Algunos teoremas de estructura

Some structure theorems

Trabajo Fin de Grado en Matemáticas
Universidad de Málaga

Autora: Iratxe Gil Vivanco

Tutor: Miguel Ángel Gómez Lozano

Área de conocimiento y/o departamento: Álgebra

Fecha de presentación: Junio, 2025

Tema: Algunos teoremas de estructura

Tipo: Trabajo de revisión bibliográfica

Modalidad: Individual

Número de páginas: 54

DECLARACIÓN DE ORIGINALIDAD DEL TFG

D./Dña. *Iratxe*, estudiante del Grado en *matemáticas* de la Facultad de Ciencias de la Universidad de Málaga,
DECLARO:

Que he realizado el Trabajo Fin de Grado titulado "*Algunos teoremas de estructura*" y que lo presento para su evaluación. Dicho trabajo es original y todas las fuentes bibliográficas utilizadas para su realización han sido debidamente citadas en el mismo.

De no cumplir con este compromiso, soy consciente de que, de acuerdo con la normativa reguladora de los procesos de evaluación de los aprendizajes del estudiantado de la Universidad de Málaga de 23 de julio de 2019, esto podrá conllevar la calificación de suspenso en la asignatura, sin perjuicio de las responsabilidades disciplinarias en las que pudiera incurrir en caso de plagio.

Índice general

Resumen

El objetivo de este trabajo es probar dos importantes teoremas de estructura de anillos: el Teorema de Artin-Wedderburn y el Teorema de Densidad de Jacobson.

En el primer capítulo sentaremos las bases sobre las que trabajaremos. En este, estudiaremos los conceptos de anillo y módulo y demostraremos resultados que serán de gran relevancia en los siguientes capítulos.

El segundo capítulo es el destinado a probar el Teorema de Artin-Wedderburn, que clasifica los anillos semisimples. Comenzaremos el capítulo trabajando sobre los anillos simples y semisimples. Tras ello, introduciremos la condición de cadena descendente y la condición de cadena ascendente y hablaremos de módulos y anillos artinianos y noetherianos. También veremos las nociones de anillos primos y semiprimos. Una vez realizado este desarrollo teórico, procederemos a demostrar el Teorema de Artin-Wedderburn. Primero veremos su versión para Anillos Simples, que utilizaremos para demostrar el Teorema de Artin-Wedderburn general.

El tercer capítulo trata sobre Teorema de Densidad de Jacobson, que clasifica los anillos primitivos. Primero veremos la noción de anillos primitivos por la derecha y por la izquierda. En la segunda subsección demostraremos el Teorema de Densidad para Módulos Semisimples y, haciendo uso de dicho resultado, probaremos el Teorema de Densidad de Jacobson para anillos primitivos por la derecha. Trabajando con módulos a izquierda en vez de módulos a derecha de obtiene el Teorema de Densidad de Jacobson para anillos primitivos por la izquierda.

Palabras clave:

Anillo, Módulo, Simple, Semisimple, Artiniano, Primo, Semiprimo, Teorema de Artin-Wedderburn, Primitivo, Teorema de Densidad para Módulos semisimples, Teorema de Densidad de Jacobson.

Some structure theorems

Abstract

The purpose of this work is to prove two important structure theorems for rings: the Wedderburn-Artin Theorem and Jacobson Density Theorem.

In the first chapter, we lay the foundational concepts upon which the subsequent developments are built. Specifically, we examine the notions of rings and modules, and we prove several preliminary results that will be highly relevant in the later chapters.

The second chapter is devoted to the proof of the Wedderburn-Artin Theorem, which provides a classification of semisimple rings. We begin by studying simple and semisimple rings in detail. Subsequently, we introduce the Descending Chain Condition (DCC) and the Ascending Chain Condition (ACC), and discuss artinian and noetherian modules and rings. We also address the notions of prime and semiprime rings. With this theoretical groundwork in place, we proceed to prove the Wedderburn-Artin Theorem. We first present the version for Simple Rings, which will be used to prove the general Wedderburn-Artin Theorem.

The third chapter concerns Jacobson Density Theorem, which classifies primitive rings. We begin by introducing the concepts of right and left primitive rings. In the second subsection, we prove the Density Theorem for Semisimple Modules. This result is then used to establish Jacobson Density Theorem for right primitive rings. Jacobson Density Theorem for left primitive rings can be derived by working analogously with left modules instead of right modules.

key words:

Ring, Module, Simple, Semisimple, Artinian, Prime, Semiprime, Wedderburn-Artin Theorem, Primitive, Density Theorem for Semisimple Modules, Jacobson Density Theorem.

Introducción

La teoría de anillos tiene gran importancia en el álgebra moderna y está relacionada con diversos campos. En el desarrollo de este trabajo probaremos varios teoremas de estructura de anillos. Los dos resultados principales son el Teorema de Artin-Wedderburn y el Teorema de Densidad para Anillos Primitivos (en sus versiones a derecha e izquierda).

El Teorema de Artin-Wedderburn clasifica los anillos semisimples. Los orígenes de este resultado se encuentran en el año 1908, cuando J.H.M Wedderburn clasificó a las álgebras semisimples finito-dimensionales sobre cuerpos. Veinte años después, E. Noether y E. Artin introdujeron las nociones de Condición de Cadena Ascendente y Condición de Cadena Descendente como sustitutos a la finito-dimensionalidad, tras lo que E. Artin extendió el Teorema de Wedderburn a anillos semisimples. Este importante resultado marcó la investigación en álgebra abstracta, sirviendo como modelo para muchos resultados similares.

Estudiaremos también varios teoremas de densidad, desarrollados a mediados del siglo XX. El primero es el Teorema de Densidad para Módulos Semisimples, también conocido como el Teorema de Densidad de Jacobson-Chevalley, al haber sido desarrollado de forma independiente por ambos autores. El segundo es el ya mencionado Teorema de Densidad para Anillos Primitivos (en sus versiones a derecha e izquierda), que clasifica a los anillos primitivos. Destacamos que este es una generalización del Teorema de Artin-Wedderburn para Anillos Simples en la que no hay suposición de finitud.

Con esto, habremos estudiado dos importantes teoremas de estructura que han influido mucho en el álgebra abstracta moderna y que son parte de la base en la que se fundamenta de teoría de anillos.

Capítulo 1

Módulos

1. Nociones básicas sobre anillos

En esta sección vamos a estudiar conceptos y resultados que necesitaremos en el desarrollo del trabajo. Comenzamos definiendo algunas de las estructuras básicas. Para ello nos basamos en los apartados I.2 de [3] y 1.1 de [7] y en los apartados III.1 y III.4 de [3].

Definición 1. *Un grupo es una dupla $(G, *)$ que consiste en un conjunto no vacío G junto con $*$ una operación binaria en G que verifica:*

1. *la propiedad asociativa:* $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$
2. $\exists e \in G$ *tal que* e *es una unidad:* $a * e = a = e * a \quad \forall a \in G$
3. *todo elemento tiene inverso:* $\forall a \in G$ *existe* $b \in G$ *con* $a * b = e = b * a$

Observación 1. *En un grupo, el inverso de un elemento es único.*

Definición 2. *Decimos que un grupo $(G, +)$ es abeliano si verifica la propiedad conmutativa: $a + b = b + a$ $\forall a, b \in G$. En tal caso, a la unidad se la denota por 0 y al inverso de a se le llama opuesto y se denota por $-a$. Dados $a, b \in G$, denotamos $a + (-b)$ por $a - b$.*

Definición 3. *Un anillo es una terna $(R, +, \cdot)$ que consiste en un conjunto no vacío R junto con dos operaciones binarias en R: una adición $+$ y un producto $\cdot$, tales que:*

1. *$(R, +)$ es un grupo abeliano, es decir, verifica:*
   - *la propiedad asociativa:* $(a + b) + c = a + (b + c) \quad \forall a, b, c \in R$
   - *la propiedad conmutativa:* $a + b = b + a \quad \forall a, b \in R$
   - $\exists 0 \in R$ *tal que* 0 *es un elemento neutro:* $a + 0 = a = 0 + a \quad \forall a \in R$
   - *todo elemento tiene opuesto:* $\forall a \in R$ *existe* $-a \in R$ *con* $a + (-a) = 0 = (-a) + a$
2. *El producto verifica la propiedad asociativa:* $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$
3. *Se verifica la propiedad distributiva:*
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ $\forall a, b, c \in R$
   - $(b + c) \cdot a = b \cdot a + c \cdot a$ $\forall a, b, c \in R$

El producto se denota por yuxtaposición.

Siempre que no exista ambigüedad, identificaremos la terna $(R, +, \cdot)$ con R, de acuerdo con el abuso de notación común en el contexto algebraico.

Definición 4. *Dado R un anillo, decimos que R es unitario si existe $1 \in R - \{0\}$ tal que 1 es neutro para el producto, es decir, tal que $a1 = a = 1a \ \forall a \in R$. A 1 le llamaremos la unidad de R.*

Definición 5. *Dados R un anillo unitario y $a \in R$, decimos que a es invertible si existe su inverso para el producto, es decir, si existe $b \in R$ con $ab = ba = 1$. De existir, es único, lo llamaremos el inverso de a y lo denotaremos por a^{-1}.*

Definición 6. *Un anillo de división es un anillo unitario tal que todo elemento distinto del neutro es inversible.*

Definición 7. *Sea R un anillo. Decimos que R es un anillo conmutativo si el producto verifica la propiedad conmutativa, es decir, si $ab = ba \ \forall a, b \in R$.*

Definición 8. *A un anillo de división conmutativo lo llamamos cuerpo.*

A continuación damos ejemplos. Han sido obtenidos del capítulo 2 de [4], donde se encuentran las definiciones, afirmaciones y demostraciones pertinentes. También damos la noción de producto directo de anillos, estudiada en el apartado 2.6 de [1], y la noción de anillo opuesto, obtenida del apartado 1.2 de [1].

Ejemplo 1. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con las operaciones usuales son anillos unitarios y conmutativos. Es más, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos, aunque $\mathbb{Z}$ no lo es. Los cuaterniones de Hamilton $\mathbb{H}$ son un ejemplo de anillo de división no conmutativo.*

Ejemplo 2. *Dado R un anillo y n un entero positivo, las matrices $M_n(R)$ con las operaciones usuales conforman un anillo. Además, si R es unitario, $M_n(R)$ lo será. En $M_n(\mathbb{Z})$ con $n > 1$ encontramos un ejemplo de anillo unitario no conmutativo que tampoco es anillo de división.*

Ejemplo 3. *Si k es mayor que 1, $k\mathbb{Z}$ es un ejemplo de anillo no unitario.*

Definición 9. *Consideramos anillos $R_1, \ldots, R_n$. Definimos el producto directo $R_1 \times \cdots \times R_n$ como el conjunto $\{(r_1, \ldots, r_k) : r_i \in R_i \ \forall i \in \{1, \ldots, k\}\}$ con adición y producto componente por componente, que le dotan de estructura de anillo con neutro $0 = (0, \ldots, 0)$. Si todos los R_i son unitarios, $R_1 \times \cdots \times R_n$ es unitario con unidad $1 = (1, \ldots, 1)$.*

Definición 10. *Sea $(R, +, \cdot)$ un anillo. Consideramos en R el producto $\cdot_{op}$ dado por $a \cdot_{op} b = b \cdot a \ \forall a, b \in R$. $(R, +, \cdot_{op})$ es un anillo, al que llamaremos anillo opuesto de R y denotaremos por R^{op}. Destacamos que $(R^{op})^{op} = R$.*

Observación 2. *Sea R un anillo con neutro 0. Sea $a \in R$. $a0 = a(0+0) = a0 + a0$, luego $0 = a0 - a0 = (a0 + a0) - a0 = a0 + (a0 - a0) = a0$. Análogamente, $0a = 0$. Además, dados $a, b \in R$, $(a + b) + (-a - b) = (a - a) + (b - b) = 0$, $ab + (-a)b = (a - a)b = 0$ y $ab + a(-b) = a(b - b) = 0$, luego $-(a + b) = -a - b$, y $(-a)b = -ab = a(-b)$.*

Observación 3. *Sea R un anillo unitario con neutro 0 y unidad 1. Sea $a \in R$. $a + a(-1) = a(1 - 1) = a0 = 0$ y $a + (-1)a = (1 - 1)a = 0a = 0$. Por tanto, $a(-1) = -a = (-1)a$.*

Definición 11. *Sea R un anillo. Decimos que $e \in R$ es idempotente si $ee = e$.*

Procedemos a dar y caracterizar las nociones de subanillo e ideal. Las definiciones y los resultados y ejemplos provienen de los apartados 1.1 de [1], III.2 de [3] y IX.1 de [3].

Definición 12. *Sea $(R, +, \cdot)$ un anillo y sea $A \subset R$. Decimos que A es un subanillo de R y escribimos $A \leq R$ si A verifica que:*

- *la adición es una operación interna: $a + b \in A \ \forall a, b \in A$*
- *el producto es una operación interna: $ab \in A \ \forall a, b \in A$*
- *$(A, +, \cdot)$ es un anillo*

Ejemplo 4. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Ejemplo 5. *Sea R un anillo. A $Z(R) := \{z \in R : za = az \ \forall a \in R\}$ le llamamos el centro de R. Según el apartado 1.1 de [1], $Z(R) \leq R$. Además, si R es unitario con unidad 1, se tiene que $1 \in Z(R)$.*

Proposición 1. *Sea R un anillo y sea $A \subset R$. Entonces $A \leq R$ si y solamente si la adición y el producto son operaciones internas, $-a \in A \ \forall a \in A$ y $0 \in A$.*

Definición 13. *Sea R un anillo y sea $I \subset R$. Decimos que I es un ideal por la derecha de R si verifica:*

- *la adición es una operación interna: $x + y \in I \ \forall x + y \in I$*
- *$(I, +)$ es un grupo*
- *$ya \in I \ \forall a \in R, y \in I$*

Decimos que I es un ideal por la izquierda de R si verifica:

- *la adición es una operación interna: $x + y \in I \ \forall x + y \in I$*
- *$(I, +)$ es un grupo*
- *$ay \in I \ \forall a \in R, y \in I$*

Decimos que I es un ideal de R y denotamos $I \triangleleft R$ si I es un ideal por la izquierda y por la derecha de R.

Ejemplo 6. *Dado R un anillo, R y $\{0\}$ son ideales de R.*

Ejemplo 7. *Como se menciona en el apartado 2.6 de [4], los ideales de $\mathbb{Z}$ son $k\mathbb{Z}$ con k un entero no negativo.*

Ejemplo 8. *Sean R un anillo unitario y $a \in R$. Consideramos el conjunto $RaR := \{\sum_{i=1}^{n} r_1^i a r_2^i : n \geq 1, r_1^i, r_2^i \in R \ \forall i = 1, \ldots, n\}$. Según la proposición 2.2 del capítulo III de [3], RaR es un ideal de R que verifica que $a \in RaR$ y que $RaR \subset I$ para todo $I \triangleleft R$ con $a \in I$. Por tanto, RaR es el menor ideal de R que contiene a a. Lo llamaremos ideal de R generado por a.*

Proposición 2. *Sea R un anillo y sea $\emptyset \neq I \subset R$. Entonces:*

1. *I es un ideal por la derecha de R si y solamente si la adición es una operación interna y se tiene que $-y, ya \in I \ \forall a \in R, y \in I$.*

2. *I es un ideal por la izquierda de R si y solamente si la adición es una operación interna y se tiene que $-y, ay \in I \ \forall a \in R, y \in I$.*

3. *I es un ideal de R si y solamente si la adición es una operación interna y se tiene que $-y, ay, ya \in I \ \forall a \in R, y \in I$.*

Corolario 1. *Sea R un anillo. Todo ideal por la derecha de R es un subanillo y todo ideal por la izquierda de R es un subanillo. Por tanto, todo ideal de R es un subanillo.*

Corolario 2. *Sea R un anillo unitario y sea $\emptyset \neq I \subset R$. Entonces:*

1. *I es un ideal por la derecha de R si y solamente si la adición es una operación interna y se tiene que $ya \in I \ \forall a \in R, y \in I$.*

2. *I es un ideal por la izquierda de R si y solamente si la adición es una operación interna y se tiene que $ay \in I \ \forall a \in R, y \in I$.*

3. *I es un ideal de R si y solamente si la adición es una operación interna y se tiene que $ay, ya \in I \ \forall a \in R, y \in I$.*

Demostración. Basta usar la proposición 2 y la observación 3, que implica que $(-1)y = -y = y(-1) \ \forall y \in I$. □

Corolario 3. *Si R es un anillo conmutativo, todo ideal por la izquierda es un ideal, al igual que todo ideal por la derecha.*

Definición 14. *Sea R un anillo y sea I un ideal (respecto ideal por la derecha/ izquierda) de R. Decimos que I es un ideal (respecto ideal por la derecha/ izquierda) maximal si $I \neq R$ y para todo J ideal (respecto ideal por la derecha/ izquierda) de R con $I \subset J$ se tiene que $J = I$ o $J = R$.*

Definición 15. *Sea R un anillo y sea I un ideal (respecto ideal por la derecha/ izquierda) de R. Decimos que I es un ideal (respecto ideal por la derecha/ izquierda) minimal si $I \neq \{0\}$ y para todo J ideal (respecto ideal por la derecha/ izquierda) de R con $J \subset I$ se tiene que $J = I$ o $J = \{0\}$.*

Observación 4. *Sea R un anillo. Consideramos el conjunto de los ideales (respecto ideales por la derecha/ izquierda) de R y la contención como relación de orden. Un ideal (respecto ideal por la derecha/ izquierda) de R es maximal si y solamente si es un elemento maximal de la familia de ideales (respecto ideales por la derecha/ izquierda) de R distintos de R. Un ideal (respecto ideal por la derecha/ izquierda) de R es minimal si y solamente si es un elemento minimal de la familia de ideales (respecto ideales por la derecha/ izquierda) de R no nulos.*

Nos basamos ahora en los apartados I.1 y III.2 de [3] para estudiar el concepto de producto de ideales.

Definición 16. *Sea R un anillo y sean $I_1, \dots, I_n$ subconjuntos de R. Se define:*

$$I_1 \cdots I_k := \{\sum_{i=1}^{n} x_1^i \cdots x_k^i : \ n \geq 1, \ x_j^i \in I_j \ \forall j = 1, \dots, k, i = 1, \dots, n\}$$

Si $I_i = I \ \forall i \in \{1, \dots, k\}$ escribimos $I^k = I_1 \cdots I_k$.

Ejemplo 9. *Dados R un anillo, $a, b \in R$ y $S \leq R$, definimos $aSb := \{a\}S\{b\} = \{asb : s \in S\}$. La adición es una operación interna, pues $as_1b + as_2b = a(s_1 + s_2)b \in aSb \ \forall s_1, s_2 \in S$. Si $S = R$, el producto es una operación interna, pues $(ar_1b)(ar_2b) = a(r_1bar_2)b \in aRb$ $\forall r_1, r_2 \in R$. Además, $0 = a0b \in aRb$ y $\forall r \in R$ tenemos que $-(arb) = a(-r)b \in aRb$. Por tanto, según la proposición 1, $aRb \leq R$.*

Proposición 3. *Sea R un anillo. Sean $I_1, \dots, I_k \subset R$. Si I_k es un ideal por la derecha de R, $I_1 \cdots I_k$ también lo es. Si I_1 es un ideal por la izquierda de R, $I_1 \cdots I_k$ también lo es. Por tanto, si $I_1, \dots, I_k \lhd R$, entonces $I_1 \cdots I_k \lhd R$.*

Demostración. Claramente, la adición es una operación interna en $I_1 \dots I_k$. Un elemento de $I_1 \cdots I_k$ es de la forma $\sum_{i=1}^{n} x_1^i \cdots x_k^i$ con $n \geq 1$, $x_j^i \in I_j \ \forall j \in \{1, \dots, k\}, i \in \{1, \dots, n\}$. Si I_k es un ideal por la derecha de R, tenemos que $-\sum_{i=1}^{n} x_1^i \cdots x_k^i = \sum_{i=1}^{n} -(x_1^i \cdots x_k^i) = \sum_{i=1}^{n} x_1^i \cdots x_{k-1}^i(-x_k^i) \in I_1 \cdots I_k$ y, dado $a \in R$, $(\sum_{i=1}^{n} x_1^i \cdots x_k^i)a = \sum_{i=1}^{n} (x_1^i \cdots x_k^i)a = \sum_{i=1}^{n} x_1^i \cdots (x_k^i a) \in I_1 \cdots I_k \ \forall a \in R$. La proposición 2 nos permite concluir que $I_1 \cdots I_k$ es un ideal por la derecha de R.

Análogamente se prueba que, si I_1 es un ideal por la izquierda de R, entonces $I_1 \cdots I_k$ es un ideal por la izquierda de R. □

Ejemplo 10. *Sean R un anillo, I un ideal por la derecha de R y $a \in R$. $aI := \{a\}I = \{ay : y \in I\}$ es un ideal por la derecha de R, según la proposición 3. Asimismo, dado $A \subset R$, se tiene que $AI = \{a_1y_1 + \cdots + a_ny_n : n \geq 1, a_i \in A, y_i \in I \ \forall i = 1, \dots, n\}$ es un ideal por la derecha de R, debido a la proposición 3.*

Ejemplo 11. *Sean R un anillo, I un ideal por la izquierda de R y $a \in R$. Por la proposición 3, $Ia := I\{a\} = \{ya : y \in I\}$ es un ideal por la izquierda de R. Asimismo, dado $A \subset R$, $IA = \{y_1a_1 + \cdots + y_na_n : n \geq 1, a_i \in A, y_i \in I \ \forall i = 1, \dots, n\}$ es un ideal por la izquierda de R, debido a la proposición 3.*

Ejemplo 12. *Sean R un anillo unitario y $A \subset R$. Entonces RAR es un ideal de R que contiene a A.*

Definimos ahora la suma interna de ideales.

Definición 17. *Sea R un anillo y sea $\{I_i\}_{i \in I}$ una familia de ideales (respecto ideales por la derecha/ por la izquierda) de R. Se define la suma interna de la familia $\{I_i\}_{i \in I}$ como:*

$$\sum_{i \in I} I_i := \{a \in R : \ a = y_{i_1} + \cdots + y_{i_k}, \ k \in \mathbb{N}, i_j \in I, y_{i_j} \in I_{i_j} \ \forall j = 1, \dots, k\}$$

Decimos que la suma es directa y la denotamos por $\bigoplus_{i \in I} I_i$ si $\forall i \in I$ se tiene que $I_i \cap (\sum_{j \neq i} I_i) = \{0\}$.

Proposición 4. *Sea R un anillo. Si $\{I_i\}_{i\in I}$ es una familia de ideales por la derecha de R, entonces $\sum_{i\in I} I_i$ es un ideal por la derecha de R. Además, si $\{I_i\}_{i\in I}$ es una familia de ideales por la izquierda de R, entonces $\sum_{i\in I} I_i$ es un ideal por la izquierda de R. Por tanto, si $\{I_i\}_{i\in I}$ es una familia de ideales de R, entonces $\sum_{i\in I} I_i$ es un ideal de R.*

Demostración. Sea $\{I_i\}_{i\in I}$ una familia de ideales por la derecha de R. Sean $a, b \in \sum_{i\in I} I_i$. Por definición, existen $k, k' \in \mathbb{N}$, $i_j \in I, y_{i_j} \in I_{i_j}$ $\forall j \in \{1,\dots,k\}$ e $i'_l \in I, y_{i'_l} \in I_{i'_l}$ $\forall l \in \{1,\dots,k'\}$ con $a = y_{i_1} + \cdots + y_{i_k}$ y $b = y_{i'_1} + \cdots + y_{i'_{k'}}$. Entonces, $a + b = y_{i_1} + \cdots + y_{i_k} + y_{i'_1} + \cdots + y_{i'_{k'}} \in \sum_{i\in I} I_i$. Ahora, $-a = (-y_{i_1}) + \cdots + (-y_{i_k}) \in \sum_{i\in I} I_i$ y $ar = (y_{i_1} + \cdots + y_{i_k})r = y_{i_1}r + \cdots + y_{i_k}r \in \sum_{i\in I} I_i$ $\forall r \in R$. La proposición 2 nos permite concluir que $\sum_{i\in I} I_i$ es un ideal por la derecha de R.

Análogamente se prueba que, si $\{I_i\}_{i\in I}$ es una familia de ideales por la izquierda de R, entonces $\sum_{i\in I} I_i$ es un ideal por la izquierda de R. □

Observación 5. *Sean R un anillo y $A \subset R$. Entonces, dado I un ideal por la derecha de R, $AI = \sum_{a\in A} aI$. Asimismo, dado I un ideal por la derecha de R, $IA = \sum_{a\in A} Ia$. Además, $RAR := \sum_{a\in A} RaR$.*

Estudiemos ahora los homomorfismos de anillos basándonos en los apartados 1.1 de [1] y 2.7 de [4].

Definición 18. *Sean R y R' dos anillos. Un homomorfismo de anillos entre R y R' es una aplicación $f : R \to R'$ tal que:*

1. $f(a + b) = f(a) + f(b) \quad \forall a, b \in R$
2. $f(ab) = f(a)f(b) \quad \forall a, b \in R$

Sean R y R' unitarios con unidades respectivas 1_R y $1_{R'}$. Si f además verifica que $f(1_R) = 1_{R'}$, decimos que f es un homomorfismo de anillos unitarios entre R y R'.

Observación 6. *Sea $f : R \to R'$ un homomorfismo de anillos. Sean 0_R y $0_{R'}$ los neutros de R y R', respectivamente. Entonces, $0_{R'} = f(0_R)$ y $f(-a) = -f(a)$ $\forall a \in R$.*

Proposición 5. *Sea $f : R \to R'$ un homomorfismo de anillos. Si $A \leq R$, entonces $f(A) \leq R'$. Además, si $A' \leq R'$, entonces $f^{-1}(A') \leq R$.*

Definición 19. *Sea $f : R \to R'$ un homomorfismo de anillos. Decimos de f que es un epimorfismo si es sobreyectivo, que es un monomorfismo si es inyectivo y que es un isomorfismo si es biyectivo, en cuyo caso decimos que R y R' son isomorfos y escribimos $R \cong R'$.*

Proposición 6. *Sea $f : R \to R'$ un epimorfismo de anillos. Si I es un ideal por la derecha (respecto izquierda) de R, $f(I)$ es un ideal por la derecha (respecto izquierda) de R'. Si $I \triangleleft R$, $f(I) \triangleleft R'$.*

Demostración. Sea I un ideal por la derecha (respecto izquierda) de R. Por la proposición 5, $f(I) \leq R'$, luego la adición es una operación interna y $-a \in f(I)$ $\forall a \in f(I)$. Además, dado $r \in R'$, como f es sobreyectiva, existe $z \in R$ con $r = f(z)$, siendo $ar = f(x)f(z) = f(xz) \in f(I)$ (respecto $ra = f(z)f(x) = f(zx) \in I$). Por tanto, la

proposición 2 nos indica que $f(I)$ es un ideal por la derecha (respecto izquierda) de R'.

