USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Clasificación de módulos sobre un dominio de Dedekind

Manuel López Bernárdez

2019/2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Clasificación de módulos sobre un dominio de Dedekind

Manuel López Bernárdez

Julio, 2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álgebra
Título: Clasificación de módulos sobre un dominio de Dedekind
Breve descrición do contido
Los dominios de Dedekind son anillos con buenas propiedades que surgen como anillos de números y también como anillos de coordenadas de las curvas algebraicas regulares. Su teoría de módulos finitamente generados es similar a los dominios de ideales principales de los que son una generalización. Veremos el Teorema de Clasificación de estos módulos en términos de ideales fraccionarios.
Recomendacións
Eisenbud, D.: Commutative algebra with a view towards Algebraic Geometry, Springer, 2004 Broue, M.: Some Topics in Algebra, Springer, 2014
Outras observacións
Haber cursado los contenidos de la asignatura "Estructuras algebraicas".

Índice general

Resumen

Los dominios de Dedekind son anillos para los que se verifica la factorización única de ideales en ideales primos, que generalizan la propiedad de factorización única en irreducibles de los elementos de un dominio de ideales principales. Dedicamos esta memoria al estudio de las propiedades de los dominios de Dedekind y a la exposición del Teorema de Clasificación de los módulos finitamente generados sobre este tipo de anillos, extendiendo la clasificación conocida para dominios de ideales principales. Un tipo particular de dominios de Dedekind son los anillos de valoración discreta, que también se tratarán en la memoria. Para abordar una demostración autocontenida del Teorema de Clasificación general, estudiaremos como paso intermedio el problema de clasificación de módulos finitamente generados sobre anillos de valoración discreta.

Abstract

Dedekind domains are rings for which the unique factorization of ideals into prime ideals is satisfied, which generalize the irreducible unique factorization property for elements in a principal ideal domain. We devote this memory to the study of the properties of Dedekind domains and the exposition of the Classification Theorem of finitely generated modules on this type of rings, extending the well-known classification for domains of principal ideals. A particular type of Dedekind domains are discrete valuation rings that are also discussed in this work. To give a self-contained proof of the Classification Theorem, we will study as an intermediate step the problem of classifying finitely generated modules on discrete valuation rings.

Introducción

Desde el nacimiento de la humanidad, las matemáticas han acompañado al hombre en su vida cotidiana y le han proporcionado de un sinfín de problemas por resolver. Uno de los más primitivos, aunque no por ello un problema sencillo, es la búsqueda de soluciones enteras a ecuaciones polinómicas. La ecuación que sin duda ha suscitado mayor interés a lo largo de la Historia es la ecuación $Z^n = X^n + Y^n$, donde n es un entero mayor o igual a dos. El primero de los casos posee gran relevancia ya que en él están intrínsecamente relacionadas la aritmética con la geometría. Las soluciones enteras de este problema, hoy en día denominadas ternas pitagóricas, ya eran bien conocidas desde la antigüedad y fueron motivadas por la resolución de triángulos rectángulos con lados de longitud entera. Tablillas de arcilla babilonias del siglo XIX a.C. nos muestran que las antiguas culturas mesopotámicas ya habían alcanzado una gran generalidad en el cálculo de estas soluciones; más incluso que la obtenida por la escuela Pitagórica en el siglo VI a.C. Hoy en día se conocen con exactitud todas las soluciones enteras de este primer caso, por lo que el problema está completamente cerrado. No obstante, cuando el parámetro n es mayor que dos, la ecuación se vuelve mucho más complicada. Según había conjeturado el matemático francés Pierre de Fermat en el año 1637 en un pequeño margen de su «Aritmética» de Diofanto, esta igualdad no parecía tener soluciones enteras positivas cuando n era mayor que dos. A día de hoy, sabemos que la conjetura dada por Fermat es cierta. El matemático británico Andrew Willes ayudado por Richard Taylor presentó una demostración de este enunciado en el año 1995.

Desde que Fermat enunciara esta famosa conjetura y afirmase que conocía una supuesta demostración de la misma, matemáticos del más alto nivel a lo largo de los siglos XVIII y XIX intentaron abordar este problema. La demostración para el caso $n = 4$ era ampliamente conocida ya que el propio Fermat la había dejado por escrito. Utilizando este resultado, se puede deducir de modo relativamente simple que para probar la conjetura al completo, basta suponer que $n = p$, con p un número primo. El matemático suízo Leonhard Euler, fue capaz de dar una demostración para el caso $n = 3$, Adrien Marie Legendre y Peter Lejeune Dirichlet lo consiguieron para $n = 5$ de modo independiente y el caso $n = 7$

fue demostrado por el matemático francés Gabriel Lamé en el año 1837. No obstante, este problema parecía resistirse para el caso más general. El propio Friedrich Gauss años antes, habiendo sido incapaz de probar algún que otro caso particular de la conjetura, le escribía a su compatriota Heinrich Olbers las siguientes palabras de desazón:

«Confieso que, por supuesto, el teorema de Fermat, como una proposición aislada, tiene muy poca importancia para mí, ya que es fácil formular una buena cantidad de tales proposiciones que uno no puede demostrar »

En vistas de la dificultad patente del problema, hasta bien entrado el siglo XIX, no se habían realizado grandes avances en el caso general $n = p$. La primera intentona se produce en la década de los 40 de manos del propio Lamé. El francés intenta factorizar el lado derecho de la ecuación $Z^p = X^p + Y^p$ en el anillo $\mathbb{Z}[\xi_p]$, con ξ_p una raíz primitiva p-ésima de la unidad. En el año 1847, Lamé presenta ante la Academia de Ciencias de París una supuesta demostración de la conjetura donde asume implícitamente la factorización única en estos dominios tal como ocurre en los números enteros; observación que había percibido Joseph Liouville el mismo día de la presentación de la prueba. Dos meses más tarde de la presentación de Lamé, Liouville recibe una carta del matemático alemán Ernst Kummer, donde muestra a modo de contraejemplo la ausencia de factorización única en $\mathbb{Z}[\xi_{23}]$. De hecho, hoy en día es conocido (1971) que en estos anillos la propiedad de la factorización única falla para todos los valores de n mayores o iguales a 23. No obstante, el mismo Kummer afirma en la correspondencia con Liuville lo siguiente sobre la factorización única en los anillos $\mathbb{Z}[\xi_n]$:

«Es posible rescatarla introduciendo un nuevo tipo de números complejos, los cuales he denominado "números complejos ideales" $(\cdots)$*. Hace tiempo que llevo considerando la aplicación de esta Teoría a la prueba del Teorema de Fermat y he conseguido probar la imposibilidad de la ecuación* $Z^n = X^n + Y^n$ $(2 < n \leq 100)$*»*

Los «números complejos ideales» son una clase especial de enteros algebraicos que utilizó Kummer para extender la unicidad de factorización en $\mathbb{Z}[\xi_n]$. Gracias a la introducción *ad hoc* de este novedoso concepto, Kummer fue capaz de probar el Teorema de Fermat para una cantidad de primos no vista hasta la fecha. A pesar de su gran labor, Kummer no logró su propósito de demostrar el teorema para todos los valores de n, pero su trabajo e ideas fueron retomadas por su alumno y colega Richard Dedekind. La relevancia de los trabajos de Dedekind es tan grande que la propia Emmy Noether solía afirmar con frecuencia la famosa frase «todo está en Dedekind», y no es de extrañar.

