que $g = f|_{e_iA}$ es no nulo para algún $i \in \{1, ..., n\}$. Así que $g : e_iA \to S$ un epimorfismo por ser S simple, y por el primer teorema de isomorfismo

$$\mathrm{Ker}(g) = rad(e_iA)$$

ya que éste es el único submódulo maximal por hipótesis. Además, por la Proposición 5.31 se tiene que $rad(e_iA)$ es superfluo, de modo que g es una cubierta proyectiva de S. Por lo tanto, todo módulo simple tiene cubierta proyectiva.

$(d \Rightarrow e)$ Sea F un sistema completo de representantes de las clases de isomorfismo de los módulos simples sobre A. Por hipótesis cada $S \in F$ tiene una cubierta proyectiva

$f_S : P_S \to S$, de manera que al ser $\mathrm{Ker}(f_S)$ un submódulo superfluo y maximal de P_S para todo $S \in F$, $\mathrm{Ker}(f_S) = rad(P_S)$, de modo que P_S es un módulo con un único submódulo maximal para todo $S \in F$.

Luego, sea $P = \bigoplus_{S\in F} P_S$. Si M es un módulo finitamente generado y

$$N = \sum_{f\in \mathrm{Hom}_A(P,M)} f(P),$$

entonces $N = M$. En efecto, si se supone $N \neq M$, entonces debido a que M es finitamente generado, el lema de Zorn implica que el conjunto

$$\{M' \text{ submódulo de } M \quad | \quad N \subseteq M' \neq M\}$$

tiene un elemento maximal K que es un submódulo maximal de M que contiene a N. Luego, debido a que M/K es simple existe una cubierta proyectiva $g : P_S \to M/K$, por lo que existe un morfismo no nulo $h = \eta\pi : P \to M$, donde $\pi : P \to P_S$ es la proyección canónica y $\eta : P_S \to M$ es el morfismo inducido por ser P_S proyectivo que hace conmutar el siguiente diagrama donde $p : M \to M/K$ es la proyección natural.

$$\begin{tikzcd}
& P_S \arrow[dl, dashed, "\eta"'] \arrow[d, phantom, "\circlearrowright"] \arrow[dr, "g"] & & \\
M \arrow[rr, "p"'] & & M/K \arrow[r] & 0
\end{tikzcd}$$

Por otro lado, si $\iota : N \to M$ es la inclusión natural, $p\iota\eta\pi = 0$ ya que $Im(\iota\eta\pi) \subseteq K$ por construcción, pero $p\iota\eta\pi = g\pi \neq 0$ ya que g y π son epimorfismos, lo cual es una contradicción. Por lo tanto, $N = M$.

$$\begin{tikzcd}
& P \arrow[r, "\pi"] \arrow[dl, "\eta\pi"'] \arrow[d, phantom, "\circlearrowright"] & P_S \arrow[dl, "\eta"'] \arrow[d, phantom, "\circlearrowright"] \arrow[dr, "g"] & & \\
N \arrow[r, "\iota"'] & M \arrow[rr, "p"'] & & M/K \arrow[r] & 0
\end{tikzcd}$$

Por otra parte, debido a que M es finitamente generado y $M = \sum_{f\in \mathrm{Hom}_A(P,M)} f(P)$, se puede tomar un conjunto finito de cardinalidad mínima $\{f_1, ..., f_n\} \subseteq \mathrm{Hom}_A(P, M)$ tal que $M = f_1(P) + ... + f_n(P)$. Esto último implica que existe un epimorfismo

$$f_1 \oplus ... \oplus f_n : P^n = \bigoplus_{S\in F} P_S^n \to M,$$

y así, también por ser M finitamente generado, la Proposición 1.30 implica que existe un conjunto finito de cardinalidad mínima $\{P_1, ..., P_m\}$ con $P_i = P_{S_i}$ para algún $S_i \in F$

para todo $i \in \{1, ..., m\}$, y un epimorfismo $f : \bigoplus_{i=1}^{m} P_i \to M$ tal que

$$f = (f_1 \oplus ... \oplus f_n)|_{\bigoplus_{i=1}^{m} P_i}.$$

Ahora, se busca probar que f es una cubierta proyectiva de M, y para ello basta probar que $\mathrm{Ker}(f)$ es un submódulo superfluo. Se ha mostrado que $rad(P_S)$ es superfluo para todo $S \in F$, lo que implica que todo submódulo de P_i es superfluo por la Proposición 5.34 para todo $i \in \{1, ..., m\}$. De manera que si $P_i \cap \mathrm{Ker}(f)$ es un submódulo distinto de P_i para toda $i \in \{1, ..., n\}$, el submódulo $P_i \cap \mathrm{Ker}(f)$ es superfluo en P_i para toda $i \in \{1, ..., m\}$, de modo que $\mathrm{Ker}(f)$ es superfluo. Por lo tanto, basta probar que $P_i \cap \mathrm{Ker}(f)$ es un submódulo de P_i distinto de P_i para todo subíndice $i \in \{1, ..., m\}$. Si se supone falso, entonces sin pérdida de generalidad $P_1 \cap \mathrm{Ker}(f) = P_1$, es decir $f(P_1) = 0$; pero en tal caso la restricción de f a $\bigoplus_{i=2}^{n} P_i$ sigue siendo un epimorfismo que es igual a $(f_1 + ... + f_n)|_{\bigoplus_{i=2}^{n} P_i}$, lo cual es una contradicción, pues $\{P_1, ..., P_n\}$ es un conjunto de cardinalidad mínima que cumple esta propiedad.

Por lo tanto, todo submódulo finitamente generado tiene cubierta proyectiva.

$(e \Rightarrow f)$ Trivial.

$(f \Rightarrow a)$ Sea $\overline{u}$ un idempotente de $A/rad(A)$. Se consideran las cubiertas proyectivas $f : P \to \overline{u}A$ y $g : Q \to (\overline{1-u})A$. Como

$$A/rad(A) = \overline{u}(A/rad(A)) \oplus (\overline{1-u})(A/rad(A)) = \overline{u}A \oplus (\overline{1-u})A,$$

$\alpha = f \oplus g : P \oplus Q \to A/rad(A)$ es una cubierta proyectiva por la Proposición 6.30. Por otro lado, como A es finitamente generado, $rad(A)$ es superfluo por la Proposición 5.31, de modo que la proyección natural $h : A \to A/rad(A)$ también es una cubierta proyectiva, lo que implica que existe un isomorfismo $\beta : A \to P \oplus Q$ tal que $h = \alpha\beta$. Por lo tanto, gracias a la Proposición 2.17 existe una descomposición en idempotentes $1_A = e_1 + e_2$ tal que las restricciones $h : e_1A \to \overline{u}(A/rad(A))$ y $h : e_2A \to (\overline{1-u})(A/rad(A))$ son cubiertas proyectivas, y entonces como

$$\overline{u} + (\overline{1-u}) = 1 + rad(A) = h(1) = h_1(e_1) + h_2(e_2),$$

$h(e_1) = u$. Por lo tanto, los idempotentes de $A/rad(A)$ se pueden levantar a A.

Ahora, para probar que $A/rad(A)$ es semisimple, por el Teorema 3.18 basta probar que todo módulo cíclico sobre $A/rad(A)$ es proyectivo. Para ello se observa que todo módulo cíclico sobre $A/rad(A)$ es también un módulo cíclico sobre A, y por hipótesis todo cíclico tiene cubierta proyectiva, se tiene por la Proposición 6.22 que todo módulo cíclico sobre $A/rad(A)$ es proyectivo. □

Corolario 8.12. *Si A es un anillo semiperfecto y $\{e_1, ...e_n\}$ es el conjunto de idempotentes referido en el punto (b) del teorema anterior, entonces todo sistema completo* *de idempotentes ortogonales primitivos* $\{f_1, ..., f_m\}$ *de* A *cumple las siguientes propiedades:*

(a) $m = n$.

(b) *Para todo* $i \in \{1, ..., n\}$ *se tiene que* $f_iA \cong e_jA$ *para algún* $j \in \{1, ..., n\}$.

(c) f_iAf_i *es local para todo* $i \in \{1, ..., n\}$.

(d) $(f_i + rad(A))(A/rad(A))$ *es simple para todo* $i \in \{1, ..., n\}$.

Demostración. Si $\{e_1, ..., e_n\}$ es el conjunto de idempotentes referido en el punto (c) y $\{f_1, ..., f_k\}$ es un sistema completo de idempotentes ortogonales primitivos, entonces

$$e_1A \oplus ... \oplus e_nA = A = f_1A \oplus ... \oplus f_kA,$$

pero $e_iAe_i \cong \mathrm{End}_A(e_iA)$ es local para todo $i \in \{1, ..., n\}$ lo que implica por el teorema de Krull-Schmidt que $n = m$ y para todo $i \in \{1, ..., n\}$ existe $j \in \{1, ..., n\}$ tal que $f_iA \cong e_jA$. Es entonces inmediato que $f_iAf_i = \mathrm{End}_A(f_iA) \cong \mathrm{End}_A(e_jA) = e_jAe_j$ es local para todo $i \in \{1, ..., n\}$, y entonces $(f_i + rad(A))(A/rad(A))$ es simple para todo $i \in \{1, ..., n\}$ por la Proposición 8.9. □

Ejemplo 8.13. Si A es semiperfecto y e es un idempotente de A, entonces eAe es semiperfecto. En efecto, por el Ejemplo 7.29 eAe es semilocal y todo idempotente $\overline{f} \in \overline{e}(A/rad(A))\overline{e}$ se puede levantar a un idempotente d tal que $de \neq 0 \neq ed$ por la Proposición 8.7, lo que implica que $d \in eAe$, y entonces los idempotentes de $eAe/rad(eAe)$ se pueden levantar.

Ejemplo 8.14. Si A es un anillo semiperfecto, entonces $\mathbb{M}_m(A)$ es semiperfecto para todo $m \in \mathbb{N}$. Se sigue del punto (c) de la proposición anterior, A tiene un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$ tal que e_iAe_i es local para todo $i \in \{1, ..., n\}$, de modo que si $1 = f_1 + ... + f_m$ es la descomposición canónica de la unidad de $\mathbb{M}_m(A)$, el conjunto $\{f_ie_jf_i\}_{i\in\{1,...,m\},j\in\{1,...,n\}}$ es un sistema completo de idempotentes ortogonales primitivos de $\mathbb{M}_m(A)$ tal que $f_ie_jf_iAf_ie_jf_i$ es local para todo i, j.

Ejemplo 8.15. Si A es el anillo generalizado de matrices

$$A = \begin{pmatrix} A_1 & M_{12} & \cdots & M_{1n} \\ M_{21} & A_2 & & \\ \vdots & & \ddots & \\ M_{n1} & & & A_n \end{pmatrix}$$

y $A_1, ..., A_n$ son anillos semiperfectos, entonces A es un anillo semiperfecto. La prueba es análoga al ejemplo anterior.

Ejemplo 8.16. Dado un módulo M. $\operatorname{End}_A(M)$ es semiperfecto si, y sólo si, existe una descomposición $M = M_1 \oplus ... \oplus M_n$ tal que $\operatorname{End}_A(M_i)$ es local. En efecto, por la proposición anterior $B = \operatorname{End}_A(M)$ es semiperfecto si, y sólo, si existe un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$ tal que e_iBe_i es local para todo $i \in \{1, ..., n\}$, y por la Proposición 2.17 dicho sistema existe si, y sólo si, $M = e_1M \oplus ... \oplus e_nM$ con $\operatorname{End}_A(e_iM) \cong e_iBe_i$ local.

Ejemplo 8.17. Todo anillo artiniano es semiperfecto. En efecto, todo anillo es artiniano es semilocal con radical nilpotente por la Proposición 5.50, lo que implica que los idempotentes se levantan por el Teorema 8.3.

Ejemplo 8.18. Si M es de longitud finita, entonces $B = \operatorname{End}_A(M)$ es semiperfecto. En efecto, por la Proposición 7.17 existe una descomposición en inescindibles

$$M = M_1 \oplus ... \oplus M_n$$

que induce una descomposición de la unidad $1_B = e_1 + ... + e_n$ tal que $e_iM = M_i$ para todo $i \in \{1, ..., n\}$. Además, M es de longitud finita, por lo que cada M_i es un submódulo inescindible de longitud finita, lo que implica que $e_iBe_i \cong \operatorname{End}_A(M_i)$ es local por el Corolario 7.14, y entonces B es semiperfecto por el punto (b) del teorema anterior.

Ejemplo 8.19. Si A es un anillo semiperfecto con un ideal bilateral $I \subseteq \operatorname{rad}(A)$, entonces $B = A/I$ es semiperfecto. Ciertamente, por el Corolario 5.23 $\operatorname{rad}(B) = \operatorname{rad}(A)/I$, de modo que

$$B/\operatorname{rad}(B) = (A/I)\,/\,(\operatorname{rad}(A)/I) \cong A/\operatorname{rad}(A),$$

lo que muestra que $B/\operatorname{rad}(B)$ es semisimple y que todo idempotente de $B/\operatorname{rad}(B)$ se levanta, ya que con el isomorfismo anterior se deduce que si

$$\alpha = (a + I) + \operatorname{rad}(A)/I \in B/\operatorname{rad}(B)$$

es un idempotente, entonces $a + I \in A/\operatorname{rad}(A)$ es un idempotente que se levanta a un idempotente $e \in A$, de tal manera que $e + I$ es un levantamiento de α.

8.3. Módulos sobre un anillo semiperfecto

Ya caracterizados los anillos semiperfectos se pueden exponer las propiedades básicas de los módulos sobre un anillo semiperfecto. Lo cual es una tarea sencilla una vez que se conocen algunas propiedades de los módulos sobre un anillo semilocal. Por lo que primero se presentarán algunos resultados sobre éstos.

Para empezar, la Proposición 5.52 se puede reformular de la siguiente manera.

Proposición 8.20. *Sea A un anillo semilocal y M es un módulo sobre A. Se cumplen los siguientes enunciados.*

(a) $rad(M) = Mrad(A)$.

(b) $rad(M) = 0$ *si, y sólo si,* M *es semisimple.*

(c) *Existe un número finito de clases de isomorfismo de módulos simples.*

Ahora, por la Proposición 5.54 los módulos simples de A son los módulos simples de $A/rad(A)$, y debido a que A es semilocal todo módulo simple de $A/rad(A)$ es isomorfo a alguno de los sumandos directos de $A/rad(A)$ por el Corolario 3.21.

De manera que si además A es semiperfecto, existe un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$ tal que

$$A/rad(A) = \bigoplus_{i=1}^{n}(e_i + rad(A))(A/rad(A))$$

es una descomposición en simples. Lo que implica que todo módulo simple sobre A y sobre $A/rad(A)$ es isomorfo a $(e_i + rad(A))(A/rad(A))$ para algún $i \in \{1, ..., n\}$. Más aún, la discusión anterior es válida para cualquier sistema completo de idempotentes ortogonales primitivos por la Proposición 8.12. Por lo tanto, se tiene el siguiente resultado.

