Teoremas de estructura de módulos y anillos con condiciones de finitud

Trabajo Fin de Grado

Autor:
José Ignacio García Moreno

Tutor:
José Escoriza López

Grado en Matemáticas

Junio, 2020
Universidad de Almería

Índice general

Abstract

Multiplicative theory of ideals, more generally multiplication modules study, is linked to several algebra areas, as number theory and algebraic geometry.

Multiplication modules are a nexus between other important families of modules like are the Noetherian and the Hopfian. This work is a first aproximation to this relations. We will study applications of the Noetherian and Artinian modules structure theorem, using in order to build alternatives demostrations over abelians Noetherian groups (finitly generated), abelian Artinian groups and abelians multiplications groups. In parallel we will talk about the structure and properties of Noetherian and Artinian rings and Noetherian multiplication rings.

The first chapter is an accout of basic results that will allow the later work. The second one establishes the main framework, prouving the Noetherian and Artinian modules structure theorem. Finally, on the third and fourth ones we will build the structure theorem that we mentioned previously.

The most interesting chapter of this work, is the one about the structure of Abelian Artinian and Noetherian groups. In Noetherian case, most proofs are done using the structure theorem of P.I.D with matix theory, we deal it with other appoach using the Noetherian mosules structure theorem. On the other hand, in Artinian case, the result, in general, is widely unknown, furthermore in a few text is detailed in depth. On the work we have done a original demostration with traditionals and new ideas.

Resumen

La teoría multiplicativa de ideales, más generalmente, el estudio de los módulos de multiplicación, esta ligado a diversos campos del algebra, como la teoría de números y la geometría algebraica.

Los módulos de multiplicación son una nexo entre otras familias importantes de módulos como son los noetherianos y los hopfianos. Este trabajo es una primera aproximación a esas relaciones. Estudiamos aplicaciones del teorema de estructura de módulos noetherianos y artinianos, usándolo para construir demostraciones alternativas sobre grupos abelianos noetheriano (finitamente generado), grupos abelianos artinianos y grupos abelianos de multiplicación. Paralelamente hablaremos de la estructura y propiedades de los anillos noetherianos y artinianos y los anillos noetherianos de multiplicación.

El primer capítulo consiste en una relación de resultados básicos que van a permitir el trabajo posterior. En el segundo se establece el marco principal de juego, demostrando los resultados que habilitan las demostraciones posteriores, entre los que están el propio teorema de estructura de módulos noetherianos y artinianos. Por último, en el tercero y el cuarto construimos los teoremas de estructura que antes mencionábamos.

El capitulo más interesante del trabajo, es el que trata de la estructura de los grupos abelianos noetherianos y artinianos. En el caso noetheriano, la mayoría de pruebas se hacen a través del teorema de estructura de D.I.P. con teoría de matrices, nosotros abordamos otro enfoque usando el teorema de estructura de módulos noetherianos. Por otro lado, en el caso artiniano, el resultado, en general, es poco conocido, además en pocos textos se detalla en profundidad. En el trabajo hemos hecho una demostración con ideas tradicionales y nuevas.

1 Introducción: Objetivos y Aproximación Histórica

Los estudios expuestos en este trabajo se hacen en el marco del caso conmutativo. Hay varias razones para ello. Primera, la importancia de los módulos y anillos de multiplicación radica principalmente en el caso conmutativo, puesto que se generalizan importantes propiedades de Teoría de Números y Geometría Algebraica. Segunda, la unicidad de la descomposición de módulos artinianos en suma de indescomponibles en el caso de anillo conmutativo (para noetherianos no se tiene). Esto hace que se deduzca fácilmente la unicidad en teoremas de estructura cuya demostración use este teorema como punto de partida. Tercera, la no correlación de las propiedades elementales de los módulos libres sobre anillos no conmutativos (en el caso finito) con las de espacios vectoriales: A^n puede ser isomorfo a A^m y, sin embargo, n ser distinto de m. Por último, por ser este un primer paso en la investigación, para abordar después el caso no conmutativo, que es más complicado. Los objetivos principales de este texto son los siguientes :

- Estudiar los resultados relacionados con la estructura de los módulos noetherianos y artinianos.
- Aplicar los teoremas de estructura de módulos notherianos y artinianos a subfamilias suyas, para obtener teoremas más específicos a partir de estos.
- Usar los resultados y técnicas anteriores para encontrar teoremas de estructura para grupos abelianos de multiplicación.

El concepto de anillo noetheriano fue introducido por Emmy Noether en sus trabajos sobre anillos donde todo ideal es finitamente generado. Demostró que esta condición de finitud equivalía a que toda cadena de ideales ascendente terminaba estacionando [20] . Posteriormente este concepto se puede extender a módulos. *Se dice que dado A un anillo y M un A-módulo, M, es noetheriano si toda cadena ascendente de submódulos estaciona*; y se prueba que esta condición equivale a que toda submódulo sea finitamente generado o que toda familia no vacía de submódulos tenga un elemento maximal. El estudio de estos módulos es de interés, precisamente, por estas condiciones de finitud, dado que, aunque sean infinitos, el número de generadores de sus submódulos son finitos y porque están controladas las cotas superiores de las cadenas de submódulos. Sendas condiciones habilitan resultados mucho más profundos. También, en el caso de los anillos noetherianos, es importante resaltar la importancia de esta propiedad, puesto que todo ideal suyo admite una descomposición primaria.

La condición dual, la introduce E.Artin en [2]. *Se dice que un módulo (resp. un Anillo) es artiniano si toda cadena descendente de submódulos (res. ideales) estaciona.* Este concepto no es solo dual por como se define, si no que, como veremos en el trabajo, si los módulos noetherianos se encuentran relacionados con los hopfianos, los artinianos se encuentran relacionados con los cohopfianos. Construyendo de esta manera, dos pares de familias duales. A estas parejas de familias relacionadas se pueden añadir los módulos de multiplicación que están relacionados con los hopfianos y los de comultiplicación que lo están con los cohopfianos.

Posteriormente en 1931 H.Hopf en [15] probó que toda aplicación de grado uno de

una superficie orientable cerrada en sí misma es una equivalencia homotópica; en el transcurso de la demostración tuvo que probar que todo endomorfismo sobreyectivo del grupo fundamental de la superficie era isomorfismo. Inspirado en este resultado G.Baumslag en [6] denomina hopfiano a un grupo donde todo endomorfismo sobreyectivo es automorfismo. La propiedad dual, todo endomorfismo inyectivo es un automorfismo, recibe el nombre de co-hopfianidad. Posteriormente J.Lewin estudia este concepto en anillos y W. Vasconcelos y J.Strookers por separado en módulos, llegando a demostrar en [26] y [25] respectivamente y de manera independiente que que para un anillo conmutativo A los A-módulos finitamente generados son hopfianos. Estas dos familias constituyen generalizaciones de los módulos noetherianos y artinianos y su estudio tiene importancia para demostrar condiciones de existencia y unicidad de sistemas de ecuaciones.

Otra de las familias de módulos con la que trabajaremos será con los módulos de multiplicación. El concepto inicialmente, como es habitual, aparece en anillos. Fue introducido por W.Krull en 1925 [18] para generalizar los dominios de Dedekind. *Un anillo, A, se dirá de multiplicación si para todo par de ideales $I, J \leqslant A$ con $J \subset I$, existe otro ideal K tal que $J = KI$* Si restringimos esta propiedad a dominios de integridad tenemos una caracterización de dominios de Dedekind. Dichos dominios son importantes porque en ellos se obtienen resultados similares a el teorema fundamental del álgebra. Aparte de esto último, los anillos de multiplicación tienen importancia porque permiten estudiar desde un mismo punto de vista otras importantes familias de anillos como son los regulares de Von Neuman y los hereditarios. No obstante, el concepto de módulo de multiplicación sobre un anillo conmutativo se lo debemos a A. Barnard que los introdujo en [4] 1981. *Diremos que M un A-módulo es de multiplicación si para todo N submódulo suyo, existe un $I \leq A$, de manera que $N = IM$* . Estos módulos son de importancia porque comparten propiedades con los proyectivos y los finitamente generados, están estrechamente relacionados con los distributivos y particularizan a los hopfianos. El concepto dual al concepto de multiplicación y que particularizan a los módulos cohopfianos es bastante actual, su introducción y primeros estudios datan de 2007 por H. Ansari-Toroghy y F. Farshadifar en [1]. En un primer momento, el trabajo tenía por objetivo estudiar estas 6 familias divididas en dos grupos, multiplicación, hopfiano, noetheriano y comultiplicación, artinianos y cohopfiano, viendo como se relacionan unas con otras y como se iban obteniendo resultados duales. Cuando nos pusimos manos a la obra, nos dimos cuenta de que era un proyecto demasiado ambicioso. Concluimos que sería mejor estudiar en profundidad dos de ellas, noetherianos y artinianos, quizás las mas accesibles por proximidad a lo estudiado en el grado y por origen histórico; aplicando sus resultados a la Teoría Multiplicativa de Ideales con objeto de obtener teoremas de estructura para grupos abelianos de multiplicación; y estudiando propiedades de estos módulos similares a las de las anteriores familias.

2 Conceptos Previos

En general, salvo que digamos lo contrario, trabajaremos con estructuras conmutativas. Algunos de los resultados que se muestran en este texto, son extensibles al caso no conmutativo. No obstante, no nos ocuparemos de ello. Durante el transcurso del trabajo, aparece el concepto de anillo, con el que siempre nos referimos a anillos unitario. Gran parte de los resultados aquí expuestos son ampliamente conocidos y se pueden encontrar en numerosos libros sobre el tema; por ejemplo en [3] o [19]. De hecho, salvo que adjuntemos alguna referencia o comentario, interprétese, para el resto de la sección, que la prueba de los resultados se encuentran en las dos anterior referencia.

2.1 Módulos

Definición 2.1. *Sea A un anillo, $(M,+)$ un grupo abeliano y $*: A\times M \to M$ una aplicación. Diremos que la terna $(M,+,*)$ es un $A-$módulo, si se verifica:*

1. $a*(x+y) = a*x + a*y$
2. $(a+b)*x = a*x + b*x$
3. $(ab)*x = a*(b*x)$
4. $1_A * x = x$

con $a,b \in A$ y $x,y \in M$.

En la práctica, cuando nos refiramos a la terna $(M,+,*)$, lo haremos simplemente usando M; en los casos donde no haya confusión sobre el anillo, diremos que M es un módulo en vez de un A-módulo; y la aplicación $*$, pasará a no escribirse (salvo que lleve a confusión), optando por la notación por yuxtaposición, típica de los productos.

Los módulos generalizan a tres estructuras algebraicas importantes: los grupos abelianos, los anillos y los espacios vectoriales. La definición de un espacio vectorial es exactamente la misma que la de un módulo, simplemente cambiando el anillo por un cuerpo. En el caso del anillo, podemos usar el producto del anillo como la aplicación $*$, cuya definición verifica las propiedades de $*$. Por último, quedan los grupos abelianos. La definición de módulo obliga a que $(M,+)$ sea un grupo abeliano. De esta forma, ya los generaliza, no obstante, en el capítulo destinado al caso $\mathbb{Z}$, veremos que los $\mathbb{Z}$-módulos son exactamente los grupos abelianos.

Definición 2.2. *Dado M, un A-módulo, diremos que N, un subconjunto suyo, es un submódulo de M, si N es un subgrupo de M y si es cerrado respecto a la multiplicación por A.*

Si volvemos sobre los ejemplos de antes, podemos apreciar que los submódulos de los espacios vectoriales son los subespacios vectoriales. Nótese, que la división en los coeficientes, diferencia fundamental entre módulos y espacios vectoriales, juega un papel central en la construcción de bases. Por otro lado, los submódulos de los grupos abelianos, vistos como $\mathbb{Z}$-módulos, son exactamente los subgrupos. Esto lo veremos en la sección dedicada a ese caso. Por último, los submódulos sobre los anillos, vistos como

módulos sobre ellos mismos, son los ideales. Esto emana directamente de la definición, subgrupos del anillo cerrados para el producto por elementos del anillo.

Definición 2.3. *Sea M un A-módulo y N un submódulo de M. Llamaremos módulo cociente a M/N, con la suma y producto por escalares usual de clases.*

Podríamos mostrar que, efectivamente, M/N tiene estructura de A-módulo.

Lema 2.1. *Sean N y M dos A-módulos, entonces $N \cap M$ es un A-módulo*

Definición 2.4. *Sean M_i, con $i \in \{1,\dots,n\}$, A-módulos, entonces $M_1 \times M_2 \times \dots \times M_n = \prod_{i=1}^{n} M_i$ es un A-módulo con la suma componente a componente y el producto por escalares componente a componente.*

Ver que esto es un A-módulo es sencillo. La operaciones en el producto funcionan como deben por que las hemos construido a partir de las operaciones en cada componente que si verifican los propiedades.

Definición 2.5. *Sea M_i, con $i \in I$, una familia de A-módulos. Se define la suma directa, $\bigoplus_{i\in I} M_1$, como $\{x_i\}_i \in I$, con $x_i \in M_i$, de forma que el cardinal de los elementos no nulos de $\{x_i\}_{i\in I}$ sea finito. Este conjunto con la suma y el producto por escalares componente a componente es un A-módulo*

En general, la suma directa está contenida dentro del producto cartesiano. En el caso finito, también se da la otra inclusión. Así que, si el producto cartesiano finito con la suma componente a componente y el producto por escalares componente a componente era un módulo, lo será también la suma directa finita. El caso infinito habría que probarlo directamente.

Si N_i es un submódulo de M_i, para todo $i \in I$, $\bigoplus_{i\in I} N_i$ es un submódulo de $\bigoplus_{i\in I} M_i$. Lo que no es cierto, es que todo submódulo de la suma sea suma de submódulos. Si consideramos el submódulo, $\mathbb{Z}(1,1) = \{(0,0),(1,1)\}$ en el grupo de Klein, este no coincide con la suma de ningún par de submódulos de $\mathbb{Z}_2$.

Lema 2.2. *La suma directa es asociativa*

A esta suma se le llama en general, suma directa externa. Como los elementos están descritos como listas finitas o infinitas no hay problema con respecto a la unicidad de escritura, cada elemento es distinto. No obstante, muchas veces querremos ver si un módulo M, es isomorfo a $\bigoplus_{i\in I} M_i$, donde cada sumando en un submódulo de M. Para mantener que la imagen $\{0,\dots,0,M_i,0\dots\}$ sea M_i, usamos la aplicación $f : \bigoplus_{i\in I} M_i \to M$ definida de la forma $:f(\{x_i\}_{i\in I}) = \sum_{i\in I} x_i$, esta suma tiene sentido por que los componentes no nulos de cada elemento eran finitos. La inyectividad de esta aplicación se traduce en que la representación de cada elemento de M como lista sea única. Para ello se exige que la intersección de un sumando con la suma del resto sea nula. De acuerdo con esto, a este tipo de sumas donde se exige dicha condición sobre las las intersecciones las denominamos sumas directas internas.
Claramente, la suma interna es una particularización de la externa, por otro lado, si $M_1 \cap M_2 \neq \{0\}$, podemos poner como sumandos $M_1 \times \{0\}$ y $\{0\} \times M_2$, que son isomorfos a M_1 y M_2, respectivamente y con intersección nula. Por tanto, en el caso finito una y otra se puede tratar de manera más o menos indistinta. De esta forma, en general, nos referiremos a suma directa de manera indistinta para referirnos a una y a otra.

Definición 2.6. *Sea M un A-módulo. Si no existen M_1 y M_2, submódulos no nulos de M, de manera que M sea suma directa interna de M_1 y M_2, diremos que M es indescomponible.*

Donde ponemos que M_1 y M_2 no sean nulos, podríamos haber puesto, de manera equivalente, que sean el propio M ó incluso ambas cosas.

2.2 Módulos Libres

La gran diferencia de un espacio vectorial a un módulo es precisamente la existencia de base. Mientras que en un espacio vectoriales siempre existe una base, cuando hablamos de un A-módulo no tiene porque. Si tomamos una combinación lineal finita igualada a cero de los generadores de un A-módulo, donde alguno de los coeficientes es no nulo, como no podemos dividir, no podemos despejar ese coeficiente con respecto a los demás y eliminarlo de la lista. Esto lleva a que el sistema generador pueda describir elementos de maneras distintas.

Veámoslo un poco más despacio, supongamos un sistema generador $\{x_1,\dots,x_s\}$ que no sea base. Entonces existirá una combinación lineal con coeficientes en A igualada a 0, $0 = a_1x_1 + \dots, a_sx_s$, donde algún $a_i \neq 0$, de esta forma, $a_ix_i = a_1x_1 + \dots + a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + \dots + a_sx_s$. Luego, ese elemento particular tiene dos escrituras distintas y como no podemos dividir, no podemos despejar a_i para poder quitarlo de la lista de generadores.

Definición 2.7. *Sea $\{x_i\}_{i\in I}$ un conjunto, con I una familia de índice no necesariamente finita. Diremos que este es **linealmente independiente** si y solamente si para cualquier combinación lineal finita de elementos del conjunto igualada a 0 todos los coeficientes son nulos.*
*Diremos que este es **sistema generador** de un A-módulo, M, si y solamente si cualquier $m \in M$ se puede poner como $\sum_{i\in I} a_ix_i$, con un conjunto finito de $a_i \neq 0$*
*Si $\{x_i\}_{i\in I}$ verifica las dos condiciones anteriores, diremos que $\{x_i\}_{i\in I}$ es una **base** de M.*

Si para M existe una familia finita que verifica que cualquier elemento de M se puede poner como combinación lineal finita de esta familia, diremos que M es **finitamente generado**.

En el caso de que exista una base para M, cualquier elemento de M se puede escribir de forma única respecto a esa base. Si $m \in M$ tiene dos escrituras, las restas y sacas factor común, tenemos una combinación lineal finita de elementos linealmente independientes, luego los coeficientes son nulos, como habíamos sacado factor común, los coeficientes de una y otra descomposición son los mismos.

Si M admite una base, diremos que **el módulo es libre**.

Proposición 2.1. *Sea M es un A-módulo, entonces $M \cong \bigoplus_{i\in I} A$ si y solamente M es libre como A-módulo, con I una familia de índices arbitraria.*

Proposición 2.2. *Sean M_i, con $i \in I$, A-módulos libres, entonces $\bigoplus_{i\in I} M_i$ es libre como A-módulo.*

Demostración:

Esta demostración es prácticamente idéntica a la que se hace en el caso de espacios vectoriales.

■

2.3 Anillo de Endomorfismos y Morfismos

Definición 2.8. *Sean M y M' A-módulos y sea $f : M \to M'$ una aplicación de M a M'. Diremos que f es un homomorfismo de módulos si $f(x+y) = f(x) + f(y)$ y $f(ax) = af(x)$, para todo $x, y \in M$ y $a \in A$*

Lema 2.3. *Sean M y N A-módulos y $f : M \to N$ un morfismo de A-módulos, entonces la preimagen de un submódulo de N y la imagen de un submódulo de M, son submódulos de M y N respectivamente.*

Con este lema queda patente que el $Ker\, f$ es un submódulo de M y la $Im\, f$ es un submódulo de M'.

Podemos mostrar que es equivalente que $Ker\, f = \{0\}$ a que f sea inyectiva. Para todo $x, y \in M$ con $f(x) = f(y)$, tenemos, $f(x) = f(y) \Leftrightarrow f(x-y) = 0 \Leftrightarrow x - y \in Ker\, f$ y además como $x = y$ es equivalente a $x - y = 0$, llegamos a lo que deseábamos.

Teorema 2.1 (Primer Teorema de Isomorfía)**.** *Sea $f : M \to M'$ un homomorfismos entre A-módulos. Entonces, se tiene que $M/Ker\, f \cong Im\, f$. (El símbolo $\cong$, como es habitual, hace referencia a ser isomorfo, es decir, que entre ellos existe un homomorfismos biyectivo).*

Con este último teorema, podemos ver que los submódulos de M/N son exactamente M'/N. Donde M' es un submódulo de M con $N \subseteq M' \subseteq M$. La idea es probar que cualquier M'/N, con las condiciones anteriores es submódulo de M/N, tal y como lo hemos hecho en varias ocasiones. Luego, partimos de S, un submódulo de M/N. Llamamos $S' := \{m \in M \text{ tal que } \overline{m} \in S\}$, probamos que S' es un submódulo de M que contiene a N. Comprobamos que $f : S' \to S$, definida por $f(s) = \overline{s}$, es un morfismo sobreyectivo con $Ker\, f = N$ y aplicamos el teorema de isomorfía.

Definición 2.9. *Dado M un A-módulo, denominaremos **anillo de endomorfismos de** M, o $End_A(M)$, al conjunto de los endomorfismos con la suma usual de funciones y la composición.*

Habría que probar que se puede hacer esta definición, es decir, que $(End_A(M), +, \circ)$ tiene estructura de anillo. No obstante, la prueba es poco más que un ejercicio y no aporta mucha información sobre nuestros principales objetivos, así que, la obviaremos.