Si $I \triangleleft R$, basta aplicar lo recién demostrado tanto a derecha como a izquierda para obtener que $f(I) \triangleleft R'$. □

Definición 20. *Se dice que una propiedad P es estructural si, en caso de que dos anillos R y R' sean isomorfos y R verifique P, se ha que tener que R' verifique P.*

Observación 7. *Sean $R_1, \ldots, R_k$ y $R'_1, \ldots, R'_k$ anillos con $R_i \cong R'_i \ \forall i \in \{1, \ldots, k\}$. Sea $f_i : R_i \to R'_i$ un isomorfismo de anillos $\forall i \in \{1, \ldots, k\}$. Es un ejercicio comprobar que $f : R_1 \times \cdots \times R_k \to R'_1 \times \cdots \times R'_k$, $f((a_1, \ldots, a_k)) = (f_1(a_1), \ldots, f_k(a_k))$, es un isomorfismo de anillos. Por tanto, $R_1 \times \cdots \times R_k \cong R'_1 \times \cdots \times R'_k$.*

Además, si $\forall i \in I$ se tiene que R_i y R'_i son unitarios y f_i es un homomorfismo de anillos unitarios, entonces f es un isomorfismo de anillos unitarios.

2. Nociones básicas sobre módulos

Salvo que se especifique lo contrario, todos los anillos serán unitarios en este texto a partir de este punto. Nos referiremos a los homomorfismos de anillos unitarios como homomorfismos u homomorfismos de anillos.

Procedemos a definir los R-módulos a derecha e izquierda basándonos en el apartado 1.2 de [1]. El resto del capítulo nos dedicaremos a estudiar los R-módulos a derecha. Todo lo que demostremos para R-módulos a derecha tendrá su equivalente para R-módulos a izquierda.

Definición 21. *Sea R un anillo. Un R-módulo a derecha (o, simplemente, un R-módulo) es un grupo abeliano $(M, +)$ junto con una operación externa $M \times R \to M$, $(m, a) \to ma$, tal que:*

1. $(m + n)a = ma + na \quad \forall a \in R, m, n \in M$
2. $m(a + b) = ma + mb \quad \forall a, b \in R, m \in M$
3. $m(ab) = (ma)b \quad \forall a, b \in R, m \in M$
4. $m1 = m \quad \forall m \in M$

Definición 22. *Sea R un anillo. Un R-módulo a izquierda es un grupo abeliano $(M, +)$ junto con una operación externa $R \times M \to M$, $(a, m) \to am$, tal que:*

1. $a(m + n) = am + an \quad \forall a \in R, m, n \in M$
2. $(a + b)m = am + bm \quad \forall a \in R, m \in M$
3. $(ab)m = a(bx) \quad \forall a \in R, m \in M$
4. $1m = m \quad \forall m \in M$

Observación 8. *Tanto al trabajar con R-módulos a derecha como a izquierda, en los casos que no haya confusión respecto al anillo, hablaremos de módulos en lugar de R-módulos. Además, siempre que no exista ambigüedad, identificaremos con M a la terna compuesta por $(M,+)$ y la operación externa, de acuerdo con el abuso de notación común en el contexto algebraico.*

Proposición 7. *Si M es un R-módulo, entonces $(M,+)$ es un R^{op}-módulo a izquierda con la operación externa $R^{op} \times M \to M$, $r \cdot m = mr$. Asimismo, si M es un R-módulo a izquierda, entonces $(M,+)$ es un R^{op}-módulo con la operación externa $M \times R^{op} \to M$, $m \cdot r = rm$.*

Demostración. Sea M un R-módulo. Consideramos la operación externa $R^{op} \times M \to M$, $r \cdot m = mr$. Sean $m, n \in M, a, b \in R$. $a \cdot (m+n) = (m+n)a = ma + na = a \cdot m + a \cdot n$, $(a+b) \cdot m = m(a+b) = ma + mb = a \cdot m + b \cdot m$, $(a \cdot_{op} b) \cdot m = m(a \cdot_{op} b) = m(ba) = (mb)a = (b \cdot m)a = a \cdot (b \cdot m)$ y $1 \cdot m = m1 = m$. Vemos así que este producto externo dota a $(M,+)$ de estructura de R^{op}-módulo a izquierda.

Se demuestra análogamente que, si M es un R-módulo a izquierda, entonces $(M,+)$ es un R^{op}-módulo con la operación externa $M \times R^{op} \to M$, $m \cdot r = rm$. □

En lo que resta de capítulo trabajaremos con R-módulos a derecha. Todos los resultados se pueden dualizar para R-módulos a izquierda.

A continuación damos ejemplos de R-módulos. Estos provienen de los apartados VIII.1 de [3] y 1.2 de [1].

Ejemplo 13. *Sea R un anillo. Todo ideal a derecha de R es un R-módulo con operación externa el propio producto de R. En particular, esto dota a R de estructura de R-módulo, denotándose por R_R a R considerado como R-módulo.*

Ejemplo 14. *Sea R un anillo. Todo ideal a izquierda de R es un R-módulo a izquierda con operación externa el propio producto de R. En particular, esto dota a R de estructura de R-módulo a izquierda, denotándose por ${}_RR$ a R considerado como R-módulo a izquierda.*

Ejemplo 15. *Sea $(G,+)$ un grupo abeliano. Dado $g \in G$, definimos inductivamente $g0 = 0$ y $gn = g(n-1) + g$ para todo n entero positivo. Se define $gn = -(g(-n))$ para todo n entero negativo. Esta operación dota a G de estructura de $\mathbb{Z}$-módulo.*

Ejemplo 16. *Obsérvese que los espacios vectoriales son los R-módulos a izquierda con R un cuerpo.*

Ejemplo 17. *Se llama espacios vectoriales (a izquierda) sobre anillos de división a los R-módulos a izquierda con R un anillo de división.*

Observación 9. *Sea M un R-módulo. Sean $m \in M$ y 0 el neutro de R. $m0 = m(0+0) = m0 + m0$, luego $m0 = m0 + (m0 - m0) = (m0 + m0) - m0 = m0 - m0 = 0$ el neutro de M. Consideremos $-1 \in R$ el opuesto de la unidad 1. Dado $m \in M$, $m + m(-1) = m1 + m(-1) = m(1-1) = m0 = 0$, luego $m(-1) = -m$ el opuesto de m. Ahora, dado $a \in R$, $-ma = (ma)(-1) = m(a(-1)) = m(-a)$ y $m(-a) = m((-1)a) = (m(-1))a = (-m)a$, luego $-ma = m(-a) = (-m)a$.*

Demostramos ahora una proposición que utilizaremos en el capítulo 2.

Proposición 8. *Sean R y R' dos anillos isomorfos. Sea $f : R' \to R$ un homomorfismo. Sea M un R-módulo. Entonces M es un R'-módulo con la operación externa $M \times R' \to M$, $ma = mf(a)$.*

Demostración. Sean $m, n \in M$ y $a, b \in R'$. Usando las propiedades de la operación externa como R-módulo obtenemos que $(m+n)a = (m+n)f(a) = mf(a) + nf(a) = ma + na$, $m(a+b) = mf(a+b) = m(f(a)+f(b)) = mf(a)+mf(b) = ma+mb$, $m(ab) = mf(ab) = m(f(a)f(b)) = (mf(a))f(b) = (ma)f(b) = (ma)b$ y $m1_{R'} = mf(1_{R'}) = m1_R = m$. Por tanto, la operación externa $M \times R' \to M$, $ma = mf(a)$, dota a $(M, +)$ de estructura de R'-módulo. □

Ahora estudiaremos las importantes nociones de submódulo y de homomorfismo entre módulos. Para ello nos basamos en el apartado 1.2 de [1] y en el apartado VIII.1 de [3].

Definición 23. *Sea M un R-módulo y sea $N \subset M$. Decimos que N es un submódulo de M y escribimos $N \leq M$ si verifica que:*

1. *la adición es una operación interna en N: $m + n \in N \ \forall m, n \in N$*
2. *el producto con R es cerrado en N: $ma \in N \ \forall m \in N, a \in R$*
3. *tiene estructura de R-módulo con estas dos operaciones.*

Proposición 9. *Sea M un R-módulo y sea $\emptyset \neq N \subset M$. Entonces $N \leq M$ si y solamente si $m + n, ma \in N \ \forall m, n \in N, a \in R$.*

Demostración. $\implies$ Si $N \leq M$, por definición se tiene que la suma es una operación interna en N y que el producto exterior es cerrado en N.

$\impliedby$ Por hipótesis, la suma y el producto exterior son operaciones internas en N. Como todo elemento de N es un elemento de M, las propiedades asociativa y conmutativa de la adición se heredan de M, así como las propiedades del producto externo de la definición 22. Ahora, como $N \neq \emptyset$, existe $n \in N$. Al ser el producto cerrado, $0 = n0 \in N$, siendo 0 neutro de N por serlo de M. Consideramos $-1 \in R$ el opuesto aditivo de la unidad 1. Dado $n \in N$, como el producto es una operación interna en N, $-n = n(-1) \in N$. Vemos así que los opuestos de los elementos de N están en N, siendo estos opuestos en N para la adición heredada de M. Por tanto, $(N, +)$ será un subgrupo aditivo de M, teniendo N estructura de R-módulo con las operaciones heredadas de M. □

Corolario 4. *Sea M un módulo. Sean $N_1 \leq M$ y $N_2 \subset N_1$. Entonces $N_2 \leq M$ si y solamente si $N_2 \leq N_1$.*

Ejemplo 18. *Dado M un módulo, $\{0\}$ y M siempre son submódulos de M.*

Ejemplo 19. *Sea M un R-módulo y sea $m \in M$. Sea $mR := \{mr : r \in R\}$. $\forall r_1, r_2 \in R$ y $a \in R$ se tiene que $mr_1 + mr_2 = m(r_1 + r_2) \in mR$ y $(mr_1)a = m(r_1 a) \in mR$. Por tanto, mR es un submódulo de M. Le llamaremos el submódulo cíclico generado por m. Si $\exists n \in M$ con $M = nR$, decimos que M es cíclico.*

Observación 10. *Sea R un anillo. Dado $N \subset R$, N es un submódulo de R_R si y solamente si la suma es una operación interna y $nr \in N\ \forall n \in N, r \in R$, lo que ocurre si y solamente si es un ideal por la derecha de R.*

Proposición 10. *Sea M un R-módulo y sea $\{N_i\}_{i\in I}$ una colección de submódulos. Entonces $\bigcap_{i\in I} N_i$ es un submódulo de M*

Demostración. $\forall m, n \in \bigcap_{i\in I} N_i, a \in R$ tenemos que $m, n \in N_i\ \forall i \in I$, siendo $m+n, ma \in N_i\ \forall i \in I$, luego $m+n, ma \in \bigcap_{i\in I} N_i$. Solo queda aplicar la proposición 9. □

Definición 24. *Sean M y M' dos R-módulos. Un homomorfismo de R-módulos entre M y M' es una aplicación $f : M \to M'$ tal que:*

1. $f(m+n) = f(m) + f(n) \quad \forall m, n \in M$
2. $f(ma) = f(m)a \quad \forall m \in M, a \in R$

Sea $f : M \to M'$ un homomorfismo de R-módulos. Decimos de f que es un endomorfismo si $M = M'$, que es un epimorfismo si es sobreyectivo, que es un monomorfismo si es inyectivo y que es un isomorfismo si es biyectivo (en cuyo caso decimos que M y M' son isomorfos y escribimos $M \cong M'$). A un endomorfismo biyectivo se le llama automorfismo.

Ejemplo 20. *Sea R un anillo y sea M un R-módulo. Sea $m \in M$ Consideramos $f : R_R \to M$, $f(r) = mr$. Esta aplicación es un homomorfismo de R-módulos, al ser $f(r_1+r_2) = m(r_1+r_2) = mr_1+mr_2 = f(r_1)+f(r_2)$ y $f(r_1a) = m(r_1a) = (mr_1)a = f(r_1)a$ $\forall r_1, r_2, a \in R$.*

En particular, dado R un anillo y $a \in R$, se define λ_a como la aplicación $\lambda_a : R_R \to R_R$, $\lambda_a(r) = ar$. Por lo anterior, λ_a es un homomorfismo de R-módulos.

Proposición 11. *Sea $f : M \to M'$ un homomorfismo de R-módulos. Si $N \leq M$, se tiene que $f(N) \leq M'$ y, si $N' \leq M'$, se tiene que $f^{-1}(N') \leq M$. En particular, $Ker f := f^{-1}(\{0\})$ es un submódulo de M y $Im f := f(M)$ es un submódulo de M'.*

Demostración. Sea $N \leq M$. Consideramos $x, y \in f(N) \subset M'$ y $r \in R$. Por definición, existen $m, n \in N$ tales que $x = f(m)$ y $y = f(n)$, siendo $x+y = f(m)+f(n) = f(m+n) \in f(N)$ y $xr = f(m)r = f(mr) \in f(N)$. Entonces, por la proposición 9, $f(N) \leq M'$.

Sea $N' \leq M'$. Consideramos $m, n \in f^{-1}(N') \subset M$ y $r \in R$. Entonces $f(m), f(n) \in N'$, siendo $f(m+n) = f(m) + f(n), f(mr) = f(m)r \in N'$, luego $m+n, mr \in f^{-1}(N')$. Entonces, por la proposición 9, $f^{-1}(N') \leq M$. □

Observación 11. *Sea $f : M \to M'$ un homomorfismo de R-módulos. Sean 0_M y $0_{M'}$ los neutros de M y M', respectivamente. Entonces $f(0_M) = 0_{M'}$.*

Observación 12. *Sea $f : M \to M'$ un homomorfismo de R-módulos. f es un monomorfismo si y solo si $Ker(f) = \{0\}$. Véase que $f(0) = 0$, luego, si f es inyectiva, $Ker(f) = f^{-1}(\{0\}) = \{0\}$. Además, $f(m) = f(n)$ si y solamente si $m - n \in Ker(f)$, luego, si $Ker(f) = \{0\}$, ocurre que $f(m) = f(n)$ si y solamente si $m = n$.*

La estructura de R-módulos también tiene una noción de propiedad estructural:

Definición 25. *Se dice que una propiedad P es estructural si, en caso de que la verifique un R-módulo M y M' sea isomorfo a M, M' también verifica P.*

Ahora estudiaremos la estructura del conjunto de endomorfismos de un módulo.

Definición 26. *Dado M un R-módulo, denotamos por $End(M_R)$ al conjunto de los endomorfismos de M.*

Proposición 12. *Sean $f : M_1 \to M_2$ y $g : M_2 \to M_3$ homomorfismos de R-módulos. Entonces $g \circ f : M_1 \to M_3$ es un homomorfismo de R-módulos.*

Demostración. $g \circ f(m+n) = g(f(m+n)) = g(f(m) + f(n)) = g(f(m)) + g(f(n)) = g \circ f(m) + g \circ f(n)$ y $g \circ f(ma) = g(f(ma)) = g(f(m)a) = g(f(m))a = (g \circ f(m))a$ $\forall m, n \in M_1, a \in R$. □

Proposición 13. *Sea M un R-módulo. Consideramos en $End(M_R)$ la adición $f_1 + f_2 : M \to M, (f_1+f_2)(m) = f_1(m)+f_2(m)$, y la composición como producto. Estas operaciones dotan a $End(M_R)$ de estructura de anillo unitario.*

Demostración. Sean $f_1, f_2 \in End(M_R)$. $\forall m, n \in M$, $a \in R$ se tiene que:

$$(f_1 + f_2)(m+n) = f_1(m+n) + f_2(m+n) = f_1(m) + f_1(n) + f_2(m) + f_2(n) = (f_1(m) + f_2(m)) + (f_1(n) + f_2(n)) = (f_1 + f_2)(m) + (f_1 + f_2)(n)$$

y

$$(f_1 + f_2)(ma) = f_1(ma) + f_2(ma) = f_1(m)a + f_2(m)a = ((f_1 + f_2)(m))a$$

Por tanto, $f_1+f_2 \in End(M_R)$. Vemos así que la adición está bien definida. El producto (la composición) está bien definido por la proposición 12.

Sean $f_1, f_2, f_3 \in End(M_R)$. $\forall m \in M$ se tiene:

$$((f_1 + f_2) + f_3)(m) = (f_1 + f_2)(m) + f_3(m) = (f_1(m) + f_2(m)) + f_3(m) = f_1(m) + (f_2(m) + f_3(m)) = f_1(m) + ((f_2 + f_3)(m)) = (f_1 + (f_2 + f_3))(m)$$

y

$$(f_1 + f_2)(m) = f_1(m) + f_2(m) = f_2(m) + f_1(m) = (f_2 + f_1)(m)$$

Por tanto, $(f_1 + f_2) + f_3 = f_1 + (f_2 + f_3)$ y $f_1 + f_2 = f_2 + f_1$. Por tanto, se verifican las propiedades asociativa y conmutativa de la adición.

Consideramos ahora $0 : M \to M$, $0(m) = 0$. $0(m+n) = 0 = 0 + 0 = 0(m) + 0(n)$ y $0(ma) = 0 = 0a = 0(m)a$ $\forall m, n \in M, a \in R$, luego $0 \in End(M_R)$. Dado $f \in End(M_R)$, $(0 + f)(m) = (f + 0)(m) = f(m) + 0(m) = f(m) + 0 = f(m)$ $\forall m \in M$, luego $0 + f = f + 0 = f$. Por tanto, 0 es neutro de $End(M_R)$.

Dado $f \in End(M_R)$, consideramos $-f : M \to M$, $(-f)(m) = -(f(m))$. $-f \in End(M_R)$, pues $(-f)(m+n) = -(f(m+n)) = -(f(m) + f(n)) = -f(m) - f(n) =$

$(-f)(m)+(-f)(n)$ y $(-f)(ma) = -(f(ma)) = -(f(m)a) = (-f(m))a = ((-f)(m))a$ $\forall m,n \in M, a \in R$. Además, $((-f)+f)(m) = (f+(-f))(m) = f(m)+(-f)(m) = f(m)-f(m) = 0$ $\forall m \in M$, luego $(-f)+f = f+(-f) = 0$. Por tanto, todo elemento tiene opuesto.

El producto es asociativo por serlo la composición de aplicaciones. Veamos, por último, que se verifica la propiedad distributiva. Sean $f_1, f_2, f_3 \in End(M_R)$. $\forall m \in M$ se tiene que:

$$(f_1 \circ (f_2+f_3))(m) = f_1((f_2+f_3)(m)) = f_1(f_2(m)+f_3(m)) = f_1(f_2(m))+f_1(f_3(m)) = (f_1\circ f_2)(m)+(f_1\circ f_3)(m) = ((f_1\circ f_2)+(f_1\circ f_3))(m)$$

y

$$((f_1+f_2)\circ f_3)(m) = (f_1+f_2)(f_3(m)) = f_1(f_3(m))+f_2(f_3(m)) = (f_1\circ f_3)(m)+(f_2\circ f_3)(m) = ((f_1\circ f_3)+(f_2\circ f_3))(m)$$

Por tanto, $f_1 \circ (f_2+f_3) = ((f_1\circ f_2)+(f_1\circ f_3))$ $(f_1+f_2)\circ f_3 = (f_1\circ f_3)+(f_2\circ f_3)$.

Ahora, $id : M \to M$, $id(m) = m$, es un endomorfismo, al ser $id(m+n) = m+n = id(m)+id(n)$ e $id(ma) = ma = id(m)a$ $\forall m,n \in M, a \in R$. Además, $f\circ id = f = id\circ f$ $\forall f \in End(M_R)$, luego $End(M_R)$ es unitario con unidad id. □

Proposición 14. *Dado $f : M \to M'$ un isomorfismo de R-módulos, se tiene que $f^{-1} : M' \to M$ es un isomorfismo de R-módulos. Consecuentemente, si $f \in End(M_R)$ es un isomorfismo, f es inversible en el anillo $End(M_R)$.*

Demostración. Sea $f : M \to M'$ un isomorfismo de R-módulos. Sean $m_1, m_2 \in M'$, $a \in R$. Entonces, $f(f^{-1}(m_1)+f^{-1}(m_2)) = f(f^{-1}(m_1))+f(f^{-1}(m_2)) = m_1+m_2 = f(f^{-1}(m_1+m_2))$, luego, como f es inyectiva, $f^{-1}(m_1)+f^{-1}(m_2) = f^{-1}(m_1+m_2)$. Asimismo, $f(f^{-1}(m_1)a) = f(f^{-1}(m_1))a = m_1a = f(f^{-1}(m_1a))$, luego, como f es inyectiva, $f^{-1}(m_1)a = f^{-1}(m_1a)$. Vemos así que f^{-1} es un homomorfismo de R-módulos.

Ahora, dado $f \in End(M_R)$ un isomorfismo, lo anterior implica que $f^{-1} \in End(M_R)$. Además, $f\circ f^{-1} = id = f^{-1}\circ f$, luego f^{-1} es inverso de f en $End(M_R)$. □

Como dijimos al inicio de la sección, todas las definiciones y resultados de lo que resta de capítulo pueden dualizarse para R-módulos a izquierda. Ahora mencionaremos algunos de estos conceptos y resultados, que serán relevantes en el capítulo 3.

Definición 27. *Sean M y M' dos R-módulos a izquierda. Un homomorfismo de R-módulos a izquierda entre M y M' es una aplicación $f : M \to M'$ tal que:*

1. $f(m+n) = f(m)+f(n) \quad \forall m,n \in M$
2. $f(am) = af(m) \quad \forall m \in M, a \in R$

Definición 28. *Dado $f : M \to M'$ un homomorfismo de R-módulos a izquierda, decimos que f es un endomorfismo si $M = M'$. Denotamos por $End({}_RM)$. al conjunto de los endomorfismos de M. Se puede ver, al igual que se hace en la proposición 13, que $End({}_RM)$ tiene estructura de anillo unitario con la suma de funciones como adición y la composición como producto.*

Procedemos a definir a los módulos cocientes y a dar resultados relacionados con estos. Para ello utilizamos información proveniente de los apartados 3.3 de [4] y VIII.2 de [3].

Proposición 15. *Sea M un R-módulo y sea $N \leq M$. Consideramos en M la siguiente relación: $m_1 \sim m_2$ si $m_1 - m_2 \in N$. Claramente, esta es una relación de equivalencia. Consideramos el conjunto $M/N = \{\overline{m} : m \in M\}$, cuyos elementos son las clases de equivalencia. La adición $\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$ y el producto externo $(\overline{m}, a) \to \overline{ma}$ lo dotan de estructura de R-módulo.*

Demostración. Sean $\overline{m_1} = \overline{m_1'}$, $\overline{m_2} = \overline{m_2'} \in M/N$ y $a \in R$. Entonces $\exists n_1, n_2 \in N$ tales que $m_1 - m_1' = n_1$ y $m_2 - m_2' = n_2$, siendo $(m_1 + m_2) - (m_1' + m_2') = (m_1 - m_1') + (m_2 - m_2') = n_1 + n_2 \in N$, luego $\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2} = \overline{m_1' + m_2'} = \overline{m_1'} + \overline{m_2'}$. Asimismo, $m_1 a - m_1' a = m_1 a + (-m_1')a = (m_1 - m_1')a = n_1 a \in N$, luego $\overline{m_1 a} = \overline{m_1' a}$. Vemos así que las operaciones están bien definidas.

La estructura de grupo se debe a que se heredan las propiedades de la adición de M, como se puede ver en el apartado 1.4 de [3]. Lo mismo ocurre con la propiedad conmutativa de la adición. El neutro es $\overline{0}$ y el opuesto de $\overline{m}$ es $\overline{-m}$. Sean $m, n \in M$ y $a, b \in R$. $(\overline{m} + \overline{n})a = \overline{m+n}a = \overline{(m+n)a} = \overline{ma + na} = \overline{ma} + \overline{na} = \overline{m}a + \overline{n}a$, $\overline{m}(a+b) = \overline{m(a+b)} = \overline{ma + mb} = \overline{m}a + \overline{m}b$, $\overline{m}(ab) = \overline{m(ab)} = \overline{(ma)b} = \overline{ma}b = (\overline{m}a)b$ y $\overline{m}1 = \overline{m1} = \overline{m}$. Vemos así que esta operación externa dota a M/N de estructura de R-módulo. □

Definición 29. *Sea M un R-módulo y sea $N \leq M$. Se define el módulo cociente asociado como M/N con las operaciones descritas en la proposición 15.*

Observación 13. *Como se menciona en la demostración de la proposición 15, el neutro de M/N es $\overline{0}$ y el opuesto de $\overline{m}$ es $\overline{-m}$.*

Proposición 16. *La proyección al cociente $\pi : M \to M/N$, $\pi(m) = \overline{m}$, es un epimorfismo de R-módulos con $Ker(\pi) = N$.*

Demostración. Dado $x \in M/N$, por definición existe $m \in M$ con $x = \overline{m} = \pi(m)$. Por tanto π es sobreyectiva. Ahora, dados $m, n \in M$ y $a \in R$, $\pi(m+n) = \overline{m+n} = \overline{m} + \overline{n} = \pi(m) + \pi(n)$ y $\pi(ma) = \overline{ma} = \overline{m}a = \pi(m)a$. Es decir, π es un homomorfismo. Si tomamos $m \in N$, tenemos que $m - 0 = m \in N$, luego $\pi(m) = \overline{m} = \overline{0}$, siendo $m \in Ker(\pi)$. Asimismo, si $m \in Ker(\pi)$, $\overline{m} = \pi(m) = \overline{0}$, siendo $m = m - 0 \in N$. Vemos así que $Ker(\pi) = N$. □

Observación 14. *Sea M un R-módulo. Sean N y T dos submódulos de M con $N \subset T$. Entonces $N \leq T$, luego podemos considerar T/N. Dada $\pi : M \to M/N$ la proyección al cociente M/N, tenemos que $T/N \cong \pi(T)$.*

Lema 1. *Sea M un R-módulo y sea $N \leq M$. Consideramos $\pi : M \to M/N$ la proyección al cociente. Para todo R-módulo M' y todo homomorfismo $f : M \to M'$ con $N \subset Ker(f)$ existe un único homomorfismo de R-módulos $F : M/N \to M'$ tal que $F \circ \pi = f$.*

Demostración. Sea $F : M/N \to M'$ un homomorfismo con $F \circ \pi = f$. Entonces $\forall \overline{m} \in M/N$ se tiene que $F(\overline{m}) = (F \circ \pi)(m) = f(m)$. Por tanto, de existir, F es única y está dada por $F(\overline{m}) = f(m)$ $\forall \overline{m} \in M/N$.