En uno de sus artículos, publicado en el año 1871, Dedekind introduce el concepto de cuerpo, anillo e ideal (en el contexto de los números complejos) asentando las bases del Álgebra Abstracta moderna tal y como se conoce hoy en día. Además, emulando a su

maestro, Dedekind fue capaz de probar que en las clausuras íntegras de las extensiones finitas de $\mathbb{Q}$ en $\mathbb{C}$, se verifica la factorización única en producto de ideales primos, de modo análogo a como lo hizo Kummer en los dominios $\mathbb{Z}[\xi_n]$. Esta propiedad es una de las más importantes que poseen los hoy en día denominados «dominios de Dedekind» y que los caracterizan completamente.

La relevancia de estos dominios en el panorama matemático actual es muy grande debido a que se encuentran por doquier en dos de las ramas más importantes de la matemática moderna: la Teoría de Números y la Geometría Algebraica.

El asunto principal de este trabajo es el estudio de los dominios de Dedekind con el objetivo de exponer la clasificación de los módulos finitamente generados sobre estos dominios. En el primer capítulo, hablaremos en profundidad sobre el concepto de ideal fraccionario, junto con otras propiedades de los submódulos del cuerpo de fracciones de un dominio. En el segundo, definiremos el concepto de anillo de valoración y haremos especial hincapié en los anillos de valoración discreta (AVD), que nos serán de utilidad más adelante en el trabajo. En el tercer capítulo, introducimos el concepto de dominio de Dedekind en términos de ideales fraccionarios y estudiaremos algunas de las caracterizaciones que poseen estos dominios. Además veremos algunos ejemplos interesantes, como los anillos de números y los anillos de coordenadas de las curvas algebraicas regulares. En el cuarto capítulo, probaremos que un dominio de Dedekind posee la propiedad de factorización única en ideales primos y cómo esta propiedad caracteriza completamente a estos dominios. En el quinto capítulo trataremos otras propiedades interesantes de los dominios de Dedekind, que simplemente completan su estudio. Esta capítulo se puede omitir, ya que no aporta información crucial para la demostración del Teorema de Clasificación. Por último, en el sexto capítulo, abordaremos el Teorema de Clasificación, empleando de modo auxiliar el Teorema de Clasificación para módulos finitamente generados sobre AVDs.

Notación

Cualquier anillo A considerado en este trabajo será conmutativo unitario y no trivial. Los homomorfismos de anillos $f\colon A \to B$ siempre serán homomorfismos de anillos unitarios, es decir tales que $f(1_A) = 1_B$. El conjunto de los ideales primos y de los ideales maximales de un anillo A se denotarán por $\mathrm{Spec}(A)$ y $\mathrm{Spm}(A)$ respectivamente. El grupo abeliano de las unidades de A se denotará por $A^\times$. Denotaremos al anillo de polinomios en una cantidad finita de variables sobre el anillo A como $A[X_1, \ldots, X_n]$ y al anillo de series de potencias en una cantidad finita de variables como $A[[X_1, \ldots, X_n]]$.

Diremos que el anillo A es un dominio si no tiene divisores de cero. Cuando el anillo A es un dominio, denotaremos su cuerpo de fracciones por K_A. Supondremos conocidos los conceptos de *dominio de factorizacón única* (DFU) y *dominio de ideales principiales* (DIP). También damos por conocidos los resultados más elementales que conciernen a esta clase de dominios.

Si A es un anillo y $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ es una cadena de ideales primos, diremos que la longitud de la cadena es n. Definimos la *altura de* $\mathfrak{p} \in \mathrm{Spec}(A)$, y escribiremos $\mathrm{alt}(\mathfrak{p})$, como el supremo de las longitudes de las cadenas de ideales primos $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$. Un ideal primo $\mathfrak{p}$ se dice minimal si $\mathrm{alt}(\mathfrak{p}) = 0$. La *dimensión de Krull* del anillo A es el supremo de las alturas de los ideales primos de A y se denota $\dim(A)$. Diremos que un anillo A es noetheriano si satisface la *condición de cadena ascendente*, o equivalentemente, si todo ideal de A es finitamente generado. Diremos que A es un anillo artiniano si satisface la *condición de cadena descendente*, o equivalentemente, si A es noetheriano y $\dim(A) = 0$ (Véase [1, Capítulos 6, 7 y 8]).

Usaremos además la notación estándar $\mathbb{N}$ para el conjunto de los números naturales, $\mathbb{Z}$ para los enteros, $\mathbb{Q}$ para los racionales, $\mathbb{R}$ para los reales y $\mathbb{C}$ para los complejos.

Capítulo 1

Ideales Fraccionarios

En este capítulo introducimos el concepto de ideal fraccionario de un dominio. Estos submódulos tendrán una posición clave en el estudio de los dominios de Dedekind y además, se utilizarán en el Teorema de Clasificación de módulos finitamente generados sobre este tipo de anillos.

1.1. Submódulos del cuerpo de fracciones de un dominio

Sea A un dominio y sea K_A su cuerpo de fracciones. Dados dos elementos c, $x \in K_A$, utilizaremos la notación $\mu_c(x) := cx$ para representar «la multiplicación por c».

Lema 1.1. *Sea A un dominio y sean $\mathfrak{f}$ y $\mathfrak{g}$ A-submódulos no nulos de K_A. Si $\varphi\colon \mathfrak{f} \to \mathfrak{g}$ es un homomorfismo de A-módulos, entonces existe un elemento $c \in K_A$ de modo que $\varphi(x) = cx$ para todo $x \in \mathfrak{f}$, es decir, tal que $\varphi = \mu_c$.*

Demostración. Como $\mathfrak{f}$, $\mathfrak{g} \subset K_A$ son A-submódulos no nulos, se tiene que $S_A^{-1}\mathfrak{g} = K_A = S_A^{-1}\mathfrak{f}$, siendo $S_A \subset A$ el subconjunto multiplicativo de los elementos no nulos de A. Localizando en S_A obtendremos a partir del homomorfismo de A-módulos $\varphi\colon \mathfrak{f} \to \mathfrak{g}$ el homomorfismo de A-módulos $\varphi' := S_A^{-1}\phi\colon K_A \to K_A$. El elemento $c := \varphi'(1) \in K_A$ es tal que $\varphi = \mu_c$. En efecto, para cada elemento $x \in \mathfrak{f}$ existe un elemento no nulo $a_x \in A$ tal que $a_x x \in A$. Entonces, por ser ϕ' un homomorfismo de A-módulos, se tiene que

$$a_x\varphi(x) = \varphi(a_x x) = \varphi'(a_x x) = \varphi'((a_x x)1) = (a_x x)\varphi'(1) = (a_x x)c = a_x(xc).$$

Dado que $a_x \neq 0$, se concluye que $\varphi(x) = \mu_c(x)$. □

Proposición 1.2. *Sea A un dominio y sean $\mathfrak{f}$, $\mathfrak{g} \subset K_A$ A-submódulos no nulos. Entonces $\mathfrak{f}$ y $\mathfrak{g}$ son isomorfos como A-módulos si, y solo si, existe $c \in K_A^\times$ tal que $\mathfrak{g} = c\mathfrak{f}$.*