Proposición 8.21. *Si A es semiperfecto y $\{e_1, ..., e_n\}$ es un sistema completo de idempotentes ortogonales primitivos, entonces el conjunto*

$$\{(e_i + rad(A))(A/rad(A)) \quad | \quad i \in \{1, ..., n\}\}$$

contiene un sistema completo de representantes de las clases de los módulos simples bajo la relación de isomorfismo.

A continuación se exponen algunas propiedades importantes de los módulos finitamente generados sobre un anillo semilocal. Antes de comenzar, el siguiente lema será de utilidad.

Lema 8.22. *Sea A un anillo y M un módulo finitamente generado sobre A. Se cumplen los siguientes enunciados.*

(a) *Todo sumando directo de M es finitamente generado.*

(b) *Si $M = M_1 \oplus ... \oplus M_n$, entonces $M/rad(M) \cong M_1/rad(M_1) \oplus ... \oplus M_n/rad(M_n)$.*

Demostración.

(a) Sea M finitamente generado y N un sumando directo de M, entonces N es isomorfo a un cociente de M, lo que implica que N es finitamente generado por la Proposición 1.33.

(b) Si $M = M_1 \oplus ... \oplus M_n$, entonces

$$M/rad(M) = \sum_{i=1}^{n}(M_i + rad(M))/rad(M)$$

y esta es una suma directa como se muestra a continuación. En efecto, si

$$m + rad(A) \in (M_k + rad(M))/rad(M)) \cap (\sum_{i=1, i\neq k}^{n} M_i + rad(M)/rad(M)),$$

entonces

$$m = m_k + r_1 = m' + r_2$$

donde $m_k \in M_k$, $r_1, r_2 \in rad(M)$ y $m' \in \sum_{i=1, i\neq k}^{n} M_i$, de manera que

$$m_k - m' = r_2 - r_1 \in rad(A),$$

lo que implica que $m_k \in rad(M)$ debido a que

$$rad(M) = \bigoplus_{i=1}^{n} rad(M_i),$$

y así $m + rad(M) = 0 + rad(M)$. En conclusión,

$$M/rad(M) = \bigoplus_{i=1}^{n} M_i + rad(M)/rad(M).$$

Pero por el segundo teorema de isomorfismo

$$(M_k + rad(M))/rad(M) \cong M_k/(rad(M) \cap M_k) = M_k/rad(M_k).$$

Por lo tanto, $M/rad(M) \cong \bigoplus_{i=1}^{n} M_i/rad(M_i)$.

□

Ya con esta proposición se pueden exponer propiedades importantes sobre los módulos finitamente generados sobre un anillo semilocal. La primera es que el cociente de un módulo finitamente generado con su radical es un módulo semisimple de longitud finita, lo que llevará a probar que todo módulo finitamente generado tenga una descomposición en inescindibles.

Así que supóngase que M es un A-módulo finitamente generado, donde A es un anillo semilocal. Es inmediato que

$$N = M/rad(M) = M/Mrad(A)$$

es un $A/rad(A)$-módulo finitamente generado, de manera que N es un A-módulo semisimple finitamente generado por la Proposición 1.9, y así N es un módulo semisimple de longitud finita por el Corolario 4.11.

Luego, considérese la familia F que consiste de los submódulos finitamente generados de M que no tienen descomposición en inescindibles. Si M no tiene descomposición en inescindibles, entonces F no es vacía, y por el principio del buen orden existe un elemento $N \in F$ tal que $N/rad(N)$ sea de longitud mínima. Luego, N no tiene descomposición en inescindibles, en particular N no es inescindible, lo que implica que $N = N_1 \oplus N_2$ con N_1 y N_2 submódulos propios de N finitamente generados por el lema anterior. Por otro lado, también por el lema anterior

$$N/rad(N) \cong (N_1/rad(N_1)) \oplus (N_2/rad(N_2)), \tag{8.1}$$

si alguno de estos sumandos fuera cero, supóngase $N_1/rad(N_1) = 0$, entonces por el lema de Nakayama $N_1 = 0$ lo cual es una contradicción. Por lo tanto, (8.1) es una descomposición no trivial, esto implica que $N_1/rad(N_1)$ y $N_2/rad(N_2)$ son de longitud estrictamente menor a $N/rad(N)$, y como esta longitud es mínima N_1 y N_2 no pertenecen a F. De modo que N_1 y N_2 tienen una descomposición en inescindibles, y así N también tiene una descomposición en inescindibles lo cual es una contradicción.

Por lo tanto, todo módulo finitamente generado sobre A tiene una descomposición en inescindibles.

Se probado la siguiente proposición.

Proposición 8.23. *Sea A un anillo semilocal y M un módulo finitamente generado sobre A. Se cumplen los siguientes enunciados.*

(a) *$M/rad(M)$ es semisimple de longitud finita.*

(b) *M se descompone como una suma directa de módulos inescindibles finitamente generados.*

La importancia de esta última proposición es clara, al ser todo módulo finitamente generado una suma directa finita de inescindibles, el estudio de la categoría de módulos finitamente generados sobre un anillo semilocal se restringe a conocer los módulos inescindibles finitamente generados. Sin embargo, cabe mencionar que tales descomposiciones en general no son únicas aún si el anillo es semiperfecto como muestra el siguiente ejemplo.

Ejemplo 8.24. Dado un campo k, sea $A = k[x,y]/\langle x^3 - x^2 + y^2\rangle$. Se observa que el conjunto $S = A\backslash(xA + yA)$ es cerrado bajo la multiplicación y no contiene al cero, por lo que se puede construir el anillo de fracciones $R = AS^{-1}$. El anillo R resulta ser local, ya que $I = xR+yR$ es un ideal maximal único. En efecto, si J es un ideal propio de R y se toma un elemento

$$\alpha = \frac{a}{b} \in J$$

entonces debido a que α no es invertible, ya que J es un ideal propio, $a \in xA + yA$, y así $\alpha \in xR + yR = I$. Por lo tanto, todo ideal está contenido en I lo que implica que I es el único ideal maximal. Más aún, por el criterio de Eisenstein el polinomio $x^3 - x^2 + y^2$ es irreducible, lo que implica que A es un dominio entero. Por lo tanto, R es un dominio entero semiperfecto tal que $rad(R) = I$, por ser local, que además es noetheriano ya que por el teorema de Hilbert $k[x, y]$ es noetheriano, lo que implica que A es noetheriano por el Ejemplo 4.27, y entonces R es noetheriano ya que todo anillo de fracciones de un anillo noetheriano es noetheriano por el Ejemplo 4.24.

Ahora, sea K el campo de fracciones de R y $T = R[z] \subseteq K$ donde $z = \frac{x}{y}$. En el anillo T se encuentran los ideales $M_1 = xT + yT + (z - 1)T$ y $M_2 = xT + yT + (z + 1)T$ que cumplen con que $M_1 + M_2 = T$, de manera que existe un isomorfismo de T-módulos $(M_1 \cap M_2) \oplus T \cong M_1 \oplus M_2$ debido a que existe una sucesión exacta

$$0 \to M_1 \cap M_2 \to M_1 \oplus M_2 \xrightarrow{f} T \to 0$$

donde $f(m, n) = m+n$ y T es proyectivo, lo que implica que la sucesión de escinde, por lo que se concluye que existe un isomorfismo de T-módulos $(M_1 \cap M_2)\oplus T \cong M_1 \oplus M_2$. Pero debido a que T es un R-módulo todo morfismo de T-módulos es un morfismo de R-módulos. De modo que existe un isomorfismo de R-módulos

$$(M_1 \cap M_2) \oplus T \cong M_1 \oplus M_2.$$

Por otro lado, es claro que T es un R-módulo generado por las potencias de z, pero debido a que

$$z^2 = \frac{x^2}{y^2} = \frac{x^2}{x^2 - x^3} = \frac{1}{1 - x} \in R$$

T es generado por el conjunto $\{1, z\}$. Así que como T es finitamente generado y R es noetheriano, todo submódulo de T es finitamente generado por la Proposición 4.25, en particular M_1, M_2 y $M_1 \cap M_2$ son finitamente generados.

Luego, para probar que M_1, M_2, T y $M_1 \cap M_2$ son R-módulos inescindibles se prueba a continuación que si M es un ideal de T que contiene a x y y, entonces $\mathrm{End}_R(M) \cong T$. Sea M un ideal que cumpla tal condición y $f \in \mathrm{End}_R(M)$. Si $f(x) = p(z)$ donde $p(z)$ es un elemento de T, se tiene que $f(x)y = f(xy) = f(y)x$, de manera que $p(z) = xp'(z)$ para algún $p'(z) \in T$ y así $f(y)x = p'(z)xy$, lo que implica que $f(y) = p'(z)y$. Luego, para todo $a_0 + a_1 z \in M$

$$f(a_0 + a_1 z)y = f(a_0 y + a_1 x) = f(a_0 y) + f(a_1 x) = (a_0 y + a_1 x)p'(z)$$

y así

$$f(a_0 + a_1 z)x = f(a_0 + a_1 z)yz = (a_0 y + a_1 x)p'(z)z = (a_0 x + a_1 xz)p'(z),$$

por lo que $f(\alpha) = (\alpha)p'(z)$ para todo $\alpha \in M$. De esta manera, todo endomorfismo $f \in \mathrm{End}_R(M)$ esta definido como $f(\alpha) = \alpha p_f(z)$ para algún $p_f(z) \in T$. De modo que si $\phi : \mathrm{End}_R(M) \to T$ es la función definida como $\phi(f) = p_f(z)$, es inmediato que ϕ es un isomorfismo de anillos. De modo que M es inescindible ya que debido a que T no tiene elementos idempotentes. En particular M_1, M_2, $M_1 \cap M_2$ y T son inescindibles.

Por otro lado, si se supone que existe un R-isomorfismo $f : T \to M_i$ para algún $i \in \{1, 2\}$, entonces con un procedimiento similar al usado en el párrafo anterior se llega a que f es un T-isomorfismo, lo cual es una contradicción ya que T es generado por un sólo elemento, mientras que M_i no puede ser generado por un sólo elemento. Por lo tanto, el módulo $(M_1 \cap M_2) \oplus T \cong M_1 \oplus M_2$ tiene dos descomposiciones distintas como suma directa de módulos inescindibles, lo que implica que M_1 ó M_2 y $M_1 \cap M_2$ ó T no son R-módulos de longitud finita.

Sin embargo si el anillo es semiperfecto y el módulo es proyectivo la descomposición es única como se muestra a continuación.

Sea A un anillo semiperfecto y $\{e_1, ..., e_n\}$ un sistema completo de idempotentes ortogonales primitivos. Si P es un módulo proyectivo inescindible finitamente generado, entonces P es sumando directo de A^m para algún $m \in \mathbb{N}$, pero A^m tiene una descomposición en inescindibles $A^m = (e_1 A \oplus ... \oplus e_n A)^m$, lo que implica por el teorema de Krull-Schmidt-Azumaya que $P \cong e_k A$ para algún $k \in \{1, ..., n\}$. Por lo que todo módulo proyectivo inescindible finitamente generado es isomorfo a uno de los sumandos inescindibles de A.

Mas aún, si P es un módulo proyectivo finitamente generado, entonces por la proposición anterior P tiene una descomposición de Krull-Schmidt, pero todo sumando de un módulo proyectivo es proyectivo, lo que implica que los sumandos de la descomposición en inescindibles de P son módulos proyectivos e inescindibles, lo que implica que $P \cong (e_1 A)^{m_1} \oplus ... \oplus (e_n A)^{m_n}$ para ciertos $m_1, ..., m_n \in \mathbb{N}$. Además, tal descomposición es única salvo isomorfismo por el teorema de Krull-Schmidt-Azumaya. Se tiene entonces la siguiente proposición.

Proposición 8.25. *Sea A un anillo semiperfecto y $\{e_1, ..., e_n\}$ un sistema completo de idempotentes orotogonales primitivos. Si P es un módulo inescindible proyectivo finitamente generado, entonces $P \cong e_k A$ para algún $k \in \{1, ..., n\}$. Si P es un módulo* *proyectivo finitamente generado, entonces* $P \cong (e_1A)^{m_1} \oplus ... \oplus (e_nA)^{m_n}$ *para ciertos* $m_1, ..., m_n \in \mathbb{N}$.

Como corolario, nótese que dado e un idempotente primitivo, eA es un proyectivo inescindible, esto implica que $eA \cong e_kA$ para algún $k \in \{1, ..., n\}$, y entonces eAe es local.

Corolario 8.26. *Si* A *es semiperfecto y* e *es un idempotente primitivo de* A*, entonces* eAe *es local.*

Ahora, si A es un anillo semiperfecto con un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$. Se ha probado que si M es finitamente generado, entonces M y $M/rad(M)$ tienen la misma cubierta proyectiva, y debido a que A es semilocal, $M/rad(M)$ es semisimple de longitud finita, lo que implica que existen $m_1, ..., m_n \in \mathbb{N}$ tales que

$$M/rad(M) \cong \bigoplus_{i=1}^{n} ((e_i + rad(A))(A/rad(A)))^{m_i}$$

ya que todo simple es isomorfo a $(e_i + rad(A))(A/rad(A))$ para algún $i \in \{1, ..., n\}$ por la Proposición 8.21. De manera que la cubierta proyectiva de $M/rad(M)$ es

$$\left(\bigoplus_{i=1}^{m_1} \pi_1\right) \oplus ... \oplus \left(\bigoplus_{i=1}^{m_n} \pi_n\right) : (e_1A)^{m_1} \oplus ... \oplus (e_nA)^{m_n} \to M/rad(M)$$

donde $\pi_i : e_iA \to e_iA/rad(A)$ es la proyección natural. Se ha probado el siguiente resultado.

Proposición 8.27. *Sea* A *un anillo semiperfecto con un sistema completo de idempotentes ortogonales primitivos. Si* M *es un* A*-módulo finitamente generado, entonces*

$$M/rad(M) \cong \bigoplus_{i=1}^{n} ((e_i + rad(A))(A/rad(A)))^{m_i}$$

para ciertos $m_1, ..., m_n \in \mathbb{N}$ *y la cubierta proyectiva de* M *es* $(e_1A)^{m_1} \oplus ... \oplus (e_nA)^{m_n}$.

Por último a continuación se prueba que todo módulo finitamente generado sobre un anillo semiperfecto es la suma directa de un módulo proyectivo y un módulo sin sumandos proyectivos.

Para ello es útil el invariante que se utilizó en la argumentación de la Proposición 8.23. Dado M un módulo finitamente generado se ha probado que $M/rad(M)$ es de longitud finita, a esta longitud se le denota $l(M/rad(M))$.

Ya se ha argumentado que si N es un sumando directo propio de M, entonces

$$l(N/rad(N)) < l(M/rad(M))$$

por el Lema 8.22 y el lema de Nakayama, por lo que se tiene el siguiente resultado.