Definimos entonces $F : M/N \to M'$, $F(\overline{m}) = f(m)$. Dados $\overline{m_1} = \overline{m_2} \in M/N$, $m_1 - m_2 \in N \subset Ker(f)$, luego $F(\overline{m_1}) = f(m_1) = f(m_2) = F(\overline{m_2})$. Vemos así que F está bien definida. Además, $\forall m \in M$ $(F \circ \pi)(m) = F(\overline{m}) = f(m)$.

Sean $\overline{m_1}, \overline{m_2} \in M/N$ y $a \in R$. $F(\overline{m_1} + \overline{m_2}) = F(\overline{m_1 + m_2}) = f(m_1 + m_2) = f(m_1) + f(m_2) = F(\overline{m_1}) + F(\overline{m_2})$ y $F(\overline{m_1}a) = F(\overline{m_1 a}) = f(m_1 a) = f(m_1)a = F(\overline{m_1})a$. Por tanto, F es un homomorfismo de R-módulos. □

Teorema 1 (Primer Teorema de Isomorfía)**.** *Sea $f : M \to M'$ un homomorfismo de dos R-módulos. Entonces $M/Ker f \cong Im f$*

Demostración. $Im(M) \leq M'$ y $f\,|_{Im(M)}$: $M \to Im(M)$ está bien definida y hereda de $f : M \to M'$ las propiedades que hacen que sea un homomorfismo de R-módulos. Además, $Ker(f\,|_{Im(M)}) = Ker(f)$. Entonces, por el lema 1, $F : M/Ker(f) \to Im(f)$, $F(\overline{m}) = f(m)$ es un homomorfismo de R-módulos.

Veamos que F es sobreyectiva. Sea $x \in Im(f)$. Entonces $\exists m \in M$ con $x = f(m) = F(\overline{m})$, $\overline{m} \in M/Ker(f)$. Veamos que F es inyectiva. Sean $\overline{m_1}, \overline{m_2} \in M/Ker(f)$ con $F(\overline{m_1}) = F(\overline{m_2})$. Entonces $f(m_1) = f(m_2)$, luego $f(m_1 - m_2) = 0$, siendo $m_1 - m_2 \in Ker(f)$, lo que implica que $\overline{m_1} = \overline{m_2}$.

Por tanto, F es un isomorfismo de R-módulos entre $M/Ker(f)$ e $Im(f)$. □

Proposición 17. *Sea M un R-módulo y sea $N \leq M$. Consideramos $\pi : M \to M/N$ la proyección al cociente. Entonces existe una biyección entre $\{T : N \subset T \leq M\}$ y $\{L : L \leq M/N\}$ dada por:*

$$\Phi : \{T : N \subset T \leq M\} \to \{L : L \leq M/N\},\ \Phi(T) = \pi(T)$$

Demostración. Sea $T \leq M$ con $N \subset T$. Como π es un homomorfismo, la proposición 11 nos dice que $\Phi(T) = \pi(T) \leq M/N$. Por tanto, Φ está bien definida. Consideramos $\Psi : \{L : L \leq M/N\} \to \{T : N \subset T \leq M\}$, $\Psi(L) = \pi^{-1}(L)$. Por la proposición 16, π es un homomorfismo. Entonces, por la proposición 11, $\pi^{-1}(L) \leq M$ $\forall L \leq M/N$, siendo $N \subset \pi^{-1}(L)$ por ser $\pi(N) = \{0\} \subset L$. Por tanto, Ψ está bien definida.

Sea $L \leq M/N$. $\Phi \circ \Psi(L) = \Phi(\pi^{-1}(L)) = \pi(\pi^{-1}(L)) \subset L$. Como π es sobreyectiva, $\forall l \in L$ existe $m \in M$ con $\pi(m) = l \in L$, siendo $m \in \pi^{-1}(L)$, luego $l = \pi(m) \in \pi(\pi^{-1}(L))$. Por tanto, $L = \pi(\pi^{-1}(L)) = \Phi \circ \Psi(L)$.

Sea $T \leq M$ con $N \subset T$. $\Psi \circ \Phi(T) = \Psi(\pi(T)) = \pi^{-1}(\pi(T)) \supset T$. Dado $m \in \pi^{-1}(\pi(T))$, $\pi(m) \in \pi(T)$, luego existe $t \in T$ con $\pi(m) = \pi(t)$, siendo $m - t \in Ker(\pi) \subset N \subset T$; entonces, $m = (m - t) + t \in T$. Vemos así que $\Psi \circ \Phi(T) = \pi^{-1}(\pi(T)) = T$.

Por tanto, Φ y Φ son inversas, siendo Φ biyectiva por ser inversible. □

Teorema 2 (Tercer Teorema de Isomorfía)**.** *Sea M un R-módulo y sean N y T dos submódulos con $N \subset T$. Entonces $M/T \cong (M/N)/(T/N)$.*

Demostración. Como $T/N \cong \pi(T) \leq M/N$, podemos entonces considerar el módulo cociente $\frac{M/N}{T/N}$. Dadas $\pi_1 : M \to M/N$ y $\pi_2 : M/N \to \frac{M/N}{T/N}$ las respectivas proyecciones al

cociente, tomamos $f = \pi_2 \circ \pi_1$, siendo $f : M \to \frac{M/N}{T/N}$, $f(m) = \overline{\overline{m}}$. Como π_1 y π_2 son epimorfismos, f también lo será.

Ahora, si $\overline{\overline{0}} = f(m) = \overline{\overline{m}}$, tenemos $\overline{m} = \overline{m} - \overline{0} \in T/N$, luego existe $t \in T$ con $\overline{m} = \overline{t}$, siendo $m - t \in N \subset T$, luego $m \in T$. Por tanto, $Ker(f) \subset T$. Además, $\forall t \in T$ se tiene que $\overline{t} \in T/N$, luego $f(m) = \overline{\overline{t}} = \overline{\overline{0}}$. Vemos así que $Ker(f) = T$. Entonces, por el Primer Teorema de Isomorfía (teorema 1), $M/T \cong (M/N)/(T/N)$. □

3. Suma directa interna y externa de módulos

Esta sección está basada en el apartado VIII.3 de [3]. En esta introducimos las sumas directas internas y externas de módulos. El principal resultado es la proposición 24, que será utilizada en los capítulos 2 y 3.

Primero trabajaremos sobre el concepto de suma interna de submódulos.

Definición 30. *Sean M un R-módulo y $\{N_i\}_{i\in I}$ una colección no vacía de R-submódulos de M. Se define la suma interna de los $\{N_i\}_{i\in I}$ como:*

$$\sum_{i\in I} N_i := \{m \in M : \ m = n_{i_1} + \cdots + n_{i_k},\ k \geq 1, i_j \in I, n_{i_j} \in N_{i_j} \ \forall j = 1, \ldots, k\}$$

Según el apartado 1.2 de [1], esta es un submódulo de M. Comprobarlo es un ejercicio.

Observación 15. *Sean M un R-módulo y $\{N_i\}_{i\in I}$ una colección no vacía de R-submódulos de M. $\forall j \in N$ tenemos que $N_j \subset \sum_{i\in I} N_i$, luego $N_j \leq \sum_{i\in I} N_i$.*

Definición 31. *Sean M un R-módulo y $\{N_i\}_{i\in I}$ una colección no vacía de R-submódulos de M. Decimos que la suma interna $\sum_{i\in I} N_i$ es directa y la denotamos por $\bigoplus_{i\in I} N_i$ si $\forall i \in I$ si se tiene que $N_i \cap (\sum_{j\neq i} N_i) = \{0\}$.*

Definición 32. *Sea M un R-módulo. Por convenio, la suma interna y suma directa interna de una colección vacía de submódulos son $\{0\}$, como indica el apartado 2 de [6].*

Observación 16. *En lo que sigue haremos sumas en conjuntos infinitos de elementos, pero bajo la condición de que el soporte sea finito, de forma que la suma tenga sentido en el módulo.*

Proposición 18. *Sean M un R-módulo y $\{N_i\}_{i\in I}$ una colección no vacía de R-submódulos de M. $M = \bigoplus_{i\in I} N_i$ si y solamente si para cada elemento m de M existen unos únicos $n_i \in N_i$ $\forall i \in I$ con $J = \{i \in I : n_i \neq 0\}$ finito y $m = \sum_{i\in I} n_i$.*

Demostración.
$\Longrightarrow$
Sea $M = \bigoplus_{i\in I} N_i$. Como $M = \sum_{i\in I} N_i$, cada elemento $m \in M - \{0\}$ se puede expresar como $m = n_{i_1} + \cdots + n_{i_k}$ con $k \geq 1$ y $n_{i_j} \in N_{i_j} - \{0\}$ $\forall j \in \{1, \ldots, k\}$. Si consideramos $n_i = 0$ $\forall i \in I - \{i_1, \ldots, i_k\}$, tenemos $m = \sum_{i\in I} n_i$.

Supongamos ahora que $m = \sum_{i\in I} n_i = \sum_{i\in I} n'_i$ con $n_i, n'_i \in N_i \ \forall i \in I$. Entonces, $\forall j \in I$ se tiene que $n'_j - n_j = \sum_{i\in I-\{j\}}(n_i - n'_i) \in N_j \cap (\sum_{i\in I-\{j\}} N_i) = \{0\}$, siendo $n_j = n'_j$.

$\Longleftarrow$
Como todo elemento de M se expresa como $m = n_1 + \cdots + n_k$ con $k \geq 1$ y $n_i \in N_i$, tenemos que $M = \sum_{i\in I} N_i$. Veamos que la suma es directa. Sea $j \in I$. Si $0 \neq m \in N_j \cap (\sum_{i\in I-\{j\}} N_i)$, entonces $m = n_{i_1} + \cdots + n_{i_k}$ con $k \geq 1$, $\{i_1, \ldots, i_k\} \in I - \{j\}$ y $n_{i_l} \in N_{i_l} \ \forall l \in \{1, \ldots, k\}$, lo que es una contradicción por la hipótesis. Vemos así que $N_j \cap (\sum_{i\in I-\{j\}} N_i) = \{0\}$. □

Observación 17. *Sean M un R-módulo y $\{N_i\}_{i\in I}$ una colección de R-submódulos de M con $M = \bigoplus_{i\in I} N_i$. Sea $j \in I$. Hemos visto que, dado $m \in M$, existe una única forma de escribir $m = \sum_{i\in I} n_i$ con $n_i \in N_i \ \forall i \in I$ y $\{i \in I : n_i \neq 0\}$ finito. Por tanto, podemos definir $\pi_j(m) = n_j$. Por lo recién mencionado, la proyección $\pi_j : M \to N_j$ está bien definida. Es un ejercicio ver que es un epimorfismo.*

El siguiente teorema puede encontrarse en el apartado VIII.2 de [3].

Teorema 3 (Segundo Teorema de Isomorfía)**.** *Sea M un R-módulo y sean N y T dos submódulos. Entonces $T \leq N + T$, $T \cap N \leq N$ y $(N + T)/T \cong N/(N \cap T)$.*

Demostración. El que $T \leq N + T$ se debe a la observación 15. La proposición 10 nos dice que $T \cap N \leq N$.

Consideremos $f : N \to (N + T)/T$, $f(n) = \overline{n}$. Esta función está bien definida por ser $n \in N+T \ \forall n \in N$. $f(n+n') = \overline{n + n'} = \overline{n}+\overline{n'} = f(n)+f(n')$ y $f(na) = \overline{na} = \overline{n}a = f(n)a$ $\forall n, n' \in N, a \in R$, luego f es un homomorfismo.

Dado $n \in N$, $\overline{0} = f(n) = \overline{n}$ si y solo si $n = n - 0 \in T$, luego $Ker(f) = N \cap T$. Ahora, dado $\alpha \in (N + T)/T$, existen $n \in N$ y $t \in T$ con $\alpha = \overline{n + t} = \overline{n} + \overline{t} = \overline{n} + \overline{0} = \overline{n} = f(n)$. Vemos así que f es sobreyectiva. Entonces, por el Primer Teorema de Isomorfía (teorema 1), $N/(N \cap T) \cong (N + T)/T$. □

La proposición siguiente será útilizada al demostrar las proposiciones 27 y 35.

Proposición 19. *Sea $f : M \to M'$ un monomorfismo de R-módulos y sean $N_1, \ldots, N_k$ submódulos de M cuya suma es directa. Entonces $f(N_1 \oplus \cdots \oplus N_k) = f(N_1) \oplus \cdots \oplus f(N_k)$. Consecuentemente, ser suma directa de n submódulos es una propiedad estructural.*

Demostración. Por la proposición 11, $f(N_i) \leq M' \ \forall i \in \{1, \ldots, n\}$. $f(N_1 + \cdots + N_k) = \{f(n_1 + \cdots + n_k) : n_i \in I_i \quad \forall i = 1, \cdots, k\} = \{f(n_1) + \cdots + f(n_k) : n_i \in I_i \ \forall i = 1, \cdots, k\} = f(N_1) + \cdots + f(N_k)$. Asimismo, $\forall i \in I$, $f(\sum_{j\neq i} N_j) = \sum_{j\neq i} f(N_j)$, siendo $f(N_i) \cap \sum_{j\neq i} f(N_j) = f(N_i) \cap f(\sum_{j\neq i} N_j)$ y, como f es inyectiva, $f(N_i) \cap f(\sum_{j\neq i} N_j) = f(N_i \cap \sum_{j\neq i} N_j) = f(\{0\}) = \{0\}$. Por tanto, la suma $f(N_1) + \cdots + f(N_k)$ es directa.

Entonces, si $M = N_1 \oplus \cdots \oplus N_k$ y $M' \cong M$, dado $f : M \to M'$ un isomorfismo de R-módulos entre M y M' tenemos que $M' = f(M) = f(N_1 \oplus \cdots \oplus N_k) = f(N_1) \oplus \cdots \oplus f(N_k)$. Vemos así que ser suma directa de n submódulos es una propiedad estructural. □

Trabajamos ahora sobre la suma externa de módulos.

Definición 33. *Dada $\{M_i\}_{i\in I}$ una familia de R-módulos no vacía, se define su producto directo como el producto cartesiano $\prod_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i \ \ \forall i \in I\}$ con operaciones $(m_i)_{i\in I} + (n_i)_{i\in I} = (m_i + n_i)_{i\in I}$ y $(m_i)_{i\in I} \cdot r = (m_i r)_{i\in I}$. Es un ejercicio comprobar que estas operaciones dotan a $\prod_{i\in I} M_i$ de estructura de R-módulo.*

Definición 34. *Dada $\{M_i\}_{i\in I}$ una familia de R-módulos no vacía, se define su suma directa externa como $\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \in \prod_{i\in I} M_i : \exists J \subset I$ finito con $m_i = 0\ \forall i \notin J\}$. Este es un submódulo del producto directo. Véase que, dados $m = (m_i)_{i\in I}, m' = (m'_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ y $r \in R$, se tiene que $J = \{j \in I : m_j \neq 0\}$ y $J' = \{j \in I : m'_j \neq 0\}$ son finitos, luego $\{i \in I : m_i + m'_i \neq 0\} \subset J \cup J'$ y $\{i \in I : m_i r \neq 0\} \subset J$ son finitos, siendo $m + m' = (m_i + m'_i)_{i\in I}, mr = (m_i r)_{i\in I} \in \bigoplus_{i\in I} M_i$.*

Definición 35. *Por convenio, el producto directo y la suma directa externa de una familia vacía de R-módulos es $\{0\}$. Esto puede comprobarse en el apartado VIII.3 de [3].*

Definición 36. *Sea M un R-módulo. Sea $n \in \mathbb{N}$. Se define M^n como $\prod_{i=1,\dots,n} M$.*

Proposición 20. *Sean M_i y N_i R-módulos isomorfos $\forall i \in I$. Entonces $\prod_{i\in I} M_i \cong \prod_{i\in I} N_i$ y $\bigoplus_{i\in I} M_i \cong \bigoplus_{i\in I} N_i$.*

Demostración. Sea $f_i : M_i \to N_i$ un isomorfismo $\forall i \in I$. Consideramos la aplicación $f : \prod_{i\in I} M_i \to \prod_{i\in I} N_i$, $f((m_i)_{i\in I}) = (f_i(m_i))_{i\in I}$.

Sean $(m_i)_{i\in I}, (m'_i)_{i\in I} \in \prod_{i\in I} M_i$ y sea $r \in R$. $f((m_i)_{i\in I} + (m'_i)_{i\in I}) = f((m_i + m'_i)_{i\in I}) = (f_i(m_i + m'_i))_{i\in I} = (f_i(m_i) + f_i(m'_i))_{i\in I} = (f_i(m_i))_{i\in I} + (f_i(m'_i))_{i\in I} = f((m_i)_{i\in I}) + f((m'_i)_{i\in I})$ y $f((m_i)_{i\in I} r) = f((m_i r)_{i\in I}) = (f_i(m_i r))_{i\in I} = (f_i(m_i)r)_{i\in I} = (f_i(m_i))_{i\in I} r = f((m_i)_{i\in I})r$. Por tanto, f es un homomorfismo.

Definimos ahora $g : \prod_{i\in I} N_i \to \prod_{i\in I} M_i$, $g((m_i)_{i\in I}) = (f_i^{-1}(m_i))_{i\in I}$. Se tiene que $g \circ f((m_i)_{i\in I} = g((f_i(m_i))_{i\in I}) = (f_i^{-1}(f_i(m_i)))_{i\in I} = (m_i)_{i\in I}\ \forall (m_i)_{i\in I} \in \prod_{i\in I} M_i$ y que $f \circ g((n_i)_{i\in I} = f((f_i^{-1}(n_i))_{i\in I}) = (f_i(f_i^{-1}(n_i)))_{i\in I} = (n_i)_{i\in I}\ \forall (n_i)_{i\in I} \in \prod_{i\in I} N_i$. Por tanto, f es inversible con inversa g. Esto indica que f es un isomorfismo y $\prod_{i\in I} M_i \cong \prod_{i\in I} N_i$.

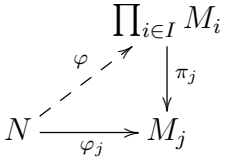
Sea $(m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$. Entonces $J = \{i \in I : m_i \neq 0\}$ es finito. Ahora, $\forall i \in I$ se tiene que $f_i(m_i) = 0$ si y solo si $m_i = 0$, luego $J = \{i \in I : f_i(m_i) \neq 0\}$. Por tanto, $f((m_i)_{i\in I}) = (f_i(m_i))_{i\in I} \in \bigoplus_{i\in I} N_i$. Vemos así que $f(\bigoplus_{i\in I} M_i) \subset \bigoplus_{i\in I} N_i$.

Análogamente, $g(\bigoplus_{i\in I} N_i) \subset \bigoplus_{i\in I} M_i$, luego $\bigoplus_{i\in I} N_i = f(g(\bigoplus_{i\in I} N_i)) \subset f(\bigoplus_{i\in I} M_i)$. Tenemos entonces que $f(\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I} N_i$, luego $f\ |_{\bigoplus_{i\in I} M_i} : \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} N_i$ es un isomorfismo, siendo $\bigoplus_{i\in I} M_i \cong \bigoplus_{i\in I} N_i$. □

Estudiemos las proyecciones ligadas al concepto de producto directo de módulos.

Definición 37. *Dada $\{M_i\}_{i\in I}$ una familia de R-módulos, tenemos $\forall j \in I$ a la proyección $\pi_j : \prod_{i\in I} M_i \to M_j$ que envía $(m_i)_{i\in I}$ a m_j. Es un ejercicio ver que esta es un epimorfismo.*

Proposición 21. *Sean N y $\{M_i\}_{i\in I}$ R-módulos. Por cada familia $\{\varphi_i : N \to M_i\}_{i\in I}$ de homomorfismos existe un único homomorfismo $\varphi : N \to \prod_{i\in I} M_i$ tal que $\pi_j \circ \varphi = \varphi_j$ $\forall j \in I$.*



Demostración. Si existe un tal homomorfismo φ, $\forall n \in N$ se tiene $\varphi(n) = (m_i)_{i\in I} \in \prod_{i\in I} M_i$. Entonces, $\forall j \in I$, $m_j = \pi_j((m_i)_{i\in I}) = \pi_j(\varphi(n)) = \varphi_j(n)$. Por tanto, de existir, esta φ es única y viene dada por $\varphi(n) = (\varphi_i(n))_{i\in I}$.

Ahora, $\varphi : N \to \prod_{i\in I} M_i$, $\varphi(n) = (\varphi_i(n))_{i\in I}$ está bien definida y verifica $\pi_j \circ \varphi = \varphi_j$ $\forall j \in I$. Además, $\varphi(n) + \varphi(n') = (\varphi_i(n))_{i\in I} + (\varphi_i(n'))_{i\in I} = (\varphi_i(n) + \varphi_i(n'))_{i\in I} = (\varphi_i(n + n'))_{i\in I} = \varphi(n + n')$ y $\varphi(n)r = (\varphi_i(n))_{i\in I}r = (\varphi_i(n)r)_{i\in I} = (\varphi_i(nr))_{i\in I} = \varphi(nr)$ $\forall n, n' \in N, r \in R$, luego φ es un homomorfismo. □

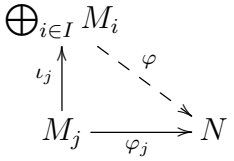
Estudiemos ahora las inclusiones ligadas a la suma directa externa de módulos.

Definición 38. *Dada $\{M_i\}_{i\in I}$ una familia de R-módulos, tenemos para todo $j \in I$ a la inclusión $\iota_j : M_j \to \bigoplus_{i\in I} M_i$ definida por sus componentes como: $(l_j(x))_j = x$ $\forall x \in M_j$ y $(l_j(x))_i = 0$ $\forall i \neq j$. Es un ejercicio ver que esta es un monomorfismo.*

Lema 2. *Si $m = (m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$, entonces $m = \sum_{i\in I} \iota_i(m_i)$. Además, $\forall (n_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ con $m = \sum_{i\in I} \iota_i(n_i)$, se tiene que $m_i = n_i$ $\forall i \in I$. Podemos entonces considerar que esta expresión es única.*

Demostración. Sea $m = (m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$. $(\sum_{i\in I} \iota_i(m_i))_j = \sum_{i\in I}(\iota_i(m_i))_j = m_j$ $\forall j \in I$, luego $m = \sum_{i\in I} \iota_i(m_i)$. Además, si $(n_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ es tal que $m = \sum_{i\in I} \iota_i(n_i)$, entonces $(n_i)_{i\in I} = \sum_{i\in I} \iota_i(n_i) = m = (m_i)_{i\in I}$, siendo $n_i = m_i$ $\forall i \in I$. □

Proposición 22. *Sean $\{M_i\}_{i\in I}$ y N R-módulos. Por cada familia $\{\varphi_i : M_i \to N\}_{i\in I}$ de homomorfismos existe un único homomorfismo $\varphi : \bigoplus_{i\in I} M_i \to N$ tal que $\varphi \circ \iota_j = \varphi_j$ $\forall j \in I$, siendo $\varphi((m_i)_{i\in I}) = \sum_{i\in I} \varphi_i(m_i)$ $\forall (m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$.*



Demostración. Supongamos que existe un tal homomorfismo φ. Dado $m = (m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$, $m = \sum_{i\in I} \iota_i(m)$ por el lema 2. Al ser φ un homomorfismo, ha de verificarse que $\varphi(m) = \varphi(\sum_{i\in I} \iota_i(m)) = \sum_{i\in I} \varphi(\iota_i(m)) = \sum_{i\in I} \varphi_i(m_i)$. Por tanto, de existir, el homomorfismo φ es único y viene dado por $\varphi((m_i)_{i\in I}) = \sum_{i\in I} \varphi_i(m_i)$.

Definimos ahora $\varphi : \bigoplus_{i\in I} M_i \to N$, $\varphi((m_i)_{i\in I}) = \sum_{i\in I} \varphi_i(m_i)$. Esto define una aplicación con $\varphi \circ \iota_j = \varphi_j$ $\forall j \in I$, ya que $(\varphi \circ \iota_j)(n) = \varphi(\iota_j(n)) = \sum_{i\in I} \varphi_i((\iota_j(n))_i) = 0 + \varphi_j((\iota_j(n))_j) = \varphi_j(n)$ $\forall n \in M_i$. Veamos que φ es un homomorfismo.

Sean $(m_i)_{i\in I}, (m'_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ y $r \in R$.

$\varphi((m_i)_{i\in I}+(m'_i)_{i\in I}) = \varphi((m_i+m'_i)_{i\in I}) = \sum_{i\in I}\varphi_i(m_i+m'_i) = \sum_{i\in I}(\varphi_i(m_i)+\varphi_i(m'_i))$. La propiedad asociativa nos dice que $\sum_{i\in I}(\varphi_i(m_i)+\varphi_i(m'_i)) = (\sum_{i\in I}\varphi_i(m_i))+(\sum_{i\in I}\varphi_i(m'_i)) = \varphi((m_i)_{i\in I}) + \varphi((m'_i)_{i\in I})$. Por tanto, $\varphi((m_i)_{i\in I} + (m'_i)_{i\in I}) = \varphi((m_i)_{i\in I}) + \varphi((m'_i)_{i\in I})$.

Asimismo, $\varphi((m_i)_{i\in I}r) = \varphi((m_ir)_{i\in I}) = \sum_{i\in J}\varphi_i(m_ir) = \sum_{i\in I}(\varphi_i(m_i)r)$. La propiedad distributiva nos dice que $\sum_{i\in I}(\varphi_i(m_i)r) = (\sum_{i\in I}\varphi_i(m_i))r = \varphi((m_i)_{i\in I})r$. Por tanto, $\varphi((m_i)_{i\in I}r) = (\sum_{i\in I}\varphi_i(m_i))r$. □

Ahora relacionaremos las sumas directas interna y externa.

Proposición 23. *$M \cong \bigoplus_{i\in I} M_i$ suma directa externa si y solo si M contiene submódulos $(A_i)_{i\in I}$ con $A_i \cong M_i$ $\forall i \in I$ y $M = \bigoplus_{i\in I} A_i$ suma directa interna.*

Demostración.
$\Longrightarrow$
Sea $N_i = \iota_i(M_i)$ $\forall i \in I$. Entonces, dado $i \in I$, como ι_i es un monomorfismo, tenemos que $\iota_i\,|_{N_i}\colon M_i \to N_i$ es un isomorfismo, siendo $N_i \cong M_i$. Consideramos ahora un isomorfismo $\varphi : \bigoplus_{i\in I} M_i \to M$ y $A_i = \varphi(N_i)$ $\forall i \in I$. Entonces $A_i \cong N_i \cong M_i$ $\forall i \in I$.