2.4 Series Exactas Cortas

Definición 2.10. *Sean M_i y f_i, con $i \in I$ una familia de A-módulos y A-morfismos respectivamente, diremos que la serie de A-módulos:*

$$\ldots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \ldots$$

*es **exacta** en M_i si $Im\, f_i = Ker\, f_{i+1}$. Diremos que la serie es exacta, si lo es en cada término.*

Proposición 2.3. *Sean M', M y M'' A-módulos, se tiene que:*

- *i). $0 \longrightarrow M' \xrightarrow{f} M$ es exacta si y solamente si f es un morfismo inyectivo.*

- *ii).*$M \xrightarrow{g} M'' \longrightarrow 0$ *es exacta si y solamente si* g *es un morfismo sobreyectivo.*
- *iii).*$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *es exacta si.i.* f *es un morfismo inyectivo,* g *es un morfismo sobreyectivo e* $Im\, f = Ker\, g$

A las series con la misma forma que la del apartado iii), las llamaremos **series exactas cortas**.

Queremos definir los módulos proyectivos, pero para ello, antes necesitamos hablar del concepto de escisión.

Lema 2.4 (de Escisión)**.** *Sean* M', M *y* M'' *A-módulos, sea:*

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

una serie exacta corta. Entonces, son equivalentes las tres siguientes afirmaciones:

- *i) Existe un morfismo* $t : M \to M'$ *tal que* tf *es la identidad en* M'*.*
- *ii) Existe un morfismo* $u : M'' \to M$ *tal que* gu *es la identidad en* M''*.*
- *iii)* M *es isomorfo a la suma directa de* M *y* M'

Para una prueba de este resultado véase la sección 1.4 de [28].

Pasemos ahora, a definir los módulos proyectivos, estos serán de utilidad en nuestro trabajo.

Definición 2.11. *Sea* A *un anillo, diremos que* P*, un* A*-módulo, es* ***proyectivo*** *si cumple alguna de las siguientes condiciones equivalentes:*

i) P *es suma directa de* A*-módulos libres.*

ii) Para todo morfismo sobreyecitvo de A*-módulos* $N \xrightarrow{f} M \longrightarrow 0$ *y cualquier morfismo de* P *en* M*,* g*,* $\exists h : P \longrightarrow N$*, morfismo, tal que* $fh = g$*.*

iii) Toda sucesión exacta corta que llegue a P *escinde.*

Definición 2.12. *Sea* A *un anillo, diremos que* M*, un* A*-módulo, es* ***inyectivo****, si para todo morfismo inyectivo de* A*-módulos,* $0 \longrightarrow N \xrightarrow{f} H$*, y cualquier morfismo de* N *en* M*,* g*,* $\exists h : H \longrightarrow M$ *tal que* $hf = g$*.*

3

Modulos Noetherianos y Artinianos

3.1 Módulos Noetherianos

Definición 3.1. *Sea A un anillo , diremos que M, un A-módulo, es* ***noetheriano*** *si toda cadena ascendente de submódulos propios estaciona (C.C.A), i.e., para toda cadena de submódulos propios* $M_1 \subseteq M_2 \ldots \subseteq M_i \subseteq M_{i+1} \ldots$ *se verifica que* $\exists m \in \mathbb{N}$ *tal que* $M_m = M_k \quad \forall k \geq m$.

Aunque esta es la definición más usual, existen dos condiciones equivalentes de gran importancia teórica y técnica, puesto que habilitan mecanismos muy usados en demostraciones que involucran la propiedad de noetherianidad.

Proposición 3.1. *Sea M un A-módulo las siguientes condiciones son equivalentes:*

i) M es noetheriano.

ii) Toda familia de submódulos propios de M no vacía tiene un elemento maximal.

iii) Todo submódulo de M es finitamente generado como A-módulo.

Demostración:

$i) \Rightarrow ii)$

Hagámoslo por reducción al absurdo. Supongamos que dada una familia no vacía de submódulos propios, $\{M_i\}_{i \in I}$, no existe submódulo maximal. Tomemos un módulo M_1 de dicha familia. Como no hay maximal , existirá otro submódulo M_2 de manera que $M_1 \subsetneq M_2$, como no existe submódulo maximal en la familia podemos reiterar este proceso y construir una cadena ascendente infinita, llegando a un absurdo.

$ii) \Rightarrow iii)$

Supongamos que N es un submódulo no trivial de M. En el caso de que N=0, obviamente N=A0, y N es finitamente generado como A-módulo. Por tanto, existirá por lo menos un elemento $x \in N$ y $Ax \subseteq N$. De este modo, la familia S:=$\{N_i$ submódulos de N / N_i es finitamente generado como A-módulo$\} \neq \emptyset$. Por ii), sabemos que S tiene un elemento maximal; llamémoslo N_m. Como N_m es finitamente generado, $N_m =< a_1, a_2, \ldots, a_n >$. Veamos que $N_m = N$. Si no lo fuese, $\exists a \in N - N_m$. Tomando ahora $< a_1, a_2, \ldots, a_n, a >$, tendríamos un módulo de la familia S estrictamente mayor que N_m y llegaríamos a una contradicción. De este modo, $N_m = N$ y es N es finitamente generado como A-módulo. Queda por ver que M también es finitamente generado. Elijamos N=M. Razonando de manera análoga, mostramos que M es finitamente generado.

$iii) \Rightarrow i)$

Veamos que toda cadena ascendente de submódulos estaciona. Tomemos una cadena ascendente infinita de submódulos $N_1 \subseteq N_2, \ldots$. Se puede ver que $\cup_{i \in \mathbb{N}} N_i$ es un submódulo de M, porque la condición de cadena permite que en la unión la suma siga siendo interna (manteniendo la estructura de grupo). Entonces, por i), $\bigcup_{i \in \mathbb{N}} N_i =< m_1, \ldots, m_n >$. Como es claro $\forall m_j, \exists N_{i(j)} / m_j \in N_{i(j)}$. Si llamamos k=max($\{i(j)\}$), $\cup_{i \in \mathbb{N}} N_i = N_k = N_{k+1} = \ldots$ y la cadena estaciona.

■

El ser noetheriano es una propiedad que se hereda para cocientes, submódulos y sumas directas de módulos. De hecho se puede probar algo más general que habilita más "herencias".

Proposición 3.2. *Sea* $0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\varphi} M'' \longrightarrow 0$, *una sucesión exacta corta de A-módulos, entonces M es noetheriano si y solamente si M' y M'' lo son.*

Demostración:

$\Rightarrow$

Cualquier familia no vacía, S′, de submódulos en M′ al aplicarle ϕ origina una familia no vacía, S:={N, submódulos de M/ $\exists N' \in S$ con $\phi(N') = N$}. De esta manera, tenemos un elemento maximal de S y al tomar imágenes inversas, la imagen inversa del máximal en S es maximal en S′. Como la función ϕ es inyectiva, la imagen inversa de la imagen de un conjunto es el propio conjunto por tanto la preimagen del maximal de S está en S′. Para el caso de M″ usamos una técnica similar. Elijamos una familia arbitraria no vacía, L″, de submódulos de M″. Calculando la imagen inversa se tiene que L=:{N, submódulos de M/ $\exists N'' \in L''$ con $\varphi^1(N'') = N$} es una familia no vacía. Podemos afirmar esto último porque la aplicación φ es sobreyectiva y todo elemento de M″ tiene una preimagen. Como M es noetheriano, existe elemento máximal y aplicando φ, la imagen del maximal en L es maximal en L″. La imagen de la imagen inversa de un conjunto es el propio conjunto lo cual hace que la imagen del maximal de L este en L″.

$\Leftarrow$

Sea $0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\varphi} M'' \longrightarrow 0$, una sucesión exacta corta de A-módulos. Probemos que si M′ y M″ son noetherianos, lo será M. Para ello, primero probamos que si M′ y M″ son finitamente generados (f.g.) lo es M. Como M′ y M″ son f.g., entonces tenemos que M′=$< m_1 \dots m_r >$ y M″= $< n_1 \dots n_s >$. Por otro lado como φ es sobreyectiva $\exists x_1, \dots, x_s \in M$ tales que $\varphi(x_i) = n_i$, $(1 \leq i \leq s)$. A priori, puede haber más de una preimagen para cada n_i; no obstante, si la hay, se toma una cualquiera de ellas. Veamos que M=$< \phi(m_1), \dots, \phi(m_r), x_1, \dots, x_s >$. Sea $x \in M$, como $\varphi(x) \in M''$, existen $a_1, \dots, a_s \in A$ de manera que, $\varphi(x) = \sum_{i=1}^{s} a_i n_i = \sum_{i=1}^{s} a_i \varphi(x_i) = \varphi(\sum_{i=1}^{s} a_i x_i)$. Esta cadena de desigualdades se tiene porque φ es un homomorfismo de A-módulos. De aquí, $\varphi(x - \sum_{i=1}^{s} a_i x_i) = 0$ y de este modo, $x - \sum_{i=1}^{s} a_i x_i \in Ker\,\varphi = Im\,\phi$ por ser una sucesión exacta corta. Como $Im\,\phi$ está generado por $\phi(m_1), \dots, \phi(m_r)$, afirmación que se deriva de la definición de homomorfismo de A-módulos, existirán $b1, \dots, b_r \in A$ tales que $x - \sum_{i=1}^{s} a_i x_i = \sum_{j=1}^{r} b_j \phi(m_j)$. Se deduce que $x = \sum_{i=1}^{s} a_i x_i + \sum_{j=1}^{r} b_j \phi(m_j) \in <$ $\phi(m_1), \dots, \phi(m_r), x_1, \dots, x_s >$. Con lo que M es f.g. Ahora considerando la serie exacta corta de partida y N un submódulo cualquiera de M, tenemos que ver que N es f.g. Construimos:

$$0 \longrightarrow \phi^{-1}(N) \xrightarrow{\phi} N \xrightarrow{\varphi|_N} Im\,\varphi|_N \longrightarrow 0$$

Veamos que la expresión de arriba es una sucesión exacta corta. Para ello necesitamos probar que ϕ es inyectiva, $\varphi|_N$ es sobreyectiva, $Ker\,\varphi|_N = Im\,\phi$ y ambas son morfismos de A-módulos. Del enunciado sabemos que ϕ es un morfismo inyectivo y claramente como φ es un morfismo, su restricción lo es. Como estamos restringiendo φ a N y el conjunto de llegada es $Im\,\varphi|_N$, estamos forzando que $\varphi|_N$ sea sobreyectiva. Faltaría probar que $Ker\,\varphi|_N = Im\,\phi$. Sabemos que $Ker\,\varphi = Im\,\phi$. Si restingimos a N, se demuestra que $Ker\,\varphi|_N = Im\,\phi$. De este modo hemos construido una sucesión exacta corta. Además $\phi^{-1}(N) \leq M'$ y es f.g. por ser M′ noetherianno. Por cuestiones similares, es f.g. $Im\,\varphi|_N \leq M''$. Aplicando lo anteriormente demostrado N es f.g.

■

De esta proposición podemos deducir que la propiedad de noetherianidad se hereda en submódulos, cocientes y sumas directas finitas. La prueba se hace ajustando las sucesiones exactas cortas y usando el resultado anterior.

Proposición 3.3. *Si M es un A-módulo noetheriano y N un submódulo suyo, entonces N y M/N son A-módulos noetherianos. Recíprocamente, si existe un submódulo N de M tal que M/N y N sean noetherianos, entonces M es noetheriano como A-módulo.*

Demostración:

$\Rightarrow$)

Construimos:

$$0 \to N \hookrightarrow M \xrightarrow{\rho} \frac{M}{N} \to 0$$

Donde ρ es la proyección canónica, que es sobreyectiva, y $\hookrightarrow$ es la inclusión, que es inyectiva. Aplicando la proposición anterior se tiene automaticamente lo que se quiere.

$\Leftarrow$)

Se hace exactamente igual que el apartado anterior, pero en vez de usar la implicación hacia la derecha de (3.2) se usa la implicación hacia la izquierda.

■

Proposición 3.4. *La suma directa finita de módulos noetherianos es un módulo noetheriano*

Demostración:

Apliquemos inducción sobre n, número de sumandos.

Caso n=2: (Partimos de n=2 porque no tiene sentido n=1)

$$0 \to M_1 \hookrightarrow M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \to 0$$

Donde $\xrightarrow{\pi_2}$ es la proyección canónica sobre la segunda componente, que es sobreyectiva. Sin más que aplicar la proposición anterior, tenemos que, como M_1 y M_2 son noetherianos, la suma directa lo es.

Caso n=j+1:

Se hace exactamente como el caso anterior, pero se sustituye M_2 por $\bigoplus_{i=1}^{j} M_i$, que es noetheriano por hipótesis de inducción.

■

Las propiedades arriba mostradas van directamente encaminadas a tener herramientas para demostrar el teorema de estructura que pondrá final a esta sección. No obstante, parece interesante resaltar una estrecha relación que tienen los módulos noeteherianos con otras familias de módulos, los hopfianos.

Definición 3.2. *Sea A un anillo, diremos que M un A-módulo es **hopfiano** si todo $f \in End_A(M)$ sobreyectivo es inyectivo.*

El conocimiento sobre estos módulos es de gran importancia para el estudio de resolución de ecuaciones; pues sobre estos módulos cualquier ecuación que tenga solución automáticamente es única.

Proposición 3.5. *Todo M, A-módulo noetheriano es hopfiano.*

Demostración:

Sea $f \in End_A(M)$, claramente f^m (aplicar f m-veces) también pertenece a $End_A(M)$, tomemos la siguiente cadena de submódulos de M:

$$Ker\, f \subseteq Ker\, f^2 \subseteq Ker\, f^3 \subseteq \dots$$

Como M es noetheriano dicha cadena estaciona, i.e. $\exists n$ de manera que $Ker\, f^n = Ker\, f^{n+1} = \dots$. Como f es sobreyectiva lo es también f^n y tomando $x \in Ker\, f$, se tiene que $\exists y \in M$ tal que $f^n(y) = x$. Pero como $f(x) = 0$ podemos aplicar la función y $f^{n+1}(y) = 0$; por tanto $y \in Ker\, f^{n+1} = Ker\, f^n$. Así que $x = f^n(y) = 0$ y tenemos que el endomorfismo es inyectivo.

■

3.2 Módulos Artinianos

La definición dual a la noetherianidad es la de artinianidad. Estas condiciones si bien se formulan de manera dual, no lo son los resultados derivados de ellas. Esto podremos verlo en este capítulo con el teorema de Hopkins-Levitzki, aunque en esta sección se pueden obtener resultados análogos a los vistos para A-módulos noetherianos en el caso artiniano. Las pruebas de los resultados mentados se realizan, en muchos casos, utilizan las ideas ya vistas, ligeramente adaptadas. Por tanto se omitirán salvo cuando los cambios sean sustanciales.

Definición 3.3. *Sea A un anillo, diremos que M un A-módulo es* ***ariniano*** *si toda cadena descendente de submódulos propios estaciona (C.C.D), i.e. para toda cadena de submódulos* $M_1 \supseteq M_2 \dots \supseteq M_i \supseteq M_{i+1} \dots$ *se verifica que* $\exists m \in \mathbb{N}$ *tal que* $M_m = M_k \quad \forall k \geq m.$

Al igual que en el caso noetheriano existen condiciones equivalentes.

Proposición 3.6. *Sea M un A-módulo las siguientes condiciones son equivalentes:*

i) M es artiniano.

ii) Toda familia de submódulos propios de M no vacía tiene un elemento minimal.

En el caso artiniano, se podría construir también una tercera condición equivalente: el conjunto de los cogeneradores de M es finito. No obstante, habría que introducir la noción de cogenerador de un módulo y como no lo necesitaremos posteriormente, vamos a obviarla.

Las sumas directas, submódulos y cocientes de módulos artinianos lo son; es más, también se puede probar que:

Proposición 3.7. *Sea* $0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\varphi} M'' \longrightarrow 0$, *una sucesión exacta corta de A-módulos, entonces M es artiniano si y solamente si M' y M" lo son.*

Demostración:

$\Rightarrow$

La demostración es análoga al caso noetheriano si más que cambiar maximal por minimal y en vez de usar C.C.A., usar C.C.D.

$\Leftarrow$

Supongamos que M′ y M″ son artinianos. Sea $M_1 \supseteq M_2 \supseteq \ldots$ una cadena descendente de submódulos de M. Entonces $\phi^{-1}(M_1) \supseteq \phi^{-1}(M_2) \supseteq \ldots$ es una cadena descendente de submódulos de M′ y $\varphi(M_1) \supseteq \varphi(M_2) \supseteq \ldots$ es una cadena descendente de submódulos de M″. Como ambos son artinianos, existirán k′ y k″ de manera que las cadenas estacionen. Llamamos k al máximo de k′ y k″, esta claro que ambas cadenas estacionan para k. Veamos entonces, que la cadena $M_1 \supseteq M_2 \supseteq \ldots$ verifica que $M_k = M_j,\ \forall j \geq k$. Tenemos que ver que $M_k \supseteq M_j,\ \forall j \geq k$, tomemos un j fijo pero arbitrario mayor que k. Sea $x \in M_j$, de este modo $\varphi(x) \in \varphi(M_j) = \varphi(M_k)$, por tanto $\exists x_1 \in M_k$ tal que $\varphi(x) = \varphi(x_1)$. Luego $x - x_1 \in ker\,\varphi = Im\,\phi$, por constituir estas aplicaciones una sucesión exacta corta. De esta forma existirá un $x_2 \in M'$ de manera que $\phi(x_2) = x - x_1 \in M_j$. De donde $x_2 \in \phi^{-1}(M_j) = \phi^{-1}(M_k)$. Entonces, como $x_1 \in M_k$ y $\phi(x_2) \in M_k$, llegamos a que $x = x_1 + \phi(x_2) \in M_k$

■

En el caso noetheriano se podría haber hecho una demostración análoga a esta. No obstante nos ha parecido interesante introducir otra distinta, ya que aporta información extra sobre los módulos finitamente generados.

Usando los mismos razonamientos que en el caso noetheriano, se puede comprobar:

Proposición 3.8. *Si M es un A-módulo artiniano y N un submódulo suyo, entonces N y M/N son A-módulos artinianos. Recíprocamente, si existe un submódulo N de M tal que M/N y N sean artinianos, entonces M es artiniano como A-módulo.*

Proposición 3.9. *La suma directa finita de módulos artinianos es un módulo artiniano.*

Existe una definición dual al concepto de hopfiano que introdujimos anteriormente, el concepto de cohopfiano.

Definición 3.4. *Sea A un anillo, diremos que M un A-módulo es* ***cohopfiano*** *si todo $f \in End_A(M)$ que sea inyectivo es sobreyectivo.*

Lo que en términos de soluciones de ecuaciones definidas por estas aplicaciones quiere decir que: si somos capaces de demostrar la unicidad de solución, automáticamente se tiene garantizada su existencia.

Proposición 3.10. *Todo M, A-módulo artiniano es cohopfiano.*

Demostración:

Sea $f \in End_A(M)$, entonces f^m (aplicar f m-veces) también pertenece a $End_A(M)$, tomemos la siguiente cadena de submódulos de M:

$$Im\,f \supseteq Im\,f^2 \supseteq Im\,f^3 \supseteq \ldots$$

Como M es artiniano, dicha cadena estaciona , i.e., $\exists n$ de manera que $Im\,f^n = Im\,f^{n+1} = \ldots$. Como f es inyectiva, lo es también $f^n, \forall n \in \mathbb{N}$. Veamos que $Im\,f = M$. Sabemos que $Im\,f \subseteq M$ porque $f \in End_A(M)$. Falta ver $Im\,f \supseteq M$. Tomemos $m \in M$, probemos que $\exists m' \in M / f(m') = m$. Tenemos que $f^n(m) \in Im\,f^n = Im\,f^{n+1}$, por tanto $\exists m' \in M$ de manera que $f^{n+1}(m') = f^n(m)$. Aplicando que $f \in End(M)$, llegamos a que $f^{n+1}(m') - f^n(m) = 0 = f^n(f(m') - m)$ y por la inyectividad de $f^n, f(m') - m = 0$.Queda probado que $m = f(m')$

■

3.3 Teorema de Estructura

En capítulos sucesivos aplicaremos el teorema de estructura obtenido en esta sección para deducir otros teoremas de estructura ligados a grupos abelianos y a módulos.

Teorema 3.1 (Estructura de Módulos Noetherianos y/o Artinianos)**.** *Todo A-módulo no trivial, M, noetheriano o artiniano es suma directa finita (no necesariamente única) de submódulos indescomponibles.*

Demostración:

Previamente a la demostración propiamente dicha, notemos que un módulo M indescomponible es suma directa finita de módulos indescomponibles, tomando la suma de sí mismo y el módulo trivial. Este comentario tiene como objeto acelerar la demostración. En muchos caso diremos que un módulo es suma directa finita de módulos indescomponibles para referirnos a que es indescomponible o suma de dos o mas indescomponibles. Luego si M, es indescomponible, $M = \{0\} \oplus M$ y queda concluida la prueba. De aquí en adelante supongamos que M no es indescomponible.

a) Caso artiniano.