Demostración. Si $c \in K_A^\times$ es tal que $\mathfrak{g} = c\mathfrak{f}$, entonces la aplicación inyectiva $\mu_c \colon \mathfrak{f} \to \mathfrak{g}$ «multiplicar por c» es un isomorfismo de A-módulos (con inverso $\mu_{c^{-1}} \colon \mathfrak{g} \to \mathfrak{f}$). Recíprocamente, si $\varphi \colon \mathfrak{f} \to \mathfrak{g}$ es un isomorfismo de A-módulos, por el Lema 1.1, será de la forma $\varphi = \mu_c$ para un elemento $c \in K_A^\times$. Como $\varphi = \mu_c$ es biyectiva, se concluye que $\mu_c(\mathfrak{f}) = \mathfrak{g}$, es decir que $c\mathfrak{f} = \mathfrak{g}$. □

Corolario 1.3. *Sea A un dominio. Un A-submódulo no nulo $\mathfrak{f} \subset K_A$ es isomorfo a un ideal de A si, y solo si, existe un elemento no nulo $a \in A$ tal que $a\mathfrak{f} \subset A$.*

Demostración. Si $\mathfrak{f}$ es isomorfo a un ideal de A, empleando la Proposición 1.2 se obtiene el resultado. Recíprocamente, supongamos que existe $c \in K_A^\times$ tal que $c\mathfrak{f} = I$, siendo I un ideal de A. Sean b, $s \in A \setminus \{0\}$ tales que $c = \frac{b}{s}$. Entonces $a := sc \in A \setminus \{0\}$ es tal que $a\mathfrak{f} = sc\mathfrak{f} = sI \subset A$, concluyendo la prueba. □

1.2. Ideales fraccionarios

La siguiente definición viene motivada por el Corolario 1.3.

Definición 1.4. Sea A un dominio. Diremos que un A-submódulo no nulo $\mathfrak{f} \subset K_A$ es un *ideal fraccionario de A* si es isomorfo como A-módulo a un ideal de A, es decir, si existe un elemento $a \in A \setminus \{0\}$ de modo que $a\mathfrak{f} \subset A$, o de modo equivalente $\mathfrak{f} \subset \frac{1}{a}A$. El conjunto de los ideales fraccionarios de A se denotará $\texttt{Frac}(A)$.

Observación 1.5. Todo ideal no nulo de A es un ideal fraccionario. Para distinguir los ideales usuales de A de los ideales fraccionarios, diremos que los primeros son *ideales enteros de A*.

Definición 1.6. Un *ideal fraccionario* $\mathfrak{f}$ de A es *principal* si $\mathfrak{f}$ está generado como A-módulo por un elemento $x \in K_A^\times$. En este caso usaremos la notación $\mathfrak{f} = xA$.

Observación 1.7. Una consecuencia directa del Corolario 1.3 es que todo ideal fraccionario $\mathfrak{f} \subset K_A$ del dominio A es de la forma $\mathfrak{f} = \frac{1}{a}I$, siendo $a \in A$ un elemento distinto de cero tal que $a\mathfrak{f} = I \subset A$ es un ideal entero y no nulo. En particular si A es un DIP todos los ideales fraccionarios son principales, es decir, son de la forma xA con $x \in K_A^\times$.

Lema 1.8. *Sea A un dominio y $\mathfrak{f} \subset K_A$ un A-submódulo. Son equivalentes:*

(1) *$\mathfrak{f}$ es un ideal fraccionario principal.*

(2) *$\mathfrak{f} \cong A$ como A-módulos.*

Demostración. Si $x \in K_A^\times$ es un elemento tal que $\mathfrak{f} = xA$, entonces $\mu_x \colon A \to \mathfrak{f}$ proporciona un isomorfismo de A-módulos. Recíprocamente, supongamos que $h \colon A \to \mathfrak{f}$ es un isomorfismo de A-módulos. Entonces $\mathfrak{f} = xA$ siendo $x := h(1)$. □

Lema 1.9. *Sea A un dominio noetheriano y $\mathfrak{f} \subset K_A$ un A-submódulo. Entonces $\mathfrak{f}$ es un ideal fraccionario de A si, y solo si, es un A-módulo finitamente generado.*

Demostración. Supongamos que $\mathfrak{f}$ es un A-submódulo de K_A finitamente generado. Entonces existe una familia de elementos no nulos $\{\frac{x_1}{y_1}, \ldots, \frac{x_n}{y_n}\} \subset K_A$ de modo que $\mathfrak{f} = \sum_{i=1}^n \frac{x_i}{y_i} A$. Tomando $a := \prod_{i=1}^n y_i$, tendremos que $a\mathfrak{f} \subset A$. Recíprocamente, si $\mathfrak{f}$ es un ideal fraccionario de A, existirá un elemento $a \in A$ de modo que $a\mathfrak{f} \subset A$ es un ideal de A. Dado que A es noetheriano, este ideal será finitamente generado por una familia $\{x_1, \ldots, x_n\}$ de elementos de A. Basta observar que $\{\frac{x_1}{a}, \ldots, \frac{x_n}{a}\}$ es un conjunto de generadores de $\mathfrak{f}$. □

Teorema 1.10. *Sea A un dominio y sean $\mathfrak{f}, \mathfrak{g}, \mathfrak{h}$ ideales fraccionarios de A.*

(1) *Los siguientes conjuntos, llamados respectivamente suma, intersección, producto y transportador de $\mathfrak{g}$ en $\mathfrak{f}$ sobre K_A, son ideales fraccionarios de A:*

- $\mathfrak{f} + \mathfrak{g} = \{x + y \mid x \in \mathfrak{f},\ y \in \mathfrak{g}\}$
- $\mathfrak{f} \cap \mathfrak{g} = \{x \mid x \in \mathfrak{f},\ x \in \mathfrak{g}\}$
- $\mathfrak{f}\mathfrak{g} = \{\sum_{i=1}^n x_i y_i \mid x_i \in \mathfrak{f},\ y_i \in \mathfrak{g},\ n \in \mathbb{Z}^+\}$
- $(\mathfrak{f} :_{K_A} \mathfrak{g}) = \{x \in K_A \mid x\mathfrak{g} \subset \mathfrak{f}\}$

(2) *Ordenando el conjunto de los ideales fraccionarios de A mediante la inclusión, $\mathfrak{f}+\mathfrak{g}$ es el menor ideal fraccionario que contiene a $\mathfrak{f}$ y $\mathfrak{g}$ y $\mathfrak{f} \cap \mathfrak{g}$ es el mayor ideal fraccionario contenido en $\mathfrak{f}$ y $\mathfrak{g}$. Además si $\mathfrak{f} \subset \mathfrak{g}$, entonces $\mathfrak{f}\mathfrak{h} \subset \mathfrak{g}\mathfrak{h}$.*

Demostración.

(1) Es inmediato verificar que $\mathfrak{f}+\mathfrak{g}$, $\mathfrak{f}\cap\mathfrak{g}$, $\mathfrak{f}\mathfrak{g}$ y $(\mathfrak{f} :_{K_A} \mathfrak{g})$ son A-submódulos de K_A. Basta ver que estos conjuntos verifican las condiciones de la Definición 1.4. Supongamos que existen $a, b \in A$ de modo que $\mathfrak{f} \subset \frac{1}{a}A$ y $\mathfrak{g} \subset \frac{1}{b}A$:

$0 \neq \mathfrak{f} \subset \mathfrak{f} + \mathfrak{g} \subset \frac{1}{ab}A \implies \mathfrak{f} + \mathfrak{g}$ es un ideal fraccionario.