Veamos que para cada elemento de M existen unos únicos $a_i \in A_i$ $\forall i \in I$ con $m = \sum_{i\in I} a_i$.

Dado $m \in M$, existe un único $m' \in \bigoplus_{i\in I} M_i$ con $m = \varphi(m')$. Por el lema 2, m' se escribe de forma única como $\sum_{i\in I} n_i$ con $n_i \in N_i$ $\forall i \in I$. Consideramos ahora $a_i = \varphi(n_i) \in A_i$ $\forall i \in I$ y tenemos que $\{i \in I : a_i \neq 0\} = \{i \in I : n_i \neq 0\}$ es finito y $m = \varphi(m') = \varphi(\sum_{i\in J} n_i) = \sum_{i\in J}\varphi(n_i) = \sum_{i\in I} a_i$.

Ahora, si existen $a'_i \in A_i$ $\forall i \in I$ con $m = \sum_{i\in I} a'_i$, se tiene que $\sum_{i\in I} n_i = m' = \varphi^{-1}(\sum_{i\in I} a'_i) = \sum_{i\in I}\varphi^{-1}(a'_i)$, con $\varphi^{-1}(a'_i) \in N_i$ $\forall i \in I$. Entonces, ha de ocurrir que $n_i = \varphi^{-1}(a'_i)$ $\forall i \in I$, siendo $a'_i = \varphi(n_i) = a_i$ $\forall i \in I$.

Entonces, debido a la proposición 18, $M = \bigoplus_{i\in I} A_i$.

$\Longleftarrow$
Por la proposición 22, el conjunto de inclusiones $A_i \to M$ induce un homomorfismo de módulos $\phi : \bigoplus_{i\in I} A_i \to M$ con $\phi((a_i)_{i\in I}) = \sum_{i\in I} a_i$. Como $M = \bigoplus_{i\in I} A_i$, la proposición 18 nos dice que todo elemento de M se escribe de esta manera de forma única, luego concluimos que ϕ es un isomorfismo, siendo M isomorfo a la suma directa externa $\bigoplus_{i\in I} A_i$. Entonces, por la proposición 20, $M \cong \bigoplus_{i\in I} A_i \cong \bigoplus_{i\in I} M_i$. □

Observación 18. *La proposición anterior nos relaciona las sumas directas externa e interna. Véase que, si M es suma directa interna de los submódulos $(N_i)_{i\in I}$, entonces M es isomorfa a la suma directa externa de los $(N_i)_{i\in I}$ considerados como R-módulos. Asimismo, si M es la suma directa externa de los submódulos $(M_i)_{i\in I}$, entonces existen $(A_i)_{i\in I}$ submódulos de M con $A_i \cong M_i$ $\forall i \in I$ tales que M es la suma directa interna de $(A_i)_{i\in I}$. Destacamos que usaremos la misma notación para ambas.*

El siguiente resultado está basado en el apartado IX.2 de [3] y será relevante en los capítulos 2 y 3.

Proposición 24. *Para todo R-módulo N, $End((N^n)_R) \cong M_n(End(N_R))$. De hecho, para cada $\varphi \in End((N^n)_R)$ existen unos únicos $\varphi_{ij} \in End(N_R)$ $\forall i,j \in \{1,\dots,n\}$ con $\varphi((m_1,\dots,m_n)) = (\sum_{k=1}^n \varphi_{1k}(m_k),\dots,\sum_{k=1}^n \varphi_{nk}(m_k))$ $\forall (m_1,\dots,m_n) \in N^n$.*

Demostración. Sea $\iota_j : N \to \bigoplus_{k=1}^n N_k = N^n$ la j-ésima inclusión de la definición 38 $\forall j \in \{1,\dots,n\}$ y sea $\pi_i : N^n = \prod_{k=1}^n N_k \to N$ la proyección dada en la definición 37 $\forall i \in \{1,\dots,n\}$.

Definimos $\Phi : End((N^n)_R) \to M_n(End(N_R))$, $\Phi(\varphi) = (\pi_i \circ \varphi \circ \iota_j)_{i,j=1}^n$. Esta está bien definida por ser $\pi_i \circ \varphi \circ \iota_j : N \to N$ un homomorfismo $\forall i,j \in \{1,\dots,n\}$.

$$\begin{array}{ccc} N^n & \xrightarrow{\varphi} & N^n \\ {\scriptstyle \iota_j}\uparrow & & \downarrow{\scriptstyle \pi_i} \\ N & \xrightarrow[\pi_i \circ \varphi \circ \iota_j]{} & N \end{array}$$

Sean $\varphi_1, \varphi_2 \in End((N^n)_R)$. Entonces $\Phi(\varphi_1+\varphi_2) = \pi_i \circ (\varphi_1+\varphi_2) \circ \iota_j = \pi_i \circ (\varphi_1 \circ \iota_j + \varphi_2 \circ \iota_j) = \pi_i \circ \varphi_1 \circ \iota_j + \pi_i \circ \varphi_2 \circ \iota_j = \Phi(\varphi_1) + \Phi(\varphi_2)$.

Para demostrar que Φ es homomorfismo necesitaremos ver que $\sum_{i=k}^n \iota_k \circ \pi_k : N^n \to N^n$ es la identidad en N^n. Dado $(m_1,\dots,m_n) \in N^n$, $(\sum_{k=1}^n \iota_k \circ \pi_k)((m_1,\dots,m_n)) = \sum_{k=1}^n (\iota_k \circ \pi_k)((m_1,\dots,m_n)) = \sum_{k=1}^n \iota_k(m_k) = (m_1 + \sum_{i\neq 1} 0, \cdots, m_n + \sum_{i\neq n} 0) = (m_1,\dots,m_n)$. Queda así demostrado que $\sum_{k=1}^n \iota_k \circ \pi_k$ es la identidad en N^n.

Sean $\varphi_1, \varphi_2 \in End_R(N^n)$. Entonces $\Phi(\varphi_1 \circ \varphi_2) = (\pi_i \circ (\varphi_1 \circ \varphi_2) \circ \iota_j)_{i,j=1}^n = (\pi_i \circ \varphi_1 \circ (\sum_{k=1}^n \iota_k \circ \pi_k) \circ \varphi_2 \circ \iota_j)_{i,j=1}^n = (\sum_{k=1}^n (\pi_i \circ \varphi_1 \circ \iota_k \circ \pi_k \circ \varphi_2 \circ \iota_j))_{i,j=1}^n = (\sum_{k=1}^n (\Phi(\varphi_1)_{ik} \circ \Phi(\varphi_2)_{kj}))_{i,j=1}^n = (\Phi(\varphi_1)_{ik})_{i,k=1}^n \cdot (\Phi(\varphi_2)_{kj})_{k,j=1}^n = \Phi(\varphi_1) \cdot \Phi(\varphi_2)$.

Ahora, $\Phi(id) = (\pi_i \circ \iota_j)_{i,j=1}^n$. Sean $i,j \in \{1,\dots,n\}$. Dado $n \in N$, $\pi_i \circ \iota_i(n) = (\iota_i(n))_j$, siendo $\pi_i \circ \iota_i(n) = 0$ si $i \neq j$ y siendo $\pi_i \circ \iota_i(n) = n$ si $i = j$. Por tanto, Si $i \neq j$, $\pi_i \circ \iota_j$ es el homomorfismo nulo y, si $i = j$, $\pi_i \circ \iota_j$ es la identidad, que es la unidad de $End(N_R)$. Por tanto, $\Phi(id)$ es la unidad de $M_n(End(N_R))$.

Tenemos entonces que $\Phi : End((N^n)_R) \to M_n(End(N_R))$ es un homomorfismo de anillos unitarios.

Veamos ahora que es biyectiva.

Definimos $\Psi : M_n(End(N_R)) \to End((N^n)_R)$ con $\Psi((\varphi_{ij})_{i,j=1}^n) : N^n \to N^n$, $\Psi((\varphi_{ij})_{i,j=1}^n)(m_1,\dots,m_n) = (\sum_{k=1}^n \varphi_{1k}(m_k),\dots,\sum_{k=1}^n \varphi_{nk}(m_k))$ para todo $(\varphi_{ij})_{i,j=1}^n) \in M_n(End(N_R))$.

Sea $(\varphi_{ij})_{i,j=1}^n) \in M_n(End(N_R))$. Dados $(m_1,\dots,m_n),(m'_1,\dots,m'_n) \in M^n$, tenemos que $\Psi((\varphi_{ij})_{i,j=1}^n)((m_1,\dots,m_n)+(m'_1,\dots,m'_n)) = \Psi((\varphi_{ij})_{i,j=1}^n)((m_1+m'_1,\dots,m_n+m'_n)) = (\sum_{k=1}^n \varphi_{1k}(m_k + m'_k),\dots,\sum_{k=1}^n \varphi_{mk}(m_k + m'_k)) = (\sum_{k=1}^n (\varphi_{1k}(m_k) + \varphi_{1k}(m'_k)),\dots,$

$\sum_{k=1}^{n}(\varphi_{nk}(m_i)+\varphi_{nk}(m'_k))) = (\sum_{k=1}^{n}\varphi_{1k}(m_i)+\sum_{k=1}^{n}\varphi_{1k}(m'_k),\ldots,\sum_{k=1}^{n}\varphi_{nk}(m_k)+\sum_{k=1}^{n}\varphi_{nk}(m'_k)) =$
$(\sum_{k=1}^{n}\varphi_{1k}(m_k),\ldots,\sum_{k=1}^{n}\varphi_{nk}(m_k)) + (\sum_{k=1}^{n}\varphi_{1k}(m'_k),\ldots,\sum_{k=1}^{n}\varphi_{nk}(m'_k)) =$
$\Psi((\varphi_{ij})_{i,j=1}^{n})((m_1,\ldots,m_n)) + \Psi((\varphi_{ij})_{i,j=1}^{n})((m'_1,\ldots,m'_n))$.

Asimismo, dados $(m_1,\ldots,m_n)\in N^n$ y $r\in R$, tenemos $\Psi((\varphi_{ij})_{i,j=1}^{n})(m_1,\ldots,m_n)r) = \Psi((\varphi_{ij})_{i,j=1}^{n})((m_1r,\ldots,m_nr)) = (\sum_{k=1}^{n}\varphi_{1k}(m_kr),\ldots,\sum_{k=1}^{n}\varphi_{nk}(m_kr)) = (\sum_{k=1}^{n}\varphi_{1k}(m_k)r,\ldots,\sum_{k=1}^{n}\varphi_{nk}(m_r)r) = ((\sum_{k=1}^{n}\varphi_{1k}(m_k))r,\ldots,(\sum_{k=1}^{n}\varphi_{nk}(m_k))r) = (\sum_{k=1}^{n}\varphi_{1k}(m_k),\ldots,\sum_{k=1}^{n}\varphi_{nk}(m_k))r = \Psi((\varphi_{ij})_{i,j=1}^{n})((m_1,\ldots,m_n))r$. Vemos así que $\Psi((\varphi_{ij})_{i,j=1}^{n})\in End((M^n)_R)$, luego Ψ está bien definida.

Sea $(\varphi_{ij})_{i,j=1}^{n})\in M_n(End(N_R))$. Sean $i_0,j_0\in\{1,\ldots,n\}$. $\forall m\in N$ se tiene que $\Psi((\varphi_{ij})_{i,j=1}^{n})(\iota_{j_0}(m)) = \Psi((\varphi_{ij})_{i,j=1}^{n})((0,\ldots,0,m,0,\ldots,0)) = (\varphi_{1j_0}(m),\ldots,\varphi_{nj_0}(m))$, luego $(\pi_{i_0}\circ\Psi((\varphi_{ij})_{i,j=1}^{n})\circ\iota_{j_0})(m) = \pi_{i_0}((\varphi_{1j_0}(m),\ldots,\varphi_{nj_0}(m))) = \varphi_{i_0j_0}(m)$. Entonces ocurre que $\Phi(\Psi((\varphi_{ij})_{i,j=1}^{n})) = (\varphi_{ij})_{i,j=1}^{n}$. Vemos así que $\Phi\circ\Psi$ es la identidad en $M_n(End(N_R))$.

Sea $\varphi\in End((N^n)_R)$. Dado $(m_1,\ldots,m_n)\in N^n$, $(\Psi\circ\Phi(\varphi))((m_1,\ldots,m_n)) = \Psi((\pi_i\circ\varphi\circ\iota_j)_{i,j=1}^{n}))((m_1,\ldots,m_n)) = (\sum_{k=1}^{n}\pi_1\circ\varphi\circ\iota_k(m_k),\ldots,\sum_{k=1}^{n}\pi_n\circ\varphi\circ\iota_k(m_k)) = (\pi_1\circ\varphi(\sum_{k=1}^{n}\iota_k(m_k)),\ldots,\pi_n\circ\varphi(\sum_{k=1}^{n}\iota_k(m_k))) = (\pi_1\circ\varphi((m_1,\ldots,m_n)),\ldots,\pi_n\circ\varphi((m_1,\ldots,m_n))) = (\varphi((m_1,\ldots,m_n))_1,\ldots,\varphi((m_1,\ldots,m_n))_n) = \varphi((m_1,\ldots,m_n))$. Vemos así que $\Psi\circ\Phi$ es la identidad en $End((N^n)_R)$, luego Φ y Ψ son inversas.

Por tanto, Φ es un isomorfismo, siendo $End((N^n)_R)\cong M_n(End(N_R))$. □

4. Módulos simples y semisimples

4.1. Módulos simples

Esta subsección se basa en los apartados IX.1 de [3] y 1.2 de [1]. En ella estudiaremos el concepto de módulo simple, que será necesario en la subsección siguiente, y demostraremos el Lema de Shur, que utilizaremos en el capítulo 2.

Definición 39. *Sea R un anillo y sea M un R-módulo. Decimos que M es simple o irreducible si $M\neq\{0\}$ y los únicos R-submódulos de M son $\{0\}$ y M.*

Proposición 25. *Ser un R-módulo simple es una propiedad estructural.*

Demostración. Sean M_1 y M_2 R-módulos isoformos con M_1 simple. Sea $f: M_1\to M_2$ un isomorfismo. Sea N un submódulo de M_2. Entonces $f^{-1}(N)$ es un submódulo de M_1, lo que indica que este es $\{0\}$ ó M. Como f es biyectiva, si $f^{-1}(N)=\{0\}$, entonces $N=f(\{0\})=\{0\}$ y, si $f^{-1}(N)=M_1$, entonces $N=f(M_1)=M_2$. Esto implica que M_2 es simple. □

Damos ahora un importante resultado que nos permite caracterizar todos los R-módulos simples:

Proposición 26. *Un R-módulo M es simple si y solamente si es isomorfo a R_R/L para L un ideal por la derecha maximal de R.*

Demostración. $\Longleftarrow$ Por la proposición 17, como L es maximal, R_R/L solo tendrá dos submódulos, siendo simple. Entonces, por la proposición 25, M es simple.

$\Longrightarrow$ Como $M \neq \{0\}$, existe $0 \neq m \in M$. Consideramos el homomorfismo $f : R_R \to M$, $f(r) = mr$. Este es sobreyectivo, pues $f(R) = mR = M$ al ser $m = m1 \in mR \leq M$ y ser M simple. El Primer Teorema de Isomorfía (teorema 1) nos indica ahora que $M \cong \frac{R_R}{L}$ con $L = Ker(f) \leq R_R$. Como $L \leq R_R$, L es un ideal por la derecha de R. Además, como $M \cong \frac{R_R}{L}$ y M es simple, la proposición 25 nos indica que $\frac{R_R}{L}$ es simple, luego L es maximal por la proposición 17. □

Probamos ahora el Lema de Schur:

Lema 3 (Lema de Schur)**.** *Si M y M' son R-módulos simples, entonces todo homomorfismo de M a M' es ó el homomorfismo nulo ó un isomorfismo. En particular, $End_R(M)$ es un anillo de división.*

Demostración. Sea $f : M \to M'$ un homomorfismo no nulo. Entonces $Kerf \neq S$ e $Imf \neq \{0\}$, lo que implica, por ser M y M' simples, que $Kerf = \{0\}$ e $Imf = M'$. Por tanto, f es un isomorfismo. En particular, todo endomorfismo no nulo de M es un isomorfismo, luego invertible en el anillo $End(_RM)$, según la proposición 14. Vemos así que $End(_RM)$ es un anillo de división. □

Observación 19. *Sean R un anillo y $N \leq R_R$. N es simple como R-módulo si y solo si no existe N' un R-submódulo de R_R (o, equivalentemente, ideal por la derecha de R) con $\{0\} \neq N' \subsetneq N$, lo que ocurre si y solo si N es minimal como ideal por la derecha de R.*

4.2. Módulos semisimples

Esta subsección se basa en los apartados 1.2 de[6], IX.2 de [3] y 4.1 de [1]. En ella definimos los módulos semisimples, damos algunas de sus propiedades, vemos varias formas de caracterizarlos y obtenemos formas de obtener nuevos módulos semisimples a partir de otros.

Definición 40. *Sea M un R-módulo. Sea N un submódulo de M. Decimos que N es un sumando directo si existe N' un submódulo de M con $M = N \oplus N'$.*

Definición 41. *Sea M un R-módulo. Decimos que M es semisimple si todo submódulo de M es un sumando directo.*

Proposición 27. *Ser un R-módulo semisimple es una propiedad estructural.*

Demostración. Sea $f : M_1 \to M_2$ un isomorfismo. Sea N un submódulo de M_2. Entonces, $f^{-1}(N) \leq M_1$. Como M_1 es semisimple, existe $N' \leq M_1$ con $M_1 = f^{-1}(N) \oplus N'$, siendo $M_2 = f(M_1) = f(f^{-1}(N) \oplus N')$ Como f es biyectiva, por la proposición 19 $f(f^{-1}(N) \oplus N') = f(f^{-1}(N)) \oplus f(N') = N \oplus f(N')$, siendo N un sumando directo. □

Lema 4. *Todo submódulo de un R-módulo semisimple es semisimple.*

Demostración. Sea N_1 un R-submódulo de M. Veamos que N_1 es semisimple.

Sea N_2 submódulo de N_1. Como M es semisimple, existe N_2' submódulo de M con $M = N_2 \oplus N_2'$. Veamos que $N_1 = N_2 \oplus (N_2' \cap N_1)$.

$N_2 \cap (N_2' \cap N_1) \subset N_2 \cap N_2' = \{0\}$, luego la suma $N_2 + (N_2' \cap N_1)$ es directa.

Dado $n \in N_1 = M \cap N_1 = (N_2 \oplus N_2') \cap N_1$, existen $n_2 \in N_2 \subset N_1$ y $n_2' \in N_2'$ con $n = n_2 + n_2'$, siendo $n_2' = n - n_2 \in N_1$, luego $n \in N_2 + (N_2' \cap N_1)$. Por tanto, $N_1 \subset N_2 \oplus (N_2' \cap N_1)$. Además, es claro que $N_2 \oplus (N_2' \cap N_1) \subset N_1$. Por tanto, $N_2 \oplus (N_2' \cap N_1) = N_1$ y N_2 es sumando directo de N_1. □

Lema 5. *Todo módulo semisimple no nulo contiene un submódulo simple.*

Demostración. Sea M un R-módulo semisimple no nulo. Sea m un elemento no nulo de M. Consideramos el R-submódulo cíclico $M' = mR$.

Consideramos $\mathcal{F}$ la familia de submódulos de M' que no contienen a m. Estos son precisamente los submódulos de M' distintos de M'; véase que, si $m \in N \leq M'$, tenemos $M' = mR \subset N$, luego $M' = N$. $\mathcal{F}$ está ordenada parcialmente por la contención.

Consideramos $\mathcal{X}$ una cadena de esta familia. Consideramos $U = \bigcup_{N \in \mathcal{X}} N \subset M'$. Dados $n_1, n_2 \in U$, existen $N_1, N_2 \in \mathcal{X}$ con $n_1 \in N_1$ y $n_2 \in N_2$. Como $\mathcal{X}$ es una cadena, o $N_1 \subset N_2$ o $N_2 \subset N_1$. Si $N_1 \subset N_2$, tenemos que $n_1, n_2 \in N_2$, luego $n_1 + n_2 \in N_2 \subset U$. Análogamente, si $N_2 \subset N_1$, tenemos que $n_1, n_2 \in N_1$, luego $n_1 + n_2 \in N_1 \subset U$. En cualquier caso, $n_1 + n_2 \in U$. Además, dado $a \in R$, $n_1 a \in N_1 \subset U$, luego $n_1 a \in U$. Entonces, por la proposición 9, $U \leq M'$. Además, $m \notin U$, pues de lo contrario existiría $N \in \mathcal{X}$ con $m \in N$, lo que es una contradicción por ser $N \in \mathcal{F}$. Por tanto, $U \in \mathcal{F}$, siendo U una cota superior de $\mathcal{X}$.

Se demuestra así que $\mathcal{F}$ es un conjunto inductivo. Por tanto, el lema de Zorn nos dice que existe un elemento maximal N. Por el lema 4, M' es semisimple, luego existe N' un submódulo de M' (luego de M) con $M' = N \oplus N'$. Como $m \notin N$, ha de ocurrir que $N' \neq \{0\}$. Veamos que N' es simple.

Sea $N'' \leq N'$ con $N'' \neq \{0\}$. Como $N \subsetneq N \oplus N''$, por la maximalidad de N ha de ocurrir que $N \oplus N'' = M'$. Sea $n \in N'$. Como $n \in N' \subset M' = N \oplus N''$, existen $a \in N$ y $b \in N'' \subset N'$ con $n = a + b$, siendo $a = n - b \in N \cap N' = \{0\}$, luego $n = b \in N''$. Vemos así que $N'' \subset N' \subset N''$. Es decir, todo submódulo de N' distinto de $\{0\}$ es igual a N'. □

Definición 42. *Dado un R-módulo M, a $soc(M) := \sum_{N \leq M, N \text{ simple}} N$ le llamamos el zócalo de M. Destacamos que, como es suma de submódulos de M, $soc(M) \leq M$.*

Proposición 28. *Dado M un R-módulo, son equivalentes:*

1. *M es semisimple*
2. *$M = soc(M)$*
3. *M es suma de una familia de submódulos simples*
4. *M es suma directa de una familia de submódulos simples*

Además, si M es suma de una familia de submódulos simples $\mathcal{F}$, se tiene que M es suma directa de un subconjunto de $\mathcal{F}$. Es decir, si $M = \sum_{N\in\mathcal{F}} N$, entonces existe $\mathcal{T} \subset \mathcal{F}$ con $M = \bigoplus_{N\in\mathcal{T}} N$.

Demostración.

1. $\implies$ 2.
Consideramos $M_1 = soc(M)$ la suma de todos los submódulos simples de M. Como M es semisimple y $M_1 \leq M$, existe M_2 submódulo de M con $M = M_1 \oplus M_2$. Si $M_2 \neq \{0\}$, el lema 5 nos indicaría que M_2 contendría un submódulo simple N. Por definición, $N \subset M_1$, luego $N \subset M_1 \cap M_2 = \{0\}$, lo que nos llevaría a contradicción. Por tanto, $M_2 = \{0\}$, siendo $M = M_1 = soc(M)$.

2.$\implies$ 3.
$M = soc(M) = \sum_{N\leq M, N \text{ simple}} N$ es suma de submódulos simples.

3. $\implies$ 1., 4.
Por hipótesis, $M = \sum_{i\in I} M_i$ donde $\{M_i\}_{i\in I}$ es una familia de submódulos simples de M. Sea N un submódulo de M; veamos que es un sumando directo. Consideremos la familia $\mathcal{F}$ de los subconjuntos J de I tales que la suma $N + \sum_{j\in J} M_j$ es directa; es decir, que verifiquen:

a. $\sum_{j\in J} M_j$ es una suma directa

b. $N \cap \sum_{j\in J} M_j = \{0\}$

Véase que, si $J \subset I$ verifica a. y b., entonces $\forall i \in J$ tenemos que $M_i \cap (N + \sum_{j\in J-\{i\}} M_j) = \{0\}$. Esto se debe a que, dado $m \in M_i \cap (N + \sum_{j\in J-\{i\}} M_j)$, existen $n \in N$, $k \geq 1$, $j_1, \ldots, j_k \in J - \{i\}$ y $m_l \in M_{j_l}$ $\forall l \in \{1, \ldots, k\}$ con $m = n + m_1 + \cdots m_k$, siendo $n = m - (m_1 + \cdots m_k) \in N \cap \sum_{j\in J} M_j = \{0\}$, luego $m = m_1 + \cdots m_k \in M_i \cap \sum_{j\in J-\{i\}} M_j = \{0\}$.

El conjunto vacío pertenece a $\mathcal{F}$, luego $\mathcal{F} \neq \emptyset$. Consideramos a la contención como orden parcial en $\mathcal{F}$. Sea $J_1 \subset J_2 \subset \cdots \subset J_k \subset \cdots$ una cadena de elementos de $\mathcal{F}$. Consideremos $J = \bigcup_{k\geq 1} J_k$. Sea $m \in N \cap \sum_{j\in J} M_j$. Entonces existen $j_1, \ldots, j_n \in J$ y $m_i \in M_{j_i}$ $\forall i \in \{1, \ldots, n\}$ con $m = m_1 + \cdots + m_n$. Como $j_1, \ldots, j_n \in J$, tenemos que $\forall i \in \{1, \ldots, n\}$ existe J_{k_i} con $j_i \in J_{k_i}$. Dado $l = \text{máx}(k_1, \ldots, k_n)$, tenemos que $j_i \in J_l$ $\forall i \in \{1, \ldots, n\}$, luego $m = m_1 + \cdots + m_n \in N \cap \sum_{j\in J_l} M_j = \{0\}$. Vemos así que $N \cap \sum_{j\in J} M_j = \{0\}$.

Sea $j_0 \in J$. Sea $m \in M_{j_0} \cap \sum_{j\in J-\{j_0\}} M_j$. Entonces existen $j_1, \ldots, j_n \in J - \{j_0\}$ y $m_i \in M_{j_i}$ $\forall i \in \{1, \ldots, n\}$ con $m = m_1 + \cdots + m_n$. Como $j_0, j_1, \ldots, j_n \in J$, tenemos que $\forall i \in \{0, 1, \ldots, n\}$ existe J_{k_i} con $j_i \in J_{k_i}$. Dado $l = \text{máx}(k_0, k_1, \ldots, k_n)$, tenemos que

$j_i \in J_l - \{j_0\}\ \forall i \in \{1, \dots, n\}$, luego $m = m_1 + \cdots + m_n \in M_{j_0} \cap \sum_{j \in J_l - \{j_0\}} M_j = \{0\}$. Vemos así que $M_{j_0} \cap \sum_{j \in J - \{j_0\}} M_j$. Como esto ocurre $\forall j_0 \in J$, tenemos que la suma $\sum_{j \in J} M_j$ es directa.