Si M es no indescomponible, existirán submódulos propios, de manera que M, sea suma directa de esos submódulos. Por tanto, $S := \{N$ submódulo de M, con $N \neq \{0\}$ tales que son sumandos directo de $M\} \neq \emptyset$. Como M es artiniano S, tendrá un elemento minimal, M_0, tal que $M = M_0 \oplus M'$. Sabemos que M_0 es indescomponible, porque si no lo fuese, $\exists M_0', M_0''$, súbmodulos propios de M_0 de manera que $M_0 = M_0' \oplus M_0''$. Así, $M = M_0' \oplus M_0'' \oplus M'$, haciendo que M_0', M_0'', submódulos estrictamente contenidos en M_0 (el minimal), estén en S, lo que es absurdo. Falta comprobar que M′ es suma directa finita de indescomponibles. Supongamos que M′ no es suma directa finita de indescomponible. Entonces $\exists M_1$ y M_2 súbmodulos propios de M′ con $M' = M_1 \oplus M_2$. Si los dos fuesen suma directa finita de indescomponibles llegaríamos a una contradicción porque M′ no era suma directa finita de indescomponibles. Por tanto, alguno de los dos es descomponible (si no lo fuese por el apunte previo a la demostración serían suma directa finita de indescomponibles), sin pérdida de generalidad, supongamos M_1 el descomponible. De este modo, a su vez $\exists M_{11}$ y M_{12} súbmodulos propios de M_1 con $M_1 = M_{11} \oplus M_{12}$. Repitiendo el mismo argumento, si tanto M_{11} como M_{12} fuesen suma directa finita de indescomponibles, M_1 sería suma finita de indescomponibles. Llegando a una contradicción. Deducimos que al menos uno de los dos no es suma directa finita de indescomponibles. Supongamos sin pérdida de generalidad, que es M_{11}. Repitiendo este proceso de manera recursiva, conseguimos una cadena descendente infinita de la forma:

$$M \supsetneq M' \supsetneq M_1 \supsetneq M_{11} \supsetneq M_{111} \dots$$

cayendo en una contradicción, puesto que M es artiniano. Así M′ es suma directa finita de indescomponibles y de esta forma M es suma directa finita de submódulos indescomponibles.

b) Caso noetheriano.

Si M es no indescomponible, existirán submódulos propios, de manera que M, sea suma directa de esos submódulos. Por tanto $S := \{N$ submódulo de M, con $N \neq M$ tales que son sumandos directos de $M\} \neq \emptyset$. Como M es noetheriano, S tendrá un

elemento maximal, M', tal que $M = M_0 \oplus M'$. Sabemos que M_0 es indescomponible, usando un argumento análogo al caso anterior. Luego, $L := \{N \subseteq M$, con $N \in S$ y N es suma directa finita de submódulos indescomponibles de M $\} \neq \emptyset$, porque $M_0 \in L$. Por tanto, como M es noetheriano, L tendrá un elemento maximal, $M'' = \bigoplus_{i=1}^{n} N_i$, con N_i indescomponible $\forall\, i \in \{1, \ldots, n\}$. Así que $M = N_0 \bigoplus_{i=1}^{n} N_i$. Veamos que $N_0 = \{0\}$. Si $N_0 \neq \{0\}$, como N_0 es noetheriano no trivial, usando los mismos argumentos que los anteriores, llegaríamos a que N_0 tiene algún sumando indescomponible, adjuntando este sumando a $\bigoplus_{i=1}^{n} N_i$ tendríamos un elemento de L mayor, en el sentido de la inclusión, que el maximal y llegamos a una contradicción. De esta forma $N_0 = \{0\}$ y M es suma directa de submódulos indescomponibles.

■

Como todo submódulo de un noetheriano (resp. artiniano) es noetheriano (resp. artiniano), la descomposición que se hace es en submódulos indescomponibles noetherianos y/o artinianos, según el caso. En el enunciado del teorema, se especifica que M es no trivial. El cero es caso límite y como complica la demostración el hacerlo junto al resto se separa. No obstante, es claro que el $\{0\}$ es indescomponible por tanto se puede ver como la suma con un solo sumando: él mismo.

Mostremos ahora que ni en el caso artiniano, ni en el noetheriano hay unicidad. Veamos un contraejemplo. Para facilitar este contraejemplo necesitaremos algunos resultados ligados a módulos proyectivos que ya hemos visto en el capitulo anterior.

Sea A un anillo. Tomemos dos ideales I_1 y I_2, que no sean principales tales que $I_1 + I_2 = A$. Consideremos la siguiente sucesión exacta corta:

$$0 \longrightarrow I_1 \cap I_2 \xrightarrow{f} I_1 \times I_2 \cong (I_1 \oplus I_2) \xrightarrow{g} A \longrightarrow 0$$

Definidas f y g mediante $f(a) = (a, a)$ y $g(a, b) = a - b$

La idea del contraejemplo es:
Comprobar que esta sucesión de A-módulos es una sucesión exacta corta pasa por ver que f es inyectiva, g es sobreyectiva, el Ker g = Im f y que tanto f como g son morfismos de módulos. Como $f(a) = (0, 0)$ implica que $a = 0$ tenemos que f es inyectiva. Por otro lado como $I_1 + I_2 = A$, existirán $a_1 \in I_1$ y $a_2 \in I_2$ tales que $1 = a_1 + a_2$. De esta manera, sea $a \in A$, $a = aa_1 + aa_2$. Teniendo en cuenta que I_1 y I_2 son ideales, se tiene que $aa_1 \in I_1$ y $aa_2 \in I_2$ y por tanto $-aa_2 \in I_2$. Como $a = aa_1 + aa_2$, lo podemos poner como $a = aa_1 - (-aa_2)$ y se sigue que $a = g(aa_1, -aa_2)$. De esta forma g es sobreyectiva. Para probar que Ker g = Im I basta con ver lo siguiente. Si $g(a, b) = 0$ tenemos que $a - b = 0$ y por tanto $a = b$. Así que $a \in I_1 \cap I_2$ y Imf = Ker g. Queda probar que f y g son morfismos de módulos, no obstante, con objeto de no alargar en demasía la explicación del contraejemplo no lo haremos. Sabemos que A, visto como A-módulo, es libre y se tiene que A es proyectivo, de esta forma, (por iii) de la definición de módulos proyectivos) la sucesión exacta corta escinde. Lo que es equivalente a que $A \oplus (I_1 \cap I_2) \cong I_1 \times I_2 \cong I_1 \oplus I_2$. Claramente la suma directa que estamos mostrando no es interna dado que si lo fuese la intersección de I_1 e I_2 sería el 0 y no estaríamos mostrando dos descomposiciones distintas. Como la suma no es interna, $I_1 \oplus I_2$ no es un ideal de A , pero sí que es un A-módulo. Para finalizar la construcción del ejemplo tengamos en cuenta el siguiente lema.

Lema 3.1. *Cualquier ideal no trivial de un dominio de integridad es indescomponible.*

Demostración:

Sea A un D.I. e I un ideal de A no trivial. Supongamos que I descompone. Entonces existirán I′ y I″, no triviales de manera que $I = I' \oplus I''$. Existirán a′ y a″ no nulos (por ser I′ y I″ no triviales) pertenecientes a I′ y a I″ respectivamente. De aquí $a'a'' \in I'I'' \subseteq I' \cap I'' = 0$. Por tanto a′a″=0. Pero como A es D.I. llegamos a una contradicción porque a′ y a″ eran no nulos.

■

Con este lema ya estamos en disposición terminar el contraejemplo. Efectivamente, I_1, I_2, $I_1 \cap I_2$ y el propio A son ideales de A. Si A es un dominio de integridad estos ideales son irreducibles. Por otro lado, A lo podemos ver como un A-módulo principal (A=1A). Así que si elegimos I_1 y I_2 no principales no pueden ser isomorfos a A. Llegando de esta manera a dos descomposiciones distintas del mismo A-módulo. Bastaría buscar en un dominio de integridad noetheriano (buscamos que el anillo sea noetheriano porque cualquier ideal lo será por ser súbmodulo suyo y la suma de los ideales también lo será) dos ideales no principales con intersección no vacía y que su suma sea el propio anillo. De esta manera acabamos de fabricar toda una familia de contraejemplos. Demos uno para concretar.

Tomemos $\mathbb{Z}[\sqrt{-5}]$, que al ser un anillo de enteros algebraicos es un dominio de Dedekind; así que es un dominio de integridad noetheriano. No es un D.F.U., véase por ejemplo $9 = 3 \times 3 = (2+\sqrt{-5}) \times (2-\sqrt{-5})$. Por tanto no puede ser D.I.P. y tiene sentido buscar aquí un ejemplo. Podemos tomar $I_1 = (3, 2+\sqrt{-5})$ e $I_2 = (3, 2-\sqrt{-5})$. Claramente, la intersección es no vacía dado que contiene al ideal generado por el 3. Nos faltaría ver que I_1 e I_2 no son principales y que $I_1 + I_2 = \mathbb{Z}[\sqrt{-5}]$. Como $(2+\sqrt{-5}) + (2-\sqrt{-5}) - 3 = 1$, $1 \in I_1 + I_2$ y tenemos que $I_1 + I_2 = \mathbb{Z}[\sqrt{-5}]$. Por otro lado, I_1 no es principal. Esto es claro ya que ambos generadores tienen norma 9. Si existiese algún elemento $x = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tal que $(x) = I_1$, x debería dividir a ambos generadores y por tanto como la norma es multiplicativa $a^2 + 5b^2 = Norm(x) | 9$. La única posibilidad es que $a^2 + 5b^2 = \pm 3$ pero esto es imposible dado que a y b son enteros. De manera análoga se ve que I_2 no es principal. En virtud de como hemos construido el ejemplo, tenemos un $\mathbb{Z}[\sqrt{-5}]$-módulo noetheriano que descompone de dos maneras disntintas: $I_1 \oplus I_2$ y $\mathbb{Z}[\sqrt{-5}] \oplus (I_1 \cap I_2)$

En el caso artiniano conmutativo, existe unicidad de descomposición (véase [27]), el contraejemplo en el caso no conmutativo es más complejo y se tardó más en encontrarse (véase [10]). En general, la descomposición que hemos hecho en módulos indescomponibles no es trivial ni mucho menos (véase [24]).

3.4 Módulos de Longitud Finita

Hagamos una pequeña incursión en los módulos de longitud finita que tendrán utilidad posteriormente. Además, estos módulos como veremos al final de esta sección se corresponden exactamente con los que son noetherianos y artinianos a la vez.

Definición 3.5. *Sea M un A-módulo. Una **cadena de longitud n** en M en una sucesión de submódulos distintos entre sí de la forma siguiente. $\{0\} = M_0 \subseteq M_1 \ldots \subseteq M_n = M$. Si la cadena es máxima, i.e., no se pueden insertar submódulos distintos en la cadena diremos que dicha cadena es una **serie de composición de longitud n**.*

La condición de maximalidad que se exige a una cadena para que sea una serie de composición se puede expresar equivalentemente en términos de los cocientes consecutivos.

Lema 3.2. *Sea M un A-modulo y $\{0\} = M_0 \subseteq M_1 \ldots \subseteq M_n = M$ una cadena de longitud n. Dicha cadena será una serie de composición de longitud n si y solamente si M_{i+1}/M_i es simple $\forall i \in \{0,\ldots,n-1\}$*

Demostración:

La demostración de este resultado es clara teniendo en cuenta que los submódulos de M_{i+1}/M_i tienen exactamente la forma N/M_i con $M_i \leqslant N \leqslant M_{i+1}$. Por tanto es equivalente que M_{i+1}/M_i sea simple a que no haya submódulos propios entre M_i y M_{i+1}

■

Definición 3.6. *Llamaremos **longitud de un A-módulo M** , y la notaremos como $l(M)$, a la longitud más pequeña de todas las series de composición, si M no tiene serie de composición diremos que $l(M) = \infty$*

Veamos un par de aclaraciones que se derivan de la definición de longitud de M.

a) Si $N \subsetneq M$, se tiene que $l(N) < l(M)$. Sea $\{0\} = M_0 \subseteq M_1 \ldots \subseteq M_n = M$ una serie de composición de M, entonces, tomando $N_i = N \cup M_i$, se tiene que $\{0\} = N_0 \subseteq N_1 \ldots \subseteq N_n = N$, es una cadena de longitud n en N. Además, contruyendo $f : N_{i+1}/N_i \longrightarrow M_{i+1}/M_i$, definida por : $f(n + N_i) = n + M_i$, se puede comprobar que esta aplicación es inyectiva y es un morfismo de A-módulos. Por tanto, N_{i+1}/N_i se puede ver como un submódulo de M_{i+1}/M_i (realmente esto es un abuso de lenguaje porque lo que se tiene es que N_{i+1}/N_i es isomorfo a un submódulo de M_{i+1}/M_i). Como M_{i+1}/M_i es simple se tiene que $N_{i+1}/N_i = \{0\}$ o $M_{i+1}/M_i = N_{i+1}/N_i$ (efectivamente, donde ponemos =, debería poner $\simeq$). Si se da el primer caso, se elimina uno de los dos submódulos de la cadena de N y se repite el proceso hasta que estemos siempre en el segundo caso y habremos fabricado una serie de composición de longitud $k \leq n$. Veamos que $k \neq n$, si k=n se tendría que $M_{i+1}/M_i = N_{i+1}/N_i$, $\forall i = \{1,\ldots,n\}$. En particular, $N_1/\{0\} = N \cup M_1 \simeq M_1 = M_1/\{0\}$. De aquí se tiene que $N_1 = M_1$. Usando este argumento recurrentemente, tenemos que $N_i = M_i$, $\forall i = \{1,\ldots,n\}$. El *quid* de esta idea es que cuando los submódulos que usamos como denominadores en el cociente son los mismos no estamos cayendo en un abuso de lenguaje y N_{i+1}/N_i es un submódulo de M_{i+1}/M_i. Para terminar, si $N_i = M_i$, $\forall i = \{1,\ldots,n\}$. En particular, tenemos que N=M , llegando a una contradicción puesto que $N \neq M$.

b) Cualquier cadena tiene longitud menor o igual que $l(M)$. Si tenemos una cadena cualquiera: $\{0\} = M_0 \subseteq M_1 \ldots \subseteq M_n = M$, por definición $M_i \subsetneq M_{i+1}$. Luego, aplicando a), tenemos $0 < l(M_1) < l(M_2) < \ldots < l(M_n) = l(M)$. De esta forma, mostramos que hay n enteros entre 0 y $l(M)$, de donde $n \leq l(M)$

Proposición 3.11. *Si un A-módulo tiene una serie de composición de longitud n , entonces todas las series de composición tienen la misma longitud n. Además, toda cadena en M se puede extender a una serie de composición.*

Demostración:

Tomemos una serie de composición cualquiera de longitud k. De la aclaración anterior b), se tiene que $k \leq l(M)$, pero $l(M) \leq k$, por propia definición del $l(M)$, luego,

$l(M) = k$. Así demostramos que todas las series de composición tienen la misma longitud; pero también, si una cadena tiene longitud $l(M)$, automáticamente es una serie de composición. Este hecho se deriva de que una serie de composición es una cadena maximal , así si una cadena tiene longitud $l(M)$, pero no es máximal, podemos incluir algún submódulo entre dos eslabones seguidos; llegando a una cadena de longitud $l(M)+1$. No obstante, sabíamos por b), que las cadenas tienen longitud menor o igual que $l(M)$, incurriendo en una contradicción. Veamos, por último, que a partir de cualquier cadena, se puede fabricar una serie de composición. Si la longitud de la cadena es $l(M)$, entonces es una serie de composición y mientras que su longitud sea menor, no es una serie de composición y se pueden insertar submódulos hasta llegar a la longitud $l(M)$, convirtiéndola en una serie de composición.

■

A partir de ahora diremos que un módulo es de longitud finita si tiene una serie de composición. Ya estamos en disposición de finalizar esta sección con el resultado prometido.

Teorema 3.2. *Los A-módulos de longitud finita son exactamente los que son artinianos y noetherianos simultaneamente.*

Demostración:

Veamos que todo A-modulo M, de longitud finita es noetheriano y artiniano. Vamos a mostrar el caso noetheriano (el artiniano se hace de manera análoga simplemente cambiando C.C.A, por C.C.D y M por $\{0\}$). Si M es de longitud finita toda cadena de súbmodulos tiene longitud menor o igual que $l(M)$. Elijamos una cadena ascendente de submódulos de M, $M_1 \subseteq M_2 \ldots \subseteq M_i \subseteq M_{i+1} \ldots$. Si estaciona, no hay nada que comprobar. Si no estaciona, tomamos la subcadena $M_1 \subseteq M_2 \ldots \subseteq M_{l(M)} \subseteq M_{l(M)+1}$ y adjuntando $\{0\}$ y M tenemos, $\{0\} = M_0 \subseteq M_1 \subseteq M_2 \ldots \subseteq M_{l(M)} \subseteq M_{l(M)+1} \subseteq M_{l(M)+2} = M$. Esta es una cadena de longitud mayor que $l(M)$, lo que es imposible. De este modo, toda cadena ascendente estaciona. Ahora demostremos la otra implicación. Tomemos $M_0 = M$ y $S_0 =: \{N \subsetneq M\}$. Salvo que $M = \{0\}$ (caso que es trivialmente noetheriano y artiniano), $\{0\} \in S$, por tanto $S \neq \emptyset$. Así que S_0 tiene un elemento maximal (por ser M noetheriano), M_1, con $M = M_0 \supsetneq M_1$. Construimos ahora $S_1 =: \{N \subsetneq M_1\}$. Si $M_1 = \{0\}$, tenemos una cadena de longitud 1 que podemos llevar hasta una serie de composición. Si $M_1 \neq 0$, $\{0\} \in S_1$ y S_1 tiene un elemento máximal, M_2, por ser M_1 noetheriano, al ser M_1 súbmódulo de un noetheriano y obtenemos $M = M_0 \supsetneq M_1 \supsetneq M_2$. Aplicando esta idea recursivamente, llegamos a construir una cadena descendente y como M es artiniano estacionará. Hemos conseguido una cadena de longitud n, $M = M_0 \supsetneq M_1 \supsetneq M_2 \ldots \supsetneq M_{n-1} \supsetneq M_n = 0$, que podremos transformar en una serie de composición y demostrando con ello que M es de longitud finita.

■

Queremos mostrar un último resultado muy usado como herramienta en demostraciones.

Lema 3.3 (de Fitting)**.** *Sea M un A-módulo indescomponible y de longitud finita. Entonces todo f endomorfismo de M es automorfismo o nilpotente.*

Demostración:

Tomemos las siguientes cadenas:
1) $Im\,f \supseteq Im\,f^2 \supseteq Im\,f^3 \supseteq \ldots$
2) $Ker\,f \subseteq Ker\,f^2 \subseteq Ker\,f^3 \subseteq \ldots$

Como M es de longitud finita, i.e., artiniano y noetheriano, sendas cadenas estacionan. Tomando un n lo suficientemente grande tendremos que: $Im\,f^n = Im\,f^{n+1} = \ldots$ y $Ker\,f^n = Ker\,f^{n+1} = \ldots$. Veamos que $M = Im\,f^n \oplus Ker\,f^n$. Primero mostremos que $\{0\} = Im\,f^n \cap Ker\,f^n$. Sea $x \in Im\,f^n \cap Ker\,f^n$. Sabemos que existirá un $y \in M$ tal que $x = f^n(y)$. Aplicando f^n, como $x \in Ker\,f^n$, tenemos que $0 = f^n(x) = f^{2n}(y) = f^n(y) = x$. Luego, $\{0\} = Im\,f^n \cap Ker\,f^n$. A continuación, vamos a ver que, efectivamente, $M = Im\,f^n + Ker\,f^n$. Tomemos $x \in M$. Debe existir un $y \in M$ de manera que $f^n(x) = f^{2n}(y)$, puesto que $Im\,f^n = Im\,f^{2n}$. Entonces $f^n(x) - f^{2n}(y) = 0$, como f es un A-morfismo, tenemos que $f^n(x - f^n(y)) = 0$. De esta forma, $x - f^n(y) \in Ker\,f^n$. Así que existirá $y' \in Ker\,f^n$ de forma que $x = f^n(y) + y'$. Equivalentemente $x \in Im\,f^n + Ker\,f^n$. Demostrando que $M = Im\,f^n \oplus Ker\,f^n$. Como M era indescomponible, tenemos que $M = Im\,f^n = Im\,f^{n+1} = \ldots$ o $\{0\} = Im\,f^n = Im\,f^{n+1} = \ldots$. Dicho de otro modo f es automorfismo o nilpotente respectivamente.

■

Nótese, que en el la demostración, el hecho de que M sea indescomponible, no "ha entrado en juego" hasta el final. De este modo, podemos decir que si M es de longitud finita, existirá un $n \in N$ de manera que $M = Im\,f^n \oplus Ker\,f^n$

3.5 Caso del Anillo

Un caso particular de los módulos proyectivos es el del anillo, A, visto como A-módulo. Como ya comentamos en capítulos anteriores, A se puede ver como el A-módulo engendrado por el 1; por tanto, es un A-módulo proyectivo. No obstante dedicaremos una sección a su estudio de manera independiente debido a su importancia.

En la definición de A-módulo noetheriano y/o artiniano interviene el concepto de submódulo. Se habla de cadena de submódulos, familia de súbmódulos y de que todo submódulo es finitamente generado. En el caso del anillo, los submódulos son, exactamente, los ideales de dicho anillo. Esto es claro dado que los submódulos del anillo son los subgrupos que verifican que el producto de elementos del anillo por elementos del subgrupo queda dentro del subgrupo. Consecuentemente, el papel que antes desempeñaban los submódulos lo ocupan ahora los ideales. A todo anillo A que podemos ver como A-módulo noetheriano lo llamaremos a partir de ahora **anillo noetheriano**. Dicho lo cual, se derivan dos grandes familias de ejemplos de anillos noetherianos: Los DIP (dominios de ideales principales) y los cuerpos. En ambos casos todo ideal es finitamente generado. Queremos ahora mostrar dos resultados que proporcionan un gran despliegue de ejemplos de módulos y anillos noetherianos.