$0 \neq \mathfrak{f}\mathfrak{g} \subset \mathfrak{f} \cap \mathfrak{g} \subset \frac{1}{ab}A \implies \mathfrak{f}\mathfrak{g}$ y $\mathfrak{f} \cap \mathfrak{g}$ son ideales fraccionarios.

Dado que $\mathfrak{f} \cap A$ es un ideal fraccionario, existirá un elemento c no nulo en dicho ideal. De este modo, para cualquier $y \in \mathfrak{g}$ tendremos que $\frac{c}{b}y \in cA \subset \mathfrak{f}$ y así $\frac{c}{b} \in (\mathfrak{f} :_{K_A} \mathfrak{g}) \neq 0$. Por otro lado, si consideramos $0 \neq d \in \mathfrak{g}$, tendremos que $\frac{1}{ad}(\mathfrak{f} :_{K_A} \mathfrak{g}) \subset A$, concluyendo el resultado.

La demostración de (2) es muy sencilla. □

Observación 1.11. Una consecuencia directa de la Proposición 1.1 y de la definición dada en el Teorema 1.10 es que la aplicación $\boldsymbol{\mu}\colon (\mathfrak{f} :_{K_A} \mathfrak{g}) \to \mathrm{Hom}_A(\mathfrak{g}, \mathfrak{f})$ dada por $c \mapsto \mu_c$ es un isomorfismo de A-módulos.

Vamos a emplear el producto de ideales fraccionarios definido en el Teorema 1.10 para dotar de estructura algebraica al conjunto de ideales fraccionarios de A:

Teorema 1.12. *Sea A un dominio. El conjunto $(\mathtt{Frac}(A)\ ,\ \cdot)$ es un monoide conmutativo.*

Demostración. El producto de ideales fraccionarios es un ideal fraccionario (Teorema 1.10) y por tanto la operación de multiplicación en $\mathtt{Frac}(A)$ es una operación interna. El carácter conmutativo y la asociatividad de esta operación es consecuencia directa de que el producto en K_A lo es. Es inmediato verificar que $\mathfrak{e} = A$ es el neutro de esta operación. □

Definición 1.13. Sea A un dominio y $\mathfrak{f} \in \mathtt{Frac}(A)$. Diremos que $\mathfrak{f}$ *es invertible* si es una unidad del monoide $(\mathtt{Frac}(A)\ ,\ \cdot)$, es decir, si existe $\mathfrak{g} \in \mathtt{Frac}(A)$ tal que $\mathfrak{fg} = A$. El ideal $\mathfrak{g}$ está únicamente determinado por $\mathfrak{f}$ y se denomina *el inverso de* $\mathfrak{f}$. Este ideal se denotará como $\mathfrak{g} = \mathfrak{f}^{-1}$.

Observación 1.14. Todo ideal fraccionario principal es una unidad de $\mathtt{Frac}(A)$:

$$\forall x \in K_A^\times,\ \ (xA)^{-1} = \frac{1}{x}A$$

Por otro lado, el conjunto de las unidades $\mathtt{Frac}(A)^\times$ es un grupo abeliano y por lo tanto todo subgrupo del mismo será normal. En particular, destacamos el subgrupo $\mathtt{P}_A \lhd \mathtt{Frac}^\times(A)$ de ideales fraccionarios principales de A. El grupo cociente de las clases de isomorfía de los ideales invertibles, se denomina *grupo de Picard de A* y se denotará:

$$\mathtt{Pic}(A) := \mathtt{Frac}(A)^\times / \mathtt{P}_A$$

Lema 1.15. *Sea A un dominio y $\mathfrak{f}$ un ideal fraccionario de A. Si $\mathfrak{f}$ es invertible, entonces $\mathfrak{f}^{-1} = (A :_{K_A} \mathfrak{f})$. De este modo, el único candidato a ser el inverso de un ideal fraccionario $\mathfrak{f}$ es el ideal fraccionario $(A :_{K_A} \mathfrak{f})$.*

Demostración. De la definición de ideal transportador se tiene que $\mathfrak{f}(A :_{K_A} \mathfrak{f}) \subset A$. Si suponemos que $\mathfrak{f}$ es invertible, existirá $\mathfrak{g} \in \mathtt{Frac}(A)$ de modo que $\mathfrak{fg} = A$. Entonces:

$$\mathfrak{g} \subset (A :_{K_A} \mathfrak{f}) \implies A = \mathfrak{fg} \subset \mathfrak{f}(A :_{K_A} \mathfrak{f}) \subset A;$$

y por la unicidad del inverso $\mathfrak{g} = (A :_{K_A} \mathfrak{f})$. □

El siguiente ejemplo muestra que, en general, $\mathtt{Frac}(A)$ no tiene por qué ser un grupo, es decir, no todos los ideales fraccionarios de un dominio A tienen por qué ser invertibles.

Ejemplo 1.16. Consideremos el dominio $\mathbb{Z}[\sqrt{5}]$ y los ideales $I = (2)$ y $J = (2, 1-\sqrt{5})$. Veamos que el contenido $I \subset J$ es estricto. En efecto, si $1-\sqrt{5} \in I$, entonces $1-\sqrt{5} = 2(\alpha + \beta\sqrt{5})$, siendo $\alpha, \beta \in \mathbb{Z}$ y se obtiene que $1 = 2\alpha$ y $-1 = 2\beta$. No obstante estas igualdades no se verifican para números enteros, y así $1-\sqrt{5} \notin I$. Comprobemos ahora que $J^2 = IJ$. Como $I \subset J$, entonces $IJ \subset J^2$ y solamente tendremos que probar el otro contenido. Bastará verificar que $(1-\sqrt{5})^2 \in IJ$. Se tiene que $(1-\sqrt{5})^2 = 6 - 2\sqrt{5} = 2(2 + (1-\sqrt{5})) \in IJ$. De este modo, J no es invertible, ya que si lo fuera, tendríamos que $I = IJJ^{-1} = J^2J^{-1} = J$, que ya hemos visto que es falso.

1.3. Ideales fraccionarios y localización.

La siguiente proposición muestra que las operaciones aritméticas definidas en el conjunto de los ideales fraccionarios de un dominio A presentan un buen comportamiento frente a la localización. Por otro lado, adjuntamos otros resultados sobre localización en ideales que nos serán de utilidad.

Proposición 1.17. *Sean $\mathfrak{f}$, $\mathfrak{g}$ ideales fraccionarios de un dominio A y sea $S \subset A$ un subconjunto multiplicativo tal que $0 \notin S$. Entonces $S^{-1}\mathfrak{f}$ y $S^{-1}\mathfrak{g}$ son ideales fraccionarios de $S^{-1}A$, además:*

- $S^{-1}(\mathfrak{f} + \mathfrak{g}) = S^{-1}\mathfrak{f} + S^{-1}\mathfrak{g}$,
- $S^{-1}(\mathfrak{f}\mathfrak{g}) = S^{-1}\mathfrak{f}\ S^{-1}\mathfrak{g}$,
- $S^{-1}(\mathfrak{f} \cap \mathfrak{g}) = S^{-1}\mathfrak{f} \cap S^{-1}\mathfrak{g}$.
- *Si $\mathfrak{g}$ es un A-módulo finitamente generado, entonces* $S^{-1}(\mathfrak{f} :_{K_A} \mathfrak{g}) = (S^{-1}\mathfrak{f} :_{K_A} S^{-1}\mathfrak{g})$.
- *Si además $\mathfrak{f}$ es invertible, $S^{-1}\mathfrak{f}$ es un ideal fraccionario invertible de $S^{-1}A$.*