Proposición 8.28. *Sea M un módulo finitamente generado. Si N es un sumando directo propio de M, entonces $l(N/rad(N)) < l(M/rad(M))$.*

Ahora, si M es un módulo finitamente generado no proyectivo, entonces es sencillo probar que $M = N \oplus P$ donde P es un módulo proyectivo y N es un módulo sin sumandos proyectivos. En efecto, si $l(M/rad(M)) = 1$ entonces $M/rad(M)$ es simple, lo que implica que M tiene un único submódulo maximal y entonces M es inescindible, por lo que se sigue lo afirmado. Luego, supóngase que se cumple la afirmación para todo módulo K con $l(K/rad(K)) \leq k$. Si $l(M/rad(M)) = k+1$ y M no tiene sumandos proyectivos se cumple la afirmación, si M tiene un sumando proyectivo P, entonces $M = M' \oplus P$ por lo que $l(M'/rad(M')) < l(M/rad(M))$, y entonces $M' = N \oplus Q$ donde Q es proyectivo y N es libre de sumandos proyectivos, y entonces $M = N \oplus P \oplus Q$ donde N no tiene sumandos proyectivos y $P \oplus Q$ es proyectivo.

Se ha probado la siguiente proposición inductivamente.

Proposición 8.29. *Si M es un módulo finitamente generado, entonces $M = N \oplus P$ donde P es un módulo proyectivo y N es un módulo sin sumandos proyectivos.*

Ejemplo 8.30. Dado un campo k y $n \in \mathbb{N}$, sea A el anillo de matrices generalizadas

$$A = \begin{pmatrix} k & 0 & 0 \\ 0 & k & 0 \\ k^n & k & k \end{pmatrix},$$

es inmediato del Ejemplo 5.44 que $rad(A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ k^n & k & 0 \end{pmatrix}$, y se consideran los idempotentes $e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ y $e_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Entonces,

$$A_A = e_1A \oplus e_2A \oplus e_3A = \begin{pmatrix} k & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ k^n & k & k \end{pmatrix}.$$

Es claro que e_1A y e_2A son simples. Mientras que para e_3A

$$rad(e_3A) = e_3Arad(A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ k^n & k & 0 \end{pmatrix} \text{ y } rad(rad(e_3A)) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

Por lo que se tienen los módulos semisimples

$$e_3A/rad(e_3A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & k \end{pmatrix} \text{ y } rad(e_3A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & k & 0 \end{pmatrix} \oplus \left(\bigoplus_{i=1}^{n} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ f_i & 0 & 0 \end{pmatrix} \right)$$

donde f_i es el vector con la i-ésima entrada igual a 1 y las demás igual a 0. Lo que implica por el Corolario 4.50 que e_3A es un módulo inecindible de longitud $n+2$.

Por otro lado,

$$_AA = Ae_1 \oplus Ae_2 \oplus Ae_3 = \begin{pmatrix} k & 0 & 0 \\ 0 & 0 & 0 \\ k^n & 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 & 0 \\ 0 & k & 0 \\ 0 & k & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & k \end{pmatrix}.$$

Siguiendo un procedimiento análogo al anterior, Ae_3 es simple, Ae_2 es de longitud 2 y Ae_3 es de longitud $n+1$.

Ejemplo 8.31. Dado un campo k, sea A el anillo de matrices triangulares inferiores de orden 2 sobre k y $M_A = \mathbb{M}_2(k)$. Es sencillo mostrar que la descomposición de M como suma directa de inescindibles es $M = M_1 \oplus M_2$ donde

$$M_1 = \begin{pmatrix} k & k \\ 0 & 0 \end{pmatrix} \text{ y } M_2 = \begin{pmatrix} 0 & 0 \\ k & k \end{pmatrix},$$

ya que M_2 es uno de los sumandos inescindibles proyectivos de A, y todo elemento

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M_1$$

con $b \neq 0$ genera todo M_1 lo que implica que M_1 es inescindible. De esta manera sencillo mostrar que

$$0 \subseteq rad(M_2) \subseteq M_2 \subseteq M_2 \oplus \begin{pmatrix} k & 0 \\ 0 & 0 \end{pmatrix} \subseteq M_2 \oplus M_1 = M$$

es una serie de composición de M, donde $\begin{pmatrix} k & 0 \\ 0 & 0 \end{pmatrix} = M_2 rad(A) = rad(M_2)$. Por lo tanto, M es un módulo de longitud finita que se descompone como suma de dos módulos inescindibles.

Para el siguiente ejemplo se recuerda lo siguiente. Si A es un anillo con una descomposición de la unidad $1 = e_1 + ... + e_n$, entonces A es una suma directa de grupos abelianos $\bigoplus_{i,j=1}^{n} e_iAe_j$ con una familia de morfismos

$$\{\psi_{ij}^k : e_iAe_k \otimes e_kAe_j \to e_iAe_j \quad | \quad i,j,k \in \{1,...,n\}\}$$

tal que $\psi^k_{it}(\psi^j_{ik} \otimes 1) = \psi^j_{it}(1 \otimes \psi^k_{jt})$ por el Teorema 2.29.

Análogamente, si $M = M_1 \oplus ... \oplus M_n$ es una suma directa de grupos abelianos tal que M_i es un e_iAe_i-módulo para toda $i \in \{1, ..., n\}$ y existe una familia de morfismos

$$\{\varphi_{ij} : M_j \otimes e_jAe_i \to M_i \quad | \quad i, j \in \{1, ..., n\}\}$$

tal que $\varphi_{ik}(1 \otimes \psi^j_{ik}) = \varphi_{jk}(\varphi_{ij} \otimes 1)$ donde $\psi^j_{ik}(e_ia \otimes be_k) = e_iae_jbe_k$, entonces M es un A-módulo derecho con el producto definido como

$$(m_1, ..., m_n)a = (\sum_{i=1}^n \varphi_{i1}(m_i \otimes e_iae_1), ..., \sum_{i=1}^n \varphi_{in}(m_i \otimes e_iae_n))$$

para todo $(m_1, ..., m_n) \in M$ y $a \in A$. Efectivamente, si se toman $m = (m_1, ..., m_n)$, $p = (p_1, ..., p_n) \in M$ y $a, b \in A$ se tiene que

$$\begin{aligned}
m(ab) &= (\sum_{i=1}^n \varphi_{i1}(m_i \otimes e_iabe_1), ..., \sum_{i=1}^n \varphi_{in}(m_i \otimes e_iabe_n)) \\
&= (\sum_{i=1}^n \sum_{j=1}^n \varphi_{j1}(m_j \otimes e_jae_ibe_1), ..., \sum_{i=1}^n \sum_{j=1}^n \varphi_{jn}(m_j \otimes e_jae_ibe_n) \\
&= (\sum_{i=1}^n \varphi_{i1}(\sum_{j=1}^n \varphi_{ji}(m_j \otimes e_jae_i) \otimes e_ibe_1), ..., \sum_{i=1}^n \varphi_{in}(\sum_{j=1}^n \varphi_{ji}(m_j \otimes e_jae_i) \otimes e_ibe_n)) \\
&= (\sum_{i=1}^n \varphi_{i1}(m_i \otimes e_iae_1), ..., \sum_{i=1}^n \varphi_{in}(m_i \otimes e_iae_n))b \\
&= (ma)b
\end{aligned}$$

$$\begin{aligned}
m1 &= (\sum_{i=1}^n \varphi_{i1}(m_i \otimes e_i1e_1), ..., \sum_{i=1}^n \varphi_{in}(m_i \otimes e_i1e_n)) \\
&= (\varphi_{i1}(m_i \otimes e_1), ..., \varphi_{in}(m_i \otimes e_n)) \\
&= (\varphi_{i1}(m_i \otimes 1_{e_1Ae_1}), ..., \varphi_{in}(m_i \otimes 1_{e_nAe_n})) \\
&= m
\end{aligned}$$

y ya que el producto tensorial es balanceado $m(a+b) = ma+mab$ y $(m+p)a = ma+pa$, lo que implica que M es un A-módulo derecho. De ahora en adelante si M es un grupo abeliano que cumple lo anterior, me referiré a él como el A-módulo $(M_1, ..., M_n)$ dado por la familia de morfismos $\{\varphi_{ij} \quad | \quad i, j \in \{1, ..., n\}\}$.

Ejemplo 8.32. Dado un campo k, si A es el álgebra de Kronecker, es decir, el anillo generalizado de matrices con producto trivial

$$A = \begin{pmatrix} k & 0 \\ k^2 & k \end{pmatrix},$$

y M el grupo aditivo $k^n \times k^n$ con la estructura de A-módulo dada por la familia de morfismos $\{\varphi_{ij} \quad | \quad i, j \in \{1, ..., n\}\}$, donde $\varphi_{11} : k^n \otimes k \to k^n$ y $\varphi_{22} : k^n \otimes k \to k^n$ son el morfismo inducido por el producto escalar, $\varphi_{21} : k^n \otimes 0 \to k^n$ es el morfismo nulo y $\varphi_{12} : k^n \otimes k^2 \to k^n$ es el morfismo inducido por la función bilinear

$$\phi(v, (a, b)) = av + bJ(v^t)$$

donde J es la matriz de $n \times n$

$$J = \begin{pmatrix} 0 & \cdots & 0 & 0 \\ 1 & 0 & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix},$$

entonces M es un módulo inescindible y $M/rad(M)$ es la suma directa de n módulos simples. En efecto, debido a que M es de dimensión finita, M es finitamente generado, lo que implica que

$$rad(M) = Mrad(A) = (k^n, k^n) \begin{pmatrix} 0 & 0 \\ k^2 & 0 \end{pmatrix} = ((0 \cdot k^n) + \mathrm{Im}(\varphi_{12}), 0 + (0 \cdot k^n)),$$

y claramente φ_{12} es suprayectiva, por lo que $rad(M) = (k^n, 0)$, de manera que $M/rad(M)$ es de dimensión n, así que que $M/rad(M)$ es la suma de n módulos simples. Además, M es inescindible ya que si $f \in \mathrm{End}_A(M)$, entonces $f(Me) = f(M)e \subseteq Me$ donde e es cualquiera de los idempotentes canónicos, esto implica que $f = f_1 \oplus f_2$ donde $f_1 : M_1 \to M_1$ y $f_2 : M_2 \to M_2$ son transformaciones lineales tales que

$$(f_1(v), 0) = f(v, 0) = f\left((0, v)\begin{pmatrix} 0 & 0 \\ (1, 0) & 0 \end{pmatrix}\right) = f(0, v)\begin{pmatrix} 0 & 0 \\ (1, 0) & 0 \end{pmatrix} = (f_2(v), 0)$$

$$(f_1(Jv^t), 0) = f(Jv^t, 0) = f\left((0, v)\begin{pmatrix} 0 & 0 \\ (0, 1) & 0 \end{pmatrix}\right) = f(0, v)\begin{pmatrix} 0 & 0 \\ (0, 1) & 0 \end{pmatrix} = (Jf_2(v)^t, 0)$$

para todo $v \in k^n$, lo que implica que $f_1 = f_2$ y $f_1 J = J f_2$, de manera que si la matriz asociada a $f_1 = f_2$ es $(a_{ij}) \in \mathbb{M}_n(k)$

$$\begin{pmatrix} 0 & \cdots & & 0 \\ a_{11} & a_{12} & & a_{1n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{(n-1)1} & \cdots & & a_{(n-1)n} \end{pmatrix} = J \begin{pmatrix} a_{11} & \cdots & & a_{1n} \\ a_{21} & a_{22} & & \\ \vdots & \ddots & \ddots & \vdots \\ a_{n1} & \cdots & & a_{nn} \end{pmatrix} = Jf_2 = f_1 J$$

$$f_1 J = Jf_2 = \begin{pmatrix} a_{11} & \cdots & & a_{1n} \\ a_{21} & a_{22} & & \\ \vdots & \ddots & \ddots & \vdots \\ a_{n1} & \cdots & & a_{nn} \end{pmatrix} J = \begin{pmatrix} a_{12} & \cdots & a_{1n} & 0 \\ a_{22} & a_{23} & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ a_{n2} & \cdots & a_{nn} & 0 \end{pmatrix}$$

y entonces la matriz asociada a $f_1 = f_2$ es triangular inferior con $a_{ii} = a_{jj}$ para todo $i, j \in \{1, ..., n\}$. Por lo tanto, $\operatorname{End}_A(M)$ se puede identificar con un subanillo de las matrices triangulares inferiores con diagonal constante, por lo que $\operatorname{End}_A(M)$ es local como se vió en el Ejemplo 7.13. Por lo tanto, M es inescindible. Cabe notar que este ejemplo muestra que A es un anillo con una infinidad de módulos inescindibles.

8.4. Anillos básicos y descomposiciones canónicas de la unidad

En lo que sigue, dado un anillo A se denota $A/\operatorname{rad}(A)$ como $\overline{A}$ y todo $x + \operatorname{rad}(A) \in \overline{A}$ como $\overline{x}$.

Definición 8.33. Sea A un anillo semiperfecto con una descomposición de la unidad $1 = e_1 + ... + e_n$. Se dice que A es un anillo básico si $e_iA \ncong e_jA$ para toda $i \neq j$.

Observación 8.34. Si A es un anillo básico se sigue de la Proposición 8.12 que para cualquier descomposición de la unidad $1 = f_1 + ... + f_m$ se tiene que $f_iA \ncong f_jA$ para toda $i \neq j$.

Se pueden caracterizar tales anillos de la siguiente manera.

Proposición 8.35. *Sea A un anillo semiperfecto con una descomposición de la unidad $1 = e_1 + ... + e_n$. Son equivalentes los siguientes enunciados.*

(a) *A es básico.*

(b) *$S = \{e_1A, ..., e_nA\}$ es un sistema completo de representantes de las clases de isomorfismo de los módulos proyectivos inescindibles.*

(c) *$T = \{\bar{e_1}\bar{A}, ..., \bar{e_n}\bar{A}\}$ es un sistema completo de representantes de las clases de isomorfismo de los módulos simples.*

(d) *$\bar{1} = \bar{e_1} + ... + \bar{e_n}$ es una descomposición central de la unidad de $\bar{A}$.*

(e) *$\bar{A}$ es un producto finito de anillos con división.*

Demostración.

$(a \Leftrightarrow b)$ Es inmediato de la definición y de la Proposición 8.25.

$(b \Leftrightarrow c)$ Se sigue de la Proposición 8.21 ya que $e_iA \ncong e_jA$ para toda $i \neq j$ si, y sólo si,$\bar{e_i}\bar{A} \ncong \bar{e_j}\bar{A}$ para toda $i \neq j$ por el Corolario 5.48.

$(c \Leftrightarrow d)$ Por el Corolario 5.48 T es un sistema completo de representantes si, y sólo si, $\bar{e_i}\bar{A} \ncong \bar{e_j}\bar{A}$ para toda $i \neq j$, y esto último se cumple si, y sólo si,

$$\bar{e_j}\bar{A}\bar{e_i} \cong \mathrm{Hom}_A(\bar{e_i}\bar{A}, \bar{e_j}\bar{A}) = 0$$

para toda $i \neq j$, lo que es equivalente a que $\bar{1} = \bar{e_1} + ... + \bar{e_n}$ es una descomposición central de la unidad de $\bar{A}$.