Proposición 3.12. *Sea A un anillo noetheriano, todo A-módulo finitamente generado es también noetheriano.*

Demostración:

Sea $M =< m_1, \ldots, m_n >$ un A-módulo finitamente generado, veamos que M es noetheriano. Hagámoslo por inducción sobre n, el número de generadores.

Caso n=1.

Si $M =< m >$ podemos construir la siguiente aplicación: $f := A \longrightarrow M$ definida por

$f(a) = am$. Se puede probar de manera sencilla que esta aplicación es un morfismo de A-módulos sobreyectivo. Aplicando el primer teorema de isomorfía se tiene que $M \cong A/Ker\, f \cong A/Ann_A(m)$. Como el $Ker\, f$ es un súbmodulo de A sabemos por (3.3) que $A/Ker\, f$ es noetheriano y por tanto lo será M.

Caso general.
Sea $M =< m_1, \ldots, m_n >$. Entonces, $N =< m_1, \ldots, m_{n-1} >$ es un submódulo de M, que será noetheriano por hipótesis de inducción. Por otro lado $M/N =< m_n + N >$ es noetheriano por el caso anterior. Así que sin más que aplicar (3.3) se tiene que M es noetheriano.

■

Teorema 3.3 (De la Base de Hilbert)**.** *Sea A un anillo noetheriano, entonces $A[x]$ es un anillo noetheriano.*

Demostración:

Hagamos esta demostración por reducción al absurdo. Supongamos que $A[x]$ no es noetheriano. Tomemos un ideal I que no sea finitamente generado (f.g.), es claro que este ideal será no trivial (si no sería f.g.). Por tanto, podemos tomar $f_1(x)$ polinomio no nulo de grado mínimo en I. Llamemos $I_1 =< f_1(x) >$. Claramente $I_1 \subsetneq I$ debido a que I no es f.g. Tomemos ahora $f_2(x) \in I - I_1$, polinomio no nulo de grado mínimo en $I - I_1$. Definamos $I_2 =< f_1(x), f_2(x) >$. Tenemos así que $I_1 \subseteq I_2$. Si hacemos este método de manera recursiva construimos una cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$. Por otro lado si denominamos d_i al grado de $f_i(x)$, sabemos que $d_1 \leq d_2 \leq \ldots$. Designemos como b_i al coeficiente principal de $f_i(x)$. Podemos construir $< b_1 > \subseteq < b_1, b_2 > \subseteq < b_1, b_2, b_3 > \subseteq \ldots$. Esta es una cadena ascendente de ideales de A. Como A es noetheriano dicha cadena estacionará. De este modo existirá un b_{n+1} de la forma $b_{n+1} = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$ con $a_i \in A$. Construyamos ahora:

$$g(x) = f_{m+1}(x) - \sum_{i=1}^{m} a_i x^{d_{m+1} - d_i} f_i(x)$$

Si agrupamos términos tenemos que el principal (en este caso el d_{m+1}-ésimo) es $b_{m+1} - \sum_{i=1}^{m} a_i b_i = 0$. De esta forma $gr(g(x)) < d_{m+1}$. Sabemos que $g(x) \notin I_m$, porque de ser así $f_{m+1}(x) \in I_m$ y esto no es posible por cómo hemos escogido $f_{m+1}(x)$. Colegimos entonces que $g(x) \in I - I_m$. Pero entonces, como $g(x)$ tiene grado menor que d_{m+1}. Se contradice la minimalidad de grado de $f_{m+1}(x)$. Llegamos así a un absurdo, originado por el hecho de suponer que $A[x]$ no era noetheriano.

■

De manera evidente, aplicando inducción, se deduce el siguiente corolario. La prueba del mismo no entraña dificultad ninguna, ni aporta información. Así que la ignoraremos.

Corolario 3.3.1. *Sea A un anillo noetheriano, entonces $A[x_1, \ldots, x_n]$ es un anillo noetheriano.*

Con estos dos resultados, unidos a la proposición (3.3), tenemos controlada la noetherianidad de gran parte de las estructuras que podemos construir de manera finita a partir de anillos.

Nuestro objetivo, a partir de ahora y hasta el final de esta sección, es ver que lo que en principio habíamos definido como condiciones de cadena duales (noetherianidad

y artiniandidad), no tienen resultados duales. Para ello probaremos que todo anillo artiniano es noetheriano.

Definición 3.7. ***La dimensión de Krull*** *de un anillo, A, es el supremo de las longitudes de las cadenas de ideales primos de dicho anillo. Nótese que una cadena de ideales primos sobre P, ideal primo propio de A, de longitud n, es de la forma* $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n = P$.

De aquí en adelante no referiremos a la dimensión de Krull de un anillo, A, simplemente como la dimension de A e incluso como $dim_K(A)$. Es sencillo probar que la dimension de A es nula si y solamente si todo ideal primo de A es maximal.

Definición 3.8. ***El radical de Jacobson*** *de un anillo, A, notado por* $J(A)$ *es la intersección de todos los ideales maximales de A.*

Definición 3.9. ***El nilradical*** *de un anillo, A, notado por* $nil(A)$ *es el ideal formado por todo los elementos nilpotente de A.*

Para poder hacer esta última definición tendríamos que probar que, efectivamente, el conjunto formado por todos los elementos nilpotentes de un anillo tiene estructura de ideal. No obstante, esto último es un ejercicio simple que obviaremos.

Proposición 3.13. *Sea A, un anillo,* $Spec(A) := \{P,$ *ideales propios primos de* $A\}$. *Se tiene que:*

$$nil(A) = \bigcap_{P \in Spec(A)} P$$

Demostración:

En aras de no alargar esta sección más de lo necesario no comentaremos esta demostración en detalle. Tan solo bocetaremos la idea principal (véase proposición 1.8 de [3] para mas detalle). La demostración se hace por doble inclusión. Se toma un elemento del nilradical, r, y se prueba que esta en cualquier ideal primo. Usando que $r^m = 0 \in P$ e inducción. Para la otra inclusión se razona con un elemento que no está en el radical y se prueba que no está en un ideal primo en particular (que definiremos a continuación). Se construye un conjunto formado por los ideales que no contienen a ninguna potencia del elemento en cuestión . Se toma la inclusión como relación de orden parcial y se prueba la existencia de elemento máximo en cada cadena. Usamos el lema de Zorn y probamos que el maximal es primo.

■

Como es claro, si la $dim_K(A) = 0$, los ideales primos y maximal coinciden y, por tanto, su intersección es la misma. Los cuerpos, por ejemplo tiene dimensión nula. Nótese que en los casos de los D.I., el ideal $< 0 >$ es primo, así que, la dimensión será mayor que o igual que 1. En el caso particular de los D.I.P., como por ejemplo $\mathbb{Z}$, se puede probar que todo ideal no nulo primo, es maximal (véase capítulo 1 de [3]), luego, su dimensión es 1.

Proposición 3.14. *Si* $dim_K(A) = 0$, *se tiene que* $nil(A) = J(A)$

Proposición 3.15. *Todo anillo artiniano tiene un número finito de ideales maximales.*

Demostración:

Sea A, un anillo artiniano. Sea $S :=$ { las intersecciones finitas de ideales maximales de A}. Denotaremos a los ideales maximales por M_i. Si A tiene algún ideal propio (i.e. A no es ni un cuerpo ni trivial, casos extremos en los que el enunciado carece de sentido) A tiene algún ideal maximal. Por tanto, $F \neq \emptyset$ y como A es artiniano , F tiene un elemento minimal, $M_1 \cap M_2 \cap \ldots \cap M_n$. Cualquier otro ideal maximal es uno de estos y por tanto el conjunto de ideales maximales es finito. Veamoslo, suponiendo que M no es alguno de los de la intersección. Tomemos un ideal máximal de A, M. Por máximalidad $M \nsubseteq M_i$, $\forall i \in \{1,\ldots,n\}$. Escojamos $a_1 \in M_i - M$, $\forall i \in \{1,\ldots,n\}$. De aquí, inducimos que $a_1 a_2 \ldots a_n \in M_1 \cap M_2 \cap \ldots \cap M_n$, pero $a_1 a_2 \ldots a_n \notin M$, por ser M primo. De donde se deriva que $M \cap M_1 \cap M_2 \cap \ldots \cap M_n \subsetneq M_1 \cap M_2 \cap \ldots \cap M_n$. Llegando a una contradicción con la minimalidad de $M_1 \cap M_2 \cap \ldots \cap M_n$ en F

■

Proposición 3.16. *En un anillo artiniano A, el nilradical es nilpotente.*

Demostración:

Supongamos que el nilradical no es nilpotente. Podemos construirnos: $nil(A) \supsetneq nil^2(A) \supsetneq \ldots nil^n(A) \supsetneq$. Como es una cadena descendente en un anillo atiniano, estaciona i.e. $nil^n(A) = nil^{n+1}(A) = \ldots$. Por lo supuesto $nil^n(A) \neq 0$. Por tanto existen ideales de A de forma que $Inil^n(A) \neq \{0\}$. En particular tomando $nil(A) = I$, es claro que, $nil^{n+1}(A) \neq \{0\}$ porque si fuese al contrario llegaríamos a una contradicción. Como el anillo es artininano y la familia de ideales de A que al multiplicar al $nil(A)$ es no vacía, se tiene que dicha familia tiene un elemento minimal, J. Tenemos que $Jnil(A) \neq \{0\}$, por tanto, sabemos que $\exists a \in J$ de forma que $anil(A) \neq \{0\}$. Como $a \in J$, se deduce que $< a > \subseteq J$ y por la minimalidad de J, se tiene que $< a >= J$. Por otro lado, como $(anil^n(A))nil^n(A) = anil^{2n}(A) = anil^n(A) \neq \{0\}$ y $anil^n(A) \subseteq < a >= J$; por la minimalidad de J, $< a >= anil^n(A)$. De modo que existirá un $x \in nil^n(A)$ que verifique que $ax = a$. Claramente, $a = ax = ax^2 = \ldots = ax^n = \ldots ax^t = a0 = \{0\}$, debido a que $nil^n(A) \subseteq nil(A)$. Pero si $a = 0$, llegamos a una contradicción con que $anil^n(A)$. Así que el nilradical es nilpotente.

■

Necesitamos de un último lema para probar el teorema que estamos persiguiendo. La demostración de este lema previo requiere de algunos conceptos de anillos que no hemos introducido. A fin de que esta "pequeña incursión"no deje de serlo adjuntaremos una referencia para ver la demostración en vez de mostrarla.

Lema 3.4. *Sea A un anillo donde un producto finito de ideales máximos es* $\{0\}$. *Entonces A es noetheriano si y solamente si A es artiniano.*

Demostración:

Véase corolario 6.11 de [3].

■

Tras está concatenación de resultados estamos en disposición de probar el resultado prometido anteriormente.

Teorema 3.4. *Los anillos artinianos son noetherianos de dimensión de Krull nula.*

Demostración:

Tomemos A, un anillo artiniano, veamos que es noetheriano y $dim_K(A) = 0$. Probemos primero que $dim_K(A) = 0$ i.e. todo ideal primo es maximal. Tomemos P un ideal primo de A. Como sabemos de (3.8), $S = A/P$ es artiniano y un dominio de integridad. Escojamos $b \in S$ no nulo. Como S es artiniano, $< b > \supseteq < b^2 > \supseteq < b^3 > \supseteq \ldots$ estaciona. Por tanto, existirá un $n \in \mathbb{N}$ de manera que $< b^n > = < b^{n+1} >$. Así que, para algún $c \in S$, tenemos que $b^n = b^{n+1}c$. De este modo $b(b^{n-1} - b^n c) = 0$ y como $b \neq 0$ y S es un dominio, deducimos que $b^{n-1} - b^n c = 0$. Haciendo esto (n-1)-veces , llegamos a que $1 = bc$. Es decir, cada $b \in S$ no nulo es invertible. Lo que que quiere decir que S es un cuerpo y equivalentemente P es maximal. Veamos ahora que A es noetheriano. Sabemos por (3.15) que A tiene n ideales maximales (que notaremos por M_i). Es claro que $M_1 \ldots M_n \subseteq M_1 \cap \ldots \cap M_n = J(A)$. Aprovechando lo que acabamos de probar y (3.14), tenemos que $M_1 \ldots M_n \subseteq M_1 \cap \ldots \cap M_n = J(A) = nil(A)$. Por (3.16), existirá una potencia r , de manera que $(M_1 \ldots M_n \subseteq M_1)^r = 0$. Usando (3.4) A es noetheriano.

■

Se podría probar, de hecho, que los anillos artinianos son exactamente los noetherianos de dimensión de Krull nula. No obstante, necesitaríamos introducir el concepto de descomposición primaria de un ideal (véase [3]). Aún con esto, es suficiente lo obtenido para mostrar la ruptura de la presunta dualidad. Lo que acabamos de mostrar es que los anillos artinianos son una particularización de los noetherianos.

El resultado encuentra rápida aplicación como criterio negativo. Usando este teorema podemos mostrar que si $n \geq 3$, $A[x_1, x_2, \ldots, x_n]$, no es artiniano. Es claro que $A[x_1, x_2, \ldots, x_n]/ < x_1 > \cong A[x_1, x_2, \ldots, x_{n+1}]$ es un dominio de integridad (véase el lema 3.7 de [14]). De este modo $< x_1 >$ es primo. Pero no maximal pues $< x_1 > \subsetneq < x_1, x_2 > \subsetneq A[x_1, x_2, \ldots, x_n]$. Por tanto la dimensión de Krull no es nula y no puede ser Artiniano. Perdiendo la esperanza de construir un equivalente inmediato al Tª de las Bases de Hilbert en caso artiniano.

En el caso de módulos, en general, no es cierto que un módulo artiniano deba de ser noetheriano. Como contraejemplo podemos citar el grupo de Prüfer (los grupos abelianos se pueden ver como $\mathbb{Z}$-módulos).

Definición 3.10. *Se define el grupo de Prüfer, $\mathbb{Z}(p^\infty)$ para el primo p dentro de $\mathbb{Q}/\mathbb{Z}$ como el conjunto de clases de la forma $\frac{a}{p^r} + \mathbb{Z}$, con $r \in \mathbb{N}$.*

Mostremos que es un grupo y estudiemos la estructura de subrupos.
Claramente como $\mathbb{Q}/\mathbb{Z}$ es un grupo abeliano, si probamos que $\mathbb{Z}(p^\infty)$ es un subgrupo suyo será automáticamente abeliano. Tomemos $\frac{a}{p^r} + \mathbb{Z}$, un elemento en $\mathbb{Z}(p^\infty)$. Es claro que $-\frac{a}{p^r} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$. Por otro lado tomemos dos elementos de $\mathbb{Z}(p^\infty)$, por ejemplo $\frac{a}{p^r} + \mathbb{Z}$ y $\frac{b}{p^s} + \mathbb{Z}$, con r>s. Tenemos que $(\frac{a}{p^r} + \mathbb{Z}) + (\frac{b}{p^s} + \mathbb{Z}) = (\frac{a}{p^r} + \frac{b}{p^s}) + \mathbb{Z} = \frac{a - bp^{r-s}}{p^r} + \mathbb{Z}$, que está contenido en $\mathbb{Z}(p^\infty)$. Con esto hemos probado $\mathbb{Z}(p^\infty)$ es un grupo abeliano (un $\mathbb{Z}$-módulo).

Veamos ahora los órdenes de los elementos. Tomemos $\frac{a}{p^r} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$. Si multiplicamos adecuadamente, $p^r(\frac{a}{p^r} + \mathbb{Z}) = a + \mathbb{Z} = 0 + \mathbb{Z}$; por tanto $ord(\frac{a}{p^r} + \mathbb{Z}) | p^r$. Así que, $ord(\frac{a}{p^r} + \mathbb{Z})$ es una potencia de p. De este modo, $\mathbb{Z}(p^\infty)$ es un p-grupo. De hecho es un p-grupo infinito. Para ver está evidencia basta con probar que $\forall s, r \in \mathbb{N}$ distintos , $\frac{1}{p^r} + \mathbb{Z} \neq \frac{1}{p^s} + \mathbb{Z}$. Si $\frac{1}{p^r} + \mathbb{Z} = \frac{1}{p^s} + \mathbb{Z}$, tenemos que $\frac{1}{p^r} - \frac{1}{p^s} \in \mathbb{Z}$. Suponiendo que

$r > s, \dfrac{1-p^{r-s}}{p^r} = z \in \mathbb{Z}$ o equivalentemente $zp^r + p^{r-s} = 1$. Aplicando el Tª de Bezout, $p^{r-s}|1$, lo que es absurdo.

Proposición 3.17. *Sea $H \leqslant \mathbb{Z}(p^\infty)$, si existe cota superior para los órdenes de los elementos de H, entonces H es cíclico. En caso contrario H=$\mathbb{Z}(p^\infty)$.*

Demostración:

Como $\mathbb{Z}(p^\infty)$ es p-grupo, si los órdenes de los elementos de H están acotados, tomando la menor de las cotas superiores. La cota será p^r con r fijo en los naturales. Veamos que H=$< \frac{1}{p^r} + \mathbb{Z} >$. Si la cota es p^r, existirá un elemento de la forma $\frac{a}{p^r} + \mathbb{Z}$ en $\mathbb{Z}(p^\infty)$ con (a,p)=1. En caso contrario llegaríamos a un absurdo. Por el Tª de Bezout $\exists u, v \in Z$ de forma que $1 = ua + vp^r$. De esto se deduce que $\dfrac{1}{p^r} = u\dfrac{a}{p^r} + v$. Tomando clases, tenemos que $\dfrac{1}{p^r} + \mathbb{Z} = u\dfrac{a}{p^r} + v + \mathbb{Z} = u\dfrac{a}{p^r} + \mathbb{Z}$ y por tanto, H$\supseteq < \frac{1}{p^r} + \mathbb{Z} >$. Veamos la otra inclusión. Tomemos $\frac{b}{p^s} + \mathbb{Z} \in H$ con (b,p)=1. Como $ord(\frac{b}{p^s} + \mathbb{Z}) = s < r$, tenemos que $\frac{b}{p^s} + \mathbb{Z} = p^{r-s} b \frac{1}{p^r} + \mathbb{Z} \in < \frac{1}{p^r} + \mathbb{Z} >$. De este modo H es cíclico. En caso de que los órdenes de H no estén acotados. Tomando $\frac{a}{p^r} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$ con (a,p)=1, $ord(\frac{a}{p^r} + \mathbb{Z}) = r$. Como los órdenes de H no están acotados existirá un elemento de H con la forma $\frac{b}{p^n} + \mathbb{Z}$, con n>r y (b,p)=1. Si aplicamos el Tª de Bezout de la misma manera que antes, obtenemos que, $\frac{1}{p^n} + \mathbb{Z} \in$ H. Como, $\frac{a}{p^r} + \mathbb{Z} = ap^{n-r}(\frac{1}{p^n} + \mathbb{Z}) \in$H, hemos probado que $\mathbb{Z}(p^\infty) = H$.

■

Por lo demostrado en el resultado anterior, los subgrupos propios de $\mathbb{Z}(p^\infty)$ son exactamente aquellos con la forma $< \frac{1}{p^r} + \mathbb{Z} >, \forall r \in \mathbb{N}$. Claramente $< \frac{1}{p^r} + \mathbb{Z} > \subseteq < \frac{1}{p^{r+1}} + \mathbb{Z} >$, ya que $\frac{1}{p^r} + \mathbb{Z} = p(\frac{1}{p^{r+1}} + \mathbb{Z}) \in < \frac{1}{p^{r+1}} + \mathbb{Z} >$. Por otro lado, podemos probar que la inclusión es estricta. Veamos que $\frac{1}{p^{r+1}} + \mathbb{Z} \notin < \frac{1}{p^r} + \mathbb{Z} >$. Supongamos que no fuese así. Se tendría, que existiría $a \in \mathbb{Z}$, de manera que $\frac{1}{p^{r+1}} + \mathbb{Z} = \frac{a}{p^r} + \mathbb{Z}$. Equivalentemente, $\frac{1}{p^{r+1}} - \frac{a}{p^r} = z \in \mathbb{Z}$. Esto es, $\dfrac{1-ap}{p^{r+1}} = z \Rightarrow 1 = ap + p^{r+1} \Rightarrow 1 = (a + p^r)p$ y concurrimos en un absurdo, debido a que las únicas unidades en $\mathbb{Z}$ son ± 1. Por tanto todos los submódulos (subgrupos) propios de $\mathbb{Z}(p^\infty)$ se encuentran en la siguiente cadena ascendente infinita.

$$< \frac{1}{p^1} + \mathbb{Z} > \subsetneq < \frac{1}{p^2} + \mathbb{Z} > \subsetneq \ldots \subsetneq < \frac{1}{p^r} + \mathbb{Z} > \subsetneq < \frac{1}{p^{r+1}} + \mathbb{Z} > \subsetneq \ldots$$

Mostrando que cualquier cadena descendente de submódulo de $\mathbb{Z}(p^\infty)$ estaciona i.e. es artiniano. No obstante, la cadena que acabamos de escribir, por ejemplo, si la vemos como una cadena ascendente jamás estaciona i.e. no es noetheriano.