Demostración. En primer lugar, obsérvese que $K_A = K_{S^{-1}A}$ y que si $a \in A \setminus \{0\}$ es tal que $a\mathfrak{f} \subset A$, entonces $aS^{-1}\mathfrak{f} \subset S^{-1}A$. Por lo tanto, tendremos que $S^{-1}\mathfrak{f} \subset K_A$ será un ideal fraccionario de $S^{-1}A$. Por otro lado, las propiedades enunciadas son propiedades generales para la localización en un subconjunto multiplicativo (véase [1, Corolario 3.4]). Únicamente las dos últimas propiedades merecen atención. Si $x \in K_A$ es tal que $x\mathfrak{g} \subset \mathfrak{f}$, entonces trivialmente $xS^{-1}\mathfrak{g} \subset S^{-1}\mathfrak{f}$. Para demostrar el otro contenido asumiremos la hipótesis de que $\mathfrak{g}$ es un A-módulo finitamente generado. Sea $\{g_1, \ldots, g_n\}$ un conjunto de generadores de $\mathfrak{g}$ como A-módulo. Entonces dado $\alpha \in (S^{-1}\mathfrak{f} :_{K_A} S^{-1}\mathfrak{g})$, para cada $i \in \{1, \ldots, n\}$ existirán elementos $f_i \in \mathfrak{f}$ y $s_i \in S$ tales que $\alpha g_i = \frac{f_i}{s_i}$, es decir, tales que

$\alpha s_i g_i = f_i$. Definiendo $s = \prod_{i=1}^n s_i \in S$, se tiene que $s\alpha = \beta \in (\mathfrak{f} :_{K_A} \mathfrak{g})$ y por lo tanto $\alpha = \frac{\beta}{s} \in S^{-1}(\mathfrak{f} :_{K_A} \mathfrak{g})$.

Por último, si $\mathfrak{f}$ es invertible entonces existirá $\mathfrak{g} \subset K_A$ un ideal fraccionario de A tal que $\mathfrak{fg} = A$. Entonces $S^{-1}\mathfrak{f}\, S^{-1}\mathfrak{g} = S^{-1}(\mathfrak{fg}) = S^{-1}A$. □

Observación 1.18. La propiedad «ser invertible» en el conjunto de los ideales fraccionarios de un dominio noetheriano es una propiedad local (Proposición 1.20). Para la demostración de este hecho es útil el siguiente resultado:

Lema 1.19. *Sea A un subanillo de un cuerpo K. Sea M un A-módulo contenido en un K-espacio vectorial V. Entonces:*

$$M = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} M_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in \mathrm{Spm}(A)} M_{\mathfrak{m}}$$

Demostración. Es suficiente comprobar que el contenido $M \subset \bigcap_{\mathfrak{m} \in \mathrm{Spm}(A)} M_{\mathfrak{m}}$ es una igualdad. Dado $\mathfrak{m} \in \mathrm{Spm}(A)$, si $v \in V$ es tal que $v \in M_{\mathfrak{m}}$ entonces v es de la forma $v = \frac{x}{t}$ con $x \in M$ y $t \in A - \mathfrak{m}$. Por lo tanto, $t \in (M :_A v)$ y $(M :_A v) \not\subset \mathfrak{m}$. Entonces si para todo $\mathfrak{m} \in \mathrm{Spm}(A)$ se tiene que $v \in M_{\mathfrak{m}}$, necesariamente $(M :_A v) = A$. De este modo obtenemos que $v = 1 \cdot v \in M$. □

Proposición 1.20. *Sea A un dominio noetheriano y $\mathfrak{f} \subset K_A$ un ideal fraccionario. Entonces equivalen:*

(1) *El ideal fraccionario $\mathfrak{f}$ es invertible.*

(2) *Para todo $\mathfrak{m} \in \mathrm{Spm}(A)$ (equivalentemente, para todo $\mathfrak{m} \in \mathrm{Spec}(A)$), $\mathfrak{f}_{\mathfrak{m}}$ es un ideal fraccionario invertible de $A_{\mathfrak{m}}$.*

Demostración. (1) $\Rightarrow$ (2) se sigue de la Proposición 1.17. Recíprocamente, si $\mathfrak{f}_{\mathfrak{m}}$ es invertible para todo $\mathfrak{m} \in \mathrm{Spm}(A)$, entonces empleando la Proposición 1.17 y el Lema 1.19 se deduce que $\mathfrak{f}$ es invertible

$$\mathfrak{f}(A :_{K_A} \mathfrak{f}) = \bigcap_{\mathfrak{m}} (\mathfrak{f}(A :_{K_A} \mathfrak{f}))_{\mathfrak{m}} = \bigcap_{\mathfrak{m}} \mathfrak{f}_{\mathfrak{m}}(A_{\mathfrak{m}} :_{K_A} \mathfrak{f}_{\mathfrak{m}}) = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}} = A.$$ □

Lema 1.21. *Sea A un dominio local y $\mathfrak{m}$ su maximal. Un ideal fraccionario de A es invertible si, y solo si, es principal.*

Demostración. Los ideales principales no nulos son siempre invertibles. Supongamos ahora que $\mathfrak{f}$ es un ideal fraccionario de A invertible. Tendremos que $\mathfrak{f}\mathfrak{f}^{-1} = A$ y de este modo $\sum_{i=1}^n a_i b_i = 1$ para ciertos elementos $a_i \in \mathfrak{f}$ y $b_i \in \mathfrak{f}^{-1} = (A :_{K_A} \mathfrak{f})$. Notemos que $a_i b_i \in A$ para todo $i \in \{1, \ldots, n\}$ y además alguno de ellos debe ser una unidad. En efecto, si

ninguno de estos productos fuese una unidad de A, entonces todos serían elementos del maximal $\mathfrak{m}$ y en consecuencia $1 \in \mathfrak{m}$, lo que es una contradicción. Supongamos sin perder generalidad que el primero de estos productos $a_1 b_1$ es una unidad de A. Para cada $x \in \mathfrak{f}$ tendremos que $a_1 b_1 x \in a_1 A$ y usando que $a_1 b_1 \in A$ es una unidad, tendremos que $x \in a_1 A$. Conclusión:

$$\mathfrak{f} \subset a_1 A \subset \mathfrak{f} \implies \mathfrak{f} = a_1 A. \qquad \square$$

Capítulo 2

Anillos de valoración discreta

En este capítulo abordaremos el estudio de los ideales fraccionarios en un tipo de anillos con «buenas propiedades»: los anillos de valoración discreta. Antes de esto, y como requisitos previos a este estudio, introducimos las noción de dependencia entera en una extensión de anillos, y posteriormente, el concepto de anillo de valoración.

2.1. Extensiones enteras de anillos

Definición 2.1. Sean A y B anillos tales que $A \subset B$. Diremos que $A \subset B$ es una *extensión de anillos* si A es un subanillo de B.

Definición 2.2. Dada una extensión de anillos $A \subset B$, diremos que un *elemento* $x \in B$ es *entero sobre* A si existe un polinómio mónico y no nulo $f \in A[X]$ de manera que $f(x) = 0$, es decir, si x satisface una ecuación de la forma

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

donde $a_1, \ldots, a_n$ son elementos de A. Si todo elemento de B es entero sobre A diremos que la extensión $A \subset B$ es entera.