$(c \Leftrightarrow e)$ Es inmediato del teorema de Wedderburn-Artin ya que $\bar{A}$ es semisimple. $\square$

A todo anillo semiperfecto se le suele asociar un subanillo básico que se construye de la siguiente manera. Dado un anillo semiperfecto A con un sistema completo de idempotentes ortogonales primitivos $\{e_1, ..., e_n\}$, se toma $\{f_1, ..., f_k\} \subseteq \{e_1, ..., e_n\}$ tal que $\{f_1A, ..., f_kA\}$ sea un sistema completo de representantes de las clases de isomorfismo de los A-módulos proyectivos inescindibles. De manera que es sencillo probar que eAe es un subanillo básico de A donde $e = f_1 + ... + f_k$. En efecto, por el Ejemplo 8.13 eAe es semiperfecto, y por el Corolario 5.38

$$eAe/rad(eAe) \cong \bar{e}\bar{A}\bar{e} = \bigoplus_{i=1}^{k} \bar{f_i}\bar{A}\bar{f_i},$$

ya que, debido a que f_iA y f_jA son no isomorfos, $\bar{f_i}\bar{A}$ y $\bar{f_j}\bar{A}$ son módulos simples no isomorfos por el Corolario 5.48, y así $\bar{f_i}\bar{A}\bar{f_j} \cong \mathrm{Hom}_A(\bar{f_j}\bar{A}, \bar{f_i}\bar{A}) = 0$ para todo $i \neq j$. Además, $\bar{f_i}\bar{A}\bar{f_i} \cong \mathrm{Hom}_A(\bar{f_i}\bar{A}, \bar{f_i}\bar{A})$ es un anillo con división para todo $i \in \{1, ..., k\}$ por el lema de Schur. De modo que eAe es un anillo básico.

Cabe notar que el subanillo construido en el párrafo anterior es isomorfo al anillo de endomorfismos de la suma directa de los representantes de las clases de isomorfia de los módulos proyectivos inescindibles, lo que implica que no depende de la elección de los idempotentes en su construcción. Es por esto que tal anillo se suele llamar como el *subanillo básico* de A. Su importancia radica en que Mod_A es equivalente a Mod_{eAe} por el teorema de Morita, que se puede consultar en la Sección A.4 del Apéndice. De modo que en general al estudiar la categoría de módulos de un anillo semiperfecto se le puede considerar básico.

Ahora, si A es un anillo semiperfecto que no es básico, es útil construir una descomposición de la unidad de A que se comporte de manera similar a la descomposición de la unidad de un anillo básico. Para ello, dado un sistema completo de idempotentes ortogonales primitivos $S = \{e_1, ..., e_n\}$ se toma la partición $S = T_1 \cup ... \cup T_m$ inducida por la relación de equivalencia $e_i \sim e_j$ dada por $e_iA \cong e_jA$. De esta manera, si se toma $f_k = \sum_{i \in T_k} e_i$ para todo $k \in \{1, ..., m\}$ se tiene una descomposición de la unidad $1 = f_1 + ... + f_m$. Esta descomposición recibe el nombre de *descomposición canónica de la unidad* inducida por S.

Proposición 8.36. *Sea A un anillo semiperfecto con un sistema completo de idempotentes ortogonales primitivos $S = \{e_1, ..., e_n\}$ y $1 = f_1 + ... + f_m$ la descomposición canónica de la unidad inducida por S. Se cumplen los siguientes enunciados.*

(a) *$f_kA = P_k^{r_k}$ para todo $k \in \{1, ..., m\}$ donde P_k es un módulo proyectivo inescindible isomorfo a e_iA para todo $i \in T_k$ y r_k es la cardinalidad del conjunto T_k.*

(b) *$\{P_1, ..., P_m\}$ es un sistema completo de representantes de las clases de isomorfismo de los módulos proyectivos inescindibles.*

(c) *Si $S_i = P_i/\operatorname{rad}(P_i)$, entonces $\{S_1, ..., S_m\}$ es un sistema completo de representantes de las clases de isomorfismo de los módulos simples.*

(d) *Para todo $i \neq j$ se tiene que $\bar{f}_i\bar{A}\bar{f}_j = 0$.*

(e) *Para toda $k \in \{1, ..., m\}$ se tiene que $\bar{f}_k\bar{A} = \bar{A}\bar{f}_k = \bar{f}_k\bar{A}\bar{f}_k \cong \mathbb{M}_{r_k}(\operatorname{End}_A(S_k))$.*

(f) *Si $1 = g_1 + ... + g_t$ es una descomposición de la unidad tal que*

$$\bar{g}_k\bar{A} = \bar{A}\bar{g}_k \cong \mathbb{M}_{q_k}(D_k)$$

para algún anillo con división D_k y algún $q_k \in \mathbb{N}$, entonces $t = m$ y $1 = g_1 + ... + g_t$ es la descomposición canónica inducida por un sistema completo de idempotentes ortogonales primitivos.

Demostración.

(a) Por construcción $e_iA \cong e_jA$ para todo $i, j \in T_k$, lo que implica que

$$f_kA = \bigoplus_{i \in T_k} e_iA \cong P_k^{|T_k|}$$

donde $P_k = e_iA$ para algún $i \in T_k$.

(b) Por construcción $e_iA \ncong e_jA$ si $i \in T_k$ y $j \in T_t$ con $k \neq t$, entonces de la Proposición 8.25 se sigue que $\{P_1, ..., P_m\}$ es un sistema completo de representantes.

(c) Es inmediato del punto anterior y de la Proposición 8.21.

(d) Por los puntos (b) y (c) se concluye que $\bar{f}_k\bar{A} = S_k^{r_k}$ para todo $k \in \{1, ..., m\}$, entonces para todo $i \neq j$

$$\bar{f}_i\bar{A}\bar{f}_j \cong \mathrm{Hom}_A(\bar{f}_j\bar{A}, \bar{f}_i\bar{A}) \cong \bigoplus_{i\in T_i}\bigoplus_{i\in T_j}\mathrm{Hom}_A(S_j, S_i) = 0.$$

a) Por el punto anterior $\bar{1} = \bar{f}_1 + ... + \bar{f}_m$ es una descomposición central de la unidad, de modo que

$$\bar{f}_k\bar{A} = \bar{A}\bar{f}_k = \bar{f}_k\bar{A}\bar{f}_k \cong \mathrm{Hom}_A(\bar{f}_k\bar{A}, \bar{f}_k\bar{A}) \cong \mathbb{M}_{r_k}(\mathrm{End}_A(S_k)).$$

(e) Para todo $j \in \{1, ..., t\}$ se tiene que g_iA es un módulo proyectivo finitamente generado, lo que implica por la Proposición 8.25 que tiene una descomposición en inescindibles

$$g_iA = P_{i1} \oplus ... \oplus P_{im_i},$$

de manera que si $1 = \sum_{i=1}^{t}\sum_{j=1}^{m_i} e_{ij}$, donde $g_k = e_{k1} + ... + e_{km_k}$, es la descomposición de la unidad inducida por la descomposición

$$A = \bigoplus_{i=1}^{t}(P_{i1} \oplus ... \oplus P_{im_i}),$$

se tiene que $1 = g_1 + ... + g_t$ es la descomposición canónica de la unidad inducida por el sistema completo de idempotentes ortogonales primitivos

$$\{e_{ij} \quad | \quad i \in \{1, ..., t\}, j \in \{1, ..., m_i\}\}.$$

En efecto, debido a que $\bar{g_k}\bar{A} = \bar{A}\bar{g_k}$ para todo $k \in \{1, ..., t\}$, si $k \neq i$ se cumple que $\bar{e_{ij}}\bar{A}\bar{g_k} = \bar{g_k}\bar{e_{ij}}\bar{A} = 0$, lo que implica que $0 = \bar{e_{ij}}\bar{A}\bar{e_{kl}} = \mathrm{Hom}_A(\bar{e_{kl}}\bar{A}, \bar{e_{ij}}\bar{A})$, y así $\bar{e_{kl}}\bar{A} \ncong \bar{e_{ij}}\bar{A}$ y $e_{kl}A \ncong e_{ij}A$ para todo l, k. Además, debido a que

$$\bar{g_k}\bar{A} = \bar{A}\bar{g_k} \cong \mathbb{M}_{q_k}(D_k)$$

para todo $k \in \{1, ..., t\}$, $\bar{g_k}\bar{A}\bar{g_k} \cong \mathbb{M}_{q_k}(D_k)$ de modo que $\bar{e_{kl}}\bar{A} \cong \bar{e_{kj}}\bar{A}$ por el teorema de Wedderburn-Artin para todo l, j, y así $e_{kl}A \cong e_{kj}A$ para todo l, j. Por lo tanto, $1 = g_1 + ... + g_t$ es la descomposición canónica inducida por un sistema completo de idempotentes ortogonales primitivos, y entonces $t = m$ por el punto (b).

□

Observación 8.37. Los puntos (5) y (6) de la proposición anterior caracterizan a las descomposiciones canónicas de la unidad. Es sencillo deducir que si A es un anillo básico, entonces la suma de cualquier sistema completo de idempotentes ortogonales primitivos es una descomposición canónica.

La siguiente proposición muestra la fuerza de las descomposiciones canónicas.

Proposición 8.38. *Sea A un anillo semiperfecto y $1 = f_1 + ... + f_m$ la descomposición canónica de la unidad inducida por un sistema completo de idempotentes $\{e_1, ..., e_n\}$. Para todo $i \neq j$ se tiene que $f_iAf_j \subseteq \operatorname{rad}(A)$.*

Demostración. Sea $i \neq j$ con $i, j \in \{1, ..., m\}$. Por la proposición anterior

$$\bar{f}_i\bar{A}\bar{f}_j \cong \operatorname{Hom}_A(\bar{f}_j\bar{A}, \bar{f}_i\bar{A}) \cong \operatorname{Hom}_A(S_j^{r_j}, S_i^{r_i})$$

con S_i y S_j módulos simples no isomorfos, lo que implica que

$$\bar{f}_i\bar{A}\bar{f}_j = (f_iAf_j + \operatorname{rad}(A)) \,/\, \operatorname{rad}(A) = 0$$

y entonces $\bar{f}_i\bar{A}\bar{f}_j = 0$, lo que implica que $f_iAf_j \subseteq \operatorname{rad}(A)$. □

Como corolario se obtiene una manera de expresar el radical de un anillo semiperfecto usando la descomposición de Peirce del anillo.

Corolario 8.39. *Sea A un anillo semiperfecto y $1 = f_1 + ... + f_n$ una descomposición canónica de la unidad. Considerando la descomposición de Peirce del anillo inducida por $1 = f_1 + ... + f_n$*

$$\begin{pmatrix} f_1Af_1 & f_2Af_1 & \cdots & f_nAf_1 \\ f_1Af_2 & f_2Af_2 & & \\ \vdots & & \ddots & \\ f_1Af_n & & & f_nAf_n \end{pmatrix},$$

se tiene que

$$\operatorname{rad}(A) = \begin{pmatrix} \operatorname{rad}(f_1Af_1) & f_2Af_1 & \cdots & f_nAf_1 \\ f_1Af_2 & \operatorname{rad}(f_2Af_2) & & \\ \vdots & & \ddots & \\ f_1Af_n & & & \operatorname{rad}(f_nAf_n) \end{pmatrix}.$$

Demostración. Es inmediato de la proposición anterior y del Teorema 5.42. □

Lo cual lleva a un criterio para encontrar los sumandos simples de los módulos semisimples.

Proposición 8.40. *Sean A un anillo semiperfecto, $1 = f_1 + ... + f_n$ una descomposición canónica de la unidad y S un módulo simple tal que $\bar{f}_i\bar{A} \cong S^{r_i}$. Se cumplen los siguientes enunciados.*

(a) *$Sf_j = S$ si $i = j$ y $Sf_j = 0$ si $i \neq j$.*

(b) *Si M es un módulo semisimple, entonces M tiene un sumando isomorfo a S si, y sólo si, $Mf_i \neq 0$.*

Demostración.

(a) Por construcción S es isomorfo a un submódulo simple T de $\bar{f}_i\bar{A}$, entonces

$$Sf_i \cong Tf_i \subseteq \bar{f}_i\bar{A}\bar{f}_j = \delta_{ij}(\bar{f}_i\bar{A}\bar{f}_j)$$

por la Proposición 8.38.

(b) Es inmediato del punto anterior.

□

Corolario 8.41. *Sean A un anillo semiperfecto, $1 = f_1 + ... + f_n$ una descomposición canónica de la unidad y S un módulo simple tal que $\bar{f}_i\bar{A} \cong S^{r_i}$. Si M es un A-módulo de longitud finita, entonces M tiene factores de composición isomorfos a S si, y sólo si,$Mf_i \neq 0$.*

Demostración. Sea $0 = M_0 \subseteq ... \subseteq M_k = M$ una serie de composición de M. Por la proposición anterior M tiene factores de composición isomorfos a S si, y sólo si, $M_j/M_{j-1} \cong S$ para algún $j \in \{1, ..., k\}$ si, y sólo si, $M_jf_i/M_{j-1}f_i \neq 0$ para algún $i \in \{1, ..., k\}$ si, y sólo si, $Mf_i \neq 0$. □

Corolario 8.42. *Sean A un anillo semiperfecto, $\{e_1, ..., e_n\}$ un sistema completo de idempotentes ortogonales primitivos, $1 = f_1 + ... + f_n$ la descomposición canónica de la unidad inducida por $\{e_1, ..., e_n\}$ y S un A-módulo simple sumando de $\bar{f}_i\bar{A}$. El módulo S es un sumando directo de $e_k \operatorname{rad}(A)/e_k \operatorname{rad}(A)^2$ si, y sólo si, $e_k \operatorname{rad}(A)f_i \supsetneq e_k \operatorname{rad}(A)^2 f_i$.*

Demostración. Se sigue de la proposición anterior debido a que $e_k \operatorname{rad}(A)/e_k \operatorname{rad}(A)^2$ es un módulo semisimple. □

Corolario 8.43. *Si A es un anillo básico, $\{e_1, ..., e_n\}$ un sistema completo de idempotentes ortogonales primitivos, entonces $e_iA/\operatorname{rad}(e_iA)$ es sumando directo del módulo $e_k \operatorname{rad}(A)/e_k \operatorname{rad}(A)^2$ si, y sólo si,$e_k \operatorname{rad}(A)e_i \supsetneq e_k \operatorname{rad}(A)^2e_i$.*

Demostración. Inmediato del corolario anterior. □

Corolario 8.44. *Sean A un anillo semiperfecto con una descomposición canónica de la unidad $1 = f_1 + ... + f_n$ tal que $f_iA \cong P_i^{r_i}$ donde P_i es un módulo proyectivo inescindible para todo $i \in \{1, ..., n\}$. Si M es un A-módulo finitamente generado, entonces la cubierta proyectiva de M tiene sumandos directos isomorfos a P_i si, y sólo si, $Mf_i \neq 0$.*

Demostración. La cubierta proyectiva de M es isomorfa a la cubierta proyectiva de $M/\operatorname{rad}(M)$, de modo que la cubierta proyectiva de M tiene sumandos directos isomorfos a P_i si, y sólo si, $M/\operatorname{rad}(M)$ tiene sumandos directos isomorfos a $P_i/\operatorname{rad}(P_i)$ y por el Corolario 8.41 $M/\operatorname{rad}(M)$ tiene sumandos directos isomorfos a $P_i/\operatorname{rad}(P_i)$ si, y sólo si, $(M/\operatorname{rad}(M))\, f_i \neq 0$, y ésto último se cumple si, y sólo si, $Mf_i \neq 0$.