4

Caso $\mathbb{Z}$

En este capítulo, estudiaremos los teoremas de estructura para $\mathbb{Z}$-módulos noetherianos y artinianos, usando el teorema de descomposición de módulos noetherianos y artinianos. Antes de meternos propiamente en materia, notemos, que los $\mathbb{Z}$-módulos son los grupos abelianos. Por un lado, de la definición de módulo, emana que cualquier módulo es un grupo abeliano. Por otro, sea G un grupo abeliano, definimos, $* := \mathbb{Z} \times G \longrightarrow G$ como $z * g = zg$. si $z \geq 0$ y $z * g = -z(-g)$, si $z < 0$. El segundo producto es el que se origina de manera natural en el grupo al sumar z-veces. Sea $z, z_1, z_2 \in \mathbb{Z}$ y $g, g_1, g_2 \in G$, la aplicación verifica:

i) $z_1 * (z_2 * g) = z_1(z_2 g) = (z_1 z_2)g = (z_1 z_2) * g$

ii) $(z_1 + z_2) * g = (z_1 + z_2)g = z_1 g + z_2 g = z_1 * g + z_2 * g$

iii)$z * (g_1 + g_2) = z(g_1 + g_2) = zg_1 + zg_2 = z * g_1 + z * g_2$

iv)$1 * g = 1g = g$

Por tanto, (G,+,*) es un $\mathbb{Z}$-módulo. De manera análoga, se haría para los escalares negativos. Además de esta observación, veamos unos resultados que aplicaremos tanto en el caso artiniano como noetheriano.

Lema 4.1. *Sean $n, m \in \mathbb{N}^*$, se tiene que $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$ si y solamente si $(n, m) = 1$*

Demostración:

Véase teorema 2.36 de [23].

■

Lema 4.2. *Sea G un p-grupo abeliano finito, y supongamos que $g \in G$ tiene orden maximal. Entonces $G \cong < g > \oplus H$ para algún H subgrupo de G.*

Demostración:

Véase lema 13.1.9 de [17]

■

Teorema 4.1 (de Estructura de Grupos Abelianos Finitos)**.** *Todo grupo abeliano finito descompone de forma única en suma directa finita de cíclicos de orden la potencia de un primo, con las bases no necesariamente distintas*

Demostración:

Sea G un grupo abeliano finito. Entonces G es un $\mathbb{Z}$-módulo noetheriano y artiniano, por ser finito, el retículo de submódulos es finito y cualquier cadena, ascendente o descendente, estaciona. Aplicando el teorema de descomposición de módulos noetherianos y artinianos, admite una descomposición única, salvo orden, en suma directa finita de subgrupos indescomponibles. Supongamos que H es uno de estos subgrupos indescomponibles. Su orden ha de ser potencia de un primo, porque si no lo fuese, $|H|$ sería un producto finito de potencias $p_i^{e_i}$. Sin embargo, los Teorema de Sylow implicarían que H sería la suma directa finita de grupos de órdenes $p_i^{e_i}$, lo que contradice la irreducibilidad de H, a menos que solo haya un subgrupo. Con esta argumentación llegamos a que H, ha de ser de orden potencia de un primo. Faltaría ver que es cíclico. Como H es finito, tendrá un elemento de orden máximal, g, y por el lema anterior, $H =< g > \oplus H_1$, si H no es cíclico, $H_1 \neq \{0\}$ y el grupo no es indescomponible, luego, H ha de ser cíclico de orden la potencia de un primo. Además, evidentemente,

cualquier grupo cíclico de orden la potencia de un es indescomponible. Todo subgrupo de un grupo cíclico es cíclico y su orden divide al orden del grupo. De este modo, si $\mathbb{Z}_{p^e}$ descompusiese, lo haría en $\mathbb{Z}_{p^a}$ y $\mathbb{Z}_{p^b}$, con $a+b=e$, pero si $\mathbb{Z}_{p^e} = \mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}$, por (4.1), $(p^a, p^b) = 1$, lo que es absurdo, luego $\mathbb{Z}_{p^e}$ no tiene descomposiciones no triviales.

■

4.1 $\mathbb{Z}$-módulos Noetherianos

Como veremos, casi a reglón seguido, los $\mathbb{Z}$-módulos noetherianos son exactamente los grupos abelianos finitamente generados. Luego, lo que vamos a hacer en esta sección es rehacer una demostración del teorema de estructura de grupos abelianos finitamente generados (f.g.) a partir del teorema de estructura de módulos noetherianos.

Veamos que, efectivamente, los $\mathbb{Z}$-módulos noetherianos coinciden con los grupos abelianos finitamente generados. Como sabemos, todo $\mathbb{Z}$-módulo es un grupo abeliano y además al ser noetheriano cualquier submódulo suyo, en particular, él mismo, es finitamente generado. Ahora, sea G un grupo abeliano finitamente generado. Hemos visto, en el inicio del capítulo, que todo grupo abeliano se puede ver como un $\mathbb{Z}$-módulo. Si recurrimos a (3.12), concluimos que G en un $\mathbb{Z}$-módulo noetheriano. Puesto que $\mathbb{Z}$ es un anillo notheriano. Esto último, lo podemos afirmar, porque los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, i.e., son todos cíclicos (en general, f.g.).

Recordemos, que el teorema de estructura de módulos noetherianos y artinianos decía que todo A-módulo noetheriano o artiniano descomponía como suma directa de submódulos indescomponibles. Así que, la idea será ver como son esos submódulos indescomponibles.

En general, que un módulo sea finitamente generado no garantiza que un submódulo lo sea, de hecho, eso forma parte de la motivación del concepto de notheriano. Si tomamos cualquier anillo no noetheriano, por ejemplo, $\mathbb{Z}[x_1, x_2 \ldots]$; y lo consideramos como un módulo sobre sí mismo, es finitamente generado, porque está generado por el 1. Pero tiene que haber algún ideal (submódulo) que no sea finitamente generado, porque si no, el anillo sería noetheriano y no puede serlo. En nuestro ejemplo, porque la cadena $< x_1 > \subset < x_2, x_1 > \subset \ldots$ no estaciona. No obstante, en el caso de los grupos abelianos ,i.e, los $\mathbb{Z}$-módulos, sí se puede asegurar. Como los grupos abelianos finitamente generados coinciden con los $\mathbb{Z}$-módulos noetherianos, cualquier subgrupo será un submódulo de un módulo noetheriano. De esta forma, por (3.3) el submódulo será noetheriano o dicho de otro modo, un grupo abeliano finitamente generado. Luego, solo tenemos que estudiar cuales son los Z-módulos indescomponibles finitamente generados.

Definición 4.1. *Sea G un grupo, llamaremos **parte torsión de** G o $t(G)$ al siguiente conjunto:*

$$t(G) = \{g \in G \ \ tales \ \ que \ \ \exists n \in \mathbb{N}^* / ng = 0\}$$

O dicho de otro modo, los elementos de orden finito de G.

En esta definición, hemos optado por la notación aditiva, porque así estamos procediendo en todo el texto. No obstante, la parte torsión se podría definir para un grupo no abeliano sin problema. Aunque, en ese caso, no tiene porque ser, en general, un grupo; como veremos que si sucede si el grupo es abeliano.

Los módulo son, en particular, grupos abelianos, así que, cuando nos referimos a la parte torsión de un módulo, lo haremos entendiendo que es un grupo. Nótese, que ese caso, el producto que define los elementos torsión no se refiere al producto por el anillo, si no al generado por la suma.

Podemos comprobar, que en el caso abeliano, la parte torsión de un módulo en un submódulo suyo. Para ello, hay que probar que es un subgrupo y que el producto por escalares no queda fuera del subconjunto.

- La suma es interna. Supongamos $x, y \in t(M)$, tenemos que ver que $x+y \in t(M)$. Como, $x, y \in t(M)$ ambos tienen orden finito, sean estos n_1, n_2 respectivamente. Considerando $n = n_1 n_2$, tenemos, $n(x+y) = nx+ny$, por ser la suma de M conmutativa. Por otro lado, $n = n_1 + n_2$, así que, $nx + ny = n_1 n_2 x + n_1 n_2 y = n_2 n_1 x + n_1 n_2 y = 0$. Luego, $ord(x+y)$ es finito.

- Existencia de opuestos. Tenemos que probar que si $x \in t(M)$, es decir tiene orden finito, $-x$ también lo tiene. Si $ord(x) = n$, se tiene que $n(-x) = -(nx) = -0 = 0$. De esta forma, el orden de $-x$ es finito.

- El producto por escalares es cerrado. Veamos que si x tiene orden finito y $a \in A$, $a * x$ tiene orden finito. Llamemos n al orden de x. Entonces:

$$n(a*x) = \overbrace{a*x+\ldots+a*x}^{n} = a*(\overbrace{x+\ldots+x}^{n}) = a*(nx) = a*0 = 0$$

  El hecho de que $a*0 = 0$, deriva directamente de la propiedad de que $a*(x+y) = a*x + a*y$.

De esta forma, acabamos de probar que en caso de que M sea un grupo abeliano, $t(M)$ es un subgrupo suyo. La conmutatividad es fundamental. En el caso no abeliano, no sucede que $t(M)$ sea un submódulo. Veamos, por ejemplo, el $\mathbb{Z}$-módulo diédrico infinito, cuya presentación como grupo es $< s, t | s^2 = id, st = t^{-1}s >$. No es abeliano, porqué s y t no conmutan. Si conmutasen $ts = st = t^{-1}s$, y multiplicando por s^{-1} a ambos lados, llegamos a que $t = t^{-1} = id$. Lo que es absurdo, porqué t es generador. Tenemos que st^2 y st son de orden finito, $(st)(st) = (st)(t^{-1}s) = s^2 = id$ y $(st^2)(st^2) = (st^2)(t^{-1}st) = stst = id$. No obstante, su producto, $(st^2)(st) = st^2t^{-1}s = sts = t^{-1}s^2 = t^{-1}$; y t^{-1} tiene orden infinito, porque si fuese finito, t tendría orden finito, cosa que es absurda.
Hemos ido cambiando la notación de aditiva a producto, como es tradicional, en casos abelianos y no abelianos respectivamente.

Definición 4.2. *Sea M un A-módulo, diremos que M es un módulo* ***libre de torsión****, si el único elemento con orden finito, es el 0. De manera similar* ***llamaremos parte libre de*** *M o $l(M)$ a los elementos de orden no finito de M y al 0.*

El plan a seguir a partir de este punto, es el siguiente:

1. Demostrar que un grupo libre de torsión finitamente generado es libre.

2. Dividir el grupo en suma de un modulo libre de torsión y el submódulo de torsión.

3. Descomponer la parte torsión.

4. Probar la unicidad.

En el inicio, ya hemos comentado la correspondencia unívoca entre $\mathbb{Z}$-módulos noetherianos (los cuales son, particularmente finitamente generados) y grupos abelianos finitamente generados. A partir de aquí, vamos a emplear los dos conceptos, según necesitemos, de manera indistinta. Recordemos, además, que $\mathbb{Z}$ es un D.I.P.; todos sus ideales son de la forma $n\mathbb{Z}$.

Proposición 4.1. *Sea A un D.I.P. y M un A-módulo libre de rango finito, entonces, todo submódulo no trivial, N, de M es libre.*

Demostración:

Existen demostraciones que no están ligadas al caso finito, véase teorema 9.8 de [21], no obstante, en nuestro caso, como estamos estudiando módulos finitamente generados nos restringiremos al caso finito. Si M es libre, $M \cong A^n$ para algún $n \in N$. Hagamos inducción sobre n.

Caso 1.

Si $M \cong A$, cualquier submódulo $N \cong I$, donde I es un ideal de A. Como A es D.I.P. $I =< a >$, para algún $a \in A$. Si $a = 0$, $N \cong \{0\}$ y N es trivial, pero por hipótesis no podía serlo. Si $a \neq 0$, se puede probar que $A \cong< a >$. Sin más que usar el morfismo que a cada $x \in A$ lo asocia a ax. Este morfismo es, claramente, sobreyectivo y es inyectivo, porque A es un D.I.P., particularmente un D.I. Por tanto, $A \cong< a > \cong N$ y de esta forma N es libre.

Caso general.

Supongamos que para cada $k < n$ se verifica la tesis, probémoslo para el caso n. Como estamos en el caso finitamente generado, $M =< m_1, \ldots, m_n >$. Sea N un submódulo de M, tomemos la aplicación $\pi : M \to A$, definida por $\pi(x_1 m_1 + \ldots x_n m_n) = x_n$(la proyección canónica). Construimos la siguiente sucesión exacta corta:

$$0 \longrightarrow N \cap Ker\,\pi \xrightarrow{id} N \xrightarrow{\pi} \pi(N) \longrightarrow 0$$

La identidad es un morfismo inyectivo y trivial, la proyección canónica es un morfismo sobreyectivo (por la definición de finitamente generado) y $Im\,id = Ker\,\pi \cap N = Ker\,\pi|_N$. Así que, tenemos una sucesión exacta corta que termina en $\pi(N)$, un ideal de A, que por ser A un D.I.P., como se ha comentado en el caso 1, es un módulo libre, en general proyectivo, y de esta forma, la sucesión exacta corta escinde. Llegamos a que $N = (N \cap Ker\,\pi) \oplus \pi(N)$. A través del morfismo $f : Ker\,\pi \to A^{n-1}$ definido por $f(a_1 x_1, \ldots, a_{n-1} x_{n-1}) = (a_1, \ldots, x_{n-1})$, podríamos probar que $Ker\,\pi \cong A^{n-1}$, o dicho de otra manera, $Ker\,\pi$ es libre. Luego, aplicando hipótesis de inducción, $N \cap Ker\,\pi$, es libre, además, como $\pi(N)$ era libre (ya lo hemos argumentado); concluimos que $N = N \cap Ker\,\pi \oplus \pi(N)$ es libre, por ser suma directa de libres.

■

En general, podemos ver que todo submódulo de un libre no tiene porque ser libre. Si tomamos el anillo $\mathbb{Z}_6$, visto como módulo sobre sí mismo, es libre. Pero el submódulo formado por $\{0, 3\}$, no puede ser libre, porque tiene dos elementos. Si fuese libre, tendría que tener por lo menos seis elementos, los mismos que los del anillo.

Proposición 4.2. *Si A es un D.I.P., un A-módulo finitamente generado, no nulo y libre de torsión es libre.*

Demostración:

Tomemos $M =< m_1, \dots, m_s >$ un A-módulo verificando todas las hipótesis. Como A es D.I.P., todo sus ideales son finitamente generados y por tato, A es noetheriano, de este modo M es noetheriano (por ser un módulo finitamente generado sobre un anillo noetheriano). Consideramos la familia $F := \{N =< A >$, donde A es un subconjunto de $\{m_1, \dots, m_s\}$, tal que N sea un submódulo libre de $M\}$. Sabemos que M es libre de torsión, así que, si $am_1 = 0$, tenemos que $a = 0$, para todo $a \in A$. Debido a esto, $< m_1 > \in F$ y de esta forma la familia no es vacía. Denominamos al máximal de la familia N. Reordenamos, sin perdida de generalidad, $\{m_1, \dots, m_s\}$, de tal manera que $N =< m_1, \dots, m_k >$, con $k \leq s$. Si $k = s$, $N = M$ y damos por concluida la prueba. En caso contrario, para todo $i \in \{k+1 \dots s\}$, existirá un $a_i \neq 0 \in A$, de forma que $a_i m_i = \sum_{j=1}^{k} a_{j(i)} m_j$. Si esto no sucediese, tendríamos un sistema linealmente independiente y $< m_1, \dots m_k, m_i > \in F$, concluyendo en un absurdo. Debido a la maximalidad de N. Consideremos $a = a_{k+1} \dots a_s$, $am_i \in N$, para todo $i \in \{1 \dots s\}$. De esta modo, $aM \subseteq N$, por el teorema anterior, aM es libre. Consideramos, el morfismo sobreyectvo de M a aM definido por la multiplicación por a, que es inyectivo por ser M libre de torsión. Llegamos así, a que $aM \cong M$ o dicho de otro modo que M es libre.

■

Terminamos el primer punto del esquema sin más que observar que: Los grupos finitamente generados abelianos son $\mathbb{Z}$-módulos finitamente generados; y aplicar el resultado anterior. De esta forma, un grupo libre, descompone como suma directa de copias de $\mathbb{Z}$, que es indescomponible por ser un dominio de integridad no trivial, (3.1).

Vayamos al segundo punto.

Proposición 4.3. *Sea A un D.I.P., sea M, un A-módulo finitamente generado y conmutativo. Entonces M, es isomorfo a la suma directa de $t(M)$ y a un A-módulo libre de torsión.*

Demostración:

Consideramos $M/t(M)$, este módulo es libre de torsión. Supongamos que existe un elemento $\overline{x} \in M/t(M)$, de forma que $m\overline{x} = \overline{0}$, para algún $m \in \mathbb{N}^*$. Entonces, $mx \in t(M)$, lo que llevaría a que existiese $m' \in \mathbb{N}^*$, de manera que $0 = m'(mx) = (m'm)x$, luego $x \in t(M)$, o lo que es equivalente que $\overline{x} = \overline{0}$. Como el único elemento de torsión es el 0, $M/t(M)$ es libre de torsión. Consideramos la serie exacta corta:

$$0 \longrightarrow t(M) \xrightarrow{i} M \xrightarrow{\pi} M/t(M) \longrightarrow 0$$

Donde i es la inclusión y π es la aplicación que viene definida por tomar clases, ambas por definición, son morfismos, la primera es inyectivo y la segunda sobre. Bastaría probar que $Ker\,\pi = Im\,i$. Sabemos que $x \in Ker\,\pi \Leftrightarrow \overline{x} = 0 \Leftrightarrow x \in t(M) \Leftrightarrow x \in Im\,i$. Luego, efectivamente, $Ker\,\pi = Im\,i$. Como $M/t(M)$ es libre de torsión, por la proposición (4.2), es libre, en general proyectivo. Como tenemos una serie exacta corta que termina en un módulo proyectivo, la serie excinde. Concluyendo que $M = t(M) \oplus M/t(M)$.

■

Uniendo este último resultado con la proposición (4.2), tenemos que cualquier M, módulo finitamente generado sobre un D.I.P., A; lo podemos poner como $A^s \oplus t(M)$. Descompongamos $t(M)$.

La parte torsión, en el caso en el que nos encontramos, es un submódulo finito. Al principio de esta sección, comentabamos que los subgrupos de un grupo abeliano finitamente generado eran finitamente generados. Luego, $t(M) =< m_1, \ldots, m_s >$, sabemos que $ord(m_i) = n_i \in \mathbb{N}^*$, para todo $i \in I$. Como todo elemento $x \in t(M)$, es suma de los generadores, tenemos que $ord(t(M)) = n_1 \ldots n_s = n$, es decir, es finito, luego, por el teorema (4.1) es suma finita de cíclico de ordena la potencia de un primo.

Con esto, acabamos de concluir el tercer punto de nuestra planificación para la sección y podemos demostrar el teorema de estructura.

Teorema 4.2 (de Estructura de Grupos Abelianos Finitamente Generados)**.** *Sea G un grupo abeliano finitamente generado. Entonces se verifica que:*

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_2^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{a_s}}$$

Con $n \in \mathbb{N}$, $a_i \in \mathbb{N}^*$ y p_i primos (no necesariamente distinos), para todo $i \in \{1, \ldots, s\}$. Esta descomposición es única salvo isomorfismos.

Demostración:

El teorema de estructura de módulos noetherianos nos dice que todo módulo noetheriano se puede poner como suma directa de submódulos indescomponibles. Durante esta sección, hemos ido viendo cómo son esos módulos indescomponibles. Hemos visto que el grupo se podía poner como sumando de parte libre y parte torsión. La parte libre de torsión descomponía en subgrupos isomorfos a $\mathbb{Z}$ que, precisamente por ser isomorfos a un indescomponible, $\mathbb{Z}$ (es un D.I.), son indescomponibles. Después comprobamos que la parte de torsión era finita y por tanto descomponía como suma directa finita de cíclicos de orden la potencia de un primo. De este modo los subgrupos indescomponibles de un un grupo abeliano finitamente generado eran isomorfos a copias de $\mathbb{Z}$ o a cíclicos de orden la potencia de un primo. Así que, su descomposición en virtud del teorema de estructura de módulos noetherianos será isomorfa a la suma directa finita de esos grupos.

■

Lo que no hemos probado todavía, es la unicidad. En principio, si hemos visto la unicidad de descomposición de la parte torsión, faltaría la de la parte libre. Cosa que haremos ahora.

Lema 4.3. *Si M es un A-modulo e $I \leqslant A$, de manera que $I \subseteq Ann(M)$, entonces M es un A/I-módulo*

Demostración:

La estructura relacionada con la suma sigue siendo la misma, lo que cambiamos es el producto, $\overline{a} * m = rm$. Tenemos que probar que está bien definido y que verifica las propiedades pertinentes. Supongamos $(\overline{a_1}, m_1) = (\overline{a_2}, m_2)$, entonces $m_1 = m_2$ y $a_1 - a_2 \in I \subseteq Ann(M)$. De esta forma, $(a_1 - a_2)m_1 = 0 \Rightarrow a_1 m_1 = a_2 m_1$. Como el producto por elementos de A está bien definido, y $m_1 = m_2$, tenemos que $a_1 m_1 = a_2 m_2$. Con esto, el nuevo producto queda bien definido. Probemos las propiedades que ha de tener el producto por escalares para un módulo. Supongamos $\overline{a}, \overline{b} \in A/I$ y $x, y \in M$

- Asociatividad. Tenemos que $\overline{a} * (\overline{b} * x) = \overline{a} * (bx) = a(bx)$, y como el producto por elementos de A si es asociativo, $\overline{a}(\overline{b}x) = a(bx) = (ab)x = (\overline{ab}) * x = (\overline{a}\overline{b}) * x$

- Distributividad frente a la suma del módulo. Operamos y obtenemos que $\overline{a} * (x + y) = a(x + y) = ax + ay$, si aplicamos la distributividad del producto por elementos de A. Así, $\overline{a} * (x + y) = ax + ay = \overline{a} * x + \overline{a} * y$.
- Distributividad frente a la suma del anillo. Se prueba de manera muy similar al apartado anterior.
- Neutralidad de la unidad del anillo. Es claro, puesto que, $\overline{1} * x = 1 * x = x$.