Proposición 2.3. *Sea $A \subset B$ una extensión de anillos. Un elemento $x \in B$ es entero sobre A si, y solo si, $A[x]$ es un A-módulo finitamente generado.*

Demostración. [1, Proposición 5.1]. □

Corolario 2.4. *Sea $A \subset B$ una extensión de anillos y $C := \{\, x \in B \mid x \text{ es entero sobre } A \,\}$. El conjunto $C \subset B$ es un subanillo de B que contiene a A.*

Demostración. [1, Corolario 5.3]. □

Definición 2.5. En las condiciones del Corolario 2.4, el anillo C se denomina *clausura íntegra de A en B* y se denotará por $\overline{A}^B$. Cuando A es un dominio y $B = K_A$, $\overline{A}^B$ se denominará simplemente la *clausura íntegra de A* y se denotará $\overline{A}$.

Definición 2.6. Sea $A \subset B$ una extensión de anillos. Diremos que A es íntegramente cerrado en B si $\overline{A}^B = A$. En el caso en que A sea un dominio y $B = K_A$, diremos simplemente que A es un *dominio íntegramente cerrado.*

Proposición 2.7. *Sea $A \subset B$ una extensión de anillos y sea $\overline{A}^B$ la clausura íntegra de A en B. Entonces $\overline{A}^B$ es íntegramente cerrado en B.*

Demostración. [1, Corolario 5.5] □

Para un dominio la propiededad «ser integramente cerrado» es una propiedad local:

Proposición 2.8. *Para un dominio A equivalen:*

(1) *A es integramente cerrado.*
(2) *$A_{\mathfrak{p}}$ es integramente cerrado, $\forall\, \mathfrak{p} \in \mathrm{Spec}(A)$.*
(3) *$A_{\mathfrak{m}}$ es integramente cerrado, $\forall\, \mathfrak{m} \in \mathrm{Spm}(A)$.*

Demostración. [1, Proposición 5.13]. □

2.2. Anillos de valoración

Definición 2.9. Sea A un dominio. Diremos que A es un *anillo de valoración* si para cada $x \in K_A^{\times}$, se tiene que $x \in A$ o $x^{-1} \in A$.

Proposición 2.10. *Sea A un anillo de valoración. El conjunto de los ideales de A forman un conjunto totalmente ordenado respecto a la inclusión.*

Demostración. Sean I, J ideales de A distintos. Supongamos que existe $x \in I$ tal que $x \notin J$. Entonces para todo $y \in J$ no nulo tendremos que $\frac{x}{y} \notin A$ y de este modo $\frac{y}{x} \in A$. Por lo tanto $y = x \cdot \frac{y}{x} \in I$ y así $J \subset I$. □

Proposición 2.11. *Si el dominio A es un anillo de valoración, entonces A es un anillo local e íntegramente cerrado.*

Demostración. Todo ideal propio de A está contenido en un ideal maximal, y como consecuencia de la Proposición 2.10, A posee un único maximal.

Sea $\alpha \in K_A$ un elemento entero sobre A. Luego existe $p \in A[X]$ mónico y no nulo de modo que $p(\alpha) = \alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$. Supongamos que $\alpha \notin A$. Entonces $\alpha^{-1} \in A$ y de este modo $\alpha = -(c_1 + c_2\alpha^{-1} + \cdots + c_n\alpha^{1-n}) \in A$. Esto es absurdo y por lo tanto, los únicos elementos de K_A enteros sobre A son los de A. □

Definición 2.12. Sea $(G, \leq)$ un grupo abeliano totalmente ordenado. Diremos que el grupo $(G, \leq)$ es un *grupo linealmente ordenado* si dados α, $\beta \in G$ tales que $\alpha \leq \beta$, se verifica que $\alpha + \gamma \leq \beta + \gamma$, para todo $\gamma \in G$.

Definición 2.13. Sea K un cuerpo y $(G, \leq)$ un grupo abeliano linealmente ordenado. Una *valoración de* K con valores en $(G, \leq)$ es un homomorfismo sobreyectivo de grupos abelianos $\nu : (K^\times, \cdot) \longrightarrow (G, +)$ tal que $\nu(x+y) \geq \text{mín}\{\nu(x), \nu(y)\}$, para todo $x, y \in K^\times$.

Observación 2.14. Es conveniente añadir un elemento «∞» a G estableciendo que $\infty + g = \infty = g + \infty$ y que $g < \infty$ para todo $g \in G$. Así podremos extender ν a todo K definiendo $\nu(0) := \infty$. Esta extensión se seguirá llamando *valoración de* K y se denotará por $\nu\colon K \to G_\infty$. Cabe destacar que este artificio técnico simplemente pretende que las propiedades citadas anteriormente se verifiquen sin excepción.

Lema 2.15. *Sea $\nu : K \to G_\infty$ una valoración de K. El conjunto $A_\nu := \{x \in K^\times \mid \nu(x) \geq 0\}$ es un subanillo de K y se denomina* el anillo de valoración de ν.

Demostración. El subconjunto $A_\nu \subset K$ contiene al elemento neutro de la multiplicación ya que $\nu(1) = 0$; además es un subconjunto cerrado para la suma y para la multiplicación: si $x, y \in A_\nu$ entonces $\nu(xy) = \nu(x) + \nu(y) \geq 0$ y $\nu(x+y) \geq \text{mín}\{\nu(x), \nu(y)\} \geq 0$. □

Lema 2.16. *Sea $\nu\colon K \longrightarrow G_\infty$ una valoración de K y sea $A = A_\nu$ su anillo de valoración. Entonces $A^\times = \{x \in K \mid \nu(x) = 0\}$.*

Demostración. Sea $x \in A^\times$. Entonces $0 = \nu(1) = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1})$. Como $\nu(x)$, $\nu(x^{-1}) \geq 0$, entonces $\nu(x) = 0$. Recíprocamente, si $x \in K$ tal que $\nu(x) = 0$, entonces $0 = \nu(x) = -\nu(x^{-1})$ y de este modo $\nu(x^{-1}) = 0$. Por lo tanto x y $x^{-1} \in A$. □

Definición 2.17. Sea K un cuerpo. Diremos que ν y ν', dos *valoraciones de* K, son equivalentes si sus anillos de valoración A_ν y $A_{\nu'}$ son iguales. Trivialmente, esta relación es de equivalencia entre las valoraciones de K.

Teorema 2.18. *Dos valoraciones de K, $\nu : K^\times \to G$ y $\nu' : K^\times \to G'$ son equivalentes si, y solo si, existe un isomorfismo de grupos ordenados $\lambda : G \to G'$ de modo que $\nu' = \lambda \circ \nu$.*

Demostración. Supongamos que ν y ν' son equivalentes. Por hipótesis los anillos de valoración son iguales; denotemos $A = A_\nu = A_{\nu'}$. Por el Lema 2.16, se tiene que $A^\times = \text{Ker}(\nu) = \text{Ker}(\nu')$. Además cada una de las valoraciones $\nu : K^\times \to G$ y $\nu' : K^\times \to G'$ son homomorfismos sobreyectivos de grupos, por lo que inducirán isomorfismos de grupos $\mu : K^\times/A^\times \to G$ y $\mu' : K^\times/A^\times \to G'$. Tomando $\lambda := \mu' \circ \mu^{-1}$, obtenemos el resultado. El recíproco es inmediato. □

Los anillos de valoración y las valoraciones en un cuerpo K son conceptualmente la misma cosa. El siguiente teorema atribuido a Wolfgang Krull prueba esta afirmación:

Teorema 2.19 (W. Krull)**.** *Sea K un cuerpo arbitrario y A un dominio. Tendremos que:*

(1) *Si ν es una valoración de K, su anillo de valoración A_ν es un anillo de valoración cuyo cuerpo de fracciones es K.*

(2) *Si A es un anillo de valoración, existe un grupo abeliano linealmente ordenado $(G, \leq)$ y una valoración $\nu : K_A^\times \to G$ de modo que A es el anillo de valoración de (K_A, ν). En este caso diremos que ν es una* valoración asociada a A.