Por tanto, $J \in \mathcal{F}$, siendo J una mayorante de la cadena. Como toda cadena tiene una mayorante, $\mathcal{F}$ es un conjunto inductivo. Podemos aplicar entonces el lema de Zorn y obtener J un elemento maximal de la familia.

Consideramos $M' := N + \sum_{j \in J} M_j$. Como J pertenece a $\mathcal{F}$, esta suma es directa, siendo $M' = N \oplus \bigoplus_{j \in J} M_j$. Para ver que $M' = M$ basta comprobar que $M_i \subset M'\ \forall i \in I$. Sea $i \in I$. Supongamos por reducción al absurdo que $M_i \nsubseteq M'$. Esto implica que $i \notin J$. Además, como M_i es simple, esto indica que $M' \cap M_i = \{0\}$. Entones, la suma $M' + M_i$ es directa, siendo $M' + M_i = N \oplus (\bigoplus_{j \in J} M_j) \oplus M_i = N \oplus (\bigoplus_{j \in J \cup \{i\}} M_j)$, lo que nos lleva a contradicción con la maximalidad de J en $\mathcal{F}$.

Queda así demostrado que $M = M' = N \oplus \bigoplus_{j \in J} M_j$, luego N es un sumando directo. Probamos así que M es semisimple.

Ahora, si $I = \emptyset$, tenemos que $M = \{0\}$, siendo M suma directa de una familia vacía de subconjuntos. Si $I \neq \emptyset$, podemos tomar $i \in I$, siendo M_i un submódulo simple de M. Tomando $N = M_i$ y aplicando lo anteriormente demostrado se obtiene que $M = M_i \oplus \bigoplus_{j \in J} M_j$ para J un cierto subconjunto de I, siendo M una suma directa de submódulos simples.

También hemos demostrado el además.

4. $\Longrightarrow$ 3. Es trivial. □

Corolario 5. *Todo R-módulo simple es semisimple.*

Proposición 29. *Todo cociente de un módulo semisimple es un módulo semisimple.*

Demostración. Consideramos M un R-módulo semisimple y N un submódulo de M. Por definición, existe K un submódulo de M con $M = N \oplus K$. Por el Segundo Teorema de Isomorfía (teorema 3), $M/N = (N + K)/N \cong K/(N \cap K) \cong K/\{0\} \cong K$. Por el lema 4, K es semisimple, luego la proposición 27 nos indica que M/N es semisimple. □

Proposición 30. *La suma directa de R-módulos semisimples es un módulo semisimple.*

Demostración. Consideramos $(M_i)_{i \in I}$ una familia de R-módulos semisimples y $M = \bigoplus_{i \in I} M_i$. Por la proposición 23, M contiene submódulos $(A_i)_{i \in I}$ con $A_i \cong M_i\ \forall i \in I$ y $M \cong \bigoplus_{i \in I} A_i$ suma directa interna. Ahora, por la proposición 28, $\forall i \in I$ existe una familia $(N_j)_{j \in I_i}$ de submódulos simples de A_i con $A_i = \bigoplus_{j \in I_i} N_j$. Por tanto, $M \cong \bigoplus_{i \in I} A_i = \bigoplus_{i \in I} (\bigoplus_{j \in I_i} N_j) = \bigoplus_{j \in \cup_{i \in I} I_i} N_j$ con N_j submódulo simple de $M\ \forall j \in \cup_{i \in I} I_i$. La proposiciones 28 y 27 nos indican ahora que M es semisimple. □

Capítulo 2

Teorema de Artin-Wedderburn

1. Anillos simples y semisimples

1.1. Anillos simples

Esta subseción se basa en el apartado IX.1 de [3]. En ella definimos los anillos simples. Veremos también que $M_n(D)$ es un ejemplo de anillo simple $\forall n \geq 1$ y D anillo de división. Esto será relevante en la prueba de la versión para anillos simples del Teorema de Artin-Wedderburn.

Definición 43. *Un anillo R es simple si no tiene ideales distintos de $\{0\}$ y R.*

Observación 20. *Al trabajar con anillos no necesariamente unitarios, se dice que un anillo R es simple si $R^2 \neq \{0\}$ y R no tiene ideales distintos de $\{0\}$ y R. Si R es unitario, esta definición coincide con la definición 43, al ser $1 * 1 = 1 \neq 0$.*

Proposición 31. *Ser un anillo simple es una propiedad estructural.*

Demostración. Sean R un anillo simple y R' un anillo isomorfo a R. Sea $f : R' \to R$ un isomorfismo. Dado $I \lhd R'$, la proposición 6 nos indica que $f(I) \lhd R$, luego $f(I) = R$ o $f(I) = \{0\}$. Como f es biyectiva, $I = f^{-1}(f(I))$, siendo $I = f^{-1}(R) = R'$ si $f(I) = R$ y siendo $I = f^{-1}(\{0\}) = \{f^{-1}(0)\} = \{0\}$ si $f(I) = \{0\}$. Por tanto, I es R' o $\{0\}$. Vemos así que R' es simple. □

Proposición 32. *Los únicos ideales por la derecha y los únicos ideales por la izquierda de un anillo de división son $\{0\}$ y el propio anillo. Por tanto, todo anillo de división es simple.*

Demostración. Sea D un anillo de división. Sea I un ideal por la derecha no nulo. Como I es no nulo, $\exists x \in I$ con $x \neq 0$, siendo x inversible. Entonces, $1 = xx^{-1} \in I$, siendo $y = 1y \in I$ para todo $y \in D$, luego $I = D$.

Análogamente, si I es un ideal por la izquierda no nulo, $\exists x \in I$ con $x \neq 0$, siendo x inversible. Entonces, $1 = x^{-1}x \in I$, siendo $y = y1 \in I$ para todo $y \in D$, luego $I = D$. □

Corolario 6. *Sea R un anillo conmutativo. Entonces R es simple si y solo si es un cuerpo.*

Demostración. $\Longleftarrow$ Si R es un cuerpo, es un anillo de división por definición. Entonces, por la proposición 32, R es simple.

$\Longrightarrow$ Sea R es simple. Entonces, dado $a \in R$, se tiene que $RaR = R$. Además, como R es conmutativo, $RaR = Ra$, siendo $R = Ra$. Por tanto, existe $b \in R$ con $1 = ba$, siendo $1 = ba = ab$ por ser R conmutativo. Vemos así que todo elemento de R es inversible, luego R es un cuerpo. □

Proposición 33. *Todo ideal de $M_n(R)$ es de la forma $M_n(I)$ para algún ideal I de R.*

Demostración. Si I es un ideal de R, $M_n(I)$ es un ideal de $M_n(R)$, como se indica en la proposición 1.4 del apartado IX.1 de [3]. Esto es un ejercicio.

Sea J un ideal de $M_n(R)$. Sea I el conjunto formado por las entradas $(1,1)$ de las matrices de J. Si $x, y \in I$, existen $A, B \in J$ tal que la componente $(1,1)$ de A es x y la de B es y, siendo $x+y$ la de $A+B \in J$, luego $x+y \in I$. Además, dado $r \in R$, la matriz C con componente $(1,1)$ igual a r y nula en el resto de componentes pertenece a $M_n(R)$. Entonces, $CA, AC \in J$, teniendo CA como componente $(1,1)$ a rx y teniendo AC a xr, lo que indica que $rx, xr \in I$. Vemos así que I es un ideal de R.

Sea E_{ij} la matriz con valor 1 en la componente (i,j) y nula en el resto. Para todo $A = (a_{ij}) \in M_n(R)$, $E_{ij}AE_{kl} = a_{jk}E_{il}$. Entonces, dado $A \in J$, se tiene que $a_{ij}E_{11} = E_{1i}AE_{j1} \in J$, luego $a_{ij} \in I$, $\forall i, j = 1, \ldots, n$, siendo por tanto $A \in M_n(I)$. Esto implica que $J \subset M_n(I)$.

Sea $A = (a_{ij}) \in M_n(I)$. Entonces, $A = \sum_{i,j=1}^{n} a_{ij}E_{ij}$ con $a_{ij} \in I$. Por definición, dado $x \in I$, existe $B = (b_{ij}) \in J$ con $b_{11} = x$, siendo $xE_{ij} = E_{i1}BE_{1j} \in J$. Esto indica que $A = \sum_{i,j=1}^{n} a_{ij}E_{ij} \in J$. Por ello, $M_n(I) \subset J$. □

Corolario 7. *Si D es un anillo de división, entonces $M_n(D)$ es simple.*

1.2. Anillos semisimples

En esta subsección nos basaremos en el apartado IX.3 de [3] y en la proposición 4.2.9 de [1] para presentar a los anillos semisimples. Este concepto es de vital importancia en el texto, pues el objetivo del capítulo es demostrar el Teorema de Artin-Wedderburn, que caracteriza a los anillos semisimples.

Definición 44. *Decimos que un anillo R es semisimple por la derecha si R como R-módulo a derecha es semisimple.*

Definición 45. *Decimos que un anillo R es semisimple por la izquierda si R como R-módulo a izquierda es semisimple.*

Como estamos trabajando con anillos unitarios, tenemos el siguiente resultado:

Proposición 34. *Un anillo R es semisimple por la derecha si y solo si es suma directa de una familia finita de ideales por la derecha minimales.*

Demostración. Por la proposición 28, R es semisimple por la derecha si y solo si R_R es suma directa interna de una familia $(N_i)_{i\in I}$ de R-submódulos simples de R_R, lo que, por la observación 19, ocurre si y solamente si R es suma directa de una familia de ideales por la derecha minimales.

En tal caso, existe $(L_i)_{i\in I}$ una familia de ideales por la derecha minimales con $R = \bigoplus_{i\in I} L_i$. Entonces la unidad de R se escribe como $1 = \sum_{i\in I} y_i$ con $y_i \in L_i\ \forall i \in I$ y con $J = \{i \in I : y_i \neq 0\}$ finito.

Supongamos por reducción al absurdo que $I \neq J$. Entonces podemos tomar $k \in I - J$. Sea $y \in L_k$. $y = 1y = (\sum_{i\in J} y_i)y = \sum_{i\in J} y_i y \in \sum_{i\in I-\{k\}} L_i$, al ser L_i ideal por la derecha $\forall i \in J$. Por tanto, $y \in L_k \cap \sum_{i\in I-\{k\}} L_i = \{0\}$. Esto implica que $I_k = \{0\}$, lo que entra en contradiccón con que L_k sea minimal. Vemos así que $I = J$ es finito. □

Proposición 35. *En anillos, la propiedad de ser semisimple por la derecha es estructural.*

Demostración. Sea R un anillo semisimple por la derecha y R' un anillo isomorfo a R. Sea $f : R \to R'$ un isomorfismo. Por la proposición 28, R_R es suma directa interna de una familia $\{N_i\}_{i\in\{1,\dots,k\}}$ de R-submódulos simples de R_R. Entonces, por la proposición 19, $R'_{R'} = f(R_R) = f(N_1 \oplus \cdots \oplus N_k) = f(N_1) \oplus \cdots \oplus f(N_k)$, siendo $f(N_i) \leq R'_{R'}$ $\forall i \in \{1, \dots, k\}$.

Sea $i \in \{1, \cdots, k\}$. $f(N_i)$ es un ideal por la derecha minimal de R'. Consideramos J un ideal por la derecha de R' con $J \subset f(N_i)$. f^{-1} es un isomorfismo, luego la proposición 6 nos indica que $f^{-1}(J)$ es un ideal por la derecha de R, siendo $f^{-1}(J) \subset f^{-1}(f(N_i)) = N_i$. Como N_i es minimal, obtenemos que o $f^{-1}(J) = N_i$, en cuyo caso $J = f(N_i)$, o $f^{-1}(J) = \{0\}$, en cuyo caso $J = \{0\}$. Vemos así que $f(N_i)$ es minimal.

Entonces, la proposición 28 nos dice que R' es semisimple por la derecha. □

Ejemplo 21. *Por la proposición 34 todo anillo de división es semisimple por la derecha, al ser el propio anillo un ideal por la derecha minimal.*

Ejemplo 22. *Sea I un ideal por la derecha de $\mathbb{Z}$ no nulo. Como $\mathbb{Z}$ es conmutativo, I es un ideal, luego el apartado 2.6 de [4] nos indica que existe k un entero no negativo con $I = k\mathbb{Z}$. Tenemos ahora que $(2k)\mathbb{Z}$ es un ideal de $\mathbb{Z}$ contenido en I, lo que indica que I no es minimal. Acabamos de ver que $\mathbb{Z}$ no tiene ideales por la derecha minimales, luego la proposición 34 nos indica que $\mathbb{Z}$ no es semisimple por la derecha.*

Proposición 36. *Si D es un anillo de división, entonces $M_n(D)$ es semisimple por la derecha.*

Demostración. Sea e_{ij} la matriz con valor 1 en la componente (i,j) y nula en el resto. Dados $i \in \{1,\dots,n\}$ y $A \in M_n(D)$, $e_{ii}A$ es una matriz con fila i-ésima igual a la fila i-ésima de A y nula en el resto. Por tanto $e_{ii}M_n(D)$ es el conjunto de matrices con fila i-ésima arbitraria y resto de filas nulas. Es ahora claro que $e_{ii}M_n(D)$ es un ideal por la derecha de $M_n(D)$ $\forall i \in \{1,\dots,n\}$ y que $M_n(D) = e_{11}M_n(D) \oplus \cdots \oplus e_{nn}M_n(D)$, como indica la proposición 2.6.3 de [1].

Sea $i \in \{1,\dots,n\}$. Consideramos J un ideal por la derecha de $M_n(D)$ con $\{0\} \neq J \subset e_{ii}M_n(D)$. Como $\{0\} \neq J$, existe $A \in J$ con alguna componente no nula. Como $J \subset e_{ii}M_n(D)$, esta estará en la fila i-ésima. Sea (i,j) la posición de esta componente no nula y sea d su valor. Consideramos B la matriz con valor d^{-1} en la componente (i,j) y nula en el resto. Como J es un ideal por la derecha de $M_n(D)$, $e_{ii} = AB \in J$, luego $e_{ii}M_n(D) \subset J$, siendo $J = e_{ii}M_n(D)$. Vemos así que $e_{ii}M_n(D)$ es un ideal minimal.

Entonces, por la proposición 34, $M_n(D)$ es semisimple por la derecha. □

Proposición 37. *Un anillo R es semisimple por la derecha si y solo si todo R-módulo es semisimple.*

Demostración. Es trivial que, si todo R-módulo es semisimple, R es semisimple.

Supongamos ahora que R es semisimple por la derecha. Entonces, por la proposición 28, hay una familia $(N_i)_{i\in I}$ de submódulos simples de R_R con $R_R = \bigoplus_{i\in I} N_i$.

Sea M un R-módulo. Veamos que es semisimple. Dado $m \in M$, $m \in mR = m(\bigoplus_{i\in I} N_i) = \{m(n_{i_1}+\cdots+n_{i_k}), k \in \mathbb{N}, i_j \in I, n_{i_j} \in N_{i_j}\ \forall j = 1,\dots,k\} \subset \sum_{i\in I}(mN_i)$. Ahora, es sencillo comprobar que $\forall i \in I$ se verifica que $f_i : N_i \to mN_i$, $f_i(n) = mn$, es un epimorfismo. Como $Ker(f_i) \leq N_i$, o se tiene que $Ker(f_i) = N_i$, en cuyo caso $mN_i = f_i(N_i) = \{0\}$, o se tiene que $Ker(f_i) = \{0\}$, siendo f_i un isomorfismo, luego $mN_i \cong N_i$ simple. Tomamos $I_m = \{i \in I : Ker(f_i) = \{0\}\}$, siendo $\sum_{i\in I}(mN_i) = \sum_{i\in I_m}(mN_i)$ y siendo mN_i simple $\forall i \in I_m$.

Como $m \in \sum_{i\in I_m}(mN_i) \subset M$ $\forall m \in M$, $M = \sum_{m\in M}\sum_{i\in I_m}(mN_i)$. Como mN_i es simple $\forall m \in M, i \in I_m$, la proposición 28 nos indica que M es semisimple. □

A continuación vamos a demostrar que el producto directo (finito) de anillos semisimples por la derecha es semisimple por la derecha.

Proposición 38. *Dados anillos semisimples por la derecha $R_1,\cdots,R_n$, el producto directo de los anillos, $R = R_1 \times \cdots \times R_n$, es semisimple por la derecha.*

Demostración. Sean $R_1,\cdots,R_n$ anillos semisimples y sea $R = R_1 \times \cdots \times R_n$ su producto directo. $\forall k \in \{1,\dots,n\}$, R_k es semisimple, luego la proposición 34 nos indica que existen $I_1^k,\dots,I_{m_k}^k$ ideales por la derecha minimales de R_k con $R_k = I_1^k \oplus \cdots \oplus I_{m_k}^k$.

Sean $k \in \{1, \ldots, n\}$ y $i \in \{1, \ldots, m_k\}$. Tomamos:

$$J_i^k = \{(r_1, \ldots, r_k, \ldots r_n) : r_k \in I_i^k, r_j = 0 \, \forall j \neq k\}$$

Dados $(r_1, \ldots, r_k, \ldots r_n), (r'_1, \ldots, r'_k, \ldots r'_n) \in J_i^k$, se tiene que $r_j + r'_j = 0 + 0 = 0 \; \forall j \neq k$ y que $r_k + r'_k \in I_i^k$, luego $(r_1, \ldots, r_k, \ldots r_n) + (r'_1, \ldots, r'_k, \ldots r'_n) = (r_1 + r'_1, \ldots, r_k + r'_k, \ldots r_n + r'_n) \in J_i^k$. Dados $(r_1, \ldots, r_k, \ldots r_n) \in J_i^k$, $(a_1, \ldots, a_k, \ldots a_n) \in R$, se tiene que $r_j a_j = 0 a_j = 0 \; \forall j \neq k$ y que $r_k a_k \in I_i^k$, luego $(r_1, \ldots, r_k, \ldots r_n)(a_1, \ldots, a_k, \ldots a_n) = (r_1 a_1, \ldots, r_k a_k, \ldots r_n a_n) \in J_i^k$. Vemos así que J_i^k es un ideal por la derecha de R.

Sea J un ideal por la derecha de R con $J \subset J_i^k$. Consideramos:

$$I = \{r \in R_k : \exists z \in J \text{ con valor } r \text{ en la componente } k\text{-ésima}\}$$

Como $J \subset J_i^k$, $I \subset I_i^k$. Dados $y_1, y_2 \in I$ existen $z_1, z_2 \in J$ tales que z_l tiene valor y_l en la componente k-ésima $\forall l \in \{1, 2\}$. Entonces, $y_1 + y_2$ es el valor de la componente k-ésima de $z_1 + z_2 \in J$, luego $y_1 + y_2 \in I$. Ahora, dado $a \in R_k$ podemos considerar $(0, \ldots, 0, a, 0, \ldots, 0)$ el elemento de R con valor a en la componente k-ésima y con el resto de componentes nulas. Entonces $y_1 a$ es la componente k-ésima de $z_1(0, \ldots, 0, a, 0, \ldots, 0)$, siendo $z_1(0, \ldots, 0, a, 0, \ldots, 0) \in J$ por ser J ideal por la derecha de R. Esto indica que $y_1 a \in I$. Por tanto, I es un ideal por la derecha de R_k contenido en I_i^k. Por la minimalidad de I_i^k, o se tiene que $I = \{0\}$, en cuyo caso $J = \{(0, \ldots, 0)\}$, o $I = I_i^k$, en cuyo caso $J = J_i^k$. Vemos así que J_i^k es un ideal por la derecha minimal de R.

Dado $k \in \{1, \ldots, n\}$, consideramos $A_k = \{(r_1, \ldots, r_k, \ldots r_n) : r_k \in R_k, r_j = 0 \, \forall j \neq k\}$ el conjunto de elementos de R con todas las componentes nulas excepto (posiblemente) la k-ésima. Como las operaciones en R son por componentes, A_k es un ideal por la derecha de $R \; \forall k \in \{1, \ldots, n\}$. Claramente, $R = A_1 \oplus \cdots \oplus A_n$.

Sea $k \in \{1, \ldots, n\}$. Sea $(r_1, \ldots, r_k, \ldots r_n) \in A_k$. Entonces $r_j = 0 \; \forall j \neq k$ y $r_k \in R_k = I_1^k \oplus \cdots \oplus I_{m_k}^k$, luego existen $y_i \in I_i^k \; \forall i \in \{1, \ldots, m_k\}$ con $r_k = y_1 + \cdots + y_{m_k}$. $\forall i \in \{1, \ldots, m_k\}$ consideramos $(0, \ldots, 0, y_i, 0, \ldots, 0)$ el elemento de R con valor y_i en la componente k-ésima y con el resto de componentes nulas, siendo $(0, \ldots, 0, y_i, 0, \ldots, 0) \in J_i^k$. Ahora, $(r_1, \ldots, r_k, \ldots r_n) = (0, \ldots, 0, y_1, 0, \ldots, 0) + \cdots + (0, \ldots, 0, y_{m_k}, 0, \ldots, 0) \in J_1^k + \cdots + J_{m_k}^k$. Por tanto, $A_k \subset J_1^k + \cdots + J_{m_k}^k \subset A_k$, siendo $A_k = J_1^k + \cdots + J_{m_k}^k$.

Veamos que la suma es directa. Sea $i \in \{1, \ldots, m_k\}$. Sea $z = (r_1, \ldots, r_k, \ldots r_n) \in J_i^k \cap \sum_{l \in \{1, \ldots, m_k\} - \{i\}} J_l^k$. Como $z \in J_i^k$, $r_j = 0 \; \forall j \neq k$ y $r_k \in I_i^k$. Ahora, como $z \in \sum_{l \in \{1, \ldots, m_k\} - \{i\}} J_l^k$, existen $y_l \in I_l^k \; \forall l \in \{1, \ldots, m_k\} - \{i\}$ con $r_k = \sum_{l \in \{1, \ldots, m_k\} - \{i\}} y_l \in \sum_{l \in \{1, \ldots, m_k\} - \{i\}} I_l^k$. Entonces, como $r_k \in I_i^k \cap \sum_{l \in \{1, \ldots, m_k\} - \{i\}} I_l^k = \{0\}$, tenemos que $r_k = 0$, siendo $z = (0, \ldots, 0)$. Queda así probado que $J_i^k \cap \sum_{l \in \{1, \ldots, m_k\} - \{i\}} J_l^k = \{(0, \ldots, 0)\}$.

Entonces, $R = \bigoplus_{k=1}^n A_k = \bigoplus_{k=1}^n (\bigoplus_{i=1}^{m_k} J_i^k)$ es suma directa de ideales por la derecha minimales de R. La proposición 34 nos indica entonces que R es semisimple. $\square$

2. Condiciones de cadena descendente y ascendente

2.1. Módulos artinianos y noetherianos

Comenzamos esta sección estudiando los R-módulos artinianos y noetherianos. Para ello utilizamos información obtenida del apartado 3.2 de [5] y del apartado 4.1 de [1].

Definición 46. *Decimos que un R-módulo M es artiniano si verifica la condición de cadena descendente en sus submódulos, es decir, si para toda $M_1 \supset M_2 \supset \cdots \supset M_k \supset M_{k+1} \supset \cdots$ cadena descendente de submódulos existe n tal que $M_n = M_{n+k}$ para todo natural k.*

Definición 47. *Decimos que un R-módulo M es noetheriano si verifica la condición de cadena ascendente en sus submódulos, es decir, si para toda $M_1 \subset M_2 \subset \cdots \subset M_k \subset M_{k+1} \subset \cdots$ cadena ascendente de submódulos existe n tal que $M_n = M_{n+k}$ para todo natural k.*

Ejemplo 23. *Todo R-módulo simple es artiniano y noetheriano.*

Observación 21. *Sea $(X, \leq)$ un conjunto parcialmente ordenado. Decimos que $(X, \leq)$ verifica la condición de cadena ascendente si para toda cadena ascendente de elementos de X $x_1 \leq x_2 \leq \cdots \leq x_k \leq x_{k+1} \leq \cdots$ existe n tal que $x_n = x_{n+k}$ para todo natural k.*

Entonces, dado M un R-módulo y $\mathcal{M}$ la familia de submódulos de M, se tiene que M es artiniano si y solo si $(\mathcal{M}, \supset)$ verifica la condición de cadena ascendente. Asimismo, M es noetheriano si y solo si $(\mathcal{M}, \subset)$ verifica la condición de cadena ascendente.

Proposición 39. *Sea $(X, \leq)$ un conjunto parcialmente ordenado. $(X, \leq)$ verifica la condición de cadena ascendente si y solamente si todo subconjunto no vacío de X tiene un elemento maximal.*

Demostración.
$\Longrightarrow$
Supongamos que $(X, \leq)$ verifica la condición de cadena ascendente. Sea $\emptyset \neq \mathcal{F} \subset X$. Supongamos por reducción al absurdo que $\mathcal{F}$ no tiene elementos maximales. Como $\mathcal{F}$ es no vacío, existe $x_1 \in \mathcal{F}$. Como x_1 no es maximal, $\exists x_2 \in \mathcal{F}$ con $x_1 \neq x_2$ y $x_1 \leq x_2$. Como x_2 no es maximal, $\exists x_3 \in \mathcal{F}$ con $x_2 \neq x_3$ $x_2 \leq x_3$. Repitiendo este argumento sucesivas veces obtenemos la cadena ascendente de elementos de X $x_1 \leq x_2 \leq x_3 \leq \cdots \leq x_k \leq x_{k+1} \leq \cdots$ con $x_k \neq x_{k+1}$ $\forall k \geq 1$, lo que entra en contradicción con que$(X, \leq)$ verifique la condición de cadena ascendente.