Ejemplo 8.45. Dado un campo k. Sean A es el álgebra de Kronecker, es decir, el anillo generalizado de matrices con producto trivial

$$A = \begin{pmatrix} k & 0 \\ k^2 & k \end{pmatrix},$$

y M el grupo aditivo $k^n \times k^n$. De manera similar al Ejemplo 8.32, dada una matriz arbitraria K de $n \times n$, se considera la estructura de M como A-módulo derecho dada por la operación $M \times A \to M$ definida como

$$(v, w) \begin{pmatrix} \lambda_1 & 0 \\ (a, b) & \lambda_2 \end{pmatrix} = (\lambda_1 v + aw + bKw^t, \lambda_2 w).$$

Siguiendo los pasos de Ejemplo 8.32. El módulo M es de dimensión finita, de manera que es finitamente generado como A-módulo. Así que

$$\operatorname{rad}(M) = M \operatorname{rad}(A) = k^n \times k^n \begin{pmatrix} 0 & 0 \\ k^2 & 0 \end{pmatrix} = k^n \times 0.$$

De modo que

$$M/\operatorname{rad}(M) = (k^n \times k^n) / (k^n \times 0),$$

y así

$$M/\operatorname{rad}(M) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 0 \text{ y}$$

$$M/\operatorname{rad}(M) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = M/\operatorname{rad}(M).$$

Esto muestra que si $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ y $e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, entonces

$$M/\operatorname{rad}(M) \cong \left(e_2\overline{A}\right)^n,$$

debido a que $\dim_k e_2\overline{A} = 1$, $\dim_k M/\operatorname{rad}(M) = n$ y a que $M/\operatorname{rad}(M)$ es una suma directa de copias de $e_2\overline{A}$ por la Proposición 8.40. Y así la cubierta proyectiva de M es $(e_2A)^n$ por la Proposición 8.27.

□

A. Nociones Básicas en Teoría de Categorías

A.1. Categorías y Funtores

Definición A.1. Una categoría C es una terna $(\mathrm{Ob}_C, \mathrm{Hom}_C, \circ)$, donde

- Ob_C es una clase cuyos elementos reciben el nombre de objetos de C.
- Hom_C es una clase que es igual a una unión disjunta

$$\mathrm{Hom}_C = \bigcup_{(M,N)\in \mathrm{Ob}_C \times \mathrm{Ob}_C} \mathrm{Hom}_C(M,N),$$

  donde $\mathrm{Hom}_C(M,N)$ es un conjunto cuyos elementos, denotados como

$$f : M \to N,$$

  reciben el nombre de morfismos de M a N para cada pareja (M,N).
- $\circ$ es una operación binaria parcial en Hom_C que recibe el nombre de composición, definida por la unión de una colección de funciones

$$\{\mathrm{Hom}_C(N,P) \times \mathrm{Hom}_C(M,N) \to \mathrm{Hom}_C(M,P) \quad | \quad (M,N,P) \in T\}$$

  donde T es la clase de ternas ordenadas de objetos de C. En la que se cumplen los siguientes axiomas:

(a) Para todo objeto M de C existe un morfismo $1_M \in \mathrm{Hom}_C(M,M)$ tal que

$$f \circ 1_M = f \;\text{ y }\; 1_M \circ g = g$$

para cualquier $f \in \mathrm{Hom}_C(M,N)$ y $g \in \mathrm{Hom}_C(N,M)$, dado cualquier objeto N.

(b) Para cualesquiera $f : M \to N$, $g : N \to P$ y $h : P \to Q$ se cumple que $h \circ (g \circ f) = (h \circ g) \circ f$.

De ahora en adelante se denota la composición de morfismos como $g \circ f = gf$.

Ejemplo A.2. *Set* denota a la categoría de conjuntos, cuyos objetos son todos los conjuntos y sus morfismos son las funciones entre conjuntos.

Ejemplo A.3. *Ab* denota a la categoría de grupos abelianos, cuyos objetos son los grupos abelianos y sus morfismos los morfismos de grupo.

Ejemplo A.4. *Ring* denota a la categoria de anillos, cuyos objetos son los anillos asociativos con uno y sus morfismos son los morfismos de anillo.

Ejemplo A.5. Dado un anillo A, Mod_A denota la categoría cuyos objetos son los módulos derechos sobre A y sus morfismos son los morfismos de A-módulos. De manera similar, mod_A es la categoría cuyos objetos son los A-módulos derechos finitamente generados y los morfismos son los morfismos de A-módulos. De la misma manera, ${}_AMod$ y ${}_Amod$ son las respectivas categorías de A-módulos por la izquierda.

Ejemplo A.6. Dadas dos categorías $C = (\mathrm{Ob}_C, \mathrm{Hom}_C, \bullet)$ y $C' = (\mathrm{Ob}_{C'}, \mathrm{Hom}_{C'}, \star)$ se define la categoría producto $B = C \times C'$ como la categoría $(\mathrm{Ob}_B, \mathrm{Hom}_B, \circ)$, donde

$$\mathrm{Ob}_B = \{(A, A') \quad | \quad A \in \mathrm{Ob}_C, A' \in \mathrm{Ob}_{C'}\},$$

$$\mathrm{Hom}_B = \{(f, f') : (A, B) \to (A', B') \quad | \quad f : A \to B \in \mathrm{Hom}_C, f' : A' \to B' \in \mathrm{Hom}_{C'}\}$$

y $(f, f') \circ (g, g') = (f \bullet g, f' \star g')$ para cualesquiera $f : M \to N, g : P \to N \in \mathrm{Hom}_C$ y $f' : M' \to N', g' : P' \to N' \in \mathrm{Hom}_{C'}$.

Ya definidas las categorías se define la importante noción de funtor.

Definición A.7. Un funtor covariante F de la categoría C a la categoría C', denotado como $F : C \to C'$, es una correspondencia que a cada objeto $A \in \mathrm{Ob}_C$ le asigna un objeto $F(A) \in \mathrm{Ob}_{C'}$, y que a cada morfismo $f : A \to B \in \mathrm{Hom}_C$ le asigna un morfismo

$$F(f) : F(A) \to F(B) \in \mathrm{Hom}_{C'},$$

de tal manera que se cumplan las siguientes condiciones:

(a) $F(1_A) = 1_{F(A)}$ para todo objeto $A \in \mathrm{Ob}_C$.

(b) $F(fg) = F(f)F(g)$ para cualesquiera morfismos $f : M \to N$, $g : P \to M$ en C.

Definición A.8. Un funtor contravariante F de la categoría C a la categoría C', denotado como $F : C \to C'$, es una correspondencia que a cada objeto $A \in \mathrm{Ob}_C$ le asigna un objeto $F(A) \in \mathrm{Ob}_{C'}$, y que a cada morfismo $f : A \to B \in \mathrm{Hom}_C$ le asigna un morfismo $F(f) : F(B) \to F(A) \in \mathrm{Hom}_{C'}$, de tal manera que se cumplan las siguientes condiciones:

(a) $F(1_A) = 1_{F(A)}$ para todo objeto $A \in \mathrm{Ob}_C$.

(b) $F(fg) = F(g)F(f)$ para cualesquiera morfismos $f : M \to N$, $g : P \to M$ en C.

Ejemplo A.9. $F : Ring \to Ab$ definido como $F(A) = A$ para todo $A \in \mathrm{Ob}_{Ring}$ y $F(f) = f$ para todo $f \in \mathrm{Hom}_{Ab}$ es un funtor.

Ejemplo A.10. Sean A un anillo y $B = \mathbb{M}_n(A)$. Si se define la correspondencia $F : Mod_A \to Mod_B$ como $F(M) = M^n$ y $F(f) = (f)^n$ para todo $M \in Mod_A$ y $f \in \mathrm{Hom}_{Mod_A}$, entonces F es un funtor covariante. En efecto, dado $M \in Mod_A$ se tiene que $F(M) = M^n$ es el producto cartesiano de m copias de M, es claro que M^n es un B-módulo ya que debido a que $M \in Mod_A$, por el Lema 1.3 que existe un morfismo de anillos $\phi : A \to \mathrm{End}(M)^{op}$, por lo que se puede definir un morfismo de anillos $\psi : \mathbb{M}_n(A) \to \mathbb{M}_n(\mathrm{End}(M)^{op})$ como $\psi(a_{ij}) = (f_{a_{ij}})$, y como $\mathbb{M}_n(R^{op}) \cong \mathbb{M}_n(R)^{op}$ bajo la función $f(a_{ij}) = (a_{ji})$ para todo anillo R, existe un morfismo de anillos

$$\mathbb{M}_n(A) \to \mathbb{M}_n(\mathrm{End}(M)^{op}) \cong \mathbb{M}_n(\mathrm{End}(M))^{op} \cong \mathrm{End}(M^n)$$

que induce la estructura de B-módulo de M^n. Luego, dado $f : M \to N$ un morfismo en Mod_A la función $(f)^n$ asigna $(f(m_1), ..., f(m_n))$ a cada $(m_1, ..., m_n) \in M^n$, por lo que claramente es un morfismo de B-módulos y claramente tal asignación cumple los puntos (a) y (b).

Ejemplo A.11. Dado un anillo A y un A-módulo M, la correspondencia

$$\mathrm{Hom}_A(M, \_) : Mod_A \to Ab$$

que asigna a cada $N \in Mod_A$ el grupo abeliano $\mathrm{Hom}_A(M, N)$ y a cada morfismo $f : N \to P \in Mod_A$ la función

$$f_* = \mathrm{Hom}_A(M, f) : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, P)$$

definida como $f_*(g) = fg$ es un funtor covariante. En efecto, es sencillo probar que $(1_N)_* = 1_{\mathrm{Hom}_A(M,N)}$ para todo $N \in Mod_A$ y que $(fg)_* = f_*g_*$, de modo que $\mathrm{Hom}_A(M, \_)$ es un funtor covariante. De la misma manera se prueba que $\mathrm{Hom}_A(\_, M)$ es un funtor contravariante. Cabe hacer notar que si además M es un S-A bimódulo, entonces por la Proposición 1.10 $\mathrm{Hom}_A(M, N)$ es un S-módulo derecho y $\mathrm{Hom}_A(N, M)$ es un S-módulo izquierdo para todo $N \in Mod_A$, de manera que los funtores los funtores $\mathrm{Hom}_A(M, \_)$ y $\mathrm{Hom}_A(\_, M)$ van de la categoría de A-módulos a la categoría de S-módulos.

$$\mathrm{Hom}_A(M, \_) : Mod_A \to Mod_S$$

$$\mathrm{Hom}_A(\_, M) : Mod_A \to_S Mod$$

Otro funtor importante que se utilizará mas adelante es el que se induce a partir del producto tensorial. Por esta razón a continuación se presenta la construcción de éste, junto con algunas propiedades.

A.2. Producto Tensorial

Definición A.12. Sean A un anillo, M un A-módulo derecho, N un A-módulo izquierdo y G un grupo abeliano aditivo. Se dice que una función $f : M \times N \to G$ es A-*balanceada* si cumple las siguientes condiciones

(a) $f(a + a', b) = f(a, b) + f(a', b)$,

(b) $f(a, b + b') = f(a, b) + f(a, b')$,

(c) $f(a\lambda, b) = f(a, \lambda b)$

para todo $a, a' \in M$, $b, b' \in N$ y $\lambda \in A$.

Definición A.13. Sean A un anillo, M un A-módulo derecho, N un A-módulo izquierdo. Se define el producto tensorial de M y N sobre A como un grupo abeliano $M \otimes N$ junto con una función A-balanceada $h : M \times N \to M \otimes N$, tales que cumplen la propiedad universal de que para cada función A-balanceada $f : M \times N \to G$ existe un único morfismo $\bar{f} : M \otimes N \to G$ tal que $\bar{f}h = f$.

Cabe resaltar que si hace falta señalar el anillo sobre el que se está trabajando, el producto tensorial se suele denotar como $M \otimes_A N$.

Tal objeto existe para todo $M \in Mod_A$ y $N \in {}_AMod$ ya que si F es el $\mathbb{Z}$-módulo libre con base $M \times N$, es decir

$$F = \{\sum_{i=1}^{n} a_i(m_i, n_i) \quad | \quad (m_i, n_i) \in M \times N, a_i \in \mathbb{Z}\, \forall i \in \{1, ..., n\}\},$$

y H es el subgrupo generado por los elementos

$$\begin{gathered} (m + m', n) - (m, n) - (m', n) \\ (m, n + n') - (m, n) - (m, n') \\ (ma, n) - (m, an) \end{gathered}$$

para todo $m, m' \in M$, $n, n' \in N$ y $a \in A$, entonces F/H junto con la proyección natural $h : M \times N \to F/H$ es el producto tensorial de M y N. En efecto, si se denota como $m \otimes n$ a todo $(m, n) + H \in F/H$, entonces

$$\begin{gathered} h(m + m', n) = (m + m') \otimes n = m \otimes n + m' \otimes n = h(m, n) + h(m', n), \\ h(m, n + n') = m \otimes (n + n') = m \otimes n + m \otimes n' = h(m, n) + h(m, n') \text{ y} \\ h(ma, n) = ma \otimes n = m \otimes an = h(m, an) \end{gathered}$$

para todo $m, m' \in M$, $n, n' \in N$ y $a \in A$, de modo que h es A-balanceada. Además, toda función A-balanceada $f : M \times N \to G$, induce un morfismo $f' : F \to G$ tal que

$f'(m,n) = f(m,n)$ para todo $(m,n) \in M \times N$. Asi que, debido a que f es A-balanceada, es claro que $H \subseteq \mathrm{Ker}(f')$, lo que implica que existe un morfismo $\bar{f} : F/H \to G$ tal que $\bar{f}(h(m,n)) = f(m,n)$ para todo $(m,n) \in M \times N$, el cual es único ya que esta definido en los generadores de F/H. Por lo tanto, el grupo F/H junto con el morfismo h es un producto tensorial.

De ahora en adelante se denotará al grupo F/H como $M \otimes N$, y sus generadores como $m \otimes n$ para todo $(m,n) \in M \times N$.