Demostración. (1) Sea $A = A_\nu$ al anillo de valoración asociado a ν, la valoración de K. Sea $x \in K \setminus A$. Luego $\nu(x) < 0$. Ya que $\nu(x) + \nu(x^{-1}) = 0$, se verifica que $\nu(x^{-1}) > 0$ y así, $x^{-1} \in A$. Veamos además que K es el cuerpo de fracciones de A. Sea K_A el cuerpo de fracciones de A. Se tiene entonces que $A \subset K_A \subset K$. Sea $x \in K$: si $x \in A$ tendremos que $x \in K_A$; si $x \in K \setminus A$, entonces $x^{-1} \in A$ y de este modo $x = \frac{1}{x^{-1}} \in K_A$. Concluimos entonces que $K = K_A$.

(2) Sea $G := \{xA \mid x \in K_A^\times\}$ el grupo multiplicativo con el producto $xA \cdot yA = xyA$. Consideremos en G el orden determinado por:

$$x, y \in K_A^\times : \quad xA \leq yA :\Longleftrightarrow xA \supset yA$$

Esta relación es un orden total y lineal: que esta relación de orden es total es una comprobación análoga a la demostración de la Proposición 2.10 y la linealidad del orden se sigue de que dados xA, yA y $zA \in G$:

$$xA \supset yA \implies zxA \supset zyA :\Longleftrightarrow zA \cdot xA \supset zA \cdot yA \implies zA \cdot xA \leq zA \cdot yA$$

La aplicación $\nu : K_A^\times \to G$ dada por $\nu(x) := xA$ es una valoración de K_A mediante unas comprobaciones rutinarias. Además A es el anillo de valoración de la extensión $\nu\colon K_A \to G_\infty$. □

Corolario 2.20. *Sea ν una valoración en K y sea A_ν su anillo de valoración. Entonces A_ν es un anillo local con ideal maximal $\mathfrak{m} = \{x \in K_A \mid \nu(x) > 0\}$ y es íntegramente cerrado.*

Demostración. En virtud del Teorema 2.19, A_ν es un anillo de valoración y por lo tanto el resultado se deduce aplicando la Proposición 2.11. □

Teorema 2.21. *Sea K un cuerpo y sea A un subanillo de K. La clausura entera de A en K es la intersección de todos los anillos de valoración de K que contienen a A.*

Demostración. [6, Theorem 9.4.4]. □

2.3. Anillos de valoración discreta

Definición 2.22. Sea K un cuerpo. Diremos que una valoración $\nu : K^\times \to G$ es una *valoración discreta* si existe un isomorfismo de grupos ordenados (necesariamente único) entre G y $\mathbb{Z}$. De este modo podemos suponer sin perder generalidad que el rango de una valoración discreta es siempre $\mathbb{Z}$. Por otra parte, diremos que un anillo A es un *anillo de valoración discreta* (AVD) si A es el anillo asociado a una valoración discreta de su cuerpo de fracciones K_A.

Ejemplo 2.23.

(*a*) Dado $p \in \mathbb{Z}$ un número primo, todo racional no nulo $\frac{a}{b}$ se puede escribir de forma única como $p^r \frac{a'}{b'}$, donde $r \in \mathbb{Z}$ y p es coprimo con los enteros a' y b'. La aplicación $v_p : \mathbb{Q}^\times \to \mathbb{Z}$ determinada por $\frac{a}{b} \mapsto r$ es una valoración discreta de $\mathbb{Q}$ cuyo anillo de valoración asociado es $\mathbb{Z}_{(p)}$.

(*b*) Sea K un cuerpo. Para un polinomio irreducible $f \in K[X]$, la localización $K[X]_{(f)}$ es el anillo de valoración de $\nu_f : K(X)^\times \to \mathbb{Z}$, homomorfismo que viene dado por $\nu_f(f^n \frac{a}{b}) := n$; siendo $a, b \in K[X]$ polinomios coprimos con f.

(*c*) Sea $K[[X]]$ el anillo de las series de potencias en la variable X con coeficienes en el cuerpo K. El anillo $K[[X]]$ es el anillo de valoración de $\nu : K((X))^\times \to \mathbb{Z}$, aplicación definida por $\nu(\frac{f_1}{f_2}) := n_1 - n_2$, donde, para cada $i \in \{1, 2\}$, $n_i \in \mathbb{N}$ es el mayor natural tal que X^{n_i} divide a f_i en $K[[X]]$.

Definición 2.24. Sea A un AVD. Se dirá que $t \in A$ es un parámetro de uniformización (PU) si $\nu(t) = 1$ para alguna (equivalentemente cualquier) valoración ν asociada a A.

Observación 2.25. La definición no depende de la elección de ν por el Lema 2.18 y el hecho de que el único isomorfismo de grupos ordenados de $\mathbb{Z}$ es la identidad.

Lema 2.26. *Sea A un* AVD *y sea $t \in A$ un* PU. *Se verifica:*

(1) *Si $a \neq 0$ en A, entonces $a = ut^n$ donde $u \in A^\times$ y $n = \nu(a) \in \mathbb{N}$.*

(2) *Si $x \neq 0$ en K_A, entonces $x = ut^n$ donde $u \in A^\times$ y $n = \nu(x) \in \mathbb{Z}$.*

(3) *Los únicos ideales propios no nulos de A son de la forma (t^n) con $n \in \mathbb{Z}^+$.*

(4) *El ideal maximal de A es $\mathfrak{m} = (t)$ y además, es el único ideal primo no nulo de A.*

(5) *Los únicos ideales fraccionarios de A son de la forma (t^n) con $n \in \mathbb{Z}$.*

Demostración.

(1) Sea $a \in A$ no nulo y $n := \nu(a)$. Tendremos que $a = ut^n$ donde por definición $u = at^{-n}$, que es una unidad en A pues $\nu(u) = 0$.

(2) Análogo al apartado anterior.

(3) Sea I un ideal propio y no nulo de A. Consideremos el conjunto $\{\nu(a) \mid a \in I\backslash\{0\}\} \subset \mathbb{Z}^+$ y tomemos n el mínimo de ese conjunto. Sea $a \in I$ de modo que $\nu(a) = n$. En virtud de (1), existe $u \in A^\times$ tal que $a = ut^n$. De esta manera, tendremos que $(t^n) \subset I$. Si $b \in I$, tendremos que existe $u' \in A^\times$ de modo que $b = u't^q$, con $q \geq n$ y por lo tanto $b \in (t^n)$; verificándose así el otro contenido y obteniéndose la igualdad.