$\Longleftarrow$
Sea $x_1 \leq x_2 \leq x_3 \leq \cdots \leq x_k \leq x_{k+1} \leq \cdots$ una cadena ascendente de elementos de X. Consideramos $\mathcal{F} = \{x_1, x_2, \cdots, x_k, x_{k+1}, \cdots\}$. Entonces existe x_q elemento maximal de $\mathcal{F}$. Ahora, $\forall t \geq q$, como $x_t \in \mathcal{F}$ y $x_q \leq x_t$, ha de ocurrir que $x_q = x_t$. □

Corolario 8. *Un R-módulo M es artiniano si y solamente si cualquier colección no vacía de submódulos tiene un elemento minimal (con la contención $\subset$ como relación de orden).*

Corolario 9. *Sea M un R-módulo artiniano no nulo. Entonces posee un R-submódulo simple.*

Demostración. Tomamos $\mathcal{F} = \{N \leq M : \{0\} \neq N\}$. Como $M \in \mathcal{F}$, la colección no es vacía. Entonces, por el corolario 8, $\mathcal{F}$ tiene un elemento minimal N. Dado $N' \leq N$, si $N' \neq \{0\}$ tenemos que $N' \in \mathcal{F}$ y $N' \subset N$, luego $N' = N$ por la minimalidad de N. Por tanto, N es simple. □

Corolario 10. *Un R-módulo M es noetheriano si y solamente si cualquier colección no vacía de submódulos tiene un elemento maximal (con la contención $\subset$ como relación de orden).*

A continuación utilizaremos el concepto de sucesión exacta corta para demostrar que, dados un R-módulo M y $N \leq M$, se tiene que M es artiniano si y solamente si N y M/N lo son y que M es noetheriano si y solamente si N y M/N lo son. Para ello nos basamos en la sección 3.1 de [5] y en los apartados 2.4 y 4.1 de [1].

Definición 48. *Sean M_1,M_2 y M_3 R-módulos. Sean j y p homomorfismos de R-módulos con:*

$$\{0\} \longrightarrow M_1 \xrightarrow{j} M_2 \xrightarrow{p} M_3 \longrightarrow \{0\}$$

Decimos que esta sucesión de homomorfismos es una sucesión exacta corta si j es un monomorfismo, p es un epimorfismo e $Im(j) = Ker(p)$.

Ejemplo 24. *Dado M un R-módulo y $N \leq M$, $\{0\} \longrightarrow N \xrightarrow{i} M \xrightarrow{p} M/N \longrightarrow \{0\}$ (con i la inclusión y p la proyección al cociente) es una sucesión exacta corta.*

Proposición 40. *Dada $\{0\} \longrightarrow M_1 \xrightarrow{j} M_2 \xrightarrow{p} M_3 \longrightarrow \{0\}$ una sucesión exacta corta, M_1 y M_3 son artinianos si y solamente si M_2 es artiniano.*

Demostración.
$\Longrightarrow$
Supongamos que M_1 y M_3 son artinianos.

Sea $N_1 \supset N_2 \supset \cdots \supset N_k \supset N_{k+1} \supset \cdots$ una cadena descendiente de submódulos de M_2. Entonces $p(N_1) \supset p(N_2) \supset \cdots \supset p(N_k) \supset p(N_{k+1}) \supset \cdots$ es una cadena descendiente de submódulos de M_3, luego existe k_1 con $p(N_{k_1}) = p(N_{k_1+l})$ para todo l natural. Asimismo, $j^{-1}(N_1) \supset j^{-1}(N_2) \supset \cdots \supset j^{-1}(N_k) \supset j^{-1}(N_{k+1}) \supset \cdots$ es una cadena descendiente de submódulos de M_1, luego existe k_2 con $j^{-1}(N_{k_2}) = j^{-1}(N_{k_2+l})$ para todo l natural. Sea $q = max(k_1, k_2)$.

Sea k un natural. Sea $n \in N_{q+k}$. $p(n) \in p(N_{q+k}) = p(N_q)$, luego existe $m \in N_q$ con $p(n) = p(m)$, siendo $n - m \in Ker(p) = Im(j)$. Por tanto, $\exists t \in M_1$ con $j(t) = n - m$. Como $n, m \in N_{q+k}$, tenemos $j(t) \in N_{q+k}$, siendo $t \in j^{-1}(N_{q+k}) = j^{-1}(N_q)$, luego $j(t) \in N_q$. Esto implica que $n = m + j(t) \in N_q$. Vemos así que $N_{q+k} \subset N_q$. Entonces, $N_{q+k} = N_q$

$\Longleftarrow$
Supongamos que M_2 es artiniano.

Veamos que M_1 es artiniano. Sea $N_1 \supset N_2 \supset \cdots \supset N_k \supset N_{k+1} \supset \cdots$ una cadena descendiente de submódulos de M_1. Entonces, $j(N_1) \supset j(N_2) \supset \cdots \supset j(N_k) \supset j(N_{k+1}) \supset \cdots$ es una cadena descendiente de submódulos de M_2, luego existe q con $j(N_q) = j(N_{q+l})$ para todo l natural. Sea k un natural. Sea $n \in N_{q+k}$. $j(n) \in j(N_{q+k}) = j(N_q)$, luego existe $m \in N_q$ con $j(n) = j(m)$. Como j es inyectiva, $n = m \in N_q$. Por tanto, $N_q = N_{q+k}$.

Veamos que M_3 es artiniano. Consideramos $N'_1 \supset N'_2 \supset \cdots \supset N'_k \supset N'_{k+1} \supset \cdots$ una cadena descendiente de submódulos de M_3. Entonces, tenemos que $p^{-1}(N'_1) \supset p^{-1}(N'_2) \supset \cdots \supset p^{-1}(N'_k) \supset p^{-1}(N'_{k+1}) \supset \cdots$ es una cadena descendiente de submódulos de M_2, luego existe q' con $p^{-1}(N'_{q'}) = p^{-1}(N'_{q'+l})$ para todo l natural. Sea k un natural. Sea $n \in N'_{q'+k}$. Como p es sobreyectiva, existe $m \in M_2$ con $n = p(m)$, siendo $m \in p^{-1}(N'_{q'+k}) = p^{-1}(N'_{q'})$, luego $n = p(m) \in N'_{q'}$. Por tanto, $N'_{q'} = N'_{q'+k}$.

□

Proposición 41. *Dada* $\{0\} \longrightarrow M_1 \xrightarrow{j} M_2 \xrightarrow{p} M_3 \longrightarrow \{0\}$ *una sucesión exacta corta,* M_1 *y* M_3 *son noetherianos si y solamente si* M_2 *es noetheriano.*

Demostración. Es análoga a la de la proposición 40. □

Corolario 11. *Sean* M *un* R*-módulo y* N *un submódulo.* M *es artiniano si y solamente si* N *y* M/N *lo son.* M *es noetheriano si y solamente si* N *y* M/N *lo son.*

Ahora definiremos las series de composición y caracterizaremos los R-módulos que son a la vez artinianos y noetherianos como aquellos R-módulos que contengan una serie de composición, lo que nos ayudará a demostrar la importante proposición 43 al final de la sección. La información ha sido obtenida del apartado 4.1 de [1].

Definición 49. *Sea* M *un* R*-módulo. Decimos que una cadena de submódulos* $N_0 \supset N_1 \supset \cdots \supset N_{k-1} \supset N_k$ *es propia si las inclusiones son estrictas.*

Definición 50. *Sea* M *un* R*-módulo. Decimos que una cadena propia* $N'_0 \supset N'_1 \supset \cdots \supset N'_{l-1} \supset N'_l$ *es un refinamiento de la cadena propia* $N_0 \supset N_1 \supset \cdots \supset N_{k-1} \supset N_k$ *si* $\{N_0, N_1, \cdots, N_{k-1}, N_k\} \subset \{N'_0, N'_1, \cdots, N'_{l-1}, N'_l\}$.

Definición 51. *Una serie de composición de un* R*-módulo* M *es una cadena propia* $M = M_0 \supset M_1 \supset \cdots M_i \supset M_{i+1} \supset \cdots \supset M_{k-1} \supset M_k = \{0\}$ *de submódulos de* M *tales que* M_{i-1}/M_i *es simple* $\forall i = 1, \ldots, k$*. A* k *la llamamos longitud de la serie de composición.*

Observación 22. *Como* $\forall i = 1, \ldots, k$ *hay una biyección entre los submódulos de* M_{i-1}/M_i *y los submódulos de* M_i *que contienen a* M_{i-1} *(proposición 17), una cadena propia será una serie de composición si y solamente si no admite refinamientos aparte de sí misma.*

Proposición 42. *Sea* M *un* R*-módulo. Son equivalentes:*

1. M *es artiniano y noetheriano*
2. M *tiene una serie de composición*

Demostración.

1. $\Longrightarrow$ 2.
Si $M = \{0\}$, M es una serie de composición. Supongamos ahora que M es no nulo.

Supongamos por reducción al absurdo que M no tiene ninguna serie de composición. Entonces $M \supset \{0\}$ no es serie de composición, lo que indica que $M \cong M/\{0\}$ no es simple. Como M es noetheriano, el corolario 10 nos indica que existe $N_1 \leq M$ elemento maximal de $\mathcal{F} = \{N \leq M : N \neq M\}$.

Como M no es simple, ha de ocurrir que $N_1 \neq \{0\}$. Como hay una biyección entre los submódulos de M/N_1 y los submódulos de M que contienen a N_1 (proposición 17), la maximalidad de N_1 implica que M/N_1 ha de ser simple.

Si N_1 fuera simple, $M \supset N_1 \supset \{0\}$ sería una serie de composición. Por tanto, N_1 no es simple. Además, por el corolario 11, N_1 es noetheriano. Repitiendo el procedimiento anterior obtenemos N_2 un submódulo de N_1 distinto de $\{0\}$ con N_1/N_2 simple. Tenemos así N_1 y N_2 submódulos de M con $M \supset N_1 \supset N_2 \supset \{0\}$ y M/N_1 y N_1/N_2 simples.

Repitiendo este proceso sucesivas veces obtenemos una cadena descendente de submódulos $M \supset N_1 \supset N_2 \supset \cdots N_k \supset N_{k+1} \supset \cdots$, lo que entra en contradicción con que M sea artiniano.

2. $\Longrightarrow$ 1.

Sea M un R-módulo con una serie de composición de longitud 0. Entonces $M = \{0\}$ y, por tanto, M es artiniano y noetheriano.

Supongamos ahora que M es un R-módulo con una serie de composición de longitud mayor 1. Sea $M \supset M_1 \supset M_2 \supset \cdots\cdots \supset M_k \supset M_{k+1} = \{0\}$ una serie de composición de M. Como estamos ante una serie de composición, $M_k \cong M_k/\{0\}$ es simple, luego artiniano y noetheriano.

Supongamos como hipótesis de inducción que para un cierto $i \in \{1, \ldots, k\}$ se tiene que M_i es artiniano y noetheriano. Como estamos ante una serie de composición, M_{i-1}/M_i es simple, luego artiniano y noetheriano. Entonces, por el corolario 11, M_{i-1} es artiniano y noetheriano.

Probamos así por inducción que M_i es artiniano y noetheriano $\forall i \in \{0, \ldots, k\}$. En particular, $M = M_0$ es artiniano y noetheriano. □

2.2. Anillos artinianos y noetherianos

Procedemos a definir los anillos artinianos y noetherianos por la derecha, como se hace en el apartado 3.5 de [7] o en el apartado 3.2 de [5]. Tras ello los caracterizamos usando información obtenida de la sección 4.2 de [1] y damos algunos resultados relevantes.

Definición 52. *Decimos que un anillo R es artiniano por la derecha si R como R-módulo a derecha es artiniano.*

Definición 53. *Decimos que un anillo R es noetheriano por la derecha si R como R-módulo a derecha es noetheriano.*

Observación 23. *Dado un anillo R, R es artiniano por la derecha si y solamente si para toda cadena descendente de ideales a derecha $I_1 \supset I_2 \supset \cdots \supset I_k \supset I_{k+1} \supset \cdots$ existe n tal que $I_n = I_{n+1} = \cdots$. Asimismo, R es noetheriano por la derecha si y solamente si para toda cadena ascendente de ideales a derecha $I_1 \subset I_2 \subset \cdots \subset I_k \subset I_{k+1} \subset \cdots$ existe n tal que $I_n = I_{n+1} = \cdots$.*

Utilizando los corolarios 8 y 10 y aplicando nuevamente la equivalencia entre ideales por la derecha de R y submódulos de R_R obtenemos el siguiente corolario:

Corolario 12. *Un anillo R es artiniano por la derecha si y solamente si cualquier colección no vacía de ideales a derecha tiene un elemento minimal (con la contención como relación de orden). Un anillo R es noetheriano por la derecha si y solamente si cualquier colección no vacía de ideales a derecha tiene un elemento maximal (con la contención como relación de orden).*

Corolario 13. *Si R es un anillo artiniano por la derecha, para todo I ideal por la derecha de R no nulo existe J un ideal por la derecha minimal de R contenido en I. En particular, R tiene algún ideal por la derecha minimal.*

Corolario 14. *Si R es un anillo noetheriano por la derecha, para todo I ideal por la derecha de R distinto de R existe J un ideal por la derecha maximal de R que contiene a I. En particular, R tiene algún ideal por la derecha maximal.*

Procedemos a demostrar una proposición importante. Para su demostración nos hemos basado en el apartado 4 de [5].

Proposición 43. *Todo anillo semisimple por la derecha es artiniano y noetheriano por la derecha.*

Demostración. Sea R un anillo semisimple por la derecha. Por la proposción 34 existen $I_1, \ldots, I_k$ ideales por la derecha minimales de R con $R = I_1 \oplus \cdots \oplus I_k$, siendo I_i un R-submódulo simple de R_R $\forall i \in \{1, \ldots, k\}$.

Cada I_i es un submódulo no nulo de R_R, luego $R = I_1 \oplus \cdots \oplus I_k \supsetneq I_1 \oplus \cdots \oplus I_{k-1} \supsetneq I_1 \oplus \cdots \oplus I_{k-2} \supsetneq \cdots \supsetneq I_1 \supsetneq \{0\}$ es una cadena propia de submódulos de R_R. Además, por el Segundo Teorema de Isomorfía (teorema 3) $I_1 \oplus \cdots \oplus I_{q+1}/I_1 \oplus \cdots \oplus I_q \cong I_{q+1}$ $\forall q \in \{1, \ldots, k-1\}$. Entonces, como en R-módulos ser simple es propiedad estructural (proposición 25), tenemos que $I_1 \oplus \cdots \oplus I_{q+1}/I_1 \oplus \cdots \oplus I_q$ es simple $\forall q \in \{1, \ldots, k-1\}$, al ser I_q es simple. Además, $I_1/\{0\} \cong I_1$ es simple. Por tanto, la cadena es una serie de composición. La proposición 42 nos indica ahora que R_R es artiniano y noetheriano, luego R artiniano por la derecha y noetheriano por la derecha. □

Por último definimos los anillos artinianos y noetherianos por la izquierda como se hace en el apartado 3.2 de [5].

Definición 54. *Decimos que un anillo R es artiniano por la izquierda si R como R-módulo a izquierda es artiniano.*

Definición 55. *Decimos que un anillo R es noetheriano por la izquierda si R como R-módulo a izquierda es noetheriano.*

3. Anillos primos y semiprimos

Esta sección está basada en el apartado 10 de [6].

3.1. Anillos primos

Definición 56. *Sean R un anillo e $I \triangleleft R$. Decimos que I es un ideal primo si $I \neq R$ y para todo par A, B de ideales de R con $AB \subset I$ se tiene que $A \subset I$ o $B \subset I$.*

Ejemplo 25. *Sea I un ideal maximal de un anillo R. Sean A y B ideales de R no contenidos en I. Entonces, como I es maximal, $I + A = R = I + B$. Por ello, $R = RR = (I + A)(I + B) = \{\sum_{i=1}^{n}((x^i + a^i)(y^i + b^i)) : n \geq 1, x^i, y^i \in I, a^i \in A, b^i \in B\} = \{\sum_{i=1}^{n}(x^i y^i + a^i y^i + x^i b^i) + \sum_{i=1}^{n}(a^i b^i) : n \geq 1, x^i, y^i \in I, a^i \in A, b^i \in B\} = I + AB$, lo que indica que $AB \nsubseteq I$, al ser $I \neq R$. Vemos así que I es un ideal primo.*

Definición 57. *Sea R un anillo y sean I, J ideales de R (respecto ideales por la derecha/izquierda). Decimos que I y J son ortogonales si $IJ = \{0\}$.*

Definición 58. *Decimos que un anillo R es primo si $\{0\}$ es un ideal primo; es decir, si dos ideales solo pueden ser ortogonales si al menos uno de ellos es $\{0\}$.*

Ejemplo 26. *Todo anillo simple es primo, debido al ejemplo 25 aplicado al ideal maximal $\{0\}$.*

Proposición 44. *Sea R un anillo y sea $I \triangleleft R$ con $I \neq R$. Son equivalentes:*

1. *I es primo*
2. *dados $a, b \in I$, si $aRb \subset I$, entonces $a \in I$ o $b \in I$*
3. *para todo par A, B de ideales por la derecha de R con $AB \subset I$ se tiene que $A \subset I$ o $B \subset I$*
4. *para todo par A, B de ideales por la izquierda de R con $AB \subset I$ se tiene que $A \subset I$ o $B \subset I$*

Demostración.

1. $\implies$ 2.
Sean $a, b \in I$ con $aRb \in I$. Como I es un ideal, $RaRbR \subset I$, siendo $RaRbR = Ra(RR)bR = (RaR)(RbR)$ por ser R unitario. Como se ve en el ejemplo 8, RaR y RbR son ideales de R. Entonces $RaR \subset I$, en cuyo caso $a = 1a1 \in I$, o $RbR \subset I$, en cuyo caso $b = 1b1 \in I$.

2. $\implies$ 3.
Sean A y B ideales por la derecha de R con $AB \subset I$. Supongamos que $A \nsubseteq I$. Podemos entonces tomar $a \in A - I$. Sea $b \in B$. $aRb = (aR)b \subset AB \subset I$, luego $b \in I$, al ser $a \notin I$. Por tanto, si $A \nsubseteq I$, $B \subset I$.

2. $\Longrightarrow$ 4.
Sean A y B ideales por la izquierda de R con $AB \subset I$. Supongamos que $A \nsubseteq I$. Podemos entonces tomar $a \in A - I$. Sea $b \in B$. $aRb = a(Rb) \subset AB \subset I$, luego $b \in I$, al ser $a \notin I$. Por tanto, si $A \nsubseteq I$, $B \subset I$.

3., 4. $\Longrightarrow$ 1.
Se debe a que todo ideal es un ideal por la izquierda y un ideal por la derecha. □

Corolario 15. *Sea R un anillo. Son equivalentes:*

1. *R es primo*
2. *dados $a, b \in I$, si $aRb = \{0\}$, entonces $a = 0$ o $b = 0$*
3. *R no posee ideales por la derecha ortogonales no nulos*
4. *R no posee ideales por la izquierda ortogonales no nulos*

Observación 24. *En un anillo (unitario) conmutativo, dados $I \lhd R$, $a, b \in R$, tenemos que $aRb \subset I$ si y solamente si $ab \in I$. Por tanto, en un anillo (unitario) conmutativo R, un ideal I es primo si y solamente si $\forall a, b \in R$ con $ab \in I$ se verifica que $a \in I$ o $b \in I$.*

3.2. Anillos semiprimos

Definición 59. *Sean R un anillo e $I \lhd R$. Decimos que I es un ideal semiprimo si para todo $A \lhd R$ con $A^2 \subset I$ se tiene que $A \subset I$.*

Ejemplo 27. *Todo ideal primo es semiprimo.*

Proposición 45. *Sea R un anillo y sea $I \lhd R$ con $I \neq R$. Son equivalentes:*

1. *I es semiprimo*
2. *$\forall a \in I$, si $aRa \subset I$, entonces $a \in I$*
3. *para todo A ideal por la derecha de R con $A^2 \subset I$ se tiene que $A \subset I$*
4. *para todo A ideal por la izquierda de R con $A^2 \subset I$ se tiene que $A \subset I$*

Demostración.

1. $\Longrightarrow$ 2.
Sea $a \in I$ con $aRa \in I$. Como I es un ideal, $RaRaR \subset I$, siendo $RaRaR = Ra(RR)aR = (RaR)(RaR)$ por ser R unitario. Como se ve en el ejemplo 8, RaR es un ideal de R. Entonces $RaR \subset I$, luego $a = 1a1 \in I$.

2. $\Longrightarrow$ 3.
Sea A un ideal por la derecha de R con $A^2 \subset I$. Supongamos por reducción al absurdo que $A \nsubseteq I$. Podemos entonces tomar $a \in A - I$, siendo $aRa = (aR)a \subset A^2 \subset I$, luego $a \in I$. Llegamos así a contradicción.

2. $\Longrightarrow$ 4.
Sea A un ideal por la izquierda de R con $A^2 \subset I$. Supongamos por reducción al absurdo que $A \nsubseteq I$. Podemos entonces tomar $a \in A - I$, siendo $aRa = a(Ra) \subset A^2 \subset I$, luego $a \in I$. Llegamos así a contradicción.

3., 4. $\Longrightarrow$ 1.
Se debe a que todo ideal es un ideal por la derecha y un ideal por la izquierda. □

Definición 60. *Decimos que un anillo R es semiprimo si $\{0\}$ es un ideal semiprimo; es decir, si se tiene que el único $I \lhd R$ con $I^2 = \{0\}$ es $\{0\}$.*

Ejemplo 28. *Todo anillo primo es semiprimo.*

Definición 61. *Sean R un anillo e I un ideal de R (respecto ideal por la izquierda/derecha). Decimos que I es nilpotente si existe $n \geq 1$ con $I^n = \{0\}$. Al menor n tal que $I^n = \{0\}$ se le llama índice de nilpotencia de I.*

Proposición 46. *Sea R un anillo. Son equivalentes:*

1. *R es semiprimo*
2. *$\forall a \in I$, si $aRa = \{0\}$, entonces $a = 0$*
3. *R no posee ideales por la derecha nilpotentes no nulos*
4. *R no posee ideales por la izquierda nilpotentes no nulos*
5. *R no posee ideales nilpotentes no nulos*

Demostración.

1. $\Longleftrightarrow$ 2. es consecuencia directa de la propoción 45.

1. $\Longrightarrow$ 3. Sea I un ideal por la derecha de R nilpotente y sea n su índice de nilpotencia. Supongamos por reducción al absurdo que $n > 1$, siendo $n - 1$ un entero positivo menor que n. Si $n = 2$, $I^2 = \{0\}$, luego la proposición 45 nos indica que $I = \{0\}$, lo que entra en contradicción con que el índice de nilpotencia sea 2. Supongamos entonces que $n > 2$, siendo $2n - 2 > n$. En tal caso, como I es un ideal por la derecha de R, $(I^{n-1})^2 = I^{2n-2} \subset I^n = \{0\}$. La proposición 45 nos indica entonces que $I^{n-1} = \{0\}$, lo que entra en contradicción con la minimalidad de n. Por tanto, $n = 1$, siendo $I = \{0\}$.

1. $\Longrightarrow$ 4. Sea I un ideal por la izquierda de R nilpotente y sea n su índice de nilpotencia. Supongamos por reducción al absurdo que $n > 1$, siendo $n - 1$ un entero positivo menor que n. Si $n = 2$, $I^2 = \{0\}$, luego la proposición 45 nos indica que $I = \{0\}$, lo que entra en contradicción con que el índice de nilpotencia sea 2. Supongamos entonces que $n > 2$, siendo $2n - 2 > n$. En tal caso, como I es un ideal por la izquierda de R, $(I^{n-1})^2 = I^{2n-2} \subset I^n = \{0\}$. La proposición 45 nos indica entonces que $I^{n-1} = \{0\}$, lo que entra en contradicción con la minimalidad de n. Por tanto, $n = 1$, siendo $I = \{0\}$.

3., 4. $\Longrightarrow$ 5. Se debe a que todo ideal es un ideal por la derecha y un ideal por la izquierda.

5. $\Longrightarrow$ 1. Si I es un ideal de R con $I^2 = \{0\}$, I es nilpotente, luego $I = \{0\}$. □

Lema 6. *Sea R un anillo semisimple por la derecha. Sea I un ideal por la derecha de R. Entonces existe $e \in I$ un idempotente tal que $I = eR$.*

Demostración. Como R es semisimple por la derecha e $I \leq R_R$, I es un sumando directo, existiendo $K \leq R_R$ con $R = I \oplus K$. Entonces I y K son ideales por la derecha de R con $R = I \oplus K$, existiendo $e \in I$ y $k \in K$ con $1 = e + k$. Ahora, $e = 1e = e^2 + ke \in I \oplus K$, siendo $ke = e - e^2 \in I \cap K = \{0\}$, luego $e = e^2$.

Sea $z \in I$. $z = 1z = ez + kz \in I \oplus K$, siendo $kz = z - ez \in I \cap K = \{0\}$, luego $z = ez \in eR$. Vemos así que $I \subset eR$, siendo $eR \subset I$ por ser I ideal por la derecha. Por tanto, $I = eR$. □

Proposición 47. *Todo anillo semisimple por la derecha es semiprimo.*

Demostración. Sean R un anillo semisimple por la derecha e I un ideal por la derecha no nulo de R. Por el lema 6 existe $e \in I$ un idempotente tal que $I = eR$. Como I es no nulo, ha de ocurrir que $e \neq 0$. Ahora, $e = e^2 \in I^2$, luego I^2 es no nulo. Vemos así que R es semiprimo. □

A continuación damos dos resultados. El segundo se utilizará en la sección siguiente para demostrar que todo anillo semiprimo y artiniano por la derecha es semisimple por la derecha.

Lema 7 (Lema de Brauer)**.** *Sea I un ideal por la derecha minimal de un anillo R. Entonces o $I^2 = \{0\}$ o existe un idempotente $e \in I$ con $I = eR$.*

Demostración. Supongamos que $I^2 \neq \{0\}$. Entonces existe $y \in I$ con $yI \neq \{0\}$. Como yI es un ideal contenido en I e I es minimal, esto implica que $yI = I$. Entonces existe $e \in I$ con $ye = y$. Como $y \neq 0$, ha de ocurrir que $e \neq 0$, siendo $0 \neq e = e1 \in eR$. Ahora, como eR es un ideal de R contenido en I, que es minimal, ha de ocurrir que $eR = I$.