■

Teorema 4.3. *Si A es un anillo conmutativo no trivial y M un A módulo libre de tipo finito, entonces el cardinal de todas las bases de M son el mismo.*

Demostración:

Si A es un cuerpo, M es un espacio vectorial y el cardinal de la base siempre es el mismo. Si A no es un cuerpo, tendrá algún ideal maximal I. Sabemos que M/IM es un A-módulo y como $I \subseteq Ann(M/IM)$, por (4.3), M/IM es un A/I-módulo con la suma usual y el producto que definimos en el anterior lema. Como A/I es un cuerpo, M/IM será un espacio vectorial. Tomemos una base de M como A-módulo, $B = \{b_1, \ldots, b_s\}$, veamos que $\overline{B} = \{\overline{b_1}, \ldots, \overline{b_s}\}$ es una base de M/IM como A/I-espacio vectorial.

- Linealmente Independiente. Supongamos $\overline{0} = \overline{a_1}\overline{b_1} + \ldots + \overline{a_s}\overline{b_s}$, con $a_i \in A$. Entonces $\overline{0} = \overline{a_1 b_1 + \ldots + a_s b_s}$, y por tanto, $a_1 b_1 + \ldots + a_s b_s \in IM$. De esta forma, $a_i \in A$, para todo $i \in \{1, \ldots, s\}$ o equivalentemente, $\overline{a_1} = 0$, para todo $i \in \{1, \ldots, s\}$.
- Sistema generador. Probemos que para cualquier $\overline{x} \in M/IM$ existen una combinación lineal finita de elementos de $\overline{B}$ que sea igual a dicho elemento. Como B es sistema generador de M, tenemos que $x = a_1 b_1 + \ldots + a_s b_s$. Sin más que tomar clases, se tiene que $\overline{x}$ es combinación lineal de elementos de $\overline{B}$.

De esta forma, si tuviésemos dos bases en M con distinto cardinal, tendríamos dos bases en el espacio vectorial M/IM con distinto cardinal, cosa que no tiene sentido.

■

A este cardinal, que es único, lo llamamos **rango** del módulo libre M. Como el número de copias de $\mathbb{Z}$ que aparecía en la descomposición de G se correspondía con el cardinal de la base de $G/t(G)$, que era un $\mathbb{Z}$-módulo libre, con este último resultado, hemos probado que viene unívocamente determinado.

Con esto, terminamos el teorema de estructura de $\mathbb{Z}$-módulos noetherianos.

4.2 $\mathbb{Z}$-módulos Artinianos

Para este caso, necesitaremos hablar de una clase de grupos de los que todavía no hemos hablado. Los grupos divisibles. Sea G un grupo abeliano , $g \in G$ y un natural no nulo, n. Diremos que n divide a g, expresado como $n|g$, si existe un $h \in G$ de manera que $nh = g$. De esta forma, se tiene que:

Definición 4.3. *Diremos que un grupo abeliano, G, es **divisible**, si para todo $n \in \mathbb{N}^*$ y para todo $g \in G$, $n|g$. A su vez, diremos que un grupo abeliano, H, es **reducido**, si ningún subgrupo suyo salvo el trivial es divisible.*

El camino que seguiremos en esta sección para probar el teorema de estructura de grupos abelinos artiniano es el siguiente:

1. Todo grupo abeliano puede descomponer de manera única como suma de un subgrupo divisible y otro reducido.
2. Todo grupo abeliano artiniano divisible se puede ver como suma finita de grupos de Prüfer.
3. Todo grupo abeliano artiniano reducido es finito.
4. Todo grupo abeliano artiniano descompone como suma finita de grupos de Prüfer y grupos cíclicos de orden la potencia de primos (no necesariamente distintos).

Empecemos por el primer punto del esquema. Veamos que cualquier grupo abeliano lo podemos poner como suma directa de un subgrupo reducido y uno divisible. Para ello, necesitamos probar algunos resultados previos.

Proposición 4.4. *Si D es un grupo divisible, es inyectivo.*

Demostración:

Sean A y B dos grupos, $f : A \to B$, un morfismo de grupos inyectivo y $g : A \to D$ un morfismo de grupos. Veamos que existe un morfismo $h : B \to D$, de manera que, $hf = g$. Como f es un morfismo, podemos ver $f(A)$ como un subgupo de B. Consideramos G un subgrupo entre $f(A)$ y B, de manera que exista $\xi : G \to D$, un morfismo, que extienda a $gf^{-1}|_{f(A)}$. Esta inversa existe, porque al ser f inyectiva, $A \cong f(A)$

La familia de pares, F, de la forma, (G, ξ), es no vacía, puesto que, $(f(A), gf^{-1}|_{f(A)})$ pertenece a la misma. Establecemos en la familia la relación de orden parcial usual en este tipo de pares. Diremos que $(G, \xi) \leqq (G', \xi')$, si $G \supseteq G'$ y ξ' extiende a ξ. No mostraremos que esto es una relación de orden, porque esta técnica es muy usada y la prueba alargaría en exceso la demostración. Lo que si probaremos, es que es inductiva. Veamos que la cadena $(G_i, \xi_i)_{i \in I}$ tiene un elemento máximo. Tomemos $G = \cup_{i \in I} G_i$ y $\xi = G \to D$, definida por ξ_i para cada elementos en G_i. Mostremos que (G, ξ) es el elemento máximo de la cadena. Lo primero, es probar que G es un grupo entre $f(A)$ y B. Usualmente la unión arbitraria de grupos no es grupo, porque la suma de elementos no esta en la unión; pero en este caso, al estar encajados unos grupos dentro de otros, si se tiene que $x+y$ está en la unión. Tanto el elemento x como el y, estarán cada uno en un G_i, con $i \in I$, considerando el máximo entre los dos subíndices, j, ambos elementos estarán en G_j, en él la suma si es interna y de ese modo, $x + y$ estará en la unión. Además, $f(A) \subseteq G \subseteq B$, dado que $f(A) \subseteq G_1 \subseteq G$ y para cada $x \in G$, existirá un $i \in I$, de manera que $x \in G_i \subseteq B$. Respecto a ξ, está bien definida porque si $x \in G_i$ y $x \in G_j$, para $i \neq j$, tomando $k = max(i, j)$, tenemos que $\xi_(x) = \xi_k(x) = \xi_j(x) = \xi_i(x)$, porque ξ_{i+1} extiende a ξ_i, para todo $i \in I$. Usando los mismos argumentos, se prueba que ξ es un morfismo y extiende a $gf^{-1}|_{f(A)}$, porque extiende a ξ_1 que ya extendía a $gf^{-1}|_{f(A)}$. De esta forma $(G, \xi) \in F$ y por construcción, $(G_i, \xi_i) \leqq (G, \xi)$, con $i \in I$. Usando el lema de Zorn, tenemos un elemento máximal en F, (G_0, ξ_0).

Veamos que $G_0 = B$ y $\xi_0 = h$. Si $G_0 \neq B$, existirá $x \in B/G_0$. Si $G_0 \cap < x >= \{0\}$, definimos $\xi(G_0 \oplus < x >)$ como $\xi(g + nh) = \xi_0(g) + nd$, con $d \in D$ arbitrario. El par $(G_0 \oplus < x >, \xi)$ es mayor que el máximo y pertenece a la familia, lo que es un contrasentido. De igual manera, si $G_0 \cap < x > \neq \{0\}$, existirá un subconjunto de los naturales, M, de manera que

$mx \in G_0$, para todo $m \in M$. Tomamos el mínimo de M, m_0. Sabemos que $\xi_0(m_0x) \in D$ y como D es divisible, existirá un $g \in D$, de manera que $m_0g = \xi_0(m_0x)$. Considerando $\xi(x_0) = g$, se podría probar $(G_0 + < x >, \xi) \in F$ y es mayor que el maximal; llegando también a una contradicción. De esta forma, el máximo es (B, h).

Mostremos que, efectivamente, $hf = g$. Para todo $a \in A$, $hf(a) = h(f(a)) = g(a)$, porque h extendía a $gf^{-1}|_{f(A)}$.

■

El concepto de inyectivo, lo habíamos definido en la introducción para un A-módulo, no obstante, en el caso noetheriano, ya hemos hecho las consideraciones que nos permiten ver los $\mathbb{Z}$-módulos como grupos abelianos y los A-morfismos como morfismos de grupos.

Llamemos grupo divisible máximal, D_m, de un grupo, G, al grupo generado por todos los subgrupos divisibles. Veamos, que este grupo es divisible. Para ello, mostremos que $nD_m = D_m$ para cualquier $n \in \mathbb{N}^*$. Consideremos $x \in nD_m$, eso quiere decir que $x = n(a_1x_1 + \dots a_sx_s)$, donde $a_i \in \mathbb{Z}$ y $x_i \in D_i$, subgrupos divisibles, para todo $i \in \{1, \dots, s\}$. De esta forma $x = na_1x_1 + \dots + na_sx_s \in nD_1 + \dots + nD_s = D_1 + \dots + D_s \subseteq D_m$. La otra inclusión se hace de manera muy similar. Observemos, que D_m es único para cualquier grupo, G. Si en G existiesen D_{m_1} y D_{m_2}, como ambos son divisibles, formarán parte de los generadores del otros. Es decir, estaría cada uno dentro del otro. Así que, serían iguales.

Proposición 4.5. *Todo G, grupo abeliano, se puede poner como suma directa de un grupo divisible y uno reducido. Esta descomposición es única salvo isomorfismos.*

Demostración:

Primero, veamos que un grupo divisible es sumando directo de cualquier grupo que lo contenga. Sea D un subgrupo divisible de G, un grupo arbitrario. Siempre se puede encontrar un subgrupo divisible en G, porque $\{0\}$ lo es. Consideramos $i : D \to G$, la inyección canónica y $id : D \to D$, la identidad. Como D es divisible, es inyectivo. Por lo que existirá $f : G \to D$, de manera que, $fi = id$, luego, $f(G) = D$ y usando el primer teorema de isomorfía, $G/Ker\, f \cong D$. Con la aplicación $g : G/Ker\, f \oplus Ker\, f \to G$, definida por $g(\overline{a}, b) = f(a) + b$, se pude demostrar que $G \cong G/Ker\, f \oplus Ker\, f = D \oplus Ker\, f$. Lo que prueba que D es sumando directo de G. Consideremos, ahora, D_m, el grupo divisible maximal. Como es divisible, será sumando directo de G, es decir, $G \cong D_m \oplus C$. Además, C es reducido. Porque si no lo fuese, existiría un subgrupo divisible no trivial, D_1, contenido en C. Al ser D_1 divisible, tendríamos que $C = C_1 \oplus D_1$, luego $G \cong (D_m \oplus D_1) \oplus C_1$. Esto es absurdo, porque $(D_m \oplus D_1)$ es un divisible que contiene al maximal.

Para terminar la prueba, mostremos que la suma de divisibles es divisible. Consideremos un elemento de la suma, (x, y), y un natural no nulo ,n. Como ambos sumandos son divisibles y x e y pertenecen cada uno a uno, existirán x_n e y_n en cada sumando de forma que $nx_n = x$ e $ny_n = y$. Dando lugar a que $n(x_n, y_n) = (x, y)$ y la suma sea divisible.

La suma es única salvo isomorfismos. Porque D_m, para cada grupo, es único. Además, $D_m \cap C = \{0\}$, luego la suma es interna. Si $x \neq 0 \in D_m \cap C$. El grupo cíclico divisible y no trivial, $< x >$, estaría en C, lo que incurre en un contrasentido.

■

Vayamos a por la segunda parte de nuestro esquema. Mostrar la descomposición de los grupos divisibles artinianos abelianos.

Como D_m y C, son subgrupo de G, si G es artiniano entonces D_m y C son artinianos.

Veamos que todo grupo artiniano abeliano es de torsión. De esta forma probaremos que D_m es divisible y de torsión.

Proposición 4.6. *Todo grupo artiniano abeliano es de torsión.*

Demostración:

Sea G un grupo artiniano abeliano, tomemos un elemento $x \in G$. Si $x = 0$, $nx = 0$, luego x sería un elemento de torsión. Consideremos $x \neq 0$ y construyamos la cadena $< a > \supset < 2a > \supset < 4a > \supset \ldots$. Esta cadena estacionará, por tanto, existirá un $n \in \mathbb{N}^*$, de forma que $< 2^n a > = < 2^{n+1} a >$. Es decir, que existirá un $m \in \mathbb{N}$, de forma que $2^n a = m2^{n+1}a$, o lo que es equivalente $2^n(2m-1)a = 0$. Si $2^n(2m-1) = 0$, $(2m-1) = 0$ y esto es imposible. Así que a es de torsión.

■

Necesitamos conocer la estructura de un grupo de torsión abeliano arbitrario.

Definición 4.4. *Dado un grupo, G, y un primo p. Diremos que G es p-**primario**, si todos los elementos de G tiene orden una potencia de p.*

*Sea G un grupo abeliano arbitrario. Llamaremos **componente p-primaria de** G, y escribiremos G_p, al subgrupo formado por todas los elementos de G que tienen como orden una potencia del primo p.*

Mostrar que G_p es un grupo se puede hacer de manera muy parecida a como mostramos que $t(G)$ es grupo. Por construcción, G_p es único para cada p. Además, nótese que en el caso finito coinciden con los p-grupos de Sylow.

Proposición 4.7. *Sea G un grupo abeliano de torsión. Entonces $G \cong \bigoplus_{p \in P} G_p$, donde P es el conjunto de todos los primos.*

Demostración:

Consideremos la aplicación $f : \bigoplus_{p \in P} G_p \to G$, definida por $f(x_1, x_2, \ldots) = \sum_{i \in I} x_i$. Dicha aplicación está bien definida, porque el número de sumandos no nulos es finito y porqué si $x_i = x_i'$, para todo $i \in I$, entonces, $\sum_{i \in I} x_i = \sum_{i \in I} x_i'$. La prueba de que es un morfimos, ya se ha hecho en algunas demostraciones anteriores, así que la obviaremos. Fata ver que es inyectiva y sobreyectiva. Para la inyectividad veamos que su núcleo es nulo.

Supongamos $(x_1, x_2, \ldots)$ un elemento arbitrario de $\bigoplus_{p \in P} G_p$, de forma que $f(x_1, x_2, \ldots) = 0$. Eso quiere decir, que $\sum_{i \in I} x_i = 0$. Si todos los elementos son nulos no hay nada que probar. Si solo tiene un elemento no nulo, x_k, tenemos que $-x_k = \sum_{k \neq i \in I} x_i = 0$, así que legamos a un absurdo. Si hay más de un elemento no nulo, despejamos uno de ellos, y volvemos a llegar a $-x_k = \sum_{k \neq i \in I} x_i$, por un lado tenemos que $x_k \in G_{p_k}$, luego su orden será potencia de p_k y por otro, será el mínimo común múltiplo de potencias de primos distintos de p_k, dichos primos se corresponderán con los subíndices de los G_p, a los que pertenezcan los x_i no nulos. Esos dos órdenes no pueden ser iguales nunca.

Terminemos con la prueba de la sobreyectividad. Tomemos un elemento de $x \in G$. Como G es de torsión, existirá un $n \in \mathbb{N}^*$, de forma que $nx = 0$. Si n es una potencia de un primo, x pertenecerá a algún G_p y x será imagen de la lista con todos los elementos nulos menos el asociado a G_p, que será x. En caso contrario, $n = p_{1(n)}^{e_1} s_1$, con $(p, s) = 1$. Por el teorema de Bezout, existirá $a_1, b_1 \in \mathbb{Z}$, de forma que $1 = a_1 p_{1(n)}^{e_1} + b_1 s_1$.

Multiplicando por x, obtenemos $x = a_1 p_{1(n)}^{e_1} x + b_1 s_1 x$. Además $a_1 p_{1(n)}^{e_1} x$, pertenece al conjunto de los elementos de orden s y $b_1 s_1 x \in G_{p_{1(n)}^{e_1}}$, aplicando este mismo argumento recursivamente, llegamos a una familia finita (los divisores de n, lo son) de elementos pertenecientes cada uno a un G_p distinto. La lista formada por estos elementos en las posiciones debida y completadas con ceros en los huecos, tiene como imagen x.

La descomposición es única, porque los G_p, por construcción, son únicos en cada grupo. Además, como $G_{p_1} \cap G_{p_2} = \{0\}$, la suma es interna. Luego, hemos probado que los grupos abelianos de torsión, en general, no son indescomponibles.

■

El siguiente paso, consiste en mostrar que la descomposición de un grupo abeliano, G, en componentes p-primarias es isomorfa a la suma de copias del grupo de Prüfer, $\mathbb{Z}(p^\infty)$.

Antes de nada, veamos que $\mathbb{Z}(p^\infty)$ es p-primario y divisible.

- Divisible. Sea $\frac{a}{p^r}+\mathbb{Z} \in \mathbb{Z}(p^\infty)$ y $n \in \mathbb{N}^*$. Supongamos que $(n,p) = 1$. Entonces $(n,p^r) = 1$, luego existirán $u, v \in \mathbb{Z}$ tales que $1 = un + vp^r$. De aquí $un = 1 - vp^r$. Por tanto, existe $\frac{au}{p^r}+\mathbb{Z} \in \mathbb{Z}(p^\infty)$ tal que $n(\frac{au}{p^r} + \mathbb{Z}) = a(\frac{nu}{p^r} + \mathbb{Z}) = a(\frac{1-vp^r}{p^r} + \mathbb{Z}) = a[(\frac{1}{p^r} + \mathbb{Z}) - (v + \mathbb{Z})] = a(\frac{1}{p^r} + \mathbb{Z}) = \frac{a}{p^r} + \mathbb{Z}$. Ahora supongamos que $n = p^s m$, con $(p,m) = 1$. Entonces $1 = nu + vp^r$ y de aquí $nm = 1 - vp^r$. Así que $p^s m(\frac{au}{p^{r+s}} + \mathbb{Z}) = (\frac{aum}{p^r} + \mathbb{Z}) = a(\frac{1-vp^r}{p^r} + \mathbb{Z}) = \frac{a}{p^r} + \mathbb{Z}$.

- p-primario. Para cualquier $\frac{a}{p^r}+\mathbb{Z} \in \mathbb{Z}(p^\infty)$, el orden es p^r, una potencia de p.

Dado un grupo abeliano, G, denotaremos $G[n] := \{g \in G \text{ tales que } ng = 0\}$.

Mostremos que si G es p-primario, $G[p]$ es un $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial. Lo primero, sería ver, aunque lo obviaremos, por no sobreextendernos, que $G[p]$ es un subgrupo de G. Al ser un subgrupo, es un $\mathbb{Z}$-módulo y como $p\mathbb{Z} \subseteq Ann(G[p])$, aplicado el lema (4.3); tenemos tenemos que $G[p]$ es un $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial. Recordemos que $G[p]$ es un submódulo de un $\mathbb{Z}$-módulo artiniano. ¿Será $G[p]$ artiniano como espacio vectorial?. La respuesta es afirmativa. Tomemos una familia de subespacios de $G[p]$, F. Como los subespacios son en particular grupos abelianos, podemos ver la familia como un familia de $\mathbb{Z}$-submódulo, como $G[p]$ sí era artiniano como $\mathbb{Z}$-módulo, esta familia tiene un mínimo, H. Como $p\mathbb{Z} \subseteq Ann(H)$ por las misma razones que $G[p]$, H es un subespacio, que será el mínimo en F. Luego, $G[p]$ es artiniano como espacio vectorial. Esto último, nos lleva a que sea de dimensión dimensión finita. Si no lo fuese, existiría $B = \{b_i\}_{i \in I}$, una base de $G[p]$ de cardinal infinito. La cadena $G[p] \supset < B/\{b_1\} > \supset < B/\{b_1, b_2\} \supset \dots$ no estacionaría; porque si $< B/\{b_1, \dots b_n\} > = < B/\{b_1, \dots b_{n+1}\} >$ tendríamos que b_{n+1} se podría generar por una suma finita del resto de bases. Lo que violaría la independencia lineal de las mismas. Si la cadena no estaciona, llegamos a una contradicción con el hecho de ser artiniano. Por tanto, la dimensión de $G[p]$ es finita.