Ya probada su existencia, es sencillo probar que el producto tensorial es único salvo isomorfismo. Ciertamente, si un grupo P junto con una función A-balanceada

$$g : M \times N \to P$$

es un producto tensorial de M y N, entonces por la propiedad universal de producto tensorial existe un único morfismo $f_1 : P \to M \otimes N$ tal que $f_1 g = h$ y un único morfismo $f_2 : M \otimes N \to P$ tal que $f_2 h = g$. De manera que $f_2 f_1 g = g$ y $f_1 f_2 h = h$, pero por la propiedad universal del producto tensorial los únicos morfismos que cumplen ésto último son 1_P y $1_{M \otimes N}$, así que $1_P = f_2 f_1$ y $1_{M \otimes N} = f_1 f_2$. Por lo tanto, $P \cong M \otimes N$.

Se ha probado el siguiente resultado.

Proposición A.14. *Sea A un anillo. Para todo $M \in Mod_A$ y $N \in {}_AMod$ existe el producto tensorial $M \otimes N$ y es único salvo isomorfismo.*

Por otro lado, toda pareja de morfismos $f : M \to M' \in Mod_A$ y $g : N \to N' \in {}_AMod$ inducen un morfismo $f \otimes g : M \otimes N \to M' \otimes N'$ tal que $f \otimes g(m \otimes n) = f(m) \otimes g(n)$ para todo $m \otimes n \in M \otimes N$. En efecto, si se toma la función

$$\alpha : M \times N \to M' \times N'$$

definida como $\alpha(m,n) = (f(m), g(n))$ y

$$h : M' \times N' \to M' \otimes N'$$

es la función A-balanceada del producto tensorial $M' \otimes N'$, entonces la composición $h\alpha$ es una función A-balanceada, así que por la propiedad universal del producto tensorial existe un morfismo

$$\beta : M \otimes N \to M' \otimes N'$$

tal que $\beta(m \otimes n) = f(m) \otimes g(n)$ para todo $m \otimes n \in M \otimes N$, lo que prueba la existencia del morfismo $f \otimes g$.

Más aún, si se toman $f_1 : M \to M'$, $f_2 : M' \to K$ en Mod_A y $g_1 : N \to N'$, $g_2 : N' \to K'$ en ${}_AMod$

$$(f_2 \otimes g_2)(f_1 \otimes g_1)(m \otimes n) = (f_2 \otimes g_2)(f_1 m \otimes g_1 n) = (f_2 f_1 m \otimes g_2 g_1 n) = f_2 f_1 \otimes g_2 g_1 (m \otimes n)$$

para todo $m \otimes n \in M \otimes N$, de modo que $(f_2 \otimes g_2)(f_1 \otimes g_1) = f_2 f_1 \otimes g_2 g_1$.

Por lo tanto, si f y g son isomorfismos, $f \otimes g$ también es un isomorfismo, ya que

$$(f \otimes g)(f^{-1} \otimes g^{-1}) = ff^{-1} \otimes gg^{-1} = 1_{M'} \otimes 1_{N'} \text{ y}$$
$$(f^{-1} \otimes g^{-1})(f \otimes g) = f^{-1}f \otimes g^{-1}g = 1_M \otimes 1_N$$

donde claramente $1_{M'} \otimes 1_{N'}$ y $1_M \otimes 1_N$ son los endomorfismos identidad de $M' \otimes N'$ y $M \otimes N$.

Se han probado los siguientes resultados.

Proposición A.15. *Dado un un anillo A. Se consideran $f : M \to M'$, $f_1 : M \to M'$, $f_2 : M' \to K \in Mod_A$ y $g : N \to N', g_1 : N \to N', g_2 : N' \to K' \in {}_AMod$. Se cumplen los siguientes enunciados:*

(a) *Existe un morfismo $f \otimes g : M \otimes N \to M' \otimes N'$ tal que $f \otimes g(m \otimes n) = f(m) \otimes g(n)$ para todo $m \otimes n \in M \otimes N$.*

(b) $(f_2 \otimes g_2)(f_1 \otimes g_1) = f_2 f_1 \otimes g_2 g_1$.

(c) *Si f y g son isomorfismos, entonces $f \otimes g$ es isomorfismo.*

(d) $1_M \otimes 1_N = 1_{M \otimes N}$.

Ahora, es inmediato que para cada $M \in Mod_A$ se puede definir el funtor covariante $F = M \otimes \_ : {}_AMod \to Ab$ dado por $F(N) = M \otimes N$ para todo $N \in {}_AMod$ y $F(f) = 1_M \otimes f$ para todo morfismo f en ${}_AMod$. De manera similar se puede definir un funtor covariante $\_ \otimes N : Mod_A \to Ab$ para todo $N \in {}_AMod$.

Más aún, si M es un B-A bimódulo, entonces $M \otimes N$ es un B-módulo izquierdo para todo $N \in {}_AMod$. En efecto, si $\phi : B \to \mathrm{End}(M)$ es la representación asociada de ${}_BM$, entonces es inmediato de la proposición anterior que la función $\psi : B \to \mathrm{End}(M \otimes N)$ definida como $\psi(a) = \phi(a) \otimes 1_N$ es un morfismo de anillos, lo que induce la estructura de B-módulo por la izquierda de $M \otimes N$.

De esta manera si M es un B-A bimódulo, entonces el funtor $F = M \otimes \_$ va de la categoría ${}_AMod$ a la categoría Mod_A, ya que si $f : N \to N'$ es un morfismo en ${}_AMod$, entonces

$$1_M \otimes f(bm \otimes n) = bm \otimes f(n) = b(m \otimes f(n)) = b(1 \otimes f)(m \otimes n)$$

para todo $m \otimes n \in M \otimes N$ y $b \in B$, lo que implica que $F(f) = 1_M \otimes f$ es un morfismo en ${}_BMod$.

Por lo tanto, se ha probado la existencia de un funtor covariante

$$F = M \otimes \_ : {}_AMod \to {}_BMod$$

para todo B-A bimódulo M. Análogamente se prueba la existencia de un funtor covariante $\_ \otimes N : Mod_A \to Mod_B$ para todo A-B bimódulo N.

Proposición A.16. *Dado un B-A bimódulo M y un A-B bimódulo N, las asignaciones $M \otimes \_ : {}_AMod \to {}_BMod$ y $\_ \otimes N : Mod_A \to Mod_B$ son funtores covariantes.*

Por último se presenta la siguiente proposición que contiene otras propiedades básicas del producto tensorial.

Proposición A.17. *Sean N un B-A bimódulo derecho, M un C-B bimódulo y K un A-D bimódulo. Se cumplen los siguientes enunciados.*

(a) *Existe un isomorfismo de módulos $N \cong N \otimes A$.*

(b) *Existe un isomorfismo módulos $M \otimes (N \otimes K) \cong (M \otimes N) \otimes K$, a este módulo se le denota $M \otimes N \otimes K$.*

Demostración. Se puede consultar en [HGK05]. □

A.3. Equivalencia de Categorías

Una propiedad categórica es una noción que sólo depende de objetos y morfismos. Ejemplos de propiedades categóricas son los conceptos de monomorfismo, epimorfimo, isomorfismo, núcleo, conúcleo, sucesión exacta, producto, suma directa, proyectividad, inyectividad, etcétera. De modo que si se tiene un funtor $F : A \to B$, cabe preguntarse qué condiciones debe cumplir F para que preserve propiedades categóricas. En esta sección se estudian tales funtores.

Para ello se presentan las siguientes definiciones.

Definición A.18. Sean $F : A \to B$ y $G : A \to B$ funtores. Una transformación natural de F a G es una colección de morfismos $\eta = \{\eta_X : F(X) \to G(X)\}_{X \in A}$ tal que para todo morfismo $f : M \to N$ en A se cumple que $\eta_N F(f) = G(f)\eta_M$, es decir tal que conmuta el siguiente diagrama.

$$\begin{tikzcd} F(M) \arrow[r, "F(f)"] \arrow[d, "\eta_M"'] & F(N) \arrow[d, "\eta_N"] \\ G(M) \arrow[r, "G(f)"'] & G(N) \end{tikzcd}$$

Si $\eta = \{\eta_X : F(X) \to G(X)\}_{X \in A}$ es una transformación natural tal que η_X es un isomorfismo para toda $X \in A$, entonces se dice que η es un isomorfismo natural. En tal caso se dice que F y G son isomorfos y se denota $F \cong G$.

Ejemplo A.19. Para todo $M \in Mod_A$ existe un isomorfismo $\eta_M : M \to \mathrm{Hom}_A(A, M)$. La colección $\{\eta_M\}$ es un isomorfismo natural de 1_{Mod_A} en $\mathrm{Hom}_A(A, \_)$.

Ejemplo A.20. Para todo $M \in Mod_A$ existe un isomorfismo $\eta_M : M \to M \otimes A$. La colección $\{\eta_M\}$ es un isomorfismo natural de 1_{Mod_A} en $\_ \otimes M$.

Definición A.21. Si $F : A \to B$ y $G : B \to A$ son funtores tales que $FG \cong 1_B$ y $GF \cong 1_A$, entonces se dice que las categorías A y B son equivalentes, ó que existe una equivalencia de categorías dada por F y G.

Ejemplo A.22. Si A es un anillo tal que $A = A_1 \times A_2$, entonces Mod_A es equivalente a $Mod_{A_1} \times Mod_{A_2}$. En efecto, si $1_A = e_1 + e_2$ es la descomposición natural de la identidad, entonces se define $F : Mod_A \to Mod_{A_1} \times Mod_{A_2}$ como $F(M) = (Me_1, Me_2)$ para todo $M \in Mod_A$ y $F(f) = (f|_{Me_1}, f|_{Me_2})$ para todo morfismo $f : M \to N$. Por otro lado, identificando $A_1 = e_1Ae_1$ y $A_2 = e_2Ae_2$ se tiene por la Proposición 2.4 que todo $M \in Mod_{A_i}$ es un A-módulo derecho tal que $M(1 - e_i) = 0$ con $i \in \{1, 2\}$, entonces se puede definir $G : Mod_{A_1} \times Mod_{A_2} \to Mod_A$ como $G(M, M') = M \oplus M'$ y $G(f, f') = f \oplus f'$. Es sencillo probar que $GF \cong 1_{Mod_A}$ y $FG \cong 1_{Mod_{A_1} \times Mod_{A_2}}$.

Cabe observar que si $F : A \to B$ y $G : B \to A$ son funtores tales que $FG \cong 1_B$ y $GF \cong 1_A$, entonces es inmediato que para todo $X \in B$ existe $X' \in A$ tal que $F(X') \cong X$ y la función $F : \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_B(F(X), F(Y))$ es biyectiva, lo que implica que las equivalencias de categorías preservan las propiedades categóricas.

De la misma manera es inmediata la siguiente proposición.

Proposición A.23. *Sean A y B categorías tales que* $\mathrm{Hom}_A(X, Y)$ *y* $\mathrm{Hom}_B(X', Y')$ *son grupos abelianos aditivos para cualesquiera objetos $X, Y \in A$ y $X', Y' \in B$. Si existe una equivalencia de categorías dada por $F : A \to B$ y $G : B \to A$ se cumplen los siguientes enunciados.*

(a) *Existe un isomorfismo de anillos* $\mathrm{End}_A(M) \cong \mathrm{End}_B(F(A))$.

(b) *Existe un isomorfismo de* $\mathrm{End}_A(M)$*-módulos derechos*

$$\mathrm{Hom}_A(M, N) \cong \mathrm{Hom}_B(F(M), F(N))$$

.

A.4. Los teoremas de Morita

En esta sección se estudian los teoremas de Morita, los cuales caracterizan las equivalencias entre categorías de módulos.

Para empezar se contruye una equivalencia sencilla. Para ello se considera un anillo de matrices generalizadas

$$X = \begin{pmatrix} A & N \\ M & B \end{pmatrix} \text{ tal que } \begin{pmatrix} 0 & N \\ M & 0 \end{pmatrix}^2 = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \tag{A.1}$$

y los morfismos $\tau : N \otimes M \to A$ y $\tau' : M \otimes N \to B$ inducidos por el producto de X.

Por (A.1) existen $a_i, m_i \in M$ y $n_i, b_i \in N$ tales que

$$\begin{pmatrix} 1_A & 0 \\ 0 & 1_B \end{pmatrix} = \sum_{i=1}^{n} \begin{pmatrix} 0 & n_i \\ a_i & 0 \end{pmatrix} \begin{pmatrix} 0 & b_i \\ m_i & 0 \end{pmatrix},$$

esto muestra que

$$1_A = \sum_{i=1}^{n} \tau(n_i \otimes m_i) \text{ y } 1_B = \sum_{i=1}^{n} \tau'(a_i \otimes b_i). \tag{A.2}$$

Utilizando lo anterior es sencillo mostrar que τ y τ' son isomorfismos. Para probarlo se recuerda que $\tau(n \otimes m)x = n\tau'(m \otimes x)$ y $\tau'(m \otimes n)y = m\tau(n \otimes y)$ para todo $m, y \in M$ y $n, x \in N$ ya que

$$\begin{pmatrix} 0 & \tau(n \otimes m)x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ m & 0 \end{pmatrix} \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & n\tau'(m \otimes x) \\ 0 & 0 \end{pmatrix} \text{ y}$$

$$\begin{pmatrix} 0 & 0 \\ \tau'(m \otimes n)y & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ m & 0 \end{pmatrix} \begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ m\tau(n \otimes y) & 0 \end{pmatrix}.$$

Luego, de (A.1) se sigue que τ y τ' son morfismos suprayectivos, y si se toma

$$\alpha = \sum_{i=1}^{k} x_i \otimes y_i \in \operatorname{Ker}(\tau)$$

se cumple que

$$\begin{aligned} \alpha 1_A = \sum_{i=1}^{k} x_i \otimes y_i \sum_{j=1}^{n} \tau(n_j \otimes m_j) &= \sum_{i=1}^{k} \sum_{j=1}^{n} x_i \otimes y_i \tau(n_j \otimes m_j) \\ &= \sum_{i=1}^{k} \sum_{j=1}^{n} x_i \otimes \tau'(y_i \otimes n_j) m_j \\ &= \sum_{i=1}^{k} \sum_{j=1}^{n} x_i \tau'(y_i \otimes n_j) \otimes m_j \\ &= \sum_{i=1}^{k} \sum_{j=1}^{n} \tau(x_i \otimes y_i) n_j \otimes m_j = \tau(\alpha) \sum_{j=1}^{n} n_j \otimes m_j = 0 \end{aligned}$$

de manera que $\mathrm{Ker}(\tau) = 0$ y análogamente se prueba que $\mathrm{Ker}(\tau') = 0$. Por lo tanto, τ y τ' son isomorfismos.