Consideramos $J = \{z \in I : yz = 0\}$. Este es un ideal por la derecha de R contenido en I. Véase que $\forall z_1, z_2 \in J$, $a \in R$, tenemos $y(z_1 + z_2) = yz_1 + yz_2 = 0$ e $y(z_1a) = (yz_1)a = 0a = 0$, siendo $z_1 + z_2, z_1a \in J$. Como $e \notin J$, se tiene que $J \neq I$, lo que nos indica que $J = \{0\}$. Ahora, $e^2 - e \in I$ y $y(e^2 - e) = (ye)e - ye = ye - ye = 0$, siendo $e^2 - e \in J = \{0\}$. Por tanto, e es un idempotente. □

Corolario 16. *Si I es un ideal por la derecha minimal de un anillo semiprimo R, entonces existe $e \in I$ un idempotente con $I = eR$.*

Demostración. Como $I \neq \{0\}$ y R es semiprimo, $I^2 \neq \{0\}$. Entonces, por el Lema de Brauer (lema 7), existe $e \in I$ un idempotente con $I = eR$. □

4. Teorema de Artin-Wedderburn

4.1. Clasificación de anillos simples

En esta subsección aparecen resultados basados en el apartado 4.2 de [1].

Lema 8. *Sea R un anillo. Entonces $R \cong End(R_R)$.*

Demostración. Dado $f \in End(R_R)$, se tiene que $f(r) = f(1r) = f(1)r \ \forall r \in R$, luego f queda definida por $f(1)$. Además, dado $a \in R$, la aplicación λ_a es un endomorfismo en R que verifica $f(1) = a$. Por tanto, $\phi : End(R_R) \to R$, $\phi(f) = f(1)$ biyectiva. Además, $\phi(f+g) = (f+g)(1) = f(1) + g(1) = \phi(f) + \phi(g)$ y $\phi(f \circ g) = (f \circ g)(1) = f(g(1)) = f(1g(1)) = f(1)g(1) = \phi(f)\phi(g) \ \forall f, g \in End(R_R)$. Asimismo, $\phi(id) = id(1) = 1$. Por tanto, ϕ es un isomorfismo de anillos. □

Lema 9. *Si R es un anillo semisimple por la derecha y primo, entonces todos los R-módulos simples son isomorfos.*

Demostración. Veamos primero que todos los submódulos simples de R_R son isomorfos.

Sean I y J submódulos simples de R_R. Podemos entonces tomar $y \in I - \{0\}$ y $z \in J - \{0\}$. Como R es primo, $yRz \neq \{0\}$, luego ha de existir $r \in R$ con $yrz \neq 0$.

Consideramos el homomorfismo de R-módulos λ_{yr}. Como $ya \in I \ \forall a \in R$, podemos restringir $\lambda_{yr} : J \to I$, siendo este un homomorfismo de R-módulos simples. Además, $\lambda_{yr}(z) \neq 0$, luego $\lambda_{yr} : J \to I$ es no nulo. Entonces, el Lema de Shur (lema 3) nos indica que $\lambda_{yr} : J \to I$ es un isomorfismo de R-módulos.

Veamos ahora que todo R-módulo es isomorfo a un submódulo simple de R_R.

Sea M un R-módulo simple. Entonces, según la proposición 26, existe L un ideal por la derecha maximal de R con $M \cong R_R/L$.

Ahora, como R es semisimple por la derecha y $L \leq R_R$, existe $I \leq R_R$ con $R_R = L \oplus I$. Entonces, según el Segundo Teorema de Isomorfía (teorema 3), $I \cong R_R/L \cong M$. Como en R-módulos ser simple es propiedad estructural (proposición 25), I es simple como R-módulo.

Por tanto, todo R-módulo es isomorfo a un submódulo simple de R_R. Entonces, como todos los submódulos simples de R_R son isomorfos, podemos concluir que todos los R-módulos son isomorfos. □

Lema 10. *Sea R un anillo. Sea I un ideal por la derecha minimal de R. Sea $a \in R$ tal que $aI \neq \{0\}$. Entonces aI es un ideal por la derecha minimal de R.*

Demostración. En el ejemplo 10 vimos que aI es un ideal por la derecha de R. Ahora, I y aI son submódulos de R_R. Consideramos $\lambda_a : R_R \to R_R$, que es un homomorfismo de R-módulos a derecha. Como $\lambda_a(I) = aI \neq \{0\}$, $\lambda_a|_I : I \to aI$ está bien definida, es

un epimorfismo y es no nula. Entonces $Ker(\lambda_a|_I)$ un submódulo de I distinto de I, luego $Ker(\lambda_a|_I) = \{0\}$, al ser I simple. Por tanto, $\lambda_a|_I$ un isomorfismo de R-módulos. Entonces, como ser simple es estructural (proposición 25), aI es un R-módulo simple. Por tanto, aI es un ideal por la derecha minimal de R. □

Teorema 4. *Sea R un anillo. Son equivalentes:*

1. *R es semisimple por la derecha y simple*
2. *R es semisimple por la derecha y primo*
3. *R es isomorfo a $M_n(D)$ un anillo de matrices sobre un anillo de división D.*
4. *R es artiniano por la derecha y simple*

Demostración.

1. $\Longrightarrow$ 2.
Se debe a que todo anillo simple es primo.

2. $\Longrightarrow$ 3.
Por la proposición 34, existen $N_1, \cdots, N_k$ ideales por la derecha minimales con $R = N_1 \oplus \cdots \oplus N_k$. Entonces, $R_R = N_1 \oplus \cdots \oplus N_k$ con N_i un R-submódulo simple de R_R $\forall i \in \{1, \ldots, k\}$.

Por el lema 9, todos los N_i son isomorfos. Dado $N = N_1$, por la proposición 23 se tiene que $R_R \cong N^n$. Entonces, por el lema 8 y la proposición 24, $R \cong End(R_R) \cong End((N^n)_R) \cong M_n(End(N_R))$, siendo $End(N_R)$ un anillo de división por el Lema de Shur (lema 3).

3. $\Longrightarrow$ 1.
El corolario 7 nos dice que $M_n(D)$ es un anillo simple y la proposición 36 nos dice que es semisimple por la derecha.

1. $\Longrightarrow$ 4.
Se debe a la proposición 43, que nos dice que todo anillo semisimple por la derecha es artiniano por la derecha.

4. $\Longrightarrow$ 1.
Veamos que $soc(R_R)$ es un ideal de R. Como $soc(R_R)$ es suma de submódulos de R_R, tenemos que $soc(R_R)$ es suma de ideales por la derecha de R, luego es un ideal por la derecha de R. Ahora, dado $a \in R$, $a\, soc(R_R) = a \sum_{I \leq R_R, I \text{ simple}} I \subset \sum_{I \leq R_R, I \text{ simple}} aI$. Por el lema 10, aI es ideal por la derecha minimal de R, es decir, un submódulo simple de R_R. Por tanto, $a\, soc(R_R) \subset \sum_{I \leq R_R, I \text{ simple}} aI \subset soc(R_R)$, luego $soc(R_R)$ es un ideal de R.

Como R_R es artiniano, el corolario 9 nos indica que R_R tiene algún submódulo simple. Por tanto, $soc(R_R) \neq \{0\}$. Entonces, como R es simple, $soc(R_R) = R$. Entonces, según la proposición 28, R es semisimple. □

Si hubiéramos trabajado con R-módulos a izquierda hubiéramos obtenido un resultado análogo al teorema 4. Uniéndolos obtenemos el teorema 5, que es una versión del teorema de Artin-Wedderburn.

Teorema 5 (Teorema de Artin-Wedderburn para Anillos Simples)**.** *Sea R un anillo. Son equivalentes:*

1. *R es artiniano por la derecha y simple*
2. *R es semisimple por la derecha y simple*
3. *R es semisimple por la derecha y primo*
4. *R es isomorfo a $M_n(D)$ un anillo de matrices sobre un anillo de división D.*
5. *R es artiniano por la izquierda y simple*
6. *R es semisimple por la izquierda y simple*
7. *R es semisimple por la izquierda y primo*

4.2. Clasificación de anillos semisimples

Primero demostraremos que un anillo es semisimple si y solo si es isomorfo al producto directo de anillos de matrices sobre anillos de división. Para ello nos basamos en la sección 4.2 de [1].

Comenzaremos definiendo una relación de equivalencia entre ideales por la derecha minimales de un anillo semiprimo. Tras ello, demostraremos que la suma en cada clase de equivalencia es un ideal minimal (luego un subanillo simple) y que estos ideales son ortogonales entre sí. En el teorema 6 demostraremos que todo anillo semisimple R se escribe como suma directa de algunos de estos ideales, lo que nos servirá para ver que R es isomorfo al producto directo de anillos simples. Solo quedará entonces utilizar el Teorema de Artin-Wedderburn para Anillos Simples (teorema 5) para obtener que todo anillo semisimple es isomorfo al producto directo de anillos de matrices sobre anillos de división.

Definición 62. *Sea R un anillo semiprimo por la derecha. Sean I y J dos ideales por la derecha minimales de R no nulos. Decimos que I y J están relacionados y escribimos $I \sim J$ si existe $y \in I$ con $yJ = I$.*

Observación 25. *Sea R un anillo semisimple por la derecha. Sean I y J dos ideales por la derecha minimales de R no nulos. Entonces $I \sim J$ si y solamente si existe $y \in I$ con $\lambda_y(J) = I$. En tal caso, $\lambda_y\,|_{J,I}\colon J \to I$ es un isomorfismo de R-módulos, debido al Lema de Shur (lema 3), pues es un homomorfismo entre R-módulos simples sobreyectivo, luego no nulo.*

Lema 11. *Sea R un anillo semiprimo por la derecha. Sean I y J dos ideales por la derecha minimales de R no nulos. Si $IJ \neq \{0\}$, entonces $I \sim J$.*

Demostración. Como $IJ \neq \{0\}$, existe $y \in I$ con $\lambda_y(J) = yJ \neq \{0\}$. Por el ejemplo 10, yJ es un ideal por la derecha de R. Además, yJ está contenido en I por ser $y \in I$ y ser I un ideal por la derecha de R. Entonces, por la minimalidad de I, $yJ = I$, luego $I \sim J$. □

Proposición 48. *Dado R un anillo semiprimo por la derecha, la relación definida en la definición 62 es una relación de equivalencia en el conjunto de ideales por la derecha minimales de R.*

Demostración. Veamos que se satisface la propiedad reflexiva. Sea I un ideal por la derecha minimal de R. Entonces, por la proposición 46, se tiene que $I^2 \neq \{0\}$. El lema 11 nos indica entonces que $I \sim I$.

Veamos que se satisface la propiedad transitiva. Sean $I \sim J$ y $J \sim K$. Entonces existen $y \in I$ y $z \in J$ con $I = yJ$ y $J = zK$, luego $I = yJ = y(zK) = (yz)K$, siendo $yz \in I$ por ser I un ideal por la derecha. Por tanto, $I \sim K$.

Veamos que se satisface la propiedad simétrica. Sea $I \sim J$. Entonces existe $y \in I$ con $yJ = I \neq \{0\}$. En concreto, existe $z \in J$ con $yz \neq 0$. Por la proposición 46, esto indica que $\{0\} \neq (yz)R(yz) = y(zRy)z$, luego $zRy \neq \{0\}$. Como J es un ideal por la derecha, $zR \subset J$, siendo $\{0\} \neq zRy \subset JI$. Entonces, por el lema 11, $J \sim I$. □

Proposición 49. *Sean R un anillo semiprimo por la derecha e I un ideal por la derecha minimal de R no nulo. Entonces $J \sim I$ si y solamente si $\exists a \in R$ con $J = aI \neq \{0\}$.*

Demostración. $\Longrightarrow$ Como $J \sim I$, existe $x \in J \subset R$ con $xI = J \neq \{0\}$.

$\Longleftarrow$ Por el lema 10, aI es un ideal por la derecha minimal de R. Como $aI \neq \{0\}$, la proposición 46 indica que $(aI)(aI) \neq \{0\}$, luego que $I(aI) \neq \{0\}$. Entonces, por el lema 11, $aI \sim I$. □

Definición 63. *Sea I un ideal por la derecha minimal de un anillo R. Definimos $S_I := \sum_{J \sim I} J$.*

Observación 26. *Sea I un ideal por la derecha minimal de un anillo R. Sea $\mathcal{F} = \{J$ ideal por la derecha minimal de $R : J \sim I\} = \{J$ submódulo simple de $R_R : J \sim I\}$. Entonces el R-módulo S_I es $\sum_{J \in \mathcal{F}} J$ (donde todo $J \in \mathcal{F}$ es simple). Por la proposición 28, esto implica que S_I es suma directa interna de un subconjunto de $\mathcal{F}$; es decir, existe $\mathcal{T} \subset \mathcal{F}$ con $S_I = \oplus_{J \in \mathcal{T}} J$.*

Proposición 50. *Sea R semiprimo y sea I un ideal por la derecha minimal de R. S_I es un ideal minimal. Consecuentemente, S_I es un subanillo simple de R.*

Demostración. Como es suma de ideales por la derecha de R, S_I es un ideal por la derecha de R. Veamos que es un ideal por la izquierda. Dado $a \in R$, $aS_I = a(\sum_{J \sim I} J) \subset \sum_{J \sim I} aJ$. Por la proposición 49, $aJ \sim J \ \forall J \sim I$. Por la proposición 48 la relación $\sim$ es de equivalencia, luego $aJ \sim I \ \forall J \sim I$. Entonces $aS_I \subset \sum_{J \sim I} aJ \subset \sum_{K \sim I} K = S_I$. Queda así probado que S_I es un ideal.

Veamos que S_I es minimal. Para ello veremos que, dado $x \in S_I - \{0\}$, el ideal generado por x coincide con S_I. Para ello veremos primero que $I \subset RxR$ y, después, que

$S_I = RIR$, siendo entonces $S_I \subset RxR$. Esto finalizará la demostración, pues, dado K un ideal de R no nulo contenido en S_I, podemos tomar $x \in K - \{0\} \subset S_I - \{0\}$, siendo $S_I = RxR \subset K \subset S_I$, luego $K = S_I$.

Tomamos $x \in S_I - \{0\}$. Como se ve en la observación 26, $S_I = \oplus_{J \in \mathcal{T}} J$ para un cierto $\mathcal{T} \subset \{J \text{ ideal por la derecha minimal de } R : J \sim I\}$. Entonces existen $K_1, \dots, K_n \in \mathcal{T}$ y $k_i \in K_i \ \forall i \in \{1, \dots, n\}$ tales que $x = k_1 + \cdots + k_n$. Como R es semiprimo, por la proposición 46, $\{0\} \neq xRx = (k_1 + \cdots + k_n)Rx$, luego ha de existir $s \in \{1, \dots, n\}$ con $k_s Rx \neq \{0\}$. Como K_s es un ideal por la derecha, $k_s Rx \in K_s \cap RxR$, siendo $K_s \cap RxR$ un ideal por la derecha contenido en K_s. Entonces, por la minimalidad de K_s, $K_s \cap RxR = K_s$, luego $K_s \subset RxR$. Como $I \sim K_s$, existe $u \in I$ con $I = uK_s$, siendo $I = uK_s \subset RxR$.

Por ser I ideal por la derecha y ser R unitario, $RIR = RI = \sum_{a \in R} aI$. Por la proposición 49, $\sum_{a \in R} aI = \sum_{J \sim I} J = S_I$. Vemos así que $RIR = S_I$. Como $I \subset RxR$, obtenemos que $S_I = RIR \subset RxR$, siendo $RxR \subset S_I$ por ser S_I un ideal. Por tanto, $RxR = S_I$. Finalizamos así la demostración. □

Proposición 51. *Sea R semiprimo. Sean I y K ideales por la derecha minimales de R no relacionados. Entonces $S_I S_K = \{0\}$.*

Demostración. Como S_I y S_K son ideales, $S_I S_K$ es un ideal contenido en S_I y S_K. Como estos son simples, si $S_I S_K \neq \{0\}$, ha de ocurrir que $S_I = S_I S_K = S_K$, luego $K \subset S_I$.

Como K e I no están relacionados, por el lema 11 se tiene que $KJ = \{0\}$ para todo $J \sim I$. Entonces, $KS_I = K \sum_{J \sim I} J \subset \sum_{J \cong I} KJ = \{0\}$. En particular, $KK = \{0\}$, lo que es una contradicción por ser R semiprimo (proposición 46). Por tanto, ha de ocurrir que $S_I S_K \neq \{0\}$. □

Teorema 6. *Un anillo R es semisimple por la derecha si y solamente si es isomorfo al producto directo $M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$ de un número finito de anillos de matrices sobre anillos de división $D_1, \cdots, D_s$.*

Demostración.

$\Longrightarrow$

Sea R un anillo semisimple. Por la proposición 34, $R = J_1 \oplus \cdots \oplus J_n$ con $J_1, \dots, J_n$ ideales por la derecha minimales de R.

Por la proposición 47, R es semiprimo, luego podemos considerar la relación de equivalencia de la definición 62. Podemos tomar $I_1, \dots, I_k$ representantes de las clases de isomorfía de los elementos de $\{J_1, \dots, J_n\}$. Entonces $R = S_{I_1} + \cdots + S_{I_k}$.

Veamos que la suma es directa. Sea $i \in \{1, \dots, k\}$. Consideramos el ideal $K_i = S_{I_i} \cap \sum_{j \neq i} S_{I_j}$. $(K_i)^2 \subset (S_{I_i})(\sum_{j \neq i} S_{I_j}) \subset \sum_{j \neq i} (S_{I_i} S_{I_j}) = \sum_{j \neq i} \{0\} = \{0\}$, donde hemos utilizado la proposición 51. Entonces, como R es semiprimo, $S_{I_i} \cap \sum_{j \neq i} S_{I_j} = K_i = \{0\}$.

Demostramos así que $R = S_{I_1} \oplus \cdots \oplus S_{I_k}$ donde los distintos I_i no están relacionados entre sí. Ahora, como $1 \in R$, existen unos únicos $e_i \in S_{I_i} \ \forall i \in \{1, \dots, k\}$ con $1 = e_1 + \cdots + e_k$.

Dado $i \in \{1, \ldots, k\}$, $\forall x \in S_{I_i}$ tenemos que $x = 1x = (e_1 + \cdots + e_k)x = e_1x + \cdots + e_kx = e_ix + 0 = e_ix$ y que $x = x1 = x(e_1 + \cdots + e_k) = xe_1 + \cdots + xe_k = xe_i + 0 = xe_i$, donde hemos usado que $e_jx = 0 = xe_j$ $\forall j \neq i$ por ser $S_{I_i}S_{I_j} = \{0\} = S_{I_j}S_{I_i}$.

Por tanto, e_i es una unidad de S_{I_i}. Ahora, $\forall i \in \{1, \ldots, k\}$ S_{I_i} es un ideal, luego un subanillo de R; entonces, al tener unidad, S_{I_i} tiene estructura de anillo unitario. Podemos entonces considerar el producto directo de estos anillos: $S_{I_1} \times \cdots \times S_{I_k}$.

Consideramos ahora $f : S_{I_1} \times \cdots \times S_{I_k} \to S_{I_1} \oplus \cdots \oplus S_{I_k}$, $f((s_1, \ldots, s_k)) = s_1 + \cdots + s_k$. Por la proposición 23, $S_{I_1} \oplus \cdots \oplus S_{I_k}$ puede verse como la suma directa interna de submódulos a derecha de R_R. Entonces por la proposición 18, cada elemento de $S_{I_1} \oplus \cdots \oplus S_{I_k}$ se escribe de forma única como $s_1 + \cdots + s_k$ con $s_i \in S_i$ $\forall i \in \{1, \ldots, k\}$. Esto implica que f es biyectiva.

Sean $(s_1, \ldots, s_k), (s'_1, \ldots, s'_k) \in S_{I_1} \times \cdots \times S_{I_k}$. Se tiene que $f((s_1, \ldots, s_k) + (s'_1, \ldots, s'_k)) = f((s_1 + s'_1, \ldots, s_k + s'_k)) = (s_1 + s'_1) + \cdots + (s_k + s'_k) = (s_1 + \cdots + s_k) + (s'_1 + \cdots + s'_k) = f((s_1, \ldots, s_k)) + f((s'_1, \ldots, s'_k))$.

Ahora, $(s_1 + \cdots + s_k)(s'_1 + \cdots + s'_k) = (s_1s'_1) + \cdots + (s_ks'_k)$ por ser $S_{I_i}S_{I_j} = \{0\}$ $\forall i \neq j$. Por tanto, $f((s_1, \ldots, s_k))f((s'_1, \ldots, s'_k)) = (s_1 + \cdots + s_k)(s'_1 + \cdots + s'_k) = (s_1s'_1) + \cdots + (s_ks'_k) = f((s_1s'_1, \ldots, s_ks'_k)) = f((s_1, \ldots, s_k)(s'_1, \ldots, s'_k))$.

Además, $f((e_1, \cdots, e_k)) = e_1 + \cdots + e_k = 1$. Queda así probado que f es un isomorfismo de anillos unitarios.

Por el Teorema de Artin-Wedderburn para Anillos Simples (teorema 5), $\forall i \in \{1, \ldots, n\}$ existen un natural n_i y un anillo de división D_i con $S_{I_i} \cong M_{n_i}(D_i)$. Tenemos entonces que $R \cong S_{I_1} \times \cdots \times S_{I_k} \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$.

$\Longleftarrow$
Por la proposición 36, cada $M_{n_i}(D_i)$ es semisimple por la derecha, siendo el producto directo $M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$ semisimple por la derecha por la proposición 38. Entonces, como ser semisimple es una propiedad estructural (proposición 35), R es semisimple por la derecha. □

A continuación demostramos que un anillo es semisimple por la derecha si y solo si es semiprimo y artiniano por la derecha. Una de las implicaciones se deduce de las proposiciones 47 y 43. Para demostrar la otra nos basamos en los teoremas 4.14 y 10.24 de [6] y utilizamos un lema que damos a continuación.

Lema 12. *Sea R un anillo y sea $e \in R$ un idempotente. Entonces $R = eR \oplus (1 - e)R$. Por tanto, eR es un sumando directo de R_R.*

Demostración. Vemos primero que $(1-e)e = e - e^2 = 0$ y $(1-e)(1-e) = (1-e) - (1-e)e = (1 - e) - 0 = (1 - e)$.

$\forall a \in R$, $a = a(e+1-e) = ae + a(1-e) \in eR + (1-e)R$. Por tanto, $R = eR + (1-e)R$.

Sea $a \in eR \cap (1-e)R$. Entonces existen $b, c \in R$ con $a = eb$ y $a = (1-e)c$. $ea = eeb = eb = a$ y $(1-e)a = (1-e)(1-e)c = (1-e)c = a$. Por tanto, $a = (1-e)a = (1-e)ea = 0a = 0$. Vemos así que $eR \cap (1-e)R = \{0\}$.

Ahora, eR y $(1-e)R$ son ideales por la derecha de R, luego submódulos de R_R, siendo además $R = eR \oplus (1-e)R$. Por tanto, eR es un sumando directo de R_R. □

Teorema 7. *Sea R un anillo. son equivalentes:*

1. *R es semiprimo y artiniano por la derecha.*

2. *R es semisimple por la derecha.*

Demostración.

1. $\Longrightarrow$ 2.
Supongamos por reducción al absurdo que R no es semisimple por la derecha. Entonces, por la proposición 34, no se puede escribir como suma directa de ideales por la derecha minimales.

Como R es artiniano por la derecha, según el corolario 13, existe I_1 un ideal por la derecha minimal de R. Como R es semiprimo, el corolario 16 nos indica que existe $e_1 \in I_1$ un idempotente con $I_1 = e_1R$. Por el lema 12, $R = I_1 \oplus J_1$ con $J_1 = (1-e_1)R$ un ideal por la derecha de R.

Si $J_1 = \{0\}$, $R = I_1$ sería suma directa de ideales por la derecha minimales. Por tanto, $J_1 \neq \{0\}$.

Por el corolario 13 existe I_2 un ideal minimal de R con $I_2 \subset J_1$. Nuevamente, la proposición 6 nos indica que existe $e_2 \in I_2$ un idempotente con $I_2 = e_2R$. Por el lema 12, $A_2 = (1-e_2)R$ es un ideal por la derecha de R con $R = I_2 \oplus A_2$, siendo $J_1 = I_2 \oplus J_2$ con $J_2 = J_1 \cap A_2$. Como $I_2 \neq \{0\}$, $J_1 \supsetneq J_2$.

Si $J_2 = \{0\}$, $R = I_1 \oplus I_2$ sería suma directa de ideales por la derecha minimales. Por tanto, $J_2 \neq \{0\}$.

Continuando este proceso obtenemos una cadena descendente de ideales por la derecha: $J_1 \supsetneq J_2 \supsetneq J_3 \supsetneq \cdots \supsetneq J_n \supsetneq J_{n+1} \supsetneq \cdots$. Esto entra en contradicción con que R sea artiniano por la derecha.

2. $\Longrightarrow$ 1.
La proposición 47 nos dice que R es semiprimo y la proposición 43 nos dice que R es artiniano. □

Trabajando con R-módulos a izquierda en vez de con R-módulos a derecha se obtienen teoremas análogos a los teoremas 6 y 7. Esto puede verse recogido en el "Structure Theorem for Semi-Primitive Artinian Rings" de la sección 4.4 de [5]. Uniendo dichos resultados a los teoremas 6 y 7 obtenemos el Teorema de Artin-Wedderburn:

Teorema 8 (Teorema de Artin-Wedderburn)**.** *Sea R un anillo. Son equivalentes:*

1. *R es semisimple por la derecha.*
2. *R es semiprimo y artiniano por la derecha.*
3. *R es isomorfo al producto directo $M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$ de un número finito de anillos de matrices sobre anillos de división $D_1, \cdots, D_s$.*
4. *R es semisimple por la izquierda.*
5. *R es semiprimo y artiniano por la izquierda.*

Observación 27. *El Teorema de Artin-Wedderburn (teorema 8) nos indica que las nociones de anillo semisimple por la derecha y por la izquierda son equivalentes. Por tanto, hablaremos de anillos semisimples.*

Capítulo 3

Teorema de Densidad de Jacobson

1. Anillos primitivos

Ahora estudiaremos las nociones de R-módulo fiel y de anillo primitivo por la derecha. Para ello nos basamos en los apartados 10.3 de [2] y 4.1 de [5].