En el caso de $\mathbb{Z}(p^\infty)$, vimos en la sección de anillos, que el reticulo de subgrupos era $< \frac{1}{p} + \mathbb{Z} > \subseteq < \frac{1}{p^2} + \mathbb{Z} > \subseteq \dots \subseteq \mathbb{Z}(p^\infty)$. Por otro lado, $\mathbb{Z}(p^\infty)[p]$ serán los elementos de la forma $\frac{a}{p} + \mathbb{Z}$, es decir, $< \frac{1}{p} + \mathbb{Z} >$. Veamos que $\mathbb{Z}(p^\infty)[p]$ es un espacio vectorial unidimenisonal. Para ello, habría que ver que $\frac{1}{p}+\mathbb{Z}$ es un sistema generador de $\mathbb{Z}(p^\infty)[p]$ como $\mathbb{Z}_p$-módulo. Esto es sencillo, porque cualquier elemento de la forma $\frac{a}{p} + \mathbb{Z}$, será

$a(\frac{1}{p}+\mathbb{Z}) = \overline{a}(\frac{1}{p}+\mathbb{Z})$. Veamos que el sistema es linealmente independiente. Si $\overline{a}(\frac{1}{p}+\mathbb{Z}) = 0$, es porque $\frac{a}{p}+\mathbb{Z} = 0$ o lo que es lo mismo $p|a$, es decir, $\overline{a} = \overline{0}$.

Lema 4.4. *Sean G y H dos grupos abelianos divisibles y p-primarios, entonces, $G \cong H$ si y solamente si $G[p] \cong H[p]$.*

Demostración:

$\Rightarrow$)

Sea $f : G \to H$, un isomorfismos , veamos que $f(G[p]) = H[p]$. Si $x \in G[p]$, entonces $0 = f(0) = f(px) = pf(x)$, luego el $ord(f(x))|p$, así que $f(x) \in H[p]$. Supongamos $y \in H[p]$, este elemento tendrá una preimagen única, por ser f isomorfismo, x. Veamos que $x \in G[p]$. Lo que sabemos es que $f(px) = pf(x) = py = 0 = f(0)$ y como la aplicación es inyectiva, $px = 0$, por razones análogas al caso anterior, $x \in G[p]$. Luego, la restricción de f a $G[p]$ es un isomorfismo entre $G[p]$ y $H[p]$.

$\Leftarrow$)

Sea $f : G[p] \to H[p]$, un isomorfismo, probemos que se puede extender a un morfismo $g : G \to H$. Como f es un isomorfismo, existirá $f^{-1} : H[p] \to G[p]$, isomorfismo. Si componemos con i_G, la inclusión de $G[p]$ en G, tenemos una aplicación inyectiva $i_g f^{-1}$. Por otro lado, i_H, la inclusión de $H[p]$ en H es un morfismo, luego, como H es divisible, es inyectivo y existe un morfismo $g : G \to H$, de manera que $gi_G f^{-1} = i_H$. Probemos que g extiende a f. Si $x \in G[p]$, existirá $y \in H[p]$ de forma que $x = i_G f^{-1}(y)$. Si aplicamos g, obtenemos $g(x) = gi_G f^{-1}(y) = i_H(y) = y$, porque $y \in H[p]$. Es decir que $g(x) = y$. Pero como f es isomorfismo, $y = f(x)$ y llegamos a que $g(x) = f(x)$, $\forall x \in G[x]$. Veamos que g es un morfismo inyectivo y sobreyectivo

- Inyectivo. Sea x un elemento de G, este elemento, tiene orden p^n, mostremos que si $g(x) = 0$, $x = 0$. Hagámoslo por inducción sobre n. Si $n = 1$, $x \in G[p]$ y entonces $g(x) = f(x)$ y si $f(x) = 0$, tenemos que $x = 0$, porque f era inyectiva. Supongamos cierto para para n y veamos para $n+1$. Si x tiene orden p^{n+1} y $g(x) = 0$, tenemos que $g(px) = 0$, pero px tiene orden p^n. Luego por inducción, $px = 0$, pero eso contradice que x tiene orden p^{n+1}, salvo que $x = 0$.

- Sobreyectivo. Si $y \in H$, entonces $ord(y) = p^n$. Veamos por inducción sobre n que para y, existe un $x \in G$, de manera que $g(x) = y$. Si $n = 1$, $y \in H[p]$ y como f era sobreyectiva existía $x \in G[p] \subseteq G$, de manera que $f(x) = y$, pero g extendía a f, así que $g(x) = y$. Supongamos cierto para $k \leq n$ y probemos para $n+1$. Sea $y \in H$, con orden p^{n+1}, entonces $p^n y \in H[p]$, por lo mostrado en el caso $n = 1$, tenemos que existirá $x \in G$, de manera que $g(x) = p^n y$. Como G es divisible, existirá $z \in G$, con $x = zp^n$. Tenemos que $p^n(y - g(z)) = 0$. Entonces $ord(y - g(z)) = p^k$, con $k \leq n$, aplicamos hipótesis de inducción y existe un $a \in G$, de forma que $g(a) = y - g(z)$, concluimos que $y = g(a + z)$

■

Antes de mostrar el resultado hacia el que nos encaminamos, necesitamos hacer una última consideración. Si D es artiniano entonces existe un conjunto finito de D_p. Supongamos que $B = \{D_{p_i}\}_{i \in I}$, es de cardinal infinito. Consideramos la cadena de subgrupos $< B > \supset < B/\{D_{p_1}\} > \supset < B/\{D_{p_1}, D_{p_2}\} > \supset \ldots$. Esta cadena no puede estacionar, porque si lo hiciese, tendríamos que $< B/\{D_{p_1}, \ldots, D_{p_n}\} > = < B/\{D_{p_1}, \ldots, D_{p_{n+1}}\} >$, para algún

$n \in \mathbb{N}$. Pero entonces, tendriamos elementos de orden la potencia de un primo que generamos a partir de elementos de orden potencia de primos distintos, lo que es una contradicción. Luego, si D es artiniano, existe un conjunto finito de D_p.

Proposición 4.8. *Si D es un grupo divisible, artiniano y abeliano entonces es suma directa finita de grupos Prüfer.*

Demostración:

Como todo grupo abeliano artiniano es de torsión, por la proposición (4.7), D será suma directa de D_p con p primos distinto. Como D es artiniano, por la consideración anterior a este resultado, el conjunto de los primos distintos será finito, luego $D \cong D_{p_1} \oplus \ldots \oplus D_{p_s}$. Por otro lado, para cada p_i, con $i \in \{1,\ldots,s\}$, $D_{p_i}[p_i]$ tendrá dimensión finita, r_i, como $\mathbb{Z}_{p_i}$-espacio vectorial. Por otro lado, la suma directa de r_i $\mathbb{Z}(p_i^\infty)[p_i]$ es un $\mathbb{Z}_{p_i}$-espacio vectorial de dimensión r_1, recordemos que $\mathbb{Z}(p_i^\infty)[p_i]$ era unidimensional. Dos espacios vectoriales son isomorfos si y solamente si sus dimensiones son las mismas, por tanto, $D_{p_i}[p_i] \cong \bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty)[p_i]$. Observemos que $\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty)[p_i] = (\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty))[p_i]$. Es directo que $\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty)[p_i] \subseteq (\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty))[p_i]$. Veamos la otra inclusión, sea $x = (x_1,\ldots,x_{r_i})$ un elemento de orden p_1 en $\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_1^\infty)$. El orden de x será el mínimo común múltiplo de los órdenes de los x_i, que será el máximo de los órdenes de x_i, porque todos los órdenes son potencias del mismo primo. De esta forma, $ord(x_j) = p_i$, con $j \in \{1,\ldots,r_i\}$. Concluyendo que $x \in \bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty)[p_i]$. Llegamos a que $D_{p_i}[p_i] \cong (\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty))[p_i]$. Esta isomorfía es como espacios vectoriales, por tanto conserva los productos y la sumas, lo que en particular nos permite verlos como grupos isomorfos. Como D_{p_i} y $\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty)$, son p-primarios y divisibles, (probar que $\bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty)$ lo es, no lo haremos por no alargarnos y porque se hace de manera muy similar a otra pruebas que ya hemos hecho), aplicando el lema anterior, tenemos que $D_{p_i} \cong \bigoplus_{i=1}^{r_i} \mathbb{Z}(p_i^\infty)$. Finalizando con que $D \cong \bigoplus_{i=1}^{r_1} \mathbb{Z}(p_1^\infty) \ldots \bigoplus_{i=1}^{r_s} \mathbb{Z}(p_s^\infty)$

■

Recapitulemos, hasta ahora, hemos dividido un grupo artiniano abeliano en un subgrupo divisible y otro reducido. Después usando que todo grupo divisible es de torsión, conseguimos dividir el subgrupo divisible en componentes p-primarias. Debido a la artinianidad, el conjunto de las componentes p-primarias tenía cardinal finito y dichas componentes han resultado ser isomorfas a copias de grupos de Prüfer. De forma que lo que nos queda ver es cómo descomponemos la parte reducida.

Respecto a la unicidad, si recordamos, la descomposición del artiniano en el subgrupo maximal divisible y reducido era única y la descomposición en componentes p-primarias también, así que, hasta ahora, la descomposición es única.

Terminemos esta sección con la descomponiendo de la parte reducida.

Lema 4.5. *Sea A es un anillo, sea* $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *una serie exacta corta de A-módulo. Si M' y M'' son finitamente generados, lo será M.*

Demostración:

La demostración se hizo en la primera parte de condición necesaria de la proposición (3.2).

■

Proposición 4.9. *Sea A es un anillo artiniano y M un A-modulo artiniano, entonces M es finitamente generado como A-módulo.*

Demostración:

Supongamos que no lo sea, entonces la familia F, de subgrupos de M que no son finitamente generados, es no vacía. Por ser M artiniano, existe un elemento minimal en la familia, N. Claramente, cualquier subgrupo propio de N, ha de ser finitamente generado, porque si no, contravendría la minimalidad de N. Consideremos el ideal $P = Ann(N)$, veamos que este ideal es primo. Supongamos que $ab \in P$ y $a \notin P$, probemos que $b \in P$. Si $a \notin P$, el submódulo de N, $L = \{n \in N$ tales que $an = 0\}$, es un submódulo propio de N. Por tanto, L es finitamente generado. Consideramos la serie exacta corta:

$$0 \longrightarrow L \hookrightarrow N \xrightarrow{f} aN \longrightarrow 0$$

La inclusión es un morfismo inyectivo, el morfismo f que viene definida por $f(n) = an$, $\forall n \in N$, es sobreyectivo y $Ker\, f = L$, que es la imagen de la inclusión. Con esto, mostramos que la serie es, efectivamente, una serie exacta corta. Habíamos comentado que L era finitamente generado, luego, si aN fuese finitamente generado en virtud del lema(4.5), N sería f.g. Así que aN no es f.g., conllevando que $aN = N$. Deducimos así que, $bN = b(aN) = (ab)N = \{0\}$, llegando a que, $b \in P$ o equivalentemente, P es primo. Por el teorema (3.4), P es maximal. De esta forma, A/P es un cuerpo y aplicando el lema (4.3) N es un A/P espacio vectorial artiniano de dimensión infinita. Pero ya hemos visto, que los espacios vectoriales artinianos son de dimensión finita. Llegamos a una contradicción. Concluyendo que M es finitamente generado.

■

Proposición 4.10. *Todo grupo abeliano artiniano reducido, G, es finito.*

Demostración:

Consideremos la cadena de subgrupos:

$$G \supset G \cap 2G \supset G \cap 2G \cap 3G \supset \dots$$

Esta cadena de subgrupos estaciona, por ser G artiniano, es decir, existirá $k \in \mathbb{N}$, de manera que $\bigcap_{n>0} nG = \bigcap_{n=i}^{k} nG$. Por otro lado, sea $m = m.c.m(1,\dots k)$, podemos mostrar, que $mG \subseteq \bigcap_{n=i}^{k} nG$. Esto es cierto porque para cualquier $mg \in mG$ y cualquier $n \in \{1,\dots k\}$, $m = s_n n$ y por tanto, $mg = (s_n n)g = n(s_n g) = ng' \in nG$. Esto lleva, a que $mG \subseteq \bigcap_{n>0} nG = \bigcap_{n=1}^{k} nG$. La otra inclusión, es clara, porque uno de los grupos que intersecamos es el propio mG. Probemos que entonces mG es divisible. Sea $mg \in mG$ y $n > 0$, $mg \in \bigcap_{n>0} nG$, luego $mg \in mnG$, así que $mg = (mn)g' = n(mg')$. De esta forma, mG es divisible. Como el grupo es reducido y mG es divisible, $mG = \{0\}$. Con esto, llegamos a que $m\mathbb{Z} \subseteq Ann(G)$ y usando el lema (4.3), G es un $\mathbb{Z}_m$-módulo. Cualquier cadena descendente de submódulos de G, visto ahora como $\mathbb{Z}_m$-módulo, sigue siendo una cadena de subgrupos, luego estaciona, la cota, H seguirá siendo la cota de la cadena de $\mathbb{Z}_m$-módulo, porque por las mismas razones que G, H es un $\mathbb{Z}_m$-módulo. De esta forma, G es artiniano como $\mathbb{Z}_m$-módulo. Además, $\mathbb{Z}_m$ es un anillo finito, trivialmente artiniano y noetheriano, (cualquier cadena de ideales estaciona, porque $\mathbb{Z}_m$ tiene un conjunto finito de ellos). Como tenemos un módulo arininiano sobre un anillo artiniano, por el teorema anterior es finitamente generado. De este modo, el cardinal de G será menor que el producto de m y el cardinal de un sistema generador, en cualquier caso finito.

■

Con todo lo probado, estamos en disposición para demostrar el teorema de estructura de grupos abelianos artinianos.

Teorema 4.4 (de Estructura de Grupos Abelianos Artinianos)**.** *Todo grupo abeliano artiniano descompone como suma finita de grupos de Prüfer y grupos cíclicos de orden la potencia de primos (no necesariamente distintos). Esta descomposición es única salvo isomorfismos.*

Demostración:

Sea G un grupo abeliano artiniano, hemos visto que G lo podíamos descomponer en suma de parte reducida y divisible. Luego, veíamos que los grupos abelianos divisibles descomponían, a su vez, como suma finita de grupos de Prüfer. Por otro lado, como la parte reducida es finita, usando el teorema (4.1), se puede ver como suma directa finita de grupos cíclicos de orden la potencia de un primo. Así que los candidatos a indescomponibles son los cíclicos de orden la potencia de un primo y los grupos de Prüfer. Ya hemos visto que los cíclicos de orden la potencia de un primo son indescomponibles, falta ver que los grupos de Prüfer lo son. Supongamos que $\mathbb{Z}(p^\infty) \cong G \oplus H$, donde G y H son subgrupos suyos. Ya vimos que los subgrupos de $\mathbb{Z}(p^\infty)$ eran exactamente estos:

$$< \frac{1}{p} + \mathbb{Z} > \subsetneq < \frac{1}{p^2} + \mathbb{Z} > \subsetneq \dots \subsetneq < \frac{1}{p^r} + \mathbb{Z} > \subsetneq < \frac{1}{p^{r+1}} + \mathbb{Z} > \subsetneq \dots$$

Supongamos que $G =< \frac{1}{p^j} + \mathbb{Z} >$ y $H =< \frac{1}{p^k} + \mathbb{Z} >$, con $j < k$. Cualquier elemento arbitrario, (x, y) de $G \oplus H$, tendrá orden $m.c.m(ord(x), ord(y))$, que puede ser como mucho p^k. Pero $\mathbb{Z}(p^\infty)$, tiene elementos con orden p^i, con $i > k$, luego $H = \mathbb{Z}(p^\infty)$ y $G = \{0\}$, con lo que llegamos a que $\mathbb{Z}(p^\infty)$ es indescomponible. Como en el caso artiniano abeliano, la descomposición en suma directa finita de submódulos indescomponibles es única salvo isomorfismos, hemos terminado la demostración.

■

5

Módulos de Multiplicación

Los módulos de multiplicación, en especial, los definidos sobre anillos conmutativos, tienen importancia dentro de la teoría de números y la geometría algebraica. En el caso noetheriano, los anillos de multiplicación indescomponibles son los dominios de Dedekind (impotantes en teoría de números), y los anillos primarios especiales (aplicado extensivamente en Geometría Algebraica). Además, comparten buenas propiedades de finitud con familias de módulos tales como los noetherianos o los hopfianos.

Definición 5.1. *Sea A un anillo, M un A-módulo, diremos que M es de* ***multiplicación*** *como A-módulo, si para cualquier submódulo N, de M, existe un I, ideal de A, de manera que $N = IM$*

Cuando no haya confusión sobre el anillo que estamos usando para hablar de la multiplicación, no lo especificaremos.

En el caso de los anillos vistos como A-módulos sobre ellos mismos, tenemos que cualquier ideal, I, verifica $I = IA$. Por tanto, no tiene sentido definir la propiedad "ser de multiplicación"para anillos igual que para módulos. Diremos que un anillo es de multiplicación (como anillo, no como A-módulo) si todos sus ideales son de multiplicación, es decir, si para cualesquiera dos ideales, $J \subseteq I$, existe otro ideal K en A, de manera que $J = KI$ o dicho de otro modo, es un A-**módulo de multiplicación hereditario**.

5.1 Grupos Abelianos de Multiplicación

En esta sección, aplicamos los resultados que hemos ido obteniendo durante el trabajo para obtener propiedades de algunos módulos de multiplicación, en general, similares a las de los módulos noetherianos o a los finitamente generados. Vamos a estudiar el teorema de estructura de módulos de multiplicación sobre $\mathbb{Z}$, o equivalentemente, vamos a estudiar los grupos abelianos de multiplicación.

Lo primero que vamos a mostrar, es como se comporta el ser de multiplicación con la suma directa. Para ello, introducimos una serie de lemas. No sin antes hacer un comentario.

En el caso de sumas directas finitas, si $M_1 \oplus M_2 = N_1 \oplus N_2$, se tiene que $M_1 = N_1$ y $M_2 = N_2$. Veámoslo por doble inclusión, si $x \in M_1$, entonces $(x_1, 0) \in M_1 \oplus M_2 = N_1 \oplus N_2$, lo que conlleva que $x \in N_1$. Si $x \in N_1$, se se sigue el mismo camino pero al contrario. De manera análoga se prueba que $N_2 = M_2$

Lema 5.1. *Si M es un A-módulo de multiplicación, la imagen homeomorfa de M es de multiplicación.*

Demostración:

Tenemos que ver que, para todo f, homeomorfismo, $f(M)$ es de multiplicación. Lo primero, es demostrar que los submódulos de $f(M)$, son de la forma $f(M')$, donde M' es un submódulo de M. En general, sabemos que $f(M')$, será un submódulo de $f(M)$. Esto es cierto, porque $f(M') = \operatorname{Im} f|'_M$ y como $f|'_M$ es un morfismo su imagen es un módulo, al estar contenido en $f(M)$, un submódulo suyo. Mostremos, que si N es un submódulo de $f(M)$, $f^{-1}(N) = \{m \in M \text{ tales que } f(m) \in N\}$ es un submódulo

de M. Claramente $0 \in f^{-1}(N)$, dado que al ser f un morfismo, $f(0) = 0 \in N$. Sean $a, b \in A$ y $x, y \in f^{-1}(N)$, probemos que $ax + by \in f^{-1}(N)$. Se tiene que $f(ax + by) = af(x) + bf(y) \in N$, porque N es un A-módulo y $f(a), f(b) \in N$. Así que, si tomamos $M' = f^{-1}(N)$, $f(M') = N$. Por tanto, todo submódulo de $f(M)$, es de la forma $f(M')$. Luego, sea N un submódulo de $f(M)$, entonces existirá M' de forma que $f(M') = N$. Como M es multiplicación existirá I, ideal de A, de forma que $AM = M'$. Como f es un morfismo, tenemos que $N = f(M') = f(IM) = If(M)$. Concluyendo que $f(M)$ es de multiplicación.

■

Lema 5.2. *Si M es un A- módulo de multiplicación y N es un sumando directo de M, N es de multiplicación.*

Demostración:

Sabemos que $M \cong N \oplus S$, donde S será un A-módulo. Consideramos $f : N \oplus S \to N$, el A-morfismo definido por $f(n, s) = n$. Como $M \cong N \oplus S$, existirá g, un isomorfismo entre M y $N \oplus S$. Si consideramos el A-morfismo fg, tenemos que $fg(M) = N$ y por el lema anterior, N es de multiplicación.

■

Lema 5.3. *Si M es un A-módulo de multiplicación no trivial, $M \oplus M$ no es multiplicación.*

Demostración:

Supongamos que $M \oplus M$ fuese de multiplicación. Sabemos que $\{0\} \oplus M$ es un submódulo de $M \oplus M$. De este modo, existe I, ideal de A, de forma que $\{0\} \oplus M = A(M \oplus M)$. Lo que lleva a que $\{0\} = AM = M$; incurriendo en un absurdo.

■

Con estos resultados, podemos observar, que la multiplicación y la suma no se relacionan de la mejor manera posible. Esto último no es baladí. A la hora de construir teoremas de estructura con un objetos que verifica una propiedad dada, facilita muchísimo el trabajo el hecho de que si lo que hay a un lado de la igualdad verifica la propiedad, lo que hay al otro lado también la verifique. Ya lo hemos observado durante el desarrollo del trabajo en el caso noetheriano. Como observamos, en el caso de la multiplicación no se tiene todo lo que se querría. Si bien es cierto que si la suma es multiplicación los sumandos los son; no obstante, el recíproco no es cierto. Para un contraejemplo, el último resultado probado.

Aun con eso, hay algunos casos donde se pueden obtener teoremas de estructura bastante eficientes y de maneras no muy complejas. Por ejemplo, en el caso de los grupos abelianos de multiplicación. Vayamos a ello. Antes, veamos un lema de gran utilidad práctica.