La importancia de estos isomorfismos radica en que inducen la equivalencia natural buscada. En efecto, debido a que $\tau : N \otimes M \to A$ es un isomorfismo de A-módulos, para todo $K \in Mod_A$

$$K \otimes N \otimes M \cong K \otimes A \cong K,$$

de modo que si a tal isomorfismo se le denota $\eta_K : K \otimes N \otimes M \to K$, claramente definido en los generadores como $\eta_K(k \otimes n \otimes m) = k\tau(n \otimes m)$, la colección $\eta = \{\eta_K\}_{K \in Mod_A}$ es un isomorfismo natural entre la composición de funtores FG y el morfismo identidad 1_{Mod_A}, donde $G = (\_ \otimes N) : Mod_A \to Mod_B$ y $F = (\_ \otimes M) : Mod_B \to Mod_A$. En efecto, si $f : K \to K'$ es un morfismo de A-módulos, entonces para cada generador $\alpha = k \otimes n \otimes m \in K \otimes N \otimes M$,

$$f\eta_K(\alpha) = f(k\tau(n \otimes m)) = f(k)\tau(n \otimes m) = \eta_{K'}(f(k) \otimes n \otimes m) = \eta_{K'}(f \otimes 1_N \otimes 1_M)(\alpha),$$

lo que implica que el siguiente diagrama conmuta, de modo que η es un isomorfismo natural.

$$\begin{tikzcd} K \otimes N \otimes M \arrow[r, "f \otimes 1_N \otimes 1_M"] \arrow[d, "\eta_K"'] & K' \otimes N \otimes M \arrow[d, "\eta_{K'}"] \\ K \arrow[r, "f"'] & K' \end{tikzcd}$$

De esta manera, $FG \cong 1_{Mod_A}$ y análogamente se puede probar que $GF \cong 1_{Mod_B}$. Por lo tanto, se ha probado que Mod_A es equivalente a Mod_B.

Se tiene entonces el siguiente teorema.

Teorema A.24. *Si* $X = \begin{pmatrix} A & N \\ M & B \end{pmatrix}$ *es un anillo generalizado de matrices tal que* $\begin{pmatrix} 0 & N \\ M & 0 \end{pmatrix}^2 = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, *entonces se cumplen los siguientes enunciados.*

(a) *Los morfismos inducidos por el anillo generalizado de matrices* $\tau : N \otimes M \to A$ *y* $\tau' : M \otimes N \to B$ *son isomorfismos de módulos.*

(b) *Las categorías* Mod_A *y* Mod_B *son equivalentes bajo los funtores* $\_ \otimes N$ *y* $\_ \otimes M$.

Observación A.25. Es importante notar que la hipótesis sobre X en el teorema es equivalente a que τ y τ' sean suprayectivas.

De esta manera se ha cumplido el primer objetivo de esta sección. Sin embargo, el teorema no es de utilidad a menos que se pueda caracterizar un pareja de módulos N y M tal que se pueda construir el anillo X del teorema.

Con esta finalidad, se observa que para todo $x \in N$ se puede construir un morfismo de A-módulos derechos $f_x : M \to A$ definido como $f_x(m) = \tau(x \otimes m)$, y así existe una función $N \to \mathrm{Hom}_A(M, A)$ que a cada x le asigna un morfismo f_x. Tal función es un isomorfismo de B-A bimódulos, ya que para todo $x, x' \in N$, $b \in B$, $a \in A$ y $m \in M$,

$$\begin{aligned} f_{x+x'} = f_x + f_{x'} &\text{ ya que } f_{x+x'}(m) = \tau(x + x' \otimes m) = \tau(x \otimes m + x' \otimes m) = f_x + f_{x'}(m) \\ f_{bxa} = bf_x a &\text{ ya que } f_{bxa}(m) = \tau(bxa \otimes m) = b\tau(x \otimes am) = bf_x(am) = bf_x a(m), \end{aligned}$$

y si existe $x \in N$ tal que $f_x = 0$, entonces por (A.2)

$$x = x1_B = \sum_{i=1}^{n} x\tau'(a_i \otimes b_i) = \sum_{i=1}^{n} \tau(x \otimes a_i)b_i = \sum_{i=1}^{n} f_x(a_i)b_i = 0,$$

lo que implica que dicha función es inyectiva, y para probar que es suprayectiva se observa que para todo $f \in \mathrm{Hom}_A(M, A)$ y para todo $m \in M$ se tiene que $f(m)$ es igual a

$$f(1_B m) = f\sum_{i=1}^{n} \tau'(a_i \otimes b_i)m = f\sum_{i=1}^{n} a_i\tau(b_i \otimes m) = \sum_{i=1}^{n} f(a_i)\tau(b_i \otimes m) = \tau(\sum_{i=1}^{n} f(a_i)b_i \otimes m),$$

de manera que f es igual a f_y donde $y = \sum_{i=1}^{n} f(a_i)b_i$. Por lo tanto, se ha probado la existencia de un isomorfismo $N \cong \mathrm{Hom}_A(M, A)$ y más aún, tal isomorfismo está inducido por el morfismo τ, el cual a su vez está inducido por el producto del anillo, lo cual será de importancia más adelante.

De la misma manera, se observa que para todo $b \in B$ se puede construir un morfismo $g_b \in \mathrm{End}_A(M)$ definido como $g_b(m) = bm$ para todo $m \in M$, por lo que existe una función $B \to \mathrm{End}_A(M)$ que a cada $b \in B$ le asigna un morfismo g_b. Tal función es un isomorfismo de anillos ya que para todo $b, b' \in B$

$$\begin{aligned} g_{b+b'} = g_b + g_{b'} &\text{ ya que } g_{b+b'}(m) = bm + b'm = g_b + g_{b'}(m) \text{ para todo } m \in M \\ g_{bb'} = g_b g_{b'} &\text{ ya que } g_{bb'}(m) = bb'm = bg_{b'}(m) = g_b g_{b'}(m) \text{ para todo } m \in M \\ g_{1_B} = 1_B &\text{ ya que } g_{1_B}(m) = 1_B m = m \text{ para todo } m \in M \end{aligned}$$

y si existe $b \in B$ tal que $g_b = 0$, entonces por (A.2)

$$b = b1_B = \sum_{i=1}^{n} b\tau'(a_i \otimes b_i) = \sum_{i=1}^{n} \tau'(ba_i \otimes b_i) = \sum_{i=1}^{n} \tau'(g_b(a_i) \otimes b_i) = 0,$$

por lo que dicha función es inyectiva, y para probar que es suprayectiva basta observar que para todo $g \in \mathrm{End}_A(M)$ y para todo $m \in M$ se cumple que $g(m)$ es igual a

$$g(1_B m) = g\sum_{i=1}^{n} \tau'(a_i \otimes b_i)m = g\sum_{i=1}^{n} a_i\tau(b_i \otimes m) = \sum_{i=1}^{n} g(a_i)\tau(b_i \otimes m) = \sum_{i=1}^{n} \tau'(g(a_i) \otimes b_i)m$$

de manera que g es igual a g_y donde $y = \sum_{i=1}^{n} \tau'(g(a_i) \otimes b_i)$. Por lo tanto, se ha probado la existencia de un isomorfismo $B \cong \mathrm{End}_A(M)$ y más aún, una vez más tal isomorfismo está inducido por el producto del anillo X, por lo que existe un isomorfismo de anillos

$$X = \begin{pmatrix} A & N \\ M & B \end{pmatrix} \cong \begin{pmatrix} A & \mathrm{Hom}_A(M, A) \\ M & \mathrm{End}_A(M) \end{pmatrix} = Y,$$

definido como $\phi\begin{pmatrix} a & n \\ m & b \end{pmatrix} = \begin{pmatrix} a & f_n \\ m & g_b \end{pmatrix}$, donde Y es el anillo generalizado de matrices con el producto usual

$$\begin{pmatrix} a & f_n \\ m & g_b \end{pmatrix}\begin{pmatrix} a' & f_{n'} \\ m' & g_{b'} \end{pmatrix} = \begin{pmatrix} aa' + f_n(m') & af_{n'} + f_n g_{b'} \\ ma' + g_b(m') & mf_{n'} + g_b g_{b'} \end{pmatrix},$$

donde $mf_{n'} = f_{\tau'(m \otimes n')}$, ya que para todo $x \in M$

$$mf_{n'}(x) = m\tau(n' \otimes x) = \tau'(m \otimes n')x = f_{\tau'(m \otimes n')}(x).$$

Se ha probado el siguiente teorema.

Teorema A.26. *Si* $X = \begin{pmatrix} A & N \\ M & B \end{pmatrix}$ *es un anillo generalizado de matrices tal que* $\begin{pmatrix} 0 & N \\ M & 0 \end{pmatrix}^2 = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, *entonces se cumplen los siguientes enunciados.*

(a) *Existe un isomorfismo de anillos* $B \cong \mathrm{End}_A(M)$.

(b) *Existe un isomorfismo de A-B bimódulos* $N \cong \mathrm{Hom}_A(M, A)$.

(c) *Existe un isomorfismo de anillos $X \cong Y$, donde X y Y son los anillos antes mencionados.*

Ya probado que $X \cong Y$, se puede utilizar el producto de Y para caracterizar al módulo M, con este fin de ahora en adelante se hace la identificación $B = \mathrm{End}_A(M)$ y $N = \mathrm{Hom}_A(M, A)$.

Ahora, como ya se ha mencionado, la condición

$$\begin{pmatrix} 0 & N \\ M & 0 \end{pmatrix}^2 = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

es equivalente a que los morfismos $\tau : N \otimes M \to A$ y $\tau' : M \otimes N \to B$ definidos en los generadores como $\tau(f \otimes m) = f(m)$ y $\tau'(m \otimes f)(x) = mf(x)$ sean suprayectivos. Por lo que se busca caracterizar un módulo M que cumpla esta condición.

De la definición es inmediato que τ es suprayectivo si, y sólo si, $A = \sum_{f\in N} f(M)$. Los módulos que cumplen esta condición se reciben el nombre de *generadores* y se caracterizan en el siguiente lema.

Lema A.27. *Sea M un A-módulo derecho. Son equivalentes los siguientes enunciados.*

(a) *Si $H = \mathrm{Hom}_A(M, A)$, entonces $A = \sum_{f\in H} f(M)$.*

(b) *Existe un epimorfismo de A-módulos $M^n \to A$ para algún $n \in \mathbb{N}$.*

(c) *Para todo A-módulo derecho K existe un epimorfismo $M^{(I)} \to K$ para algún conjunto I.*

(d) *Para cualesquier morfismo no nulo $f : K \to S$ existe un morfismo $h : M \to K$ tal que $fh \neq 0$.*

Demostración.

($a \Rightarrow b$) Si $A = \sum_{f\in H} f(M)$, entonces $1_A = f_1m_1 + ... + f_nm_n$ para ciertos $f_1, ..., f_n \in H$ y $m_1, ..., m_n \in M$. Luego, si se define $g : M^n \to A$ como

$$g(x_1, ..., x_n) = f_1(x_1) + ... + f_n(x_n),$$

se cumple que $a = g(m_1a, ..., m_na)$ para todo $a \in A$, por lo que g es el epimorfismo deseado.

($b \Rightarrow c$) Si K es un A-módulo derecho, entonces el morfismo $h : A^{(K)} \to K$ definido como

$$h(\sum_{k\in K} a_k) = \sum_{k\in K} ka_k$$

es un epimorfismo, lo que implica que la composición hg' es el epimorfismo buscado, donde $g' : (M^n)^{(K)} \to A$ es el morfismo definido como $g'(\sum_{k\in K} x_k) = \sum_{k\in K} g(x_k)$, donde g es el morfismo del punto (b).

($c \Rightarrow a$) Por (c) existe un epimorfismo $f : M^{(I)} \to A$ para algún conjunto I, de manera que si $f = \bigoplus_{i\in I} f_i$ donde $f_i : M \to M$, se cumple que $A = \sum_{i\in I} f_i(M)$, y así $A = \sum_{f\in H} f(M)$.

($c \Rightarrow d$) Si se toma $f \in \mathrm{Hom}_A(K, S)$ de tal manera que $f \neq 0$, existe $x \in K$ tal que $f(x) \neq 0$, y por (c) existe un epimorfismo $g : M^{(I)} \to K$ para algún conjunto I. Ahora, existe $m = \sum_{i\in J} m_i \in M^{(I)}$ tal que $g(m) = x$, donde J es un subconjunto finito de I tal que $m_i \neq 0$ para todo $i \in J$. Luego, debido a que $f(x) \neq 0$,

$$0 \neq fg(m) = fg(\sum_{i\in J} m_i) = \sum_{i\in J} fg(m_i),$$

por lo que que $fg(m_j) \neq 0$ para algún $j \in J$, y entonces $fg\iota \neq 0$ donde $\iota : M \to M^{(I)}$ es la j-ésima inclusión natural. Por lo tanto, $g\iota$ es el morfismo buscado.

($d \Rightarrow a$) Sea $K = \sum_{f \in H} f(M)$. Si se supone $K \neq A$, entonces la proyección natural $\pi : A \to A/K$ no es nula, entonces por (d) existe un morfismo no nulo $h : M \to A$ tal que $\pi h \neq 0$, y así $h(A) \nsubseteq K$ lo cual es una contradicción. Por lo tanto, $A = K$. $\square$

Observación A.28. El punto (d) del lema anterior está enunciado puramente con morfismos. Por lo que la propiedad de ser generador es una propiedad categórica.

Por lo tanto, el módulo M debe ser un generador que además cumpla la condición de que $\tau' : M \otimes N \to B$ sea suprayectiva, y τ' es suprayectiva si, y sólo si, M es un módulo proyectivo finitamente generado. En efecto, si τ' es suprayectiva es claro que existen $m_1, ..., m_n \in M$ y $f_1, ..., f_n \in \mathrm{Hom}_A(M, A)$ tales que

$$1_M = \tau'(\sum_{i=1}^{n} m_i \otimes f_i) = \sum_{i=1}^{n} \tau'(m_i \otimes f_i) = \sum_{i=1}^{n} m_i f_i,$$

entonces para todo $m \in M$

$$m = 1_M m = \sum_{i=1}^{n} m_i f_i(m),$$

así que $m_1, ..., m_n$ generan a M. De esta manera el morfismo $h : A^n \to M$ definido como $h(x_1, ..., x_n) = \sum_{i=1}^{n} m_i x_i$ es un epimorfismo, y se puede definir un morfismo $g : M \to A^n$ como $g(m) = (f_1(m), ..., f_n(m))$ el cual es un inverso derecho de h ya que

$$hg(m) = h(f_1(m), ..., f_n(m)) = \sum_{i=1}^{n} m_i f_i(m) = 1_M(m),$$

de modo que M es un sumando directo de A^n y como tal es un módulo proyectivo finitamente generado.