Definición 64. *Sea R un anillo y sea M un R-módulo. Decimos que M es fiel si $\forall a \in R$ con $a \neq 0$ se tiene que $Ma \neq \{0\}$.*

Definición 65. *Sea M un R-módulo. Definimos $ann(M_R) = \{a \in R : Ma = 0\}$*

Observación 28. *Un R-módulo M es fiel si y solamente si $ann(M_R) = \{0\}$.*

Proposición 52. *Si M_1 y M_2 son dos R-módulos isomorfos, $ann((M_1)_R) = ann((M_2)_R)$*

Demostración. Sean M_1 y M_2 dos R-módulos isomorfos. Sea f un isomorfismo de R-módulos entre M_1 y M_2. Si $a \in ann((M_1)_R)$, tenemos que $(M_1)a = \{0\}$. Ahora, como f es sobreyectiva, $\forall m \in M_2$ existe $n \in M_1$ con $m = f(n)$, siendo $ma = f(n)a = f(na) = f(0) = 0$. Por tanto, $(M_2)a = \{0\}$, siendo $a \in ann((M_2)_R)$. Por ello $ann((M_1)_R) \subset ann((M_2)_R)$. Considerando ahora f^{-1} obtenemos $ann((M_2)_R) \subset ann((M_1)_R)$. □

Corolario 17. *Ser fiel es propiedad estructural en R-módulos.*

Definición 66. *Decimos que un anillo R es primitivo por la derecha si existe un R-módulo simple y fiel.*

Definición 67. *Sea R un anillo y sea I un ideal por la derecha de R. Definimos $(I : R) = \{a \in R : Ra \subset I\}$.*

Lema 13. *Dados R un anillo e I un ideal por la derecha de R, $(I : R)$ es un ideal de R contenido en I tal que, si J es un ideal por la izquierda de R contenido en I, se tiene que $J \subset (I : R)$. Podemos entonces considerar que $(I : R)$ es el mayor ideal de R contenido en I.*

Demostración. Dados $a, b \in (I : R)$, se tiene que $Ra, Rb \subset I$, luego $R(a+b) \subset Ra + Rb \subset I$, siendo $a + b \in (I : R)$.

Ahora, dados $a \in (I : R)$ y $r \in R$, $R(ar) = (Ra)r \subset Ir \subset I$ por ser I ideal por la derecha; por tanto, $ar \in (I : R)$. Asimismo, $R(ra) = (Rr)a \subset Ra \subset I$, luego $ar \in (I : R)$.

Entonces, el corolario 2 indica que $(I : R)$ es un ideal de R. Además, tenemos que $a = a1 \in aR \subset I \ \forall a \in (I : R)$, luego $(I : R) \subset I$.

Sea J un ideal por la izquierda de R contenido en I. Entonces, $\forall x \in J$, $Rx \subset J \subset I$, luego $x \in (I : R)$. Por tanto, $J \subset (I : R)$. □

Observación 29. *Sean R un anillo e I un ideal por la derecha de R. Consideramos el R-módulo $M = R_R/I$. Entonces se tiene que $ann(M_R) = \{a \in R : Ma = \{0\}\} = \{a \in R : \overline{r}a = \overline{0} \ \forall r \in R\} = \{a \in R : ra \in I \ \forall r \in R\} = \{a \in R : Ra \subset I\} = (I : R)$.*

Proposición 53. *Un anillo R es primitivo por la derecha si y solamente si existe un ideal por la derecha maximal de R que no contiene a ningún ideal no nulo de R.*

Demostración. $\Longrightarrow$ Si R es primitivo por la derecha, existe M un R-módulo simple y fiel. Como M es simple, la proposición 26 indica que existe L un ideal por la derecha maximal de R con $M \cong R_R/L$. Además, la proposición 52 indica que, como M es fiel, $ann((R_R/L)_R) = ann(M_R) = \{0\}$, siendo $(L : R) = ann((R_R/L)_R) = \{0\}$. Entonces, por el lema 13, L no contiene a ningún ideal no nulo de R.

$\Longleftarrow$
Supongamos que I es un ideal por la derecha maximal de R que no contiene a ningún ideal no nulo de R. Por la proposición 26, R_R/I es simple. Además, $ann((_RR/I)_R) = (I : R) = \{0\}$, luego $_RR/I$ es fiel. Es decir, R_R/I es un R-módulo simple y fiel. Por tanto, R es primitivo por la derecha. □

Observación 30. *La proposición 53 nos da una caracterización intrínseca del carácter primitivo.*

Proposición 54. *La propiedad de ser primitivo por la derecha es estructural.*

Demostración. Sean R y R' dos anillos con R primitivo por la derecha. Sea $f : R \to R'$ un isomorfismo de anillos. Por la proposición 53 existe I un ideal por la derecha maximal de R que no contiene a ningún ideal no nulo de R. Por la proposición 6, $f(I)$ es un ideal por la derecha de R'.

Sea I' un ideal por la derecha de R' con $f(I) \subset I'$. Entonces $I \subset f^{-1}(I')$ y, siendo $f^{-1}(I')$ un ideal por la derecha de R por la proposición 6. Como I es maximal, o $f^{-1}(I') = I$, en cuyo caso $I' = f(I)$, o $f^{-1}(I') = R$, en cuyo caso $I' = f(R) = R'$. Vemos así que $f(I)$ es un ideal por la derecha maximal de R'.

Sea J un ideal de R' contenido en $f(I)$. Entonces $f^{-1}(J) \subset I$. $f^{-1}(J)$ es un ideal de R por la proposición 6. Ha de ocurrir entonces que $f^{-1}(J) = \{0\}$, luego $J = f(\{0\}) = \{0\}$.

Es decir, $f(I)$ es un ideal por la derecha de R' que no contiene ningún ideal no nulo de R'. La proposición 53 nos indica entonces que R' es primitivo. □

Utilizamos ahora resultados obtenidos de los apartados 10 de [6] y 4.1 de [5] para relacionar a los anillos primitivos por la derecha con otros tipos de anillos previamente estudiados.

Corolario 18. *Todo anillo simple es primitivo por la derecha.*

Demostración. Sea $\mathcal{F} = \{I \text{ ideal por la derecha de } R : I \neq R\}$. Sea $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ una cadena de elementos de $\mathcal{F}$. Consideramos $J = \bigcup_{i\in\mathbb{N}} I_i$. Sean x, y in J Entonces existen $i_x, i_y \in \mathbb{N}$ con $x \in I_{i_x}$, $y \in I_{i_y}$. Sea $j = \text{máx}(i_x, i_y)$. Entonces $x, y \in I_j$, luego $x+y \in I_j \subset J$. Además, dado $a \in R$, $xa \in I_{i_x} \subset J$. Entonces J es un ideal por la derecha de R. Además, si $1 \in J$, entonces $\exists i \in I$ con $1 \in I_i$, luego $a = 1a \in I_i$ $\forall a \in R$, lo que es una contradicción por ser $I_i \neq R$. Por tanto, $1 \notin J$, lo que indica que $J \in \mathcal{F}$, siendo J una cota superior de la cadena en $\mathcal{F}$ respecto al orden $\subset$.

Vemos así que $(\mathcal{F}, \subset)$ es un conjunto inductivo. Entonces, por el lema de Zorn, $\mathcal{F}$ tiene un elemento maximal I, que será un ideal por la derecha maximal de R. Como R es un anillo simple e $I \neq R$, I no contiene ideales no nulos. La proposición 53 nos indica entonces que R es primitivo por la derecha. □

Corolario 19. *Sea R un anillo conmutativo. Entonces R es primitivo por la derecha si y solamente si es un cuerpo.*

Demostración. Por el corolario 6, R es un cuerpo si y solo es simple. Entonces, si R es un cuerpo, es simple, luego el corolario 18 nos dice que R es primitivo por la derecha. Supongamos ahora que R es un primitivo por la derecha. En tal caso, por la proposición 53 existe I un ideal por la derecha maximal de R que no contiene a ningún ideal de R. Como R es conmutativo, I es un ideal de R, luego $I = \{0\}$, siendo $\{0\}$ un ideal por la derecha maximal. Entonces, dado $J \triangleleft R$, como J es un ideal por la derecha de R, ha de ocurrir o que $J \neq \{0\}$ o que $J = R$. Vemos así que R es simple, luego un cuerpo. □

Observación 31. *Sean M un R-módulo e I un ideal por la derecha de R. Entonces $MI := \{m_1y_1 + \cdots + m_ky_k : k \geq 1, m_i \in M, y_i \in I \ \forall i = 1, \ldots, k\}$ es un submódulo de M. Véase que la suma es una operación interna y que, dados $a \in R$ y $n \in MI$, existen $k \geq 1$, $m_i \in M$ e $y_i \in I$ $\forall i = 1, \ldots, k$ con $n = m_1y_1 + \cdots + m_ky_k$, siendo $na = m_1(y_1a) + \cdots + m_k(y_ka) \in MI$ al ser $y_ia \in I$ $\forall i = 1, \ldots, k$.*

Proposición 55. *Todo anillo primitivo por la derecha es primo.*

Demostración. Sea R un anillo primitivo por la derecha. Entonces existe un R-módulo M simple y fiel. Sean I y J dos ideales no nulos de R. Como M es fiel, MI es un submódulo no nulo de M. Entonces, como M es simple, $MI = M$. Análogamente, $MJ = M$. Tenemos ahora que $M(IJ) = (MI)J = MJ = M$, lo que implica que $IJ \neq \{0\}$. Por tanto, R es primo. □

Proposición 56. *Sea R un anillo primo que contiene un ideal por la derecha minimal. Entonces R es primitivo por la derecha.*

Demostración. Sea I un ideal por la derecha minimal. Entonces I es un R-submódulo de R_R que es simple como R-módulo. Veamos que es fiel. Sea $r \in R$ con $Ir = \{0\}$. Entonces $I(Rr) = (IR)r \subset Ir = \{0\}$, siendo I y Rr ideales por la derecha con $I(Rr) = \{0\}$. Como I es no nulo, el corolario 15 nos dice que $Rr = \{0\}$, luego $r = 1r = 0$. □

Corolario 20. *Sea R un anillo primo y artiniano por la derecha. Entonces R es primitivo por la derecha.*

Demostración. Por el corolario 13, R tiene un ideal por la derecha minimal. Entonces, por la proposición 56, R es primitivo. □

Podemos también definir a los R-módulos a izquierda fieles y a los anillos primitivos por la izquierda, tal como se hace en el apartado 4.1 de [5].

Definición 68. *Sea R un anillo y sea M un R-módulo a izquierda. Decimos que M es fiel si $\forall a \in R$ con $a \neq 0$ se tiene que $aM \neq \{0\}$.*

Definición 69. *Decimos que un anillo R es primitivo por la izquierda si existe un R-módulo a izquierda simple y fiel.*

2. Teorema de Densidad de Jacobson

Primero veremos que todo R-módulo M tiene estructura de $End(M_R)$-R-bimódulo, tal y como se hace en el apartado 3.8 de [5].

Definición 70. *Sean R y S anillos. Un S-R-bimódulo es un grupo abeliano $(M, +)$ junto con dos operaciones externas $M \times R \to M$, $(m, r) \to mr$, y $S \times M \to M$, $(s, m) \to sm$, tales que:*

- *$M \times R \to M$, $(m, r) \to mr$, dota a M de estructura de R-módulo*
- *$S \times M \to M$, $(s, m) \to sm$, dota a M de estructura de S-módulo a izquierda*
- *$s(mr) = (sm)r$ $\forall s \in S, m \in M, r \in R$*

Proposición 57. *Sean R un anillo y M un R-módulo. Dado $R' = End(M_R)$, M es un R'-módulo a izquierda con la operación externa $R' \times M \to M$, $f \cdot m = f(m)$.*

Sean R un anillo y M un R-módulo a izquierda. Dado $R' = End({}_RM)$, M es un R'-módulo a izquierda con la operación externa $R' \times M \to M$, $f \cdot m = f(m)$.

Demostración. Sean R un anillo, M un R-módulo y $R' = End(M_R)$. M es un grupo abeliano por definición. Sean $f, g \in R'$ y $m, n \in M$. Entonces $f \cdot (m + n) = f(m + n) = f(m) + f(n) = f \cdot m + f \cdot n$, $(f + g) \cdot m = (f + g)(m) = f(m) + g(m) = f \cdot m + g \cdot m$, $(f \circ g) \cdot m = (f \circ g)(m) = f(g(m)) = f(gm) = f \cdot (gm)$ y $id \cdot m = id(m) = m$. Por tanto, M es un R'-módulo.

Sean R un anillo, M un R-módulo a izquierda y $R' = End({}_RM)$. M es un grupo abeliano por definición. Sean $f, g \in R'$ y $m, n \in M$. Entonces $f \cdot (m + n) = f(m + n) = f(m) + f(n) = f \cdot m + f \cdot n$, $(f + g) \cdot m = (f + g)(m) = f(m) + g(m) = f \cdot m + g \cdot m$, $(f \circ g) \cdot m = (f \circ g)(m) = f(g(m)) = f(gm) = f \cdot (gm)$ y $id \cdot m = id(m) = m$. Por tanto, M es un R'-módulo. □

Corolario 21. *Sean R un anillo y M un R-módulo. Dados $R' = End(M_R)$ y $R'' = End({}_{R'}M)$, M es un R''-módulo a izquierda con la operación externa $R'' \times M \to M$, $f \cdot m = f(m)$.*

Demostración. Por la proposición 57, M es un R'-módulo a izquierda. Entonces, la proposición 57 aplicado a M como R'-módulo a izquierda concluye la demostración. □

Proposición 58. *Sean R un anillo y M un R-módulo. Sea $R' = End(M_R)$ Entonces, M es un R'-R-bimódulo.*

Demostración. Por definición, M es un R-módulo. Por la proposición 57, M es un R'-módulo a izquierda. Además, $\forall f \in R', m \in M, r \in R$, tenemos que $f(mr) = f(m)r = (fm)r$ por ser $f \in End(M_R)$. □

Nos basamos ahora en la sección 4.3 de [5] para demostrar el Teorema de Densidad para Módulos Semisimples.

Lema 14. *Sean R un anillo y M un R-módulo. Consideramos $R' = End(M_R)$ y $R'' = End({}_{R'}M)$. Entonces, $\forall f \in R''$ se tiene que la aplicación $\phi : M^n \to M^n$, $\phi((m_1, \ldots, m_n)) = (f(m_1), \ldots, f(m_n))$, es un homomorfismo en M^n considerado como $End((M^n)_R)$-módulo a izquierda (con la estructura dada por la proposición 57).*

Demostración. Para todo $(m_1, \ldots, m_n), (m'_1, \ldots, m'_n) \in M^n$ se tiene que $\phi((m_1, \ldots, m_n) + (m'_1, \ldots, m'_n)) = \phi((m_1 + m'_1, \ldots, m_n + m'_n)) = (f(m_1 + m'_1), \ldots, f(m_n + m'_n)) = (f(m_1) + f(m'_1), \ldots, f(m_n) + f(m'_n)) = (f(m_1), \ldots, f(m_n)) + (f(m'_1), \ldots, f(m'_n)) = \phi((m_1, \ldots, m_n)) + \phi((m'_1, \ldots, m'_n))$.

Sean $(m_1, \ldots, m_n) \in M^n$ y $\varphi \in End((M^n)_R)$. Veamos que $\phi(\varphi \cdot (m_1, \ldots, m_n)) = \varphi \cdot \phi((m_1, \ldots, m_n))$. Por la proposición 24, existen $a_{ij} \in R'$, $i, j \in \{1, \ldots, n\}$, con $\varphi((m'_1, \ldots, m'_n)) = (\sum_{j=1}^n a_{1i}(m'_i), \ldots, \sum_{j=1}^n a_{ni}(m'_i))$ $\forall (m'_1, \ldots, m'_n) \in M^n$. Entonces $\phi(\varphi \cdot (m_1, \ldots, m_n)) = \phi(\varphi((m_1, \ldots, m_n))) = \phi((\sum_{j=1}^n a_{1i}(m_i), \ldots, \sum_{j=1}^n a_{ni}(m_i))) = (f(\sum_{j=1}^n a_{1i}(m_i)), \ldots, f(\sum_{j=1}^n a_{ni}(m_i))) = (\sum_{j=1}^n f(a_{1i} \cdot m_i), \ldots, \sum_{j=1}^n f(a_{ni} \cdot m_i))$. Ahora, como $f \in End({}_{R'}M)$, $(\sum_{j=1}^n f(a_{1i} \cdot m_i), \ldots, \sum_{j=1}^n f(a_{ni} \cdot m_i)) = (\sum_{j=1}^n a_{1i} \cdot f(m_i), \ldots, \sum_{j=1}^n a_{ni} \cdot f(m_i)) = \varphi((f(m_1), \ldots, f(m_n))) = \varphi \cdot \phi((m_1, \ldots, m_n))$. Concluimos así que $\phi(\varphi \cdot (m_1, \ldots, m_n)) = \varphi \cdot \phi((m_1, \ldots, m_n))$. □

Lema 15. *Sean R un anillo y M un R-módulo semisimple. Consideramos $R' = End(M_R)$ y $R'' = End({}_{R'}M)$. Por el corolario 21, M es un R''-módulo a izquierda. Se tiene que todo R-submódulo de M es un R''-submódulo a izquierda de M.*

Demostración. Sea N un R-submódulo de M. Entonces $n_1 + n_2 \in N$ $\forall n_1, n_2 \in N$. Veamos ahora que, $f \cdot n \in N$ $\forall f \in R'', n \in N$. Como M es semisimple como R-módulo, existe N' un R-submódulo de M con $M = N \oplus N'$. Consideramos π la proyección sobre N. Como se dice en la definición 37, $\pi \in R'$. Ahora, dados $f \in R''$ y $n \in N$, $f \cdot n = f(n) = f(\pi(n)) = f(\pi \cdot n)$ con $\pi \cdot n$ la operación externa en M dada por la proposición 57, que dota a M de estructura de R'-módulo a izquierda. Por último, como $f \in End({}_{R'}M)$ y $\pi \in R'$, concluimos que $f \cdot n = f(\pi \cdot n) = \pi \cdot f(n) = \pi(f(n)) \in N$. □

Teorema 9 (Teorema de Densidad para Módulos Semisimples)**.** *Sea M un R-módulo semisimple. Consideramos $R' = End(M_R)$ y $R'' = End({}_{R'}M)$. Sea $\{m_1, \dots, m_n\}$ un subconjunto finito de M y sea $f \in R''$. Entonces existe $r \in R$ con $m_i r = f(m_i)$ $\forall i \in \{1, \dots, n\}$.*

Demostración. Supongamos primero que $n = 1$. Consideramos $N = m_1 R$, que es un R-submódulo de M. Entonces, por el lema 15, N es un R''-submódulo a izquierda de M, siendo $f(m_1) = f \cdot m_1 \in N = m_1 R$. Por tanto, existe $r \in R$ con $m_1 r = f(m_1)$.

Sea n arbitrario. Por la proposición 30, M^n es semisimple. Por el lema 14, la aplicación $\phi : M^n \to M^n, \phi((m_1, \dots, m_n)) = (f(m_1), \dots, f(m_n))$, es tal que $\phi \in End_{End((M^n)_R)}(M^n)$. Además, $(m_1, \dots, m_n) \in M^n$. Entonces, utilizando el resultado para $n = 1$ sobre M^n obtenemos que existe $r \in R$ con $(m_1, \dots, m_n)r = \phi((m_1, \dots, m_n)) = (f(m_1), \dots, f(m_n))$. Por tanto, $m_i r = f(m_i)$ $\forall i \in \{1, \dots, n\}$. □

Por último, utilizamos la sección 4.3 de [5] y los apartados 10.2 y 10.3 de [2] para demostrar el Teorema de Densidad de Jacobson, también conocido como el Teorema de Densidad para Anillos Primitivos por la Derecha.

Definición 71. *Sea M un espacio vectorial (a izquierda) sobre un anillo de división Δ, es decir, un Δ-módulo a izquierda con Δ un anillo de división. Sea $S \leq End({}_{\Delta}M)$. Decimos que S es denso en M si $\forall x_1, \dots, x_n \in M$ linealmente independientes e $y_1, \dots, y_n \in M$ existe $f \in S$ con $f(x_i) = y_i$ $\forall i \in \{1, \dots, n\}$.*

Observación 32. *Sea V un espacio vectorial (a izquierda) sobre un anillo de división Δ. En V existen bases y tenemos un teorema de ampliación de la base y un teorema que indica que, dados $\{x_i\}_{i \in I}$ una base de V e $\{y_i\}_{i \in I} \subset V$, existe un único $f \in End({}_{\Delta}V)$ con $f(x_i) = y_i$ $\forall i \in I$. Destacamos que estos resultados son mencionados en la demostración del "Density Theorem for Primitive Rings" del apartado 4.3 de [5].*

Teorema 10 (Teorema de Densidad de Jacobson)**.** *Sea R un anillo. R es primitivo por la derecha si y solamente si R es isomorfo a un subanillo denso de $(End({}_{\Delta}M))^{op}$ con M un espacio vectorial (a izquierda) no nulo sobre un anillo de división Δ.*

Demostración.
$\Longrightarrow$
Sea R primitivo por la derecha. Entonces existe M un R-módulo simple y fiel. Como M es simple, M es no nulo y el Lema de Shur (lema 3) nos dice que $\Delta = End(M_R)$ es un anillo de división. Por la proposición 57, M es un Δ-módulo a izquierda, es decir, un espacio vectorial (a izquierda) sobre el anillo de división Δ.

Sea $a \in R$. Definimos σ_a como la aplicación $\sigma_a : M \to M$, $\sigma_a(m) = ma$. Esta es un homomorfismo de Δ-módulos a izquierda, pues $\sigma_a(m_1 + m_2) = (m_1 + m_2)a = m_1 a + m_2 a = \sigma_a(m_1) + \sigma_a(m_2)$ $\forall m_1, m_2 \in M$ y $\sigma_a(f \cdot m) = (f \cdot m)a = f(m)a = f(ma) = f(\sigma_a(m)) = f \cdot \sigma_a(m)$ $\forall m \in M, f \in \Delta$.

Consideramos entonces $\rho : R \to (End({}_{\Delta}M))^{op}$, $\rho(a) = \sigma_a$. Ahora, dados $a, b \in R$, se tiene que $\forall m \in M$ $\sigma_{a+b}(m) = m(a+b) = ma + mb = \sigma_a(m) + \sigma_b(m) = (\sigma_a + \sigma_b)(m)$, luego $\rho(a + b) = \sigma_{a+b} = \sigma_a + \sigma_b = \rho(a) + \rho(b)$. Además, $\forall m \in M$, $\sigma_{ab}(m) = m(ab) = (ma)b = \sigma_b(\sigma_a(m)) = (\sigma_b \circ \sigma_a)(m) = (\sigma_a \circ_{op} \sigma_b)(m)$, luego $\rho(ab) = \sigma_{ab} = \sigma_a \circ_{op} \sigma_b = \rho(a) \circ_{op} \rho(b)$.

Vemos así que ρ es un homomorfismo de anillos.

Sean $a, b \in R$ con $\rho(a) = \rho(b)$. Entonces $\rho(a-b) = \rho(a) - \rho(b)$ es nulo, luego $\sigma_{a-b} : M \to M$, $\sigma_{a-b}(m) = m(a-b)$, es el homomorfismo nulo, siendo $m(a-b) = 0$ $\forall m \in M$. Como M es fiel y $M(a-b) = \{0\}$, ha de ocurrir que $a - b = 0$, es decir, que $a = b$. Vemos así que ρ es un monomorfismo. Por tanto, R es isomorfo a $\rho(R)$, que es un subanillo de $(End({}_\Delta M))^{op}$ por la proposición 5.

Consideramos ahora M como espacio vectorial (a izquierda) sobre el anillo de división Δ. Utilizaremos los resultados mencionados en la observación 32 para demostrar que $\rho(R)$ es denso en M. Sean $x_1, \ldots, x_n \in M$ linealmente independientes e $y_1, \ldots, y_n \in M$. Como $\{x_1, \ldots, x_n\}$ es linealmente independiente, podemos ampliarlo a una base de M. Podemos entonces tomar $f \in End({}_\Delta M)$ con $f(x_i) = y_i$ $\forall i \in \{1, \ldots, n\}$. Por el corolario 5, M es semisimple como R-módulo, luego, según Teorema de Densidad para Módulos Semisimples (teorema 9), existe $a \in R$ con $x_i a = f(x_i) = y_i$ $\forall i \in \{1, \ldots, n\}$. Entonces, $\sigma_a \in \rho(R)$ es tal que $\sigma_a(x_i) = y_i$ $\forall i \in \{1, \ldots, n\}$. Vemos así que $\rho(R)$ es denso en M.

$\Longleftarrow$
Sea S un subanillo denso de $(End({}_\Delta M))^{op}$ con M un espacio vectorial (a izquierda) no nulo sobre un anillo de división Δ.

Por la proposición 57, M es un $End({}_\Delta M)$-módulo a izquierda con la operación externa $End({}_\Delta M) \times M \to M$, $fm = f(m)$. Entonces, por la proposición 7, M es un $(End({}_\Delta M))^{op}$-módulo con la operación externa $M \times (End({}_\Delta M))^{op} \to M$, $m \cdot f = fm = f(m)$. Por tanto, M es un S-módulo con la operación externa $M \times S \to M$, $m \cdot f = fm = f(m)$.

Veamos que M es simple y fiel como S-módulo. Sea $m \in M - \{0\}$. Como S es denso en M, $\forall n \in M$ $\exists f \in S$ con $n = f(m) = m \cdot f$. Por tanto, $m \cdot S = M$. Dado $f \in S$, si $\{0\} = Mf = f(M)$, entonces ha de ocurrir que f sea nula; por tanto, M es fiel como S-módulo. Además, dado N un S-submódulo de M no nulo, podemos tomar $m \in N - \{0\}$, siendo $M = m \cdot S \subset N$, luego $N = M$; esto indica que M es simple como S-módulo.

Tenemos entonces que S es un anillo primitivo por la derecha. Además, según la proposición 54 la propiedad de ser primitivo por la derecha es estructural, luego si R es un anillo isomorfo a S, entonces R es primitivo por la derecha. □

Trabajando con R-módulos a izquierda en vez de con R-módulos a derecha se obtienen el teorema siguiente:

Teorema 11 (Teorema de Densidad de Jacobson para anillos primitivos por la izquierda)**.** *Sea R un anillo. R es primitivo por la izquierda si y solamente si R es isomorfo a un subanillo denso de $End({}_\Delta M)$ con M un espacio vectorial sobre un anillo de división Δ.*

Bibliografía

[1] A. J. Berrick and M. E. Keating. *An introduction to rings and modules with K-theory in view*, volume 65 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2000.

[2] P.M. Cohn. *Algebra*, volume 3. Wiley, second edition, 1991.

[3] Pierre Antoine Grillet. *Abstract algebra*, volume 242 of Graduate Texts in Mathematics. Springer, second edition, 2007.

[4] Nathan Jacobson. *Basic algebra*. Number I. W. H. Freeman and Company, second edition, 1985.

[5] Nathan Jacobson. *Basic algebra*. Number II. W. H. Freeman and Company, second edition, 1989.

[6] T.Y. Lam. *A first course in noncommutative rings*, volume 131 of Graduate Texts in Mathematics. Springer-Verlag, second edition, 2001.

[7] Joachim Lambek. *Lectures on rings and modules*. Chelsea Publishing Co., second edition, 1976.