Lema 5.4. *Un A-módulo, M, es de multiplicación si y solamente si, para todo submódulo suyo, N, $(N : M)M = N$, donde $(N : M) = \{a \in A \text{ tales que } aM \subseteq N\}$.*

Demostración:

Observemos que $(N : M)$ es un ideal de A. Si $x, y \in (N : M)$, se verifica que $x + y \in (N : M)$, porque $(x+y)M = xM + yM \subseteq N$. También se verifica que si $a \in A$ y $x \in (N : M)$, $(ax)M = a(xM) \subseteq aN \subseteq N$, así que $ax \in (N : M)$. De este modo, la implicación hacia la izquierda es clara. Veamos, la implicación hacia la derecha. Si M es de multiplicación,

para cada N, submódulo de M, existirá $I \leqslant A$, de manera que $IM = N$, por tanto, $I \subseteq (N : M)$. Tenemos, entonces, que $N = IM \subseteq (N : M)M \subseteq N$. Concluyendo que $(N : M)M = N$

■

Obsérvese que si $N_1 \subseteq N_2 \subseteq M$, $(N_1 : M) \subseteq (N_2 : M)$. Si $x \in (N_1 : M)$, entonces, $xM \subseteq N_1 \subseteq N_2$, de esta forma, $x \in (N_2 : M)$

Proposición 5.1. *Si A es un anillo noetheriano (resp. artiniano) y M es un A-módulo de multiplicación, entonces M es noetheriano (resp. artiniano).*

Demostración:

Supongamos una cadena ascendente de submódulos de M, $N_1 \subseteq N_2 \subseteq \ldots$. Como M es de multiplicación, para cada $i \in N^*$, $N_i = (N_i : M)M$. Por la observación que hemos hecho justo antes de este resultado, tenemos una cadena de ideales de A, $(N_1 : M) \subseteq (N_2 : M) \subseteq \ldots$. Como A es noetheriano, existirá $n \in N^*$, de manera que la cadena de ideales estaciona a partir del n-ésimo ideal, es decir, $(N_n : M) = (N_{n+1} : M) = \ldots$. Siguiendo este razonamiento, $(N_n : M)M = (N_{n+1} : M)M = \ldots$ y por tanto, $N_n = N_{n+1} = \ldots$, luego, M es noetheriano. El caso artiniano se hace de manera análoga.

■

Los grupos abelianos, al ser $\mathbb{Z}$-módulos y ser noetheriano, si son de multiplicación van a ser noetherianos. Así que, podemos aplicar el teorema de estructura que ya hemos construido. De esta forma, un grupo abeliano de multiplicación será suma directa finita de copias de $\mathbb{Z}$ y cíclicos de orden la potencia de un primo. No obstante, no todo grupo de esa forma, es decir, noetheriano, es multiplicación. Basta con tomar $\mathbb{Z} \oplus \mathbb{Z}$. Ya hemos comentado, que un anillo visto como modulo sobre sí mismo es de multiplicación. Aplicando el lema (5.3), $\mathbb{Z} \oplus \mathbb{Z}$ no es de multiplicación. Así que, tendremos que afinar más la descomposición.

Lema 5.5. *Todo módulo cíclico, $M = Am$, sobre un anillo conmutativo, A, es de multiplicación.*

Demostración:

Vamos a comprobar que para todo N, submódulo de $M = Am$, $N = (N : Am)Am$. Por la definición de $(N : Am)$, se tiene que $N \supseteq (N : Am)Am$. Veamos la inclusión contraria. Como $N \subseteq M$, todo elemento de N es de la forma am, con $a \in A$. Por otro lado, $a \in (N : Am)$, puesto que todo elemento de Am es de la forma $a_1 m$, para algún $a_1 \in A$ y tenemos que $a(a_1 m) = a_1(am) \in N$. Además, como $m \in Am$, se sigue que $am \in (N : Am)Am$ y obtenemos la inclusión que faltaba para la igualdad.

■

Lema 5.6. 1. *$\mathbb{Z} \oplus \mathbb{Z}$ no es un $\mathbb{Z}$-módulo de multiplicación.*

2. *$\mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}$, con p, primo y $a, b \in \mathbb{N}^*$, no es un $\mathbb{Z}$-módulo de multiplicación.*

3. *$\mathbb{Z} \oplus \mathbb{Z}_n$, $n \in \mathbb{N}^*$, no es un $\mathbb{Z}$-módulo de multiplicación.*

Demostración:

Veamos los apartados uno a uno.

1).

Ya lo hemos probado.

2).

Si $a = b$, hacemos una prueba análoga al caso anterior. Si $a > b$, supongamos cierta la premisa. Sabemos que $\mathbb{Z}_{p^a} \oplus \{0\}$ es un subgrupo de $\mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}$. Entonces, existirá I, ideal de $\mathbb{Z}$, o lo que es equivalente, $n\mathbb{Z}$, de forma que $n\mathbb{Z}(\mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}) = \mathbb{Z}_{p^a} \oplus \{0\}$, es decir que $n\mathbb{Z}\mathbb{Z}_{p^a} \oplus n\mathbb{Z}\mathbb{Z}_{p^b} = \mathbb{Z}_{p^a} \oplus \{0\}$. De este modo, se tiene que verificar que $n\mathbb{Z}\mathbb{Z}_{p^a} = \mathbb{Z}_{p^a}$ y $n\mathbb{Z}\mathbb{Z}_{p^b} = \{0\}$. Siguiendo este razonamiento, $n\mathbb{Z} \subseteq Ann(\mathbb{Z}_{p^b})$, luego $n\mathbb{Z} = p^s\mathbb{Z}$, con $s \geq b$. Pero entonces, $= p^s\mathbb{Z}\mathbb{Z}_{p^a} \neq \mathbb{Z}_{p^a}$. Si $p^s\mathbb{Z}\mathbb{Z}_{p^a} = \mathbb{Z}_{p^a}$, $\overline{1} \in p^s\mathbb{Z}\mathbb{Z}_{p^a}$. Pero los elementos de $p^s\mathbb{Z}\mathbb{Z}_{p^a}$ son de la forma $\overline{p^s zx}$, con $z \in \mathbb{Z}$ y $x \in \mathbb{Z}_{p^a}$. Si $\overline{p^s zx} = \overline{1}$, tendríamos que $(p^s z, p^a) = 1$ y esto es imposible.

3).

Tomemos un subgrupo propio de $\mathbb{Z}_n$, G. Sabemos que $\mathbb{Z} \oplus G$ es un subgrupo de $\mathbb{Z} \oplus \mathbb{Z}_n$. Si se verificase la hipótesis, existiría $n\mathbb{Z}$, de manera que $n\mathbb{Z}\mathbb{Z} \oplus n\mathbb{Z}\mathbb{Z}_n = \mathbb{Z} \oplus G$. Pero por otro lado, sabemos que $n\mathbb{Z}\mathbb{Z} \oplus n\mathbb{Z}\mathbb{Z}_n = n\mathbb{Z} \oplus n\mathbb{Z}\mathbb{Z}_n$. Luego tenemos que $n\mathbb{Z} = \mathbb{Z}$. Entonces $G = \mathbb{Z}\mathbb{Z}_n = \mathbb{Z}_n$, llegando a un absurdo, porque G era un grupo propio de $\mathbb{Z}_n$. Si el grupo cíclico no tiene grupos propios, dicho grupo, $\mathbb{Z}_n$, tiene que ser de la forma $\mathbb{Z}_p$. Con p primo. En dicho caso, consideramos $p\mathbb{Z} \oplus \mathbb{Z}_p$. Si se verificase la premisa, existirá $n \in \mathbb{N}$, de manera que $n\mathbb{Z}(\mathbb{Z} \oplus \mathbb{Z}_n) = p\mathbb{Z} \oplus \mathbb{Z}_p$. De esta forma como $n\mathbb{Z}\mathbb{Z} = p\mathbb{Z}$, tenemos que $n = p$, pero entonces $p\mathbb{Z}\mathbb{Z}_p \neq \mathbb{Z}_p$. Los motivos de esta ultima afirmación,, son análogos a los que se esgrimen al final del apartado anterior.

■

Teorema 5.1 (de Estructura de Grupos Abelinos de Multiplicación)**.** *Los grupos abelianos de multiplicación ($\mathbb{Z}$-módulos de multiplicación) son exactamente los módulos cíclicos.*

Demostración:

El hecho de que todo cíclico sea de multiplicación es lo probado en (5.5). Veamos la otra implicación. Sea G un grupo abeliano de multiplicación, la proposición (5.1) junto con el hecho de que $\mathbb{Z}$ es noetheriano, como comentábamos, lleva a que G es noetheriano. Si G es de multiplicación, por el lema (5.2), todo sumando es de multiplicación. Como la suma directa es asociativa, en la descomposición no puede aparecer ninguno de los sumandos del lema anterior. De esta forma, en la descomposición no podemos tener más de una copia de $\mathbb{Z}$, no podemos tener ningún primo repetido entre las bases de los cíclicos, ni podemos mezclar sumandos libres con sumandos torsión. Por esto, las únicas posibilidades son $G = \mathbb{Z}$ o $G = \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \ldots \oplus \mathbb{Z}_{p_n^{e_n}} \cong \mathbb{Z}_{p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n}}$ en cualquier caso cíclicos, por tanto, hemos probado la implicación que faltaba.

■

Para concluir este apartado, veamos que en en el caso de los grupos abelianos el ser de multiplicación y el ser de multiplicación hereditarios coinciden. Evidentemente, los módulos de multiplicación hereditarios (es decir, aquellos donde todo submódulo es de multiplicación) son un subconjunto de los de multiplicación. En el caso de grupos abelianos, los de multiplicación son exactamente los cíclicos. Por otro lado, los subgrupos de un grupo cíclico son cíclicos, luego de multiplicación. De este modo, todo grupo abeliano de multiplicación es de multiplicación hereditario y viceversa.

5.2 Caso Anillo

Por último, hagamos una pequeña incursión en el caso de los anillos de multiplicación. Al principio del capítulo, hemos comentado que diremos que un anillo A, es de multiplicación, si es un A-módulo de multiplicación hereditario.

En el transcurso del trabajo, hemos hablado varias veces los dominios de Dedekind. Estos tiene varías definiciones, una de ellas es: Un dominio donde todo ideal se puede poner de forma única, salvo orden, como producto finito de ideales primos. Consecuentemente, es un importante objeto de estudio de la teoría multiplicativa de ideales.

Definición 5.2. *Dado un dominio de Dedekind, D, diremos que el D-módulo, F, contenido en el cuerpo de fracciones de D, es un* ***ideal fraccionario de*** *D, si existe un r, elemento regular de D, de forma que $rF \subseteq D$.*

Por otro lado, diremos que un ideal fraccionario, I, de D es ***invertible*** *si existe un ideal fraccionario de D, J, de forma que $IJ = D$*

Claramente, todo ideal propio de D es fraccionario. A partir de estos elementos existen otras definiciones de un dominio de Dedekind, como la que nos dice que los dominios de Dedekind son los dominios en los que todo ideal fraccionario no trivial es invertible. Para mas profundidad y demostraciones respecto a este párrafo véase el capítulo 1 de [9].

Lema 5.7. *Sea D un dominio de Dedekind, todo ideal invertible de D es un D-módulo de multiplicación. Lo que implica que D es un anillo de multiplicación.*

Demostración:

Sea I un ideal invertible, sea A un submódulo suyo. Como I es invertible, existe un ideal fraccionario, J, de forma que $IJ = D$. Como $A = DA$, (porque A es un D-módulo), $A = DA = (IJ)A = I(JA)$. Falta ver que JA es un ideal de D, evidentemente es un D-módulo, por ser producto de ellos y como $JA \subseteq JI = D$, es un submódulo de un anillo, es un ideal.

■

Proposición 5.2. *Un dominio de integridad es de multiplicación si y solamente si es un dominio de Dedekind.*

Demostración:

Evidentemente todo dominio de Dedekind es un dominio de multiplicación, porque todos sus ideales son fraccionarios y por el lema anterior, automáticamente son de de multiplicación. Falta ver la otra implicación. Supongamos un dominio de multiplicación, D, y veamos que es de Dedekind. Probemos, para ello, que todo ideal no nulo es invertible. Sea L un ideal propio no trivial. Entonces existe $l \in L - \{0\}$ y $Dl \leqslant L$. Como D es de multiplicación existirá B, ideal de D, de forma que $Dl = LB$. Como estamos en un dominio de integridad l es regular y existirá l^{-1} en el cuerpo de fracciones de D. Luego $D = DlDl^{-1} = LB(Dl^{-1}) = L(BDl^{-1})$. Claramente (BDl^{-1}), es fraccionario (solo hace falta multiplicar por l). Luego L es invertible. Faltaría ver que todo ideal fraccionario, no solo los propios son invertible, pero si I es un ideal fraccionario $\exists d \in D$ regular, de forma que $dI = C$, donde C es un ideal propio. Este si es invertible, supongamos J su inverso. Tenemos que $D = JC = J(dI) = (Jd)I$. Con lo que tenemos que cualquier fraccionario tiene inverso.

■

Esta demostración tiene importancia porque identifica los dominios que son anillos de multiplicación con los dominios de Dedekind. Esto tiene importantes consecuencias, una de ellas, en el marco en el que estamos, donde necesitamos módulos indescomponibles para aplicar los teorema de estructura que tenemos, es que los dominio de Dedekind son indescomponibles.

Definición 5.3. ***Un anillo primario especial o SPIR*** *es un anillo local (con un único ideal maximal P) cuyos ideales propios son potencias de P.*

Algunos ejemplos clásicos de SPIR son $\mathbb{Z}_{p^n}$, con p primo y $K[x]/(x^n)$, con K un cuerpo.

Proposición 5.3. *Todo SPIR es un anillo de multiplicación.*

Demostración:

Sea A un SPIR e I un ideal de A, consideremos $J \leqslant I$. Si $I = A$, $J = AJ = IJ$. En otro caso. Existirán m y n en $\mathbb{N}^*$, de forma que $I = P^m$ y $J = P^n$. Entonces $J = P^n = P^m P^{n-m} = IP^{n-m}$. Como $J \leqslant I$, $m \leq n$ y $n - m \geq 0$ y concluimos la prueba.

■

Lema 5.8. *La suma directa finita de anillos de multiplicación es un anillo de multiplicación.*

Demostración:

Sean A y R dos anillos de multiplicación, veamos que $A \oplus R$ es de multiplicación. Es conocido que si A y R son unitarios, (marco general sobre el que estamos trabajando), los ideales de $A \oplus R$, son de la forma $I \oplus J$, donde I es un ideal de A y J lo es de R. Sean $I_2 \oplus J_2 \subseteq I_1 \oplus J_1$, dos ideales de $A \oplus R$, como A y R son de multiplicación, existirán I_3 y J_3, de forma que $I_2 = I_3 I_1$ y $J_2 = J_3 J_1$. Así que, $I_2 \oplus J_2 = (I_3 \oplus J_3)(I_1 \oplus J_1)$. Concluyendo que $A \oplus R$ es un anillo de multiplicación. Si vamos agrupando de 2 en 2 de manera recursiva cuando hay más de dos sumando, obtenemos que la suma directa finita de anillos de multiplicación es un anillo de multiplicación.

■

Teorema 5.2. *Los anillos de multiplicación noetherianos son exactamente las sumas directas finitas de dominios de Dedekind y SPIR.*

Demostración:

Una de las implicaciones es clara, la suma directa finita de noetherianos es noetheriano y la suma directa finita de anillos de multiplicacion lo es. Como los Dedekind y los SPIR verifican ambas condiciones, la suma directa finita se Dedekind y SPIR es un anillo de multiplicación noetheriano. Debido al espacio, no podemos recrear la otra implicación, podemos ver un posible camino en el capítulo 3 de [9].

■

De hecho, los SPIR y los Dedekind son los anillos noetherianos de multiplicación indescomponibles.

6 Conclusiones y Agradecimientos

Las conclusiones fundamentales del trabajo se han ido resaltando en cada capítulo de este T.F.G. Además, me gustaría añadir algunas consideraciones.

A través del trabajo hemos ido aplicando el teorema de estructura de módulos noetherianos y artinianos a algunos casos particulares para obtener demostraciones de teoremas de estructura conocidos por caminos más creativos. La sección que más dificultades presentó, sobre todo porque ha pasado por varias versiones hasta llegar a su imagen final, es el caso $\mathbb{Z}$. Al principio intentamos usar la caracterización de módulos indescomponibles a través del anillo de endomorfismos, pero eso llevaba el problema a matemática no conmutativa y no parecía simplificarlo. Dejamos esa idea y abordamos la ruta que se presenta. El cómo hemos ido aplicando el teorema de estructura de módulos noetherianos y artinianos para obtener lo que deseábamos también ha sufrido cambios y retoques.

Por otro lado, el texto inicial incluía prácticamente todas las pruebas con muchísimo detalle, pero excedía la longitud del trabajo y sufrió recortes para adaptarnos al formato.

En lo referente al recorrido del trabajo, este texto está en el marco de los objetivos planteados en la beca de colaboración que tengo en el departamento. Esto es un primer paso de lo que es una posible línea investigativa que abordaría los intersticios de las relaciones entre módulos noetheriano, artinianos, hopfianos, cohopfianos, multiplicación y comultiplicación. Este ruta parece tener un recorrido interesante y fructífero que podría llegar a definir nuevas familias de módulos. En la introducción, ya comentábamos, que la idea inicial era más ambiciosa y entraba de lleno en las relaciones de las familias antes mentadas. No obstante, las limitaciones de tiempo, espacio y el salto entre esa posibilidad y lo aprendido en el grado la hacían poco viable.

Por último, antes de terminar, pese a no ser habitual en este tipo de textos, me gustaría agradecer Joaquín Porcel, un compañero y amigo, su desinteresada contribución. Él ayudó con algunos detalles de notación, en particular la de los subíndices usados en 3.1. Iluminó ciertas dudas y colaboró a que el texto final haya sido más claro. También al profesor Amin El Kaidi por sus ideas, sugerencias y ayudas bibliográficas, en especial en lo referente a módulos hopfianos y cohopfianos.

Bibliografía

[1] H. Ansari-Toroghy y F. Farshadifar *The dual notion of multiplication modules*, Taiwanese Journal of Math. **11(4)** (2007), 1189–1201.

[2] E. Artin, C.J. Nesbitt, R.M. Thrall, *Rings with minimum condition*, Univ. Michigan Press, 1946.

[3] M. F. Atiyah, I.G. Macdonalds, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[4] A. Barnard, *Multiplication modules*, J. Algebra **71** (1981), 174–178.

[5] B. Baumslag, B. Chandler *Teoria y Problemas de Teoria de Grupos*, Libros McGraw-Hill, 1972.

[6] G. Baumslag, *On abelian hopfian groups*, Mat.Z. **78** (1962), 53–54.

[7] P.M. Cohn, *Algebra vol. 1*, John Wiley and Sons Ltd., 1974.

[8] P.M. Cohn, *Algebra vol. 3*, John Wiley and Sons Ltd., 1991.

[9] J. Cuadra, J. Escoriza, *Anillos y Módulos de Multiplicación*, Editorial Universidad de Almería , 2002.

[10] A. Facchini, D. Herbera, L.S. Levi, P. Vàms, *Krull-Schmidt fails for Artinian modules*, Proced. Amer. Math. Soc. **123** (1995), 3587–3592.

[11] L. Funchs, *Abelian Groups*, Springer, 2015.

[12] L. Funchs, *Infinite Abelian Groups vol. 1*, Academic Press, 1970.

[13] L. Funchs, *Infinite Abelian Groups vol. 2*, Academic Press, 1973.

[14] B. Hartley, T.O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall, 1970.

[15] H. Hopf, *Über die Abbildungen der dreidimensionalen Sphere auf die Kuggelfläche*, Mathematische Annalen, **104**(1) (1931), 637–665.

[16] F. Kash, *Modules and Rings*, Academic Press Inc. Ltd., 1982.

[17] T. W. Judson, *Abstract Algebra and Applications*, MA: PWS Pub, 1994.

[18] W. Krull, *Über Multiplicationsringe*, S.-B. Heidelberger Akad. Wiss, **44** (1925), 13–18.

[19] S. Lang, *Algebra*, Addison-Wesley, 1993.

[20] E. Noether, *Idealtheorie in Ringbereichen*,Mathematische Annalen, **83** (1921), 24–66.

[21] J. J. Rotman *Advanced Modern Algebra*, Prentice Hall, 2002.

[22] J. J. Rotman *An Introduction to the Theory of Groups*, Springer, 1995.

[23] M. R. Sepanski, *Algebra (Pure and Applied Undergraduate Text)*, Amer. Math. Soc., 2010.

[24] B. Stenström, *Rings of Quotient*, *An Introduction to methods of Ring Theory*, Springer-Verlag, Berlin-Hidelberg- New York 1975.

[25] J. Strooker, *Lifting projetives*, Nagoya Math. J., **27** (1966), 747–751.

[26] V. W. Vasconcelos, *On Finitely generated Flat Modules*, Trans. Amer. Math.Soc., **138** (1969), 505–512.

[27] R. B. Warfield, *A Krull-Schmidt Theorem for Infinite Sums of Modules*, Proced. Amer. Math.Soc., **22**(2) (1969), 460–465.

[28] C. A. Weibel, *An Introduction to Homological Algebra*, Cambridge University Press, 1994.