Recíprocamente, si M es un módulo proyectivo finitamente generado, entonces al ser finitamente generado existe un epimorfismo $h : A^n \to M$ para algún $n \in \mathbb{N}$, y por ser proyectivo h tiene un inverso por la derecha $g : M \to A^n$. En consecuencia, si $f_i = \pi_i g$ donde $\pi_i : A^n \to A$ es la proyección natural de la i-ésima entrada para todo $i \in \{1, ..., n\}$,

$$1_M(m) = hg(m) = h(f_1(m), ..., f_n(m)) = \sum_{i=1}^{n} m_i f_i(m),$$

donde $m_i = h(e_i)$ y e_i es el elemento cuyas entradas son todas 0 con excepción de la i-ésima, la cual es igual a 1. De modo que τ' es suprayectiva, ya que para todo

$g \in \mathrm{End}_A(M)$

$$g(x) = g(\sum_{i=1}^{n} m_i f_i(x)) = \sum_{i=1}^{n} g(m_i) f_i(x) = \sum_{i=1}^{n} \tau'(g(m_i) \otimes f_i)(x) \in \mathrm{Im}(\tau').$$

Se ha probado que τ' es suprayectivo si, y sólo si, M es un módulo proyectivo finitamente generado. Más aún, en la demostración esta implícito que M es un módulo proyectivo finitamente generado si, y sólo si, existen $m_1, ..., m_n \in M$ y $f_1, ..., f_n \in \mathrm{Hom}_A(M, A)$ tales que $1_M = \tau'(\sum_{i=1}^{n} m_i \otimes f_i) = \sum_{i=1}^{n} \tau'(m_i \otimes f_i) = \sum_{i=1}^{n} m_i f_i$.

Lema A.29. *Sea M un A-módulo derecho y $N = \mathrm{Hom}_A(M, A)$. M es un módulo proyectivo finitamente generado si, y sólo si, existen $m_1, ..., m_n \in M$ y $f_1, ..., f_n \in N$ tales que $1_M = \sum_{i=1}^{n} m_i f_i$.*

Por lo tanto, los morfismos τ y τ' son suprayectivos si, y sólo si, M es un generador proyectivo finitamente generado, un módulo que cumpla esto se recibe el nombre de *progenerador*.

Observación A.30. Se ha mostrado que las propiedades de ser generador, proyectivo ó finitamente generado son propiedades categóricas. Por lo que la propiedad de ser progenerador es también una propiedad categórica.

Se ha probado el siguiente teorema.

Teorema A.31. *El anillo generalizado de matrices $\begin{pmatrix} A & N \\ M & B \end{pmatrix}$ cumple la condición de que $\begin{pmatrix} 0 & N \\ M & 0 \end{pmatrix}^2 = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ si, y sólo si, M es un progenerador.*

Ya caracterizado el módulo M se han caracterizado todas las equivalencias entre categorías de módulos, ya que como se verá a continuación, toda equivalencia entre categorías de módulos sobre distintos anillos es naturalmente equivalente a una equivalencia dada por los funtores $\_ \otimes M : Mod_B \to Mod_A$ y $\_ \otimes N : Mod_A \to Mod_B$, donde M es un A-módulo derecho progenerador, $N = \mathrm{Hom}_A(M, A)$ y $B \cong \mathrm{End}_A(M)$.

Antes de probar la afirmación anterior se considera la siguiente proposición que contiene una propiedad útil que cumplen los módulos proyectivos finitamente generados.

Proposición A.32. *Sean M un A-módulo derecho y $B = \mathrm{End}_A(M)$. Si M es un módulo proyectivo finitamente generado y $N = \mathrm{Hom}_A(M, A)$, entonces para todo A-módulo derecho K existe un isomorfismo de B-módulos derechos*

$$\phi_K : K \otimes N \to \mathrm{Hom}_A(M, K).$$

Más aún, $\phi = \{\phi_K\}_{K \in Mod_B}$ es un isomorfismo natural entre $\_ \otimes N$ y $\mathrm{Hom}_A(M, \_)$.

Demostración. Para definir ϕ_K se considera la función $f : K \times N \to \mathrm{Hom}_A(M, K)$ que a cada pareja $(k, g) \in K \times N$ le asigna el morfismo $kg \in \mathrm{Hom}_A(M, K)$ definido como $kg(x) = k(g(x))$. Es sencillo mostrar que f es A-balanceada, de modo que induce el morfismo de grupos abelianos $f' : K \otimes N \to \mathrm{Hom}_A(M, K)$ definido en los generadores como $f'(k \otimes g) = kg$, el cual es además morfismo de B-módulos derechos ya que

$$f'(k \otimes gb)(x) = k(gb)(x) = (kg)b(x)$$

para todo $x \in M$ y para todo generador $k \otimes g \in K \otimes N$ y $b \in B$. De esta manera se define $\phi_K = f'$. Por otro lado, debido a que M es un módulo proyectivo finitamente generado por el Lema A.29 existen $m_1, ..., m_n \in M$ y $f_1, ..., f_n \in N$ tales que $1_M = \sum_{i=1}^n m_i f_i$, entonces para todo $f \in \mathrm{Hom}_A(M, K)$ se cumple que

$$f = f1_M = f\sum_{i=1}^{n} m_i f_i = \sum_{i=1}^{n} f(m_i)f_i,$$

con lo que se define el morfismo de B-módulos derechos $\psi : \mathrm{Hom}_A(M, K) \to K \otimes N$ como

$$\psi(f) = \psi(\sum_{i=1}^{n} f(m_i)f_i) = \sum_{i=1}^{n} f(m_i) \otimes f_i$$

para todo $f \in \mathrm{Hom}_A(M, K)$. Luego, para todo $f \in \mathrm{Hom}_A(M, K)$

$$\phi_K\psi(f) = \phi_K(\sum_{i=1}^{n} f(m_i) \otimes f_i) = \sum_{i=1}^{n} \phi_K(f(m_i) \otimes f_i) = \sum_{i=1}^{n} f(m_i)f_i = f,$$

por lo que $\phi_K\psi = 1_{\mathrm{Hom}_A(M,K)}$, y para todo generador $k \otimes g \in K \otimes N$

$$\psi\phi_K(k \otimes g) = \psi(kg) = \sum_{i=1}^{n} kg(m_i) \otimes f_i = \sum_{i=1}^{n} k \otimes g(m_i)f_i = k \otimes g\sum_{i=1}^{n} f(m_i)f_i = k \otimes g$$

así que $\psi\phi_K = 1_{K\otimes N}$. En consecuencia, $\phi_K : K \otimes N \to \mathrm{Hom}_A(M, K)$ es un isomorfismo de B-módulos derechos. Ahora, la colección $\phi = \{\phi_K\}_{K\in Mod_B}$ es un isomorfismo natural debido a que para todo $f \in \mathrm{Hom}_B(K, K')$ se tiene que $\phi_{K'} f \otimes 1_N = \mathrm{Hom}_A(M, f)\phi_K$ ya que para todo generador $k \otimes n \in K \otimes N$

$$\phi_{K'}(f \otimes 1_N)(k \otimes g) = \phi_{K'}(f(k) \otimes g) = f(k)g = f^*(kg) = f^*\phi_K(k \otimes g),$$

donde $f^* = \mathrm{Hom}_A(M, f)$. $\square$

Ahora, si se supone que $F : Mod_A \to Mod_B$ y $G : Mod_B \to Mod_A$ son funtores tales que $FG \cong 1_{Mod_B}$ y $GF \cong 1_{Mod_A}$, y se toman $M_A = G(B)$ y $N_B = F(A)$, entonces por la Proposición A.23

$$\mathrm{End}_A(M) = \mathrm{End}_A(G(B)) \cong \mathrm{End}_B(B) = B \text{ y}$$
$$\mathrm{End}_B(N) = \mathrm{End}_B(F(A)) \cong \mathrm{End}_A(A) = A,$$

lo que implica que M es un B-A bimódulo y N un A-B bimódulo. Más aún, por la Proposición A.23

$$N \cong \mathrm{Hom}_B(B,N) \cong \mathrm{Hom}_B(FG(B),F(A)) \cong \mathrm{Hom}_A(G(B),A) \cong \mathrm{Hom}_A(M,A) \text{ y}$$
$$M \cong \mathrm{Hom}_A(A,M) \cong \mathrm{Hom}_A(GF(A),G(B)) \cong \mathrm{Hom}_B(F(A),B) \cong \mathrm{Hom}_B(N,B)$$

y M es un progenerador en Mod_A, ya que al ser la propiedad de ser progenerador una propiedad categórica, $M = G(B)$ es progenerador por ser B progenerador. Luego, por las Proposiciones A.23 y A.32, para todo $K \in Mod_A$

$$F(K) \cong \mathrm{Hom}_B(B,F(K)) \cong \mathrm{Hom}_B(FG(B),F(K)) \cong \mathrm{Hom}_A(M,K) \cong K \otimes N,$$

y análogamente se puede probar que $M \cong \mathrm{Hom}_B(N,B)$ y que N es un progenerador en Mod_B, lo que implica que

$$G(T) \cong \mathrm{Hom}_A(A,G(T)) \cong \mathrm{Hom}_A(GF(A),G(T)) \cong \mathrm{Hom}_B(M,T) \cong T \otimes N$$

para todo $T \in Mod_B$. Además, la colección de tales isomorfismos es un isomorfismo natural como ya se ha mostrado en la Proposición A.32.

Se ha probado el siguiente teorema.

Teorema A.33. *Si $F : Mod_A \to Mod_B$ y $G : Mod_B \to Mod_A$ son funtores tales que $FG \cong 1_{Mod_B}$ y $GF \cong 1_{Mod_A}$, entonces existe un progenerador M en Mod_A tal que $B \cong \mathrm{End}_A(M)$, que además cumple con que G es isomorfo a $\_ \otimes M$ y F es isomorfo a $\_ \otimes N$, donde $N = \mathrm{Hom}_A(M,A)$. Recíprocamente, si se tiene un progenerador M en Mod_A, entonces Mod_A es equivalente a Mod_B.*

Demostración. El primer enunciado se probó en la discusión anterior. El segundo se sigue de los 2 teoremas anteriores. □

Ejemplo A.34. Sea A un anillo semiperfecto, en la Sección 8.4 se ha probado que si $X = \{e_1, ..., e_n\}$ es un sistema completo de idempotentes ortogonales primitivos, entonces existe un subconjunto $Y \subseteq X$ tal que $\{e_iA\}_{e_i \in Y}$ es un sistema completo de representantes de las clases de de isomorfismo de los módulos proyectivos inescindibles, y que eAe es un anillo básico donde $e = \sum_{e_i \in Y} e_i$. Se probará a continuación que Mod_A es equivalente a Mod_{eAe}.

Para ello se observa que eA es un progenerador, ya que es un módulo proyectivo finitamente generado y $A = \sum_{f \in H} f(M)$ donde $H = \mathrm{Hom}_A(eA, A)$, esto último se cumple debido a que por construcción para todo $e_i \in X$ existe $e_j \in Y$ tal que existe un isomorfismo $f_j : e_jA \to e_iA$, de modo que si $\pi_j : eA \to e_jA$ es la proyección natural y $\iota_i : e_iA \to A$ es la inclusión natural, $\iota_i f_j \pi_j$ es un elemento de H tal que $\mathrm{Im}(\iota_i f_j \pi_j) = e_iA$, y entonces $A = \bigoplus_{i=1}^n e_iA = \bigoplus_{i=1}^n \mathrm{Im}(\iota_i f_j \pi_j)$.

Ya probado que eA es un progenerador, entonces del Teorema A.33 se sigue que Mod_A es equivalente a Mod_B, donde $B = \mathrm{End}_A(eA) \cong eAe$.

Bibliografía

[AF04] Frank W. Anderson and Kent R. Fuller. *Rings and Categories of Modules*. Springer-Verlag, New York, U.S.A., 2004.

[ASS06] Ibrahim Assem, Daniel Simson, and Andrzej Skowronski. *Elements of the Representation Theory of Associative Algebras, Volume 1 Techniques of Representaton Theory*. Cambridge University Press, New York, U.S.A., 2006.

[Bas60] Hyman Bass. Finitistic dimension and a homological generalization of semi-primary rings. *Transactions of the American Mathematical Society*, 95:466–488, 1960.

[CE56] Henri Cartan and Samuel Eilenberg. *Homological Algebra*. Princeton University Press, New Jersey, U.S.A., 1956.

[Eil56] Samuel Eilenberg. Homological dimension and syzygies. *Annals of Mathematics*, 64:328–336, 1956.

[ES53] B. Eckmann and A. Schopf. Über injective moduln. *Archiv der Mathematik*, 4:75–78, 1953.

[Fac98] Alberto Faccini. *Module Theory: Endomorphism rings and direct sum decompositions in some classes of modules*. Birkhäuser, Switzerland, 1998.

[HGK05] Michiel Hazewinkel, Nadiya Gubareni, and V.V. Kirichenko. *Algebras, Rings and Modules, Volume 1*. Kluwer Academic Publishers, Dordrecht, Holland, 2005.

[HS71] P.J. Hilton and U. Stammbach. *A Course in Homological Algebra*. Springer-Verlag, New York, U.S.A., 1971.

[Lam01] Tsi-Yuen Lam. *A First Course in Noncommutative Rings*. Springer.Verlag, New York, U.S.A., 2001.

[Pas04] Donald S. Passman. *A Course in Ring Theory*. AMS Chelsea Publishing, Rhode Island, U.S.A., 2004.

[Wei99] Charles A. Weibel. History of homological algebra. *The History of Topology*, pages 797–836, 1999.

Nomenclatura

$\bigoplus_{i\in X} N_i$	la suma directa de la familia $(N_i)_{i\in X}$
$\mathbb{C}$	el anillo de los números complejos
$\mathbb{Q}$	el anillo de los números racionales
$\mathbb{Z}$	el anillo de los números enteros
$\mathbb{Z}_n$	$\mathbb{Z}/n\mathbb{Z}$
$\mathrm{End}(M)$	El anillo de endomorfismos del grupo abeliano M.
$\mathrm{Hom}_A(M,N)$	grupo de morfismos de A-módulos de M a N
$\mathrm{Im}(f)$	La imagen del morfismo f.
$\ker(f)$	El núcleo del morfismo f.
$\mathrm{rad}(M)$	radical de M
$\mathrm{soc}(M)$	el soclo de M
$\prod_{i\in X} N_i$	el producto de la familia $(N_i)_{i\in X}$
${}_AA$	el A-módulo regular izquierdo, es decir el grupo abeliano A con la estructura de A-módulo izquierdo inducida por el producto del anillo
${}_AM$	A-módulo izquierdo
A^{op}	anillo opuesto de A
A_A	el A-módulo regular derecho, es decir el grupo abeliano A con la estructura de A-módulo derecho inducida por el producto del anillo
$H \trianglelefteq G$	H es subgrupo normal de G
$M \otimes_A N$	el producto tensorial de M y N sobre el anillo A
M_A	A-módulo derecho

$N^{(X)}$	la suma directa $\bigoplus_{i \in X} N_i$, donde $N_i = N$ para toda $i \in X$
N^X	el producto $\prod_{i \in X} N_i$, donde $N_i = N$ para toda $i \in X$; o equivalentemente, el conjunto de funciones con domimio X y contradominio N