(4) Está claro que $\mathfrak{m} = (t)$ es maximal por (3) y además será el único por el Corolario 2.20. Sea $\mathfrak{p}$ un ideal primo no nulo de A. Entonces existirá $n \in \mathbb{Z}^+$ de modo que $\mathfrak{p} = (t^n)$, y dado que $\mathfrak{p}$ es primo, tendremos que $t \in \mathfrak{p}$. De este modo concluimos que $\mathfrak{p} = (t)$.

(5) En virtud de (3), sabemos que A es un DIP y por lo tanto noetheriano. En la Observación 1.7 se indica que todo ideal fraccionario $\mathfrak{f}$ es de la forma xA, donde $x \in K_A^\times$. Empleando (2) tendremos que $x = ut^n$ para cierto $n \in \mathbb{Z}$ y cierto $u \in A^\times$ y así $\mathfrak{f} = (t^n)$. □

Los anillos de valoración discreta son en cierta medida los dominios con las «mejores» propiedades que no son cuerpos. Además de ser un dominio local, un AVD verificará las siguientes propiedades que lo caracterizarán completamente.

Teorema 2.27 (Caracterización de AVD)**.** *Sea A un dominio que no es un cuerpo. Son equivalentes:*

(1) *A es un* AVD.

(2) *A es un* DIP *local.*

(3) *A es un* DFU *con único elemento irreducible t salvo asociados.*

(4) *A es un anillo noetheriano local cuyo ideal maximal es principal.*

(5) *A es un anillo noetheriano, local, íntegramente cerrado y* $\dim(A) = 1$.

(6) *A es un anillo local y todo ideal fraccionario de A no nulo es invertible.*

Demostración. La implicación (1) ⇒ (2) se probó en el Lema 2.26.

(2) ⇒ (3) Obsérvese que si A es un DIP local y $\mathfrak{m} = (t)$ es su maximal, claramente t es el único elemento irreducible de A.

(3) ⇒ (1) El ideal (t) es primo y será maximal por la unicidad de t. Para cada $a \in A$, tendremos que existe un único $n_a \in \mathbb{N}$ tal que $a \in (t^{n_a})$ y $a \notin (t^{n_a+1})$. Definimos para cada $\frac{a}{b} \in K_A^\times$ con $\mathrm{mcd}(a, b) = 1$, $\nu(\frac{a}{b}) := n_a - n_b$. La aplicación $\nu : K_A^\times \to \mathbb{Z}$ es una valoración discreta que tiene a A como anillo de valoración.

La implicación (2) ⇒ (4) es Trivial.

(4) $\Rightarrow$ (3) Sea $\mathfrak{m} = (t)$ el maximal de A. Veamos que A es un DFU con único elemento irreducible t. Si un elemento $a \in A$ admite una factorización de la forma $a = ut^n$ con $n \in \mathbb{N}$ y $u \in A^\times$, esta factorización es única: si $u_1 t^{n_1} = u_2 t^{n_2}$ donde $n_1 \geq n_2$ son números naturales y $u_1, u_2 \in A^\times$, se tiene que $u_2 = u_1 t^{n_1 - n_2}$ es una unidad. Entonces, necesariamente $n_1 = n_2$ y $u_1 = u_2$. Veamos que todo elemento de A admite una factorización del tipo indicado demostrando que el subconjunto $T \subset A$ de los elementos de A que no admiten tal factorización es necesariamente vacío. En efecto, supongamos que existe un elemento $b \in T$, entonces $b \notin A^\times$ y por tanto $b = b_1 t$. Como $b \in T$, entonces $b_1 \in T$, ya que en otro caso $b_1 = u_1 t^{n_1}$ y entonces $b = u_1 t^{n_1+1} \in A \setminus T$ lo cual es una contradicción. Además, $(b) \subsetneq (b_1)$; de este modo construimos una cadena de elementos $b_i \in T$ tal que $(b) \subsetneq (b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq \cdots$ que formarán una cadena no estacionaria de ideales de A. Esto contradice que A sea noetheriano.

El Lema 2.26 demuestra que (1) $\Rightarrow$ (6), dado que los únicos ideales fraccionarios de un AVD A con PU t, son los de la forma (t^n) con $n \in \mathbb{Z}$. De esta manera serán invertibles.

(6) $\Rightarrow$ (4) Por hipótesis, $\mathfrak{m} \subset A$ es un ideal invertible y por el Lema 1.21 $\mathfrak{m}$ es principal.

(5) $\Rightarrow$ (4) Veamos que el ideal maximal $\mathfrak{m} \subset A$ es principal. Por el Lema de Nakayama, se tiene que $\mathfrak{m} \neq \mathfrak{m}^2$. Elegido un elemento $t \in \mathfrak{m} - \mathfrak{m}^2$, claramente $(t) \subset \mathfrak{m}$. Sea $n \in \mathbb{Z}^+$ minimal de modo que $\mathfrak{m}^n \subset (t)$. Veamos que necesariamente $n = 1$. Supongamos por reducción al aburdo que $n > 1$. Sea ahora $x \in \mathfrak{m}^{n-1}$ tal que $x \notin (t)$. Tendremos entonces que $x\mathfrak{m} \subset \mathfrak{m}^n \subset (t)$. Consideremos el elemento $y := \frac{x}{t} \in K_A$. Entonces $y \notin A$ pues $yt = x$ pero $x \notin (t)$. Veamos que y es un elemento entero sobre A y de este modo estará en A; lo que sería contradictorio. Dado que $y\mathfrak{m} \subset A$, $y\mathfrak{m}$ es un ideal entero de A. Si $y\mathfrak{m} = A$, tendremos que para cierto $m \in \mathfrak{m}$, $ym = 1$ y de esta manera, $xm = tym = t \in \mathfrak{m}^n \subset \mathfrak{m}^2$, lo que contradice la elección de t. De este modo, el ideal $y\mathfrak{m}$ debe ser un ideal propio de A, es decir $y\mathfrak{m} \subset \mathfrak{m}$ (dado que $\mathfrak{m}$ es el único ideal maximal de A). Sea $\{m_1, \ldots, m_s\}$ un sistema de generadores del ideal $\mathfrak{m}$, y sean a_{ij} elementos de A tales que para cada $j \in \{1, \ldots, n\}$ se tiene una expresión del tipo $ym_j = \sum_{i=1}^{s} a_{ij} m_i$. Reescribiendo estas igualdades matricialmente:

$$\begin{pmatrix} a_{11} - y & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} - y & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} - y \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{2.1}$$

Sea $d := \det(a_{ij} - \delta_{ij} y)$. Empleando la Regla de Cramer, deducimos que $dm_i = 0$ para todo $i \in \{1, \ldots, n\}$. Dado que $\mathfrak{m} \neq 0$, deducimos que la igualdad $d = 0$ es una relación de

dependencia entera para y sobre A.

(3) $\Rightarrow$ (5) Veamos que si A es un DFU, entonces es íntegramente cerrado en su cuerpo de fracciones. Sea $\alpha \in K_A^\times$ y supongamos que $\alpha = \frac{a}{b}$ con $a, b \in A \setminus \{0\}$ tales que $\mathrm{mcd}(a, b) = 1$. Si $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$ es una relación de dependencia entera de α con coeficientes $c_{n-1}, \ldots, c_0 \in A$, entonces se tendría que $a^n + bc_{n-1}a^{n-1} + \cdots + b^n c_0 = 0$ y de este modo $b \mid a^n$, por lo que necesariamente $b \in A^\times$ y así $\alpha \in A$. Por último, dado que (3) y (2) son equivalentes, A es un DIP local y por lo tanto será noetheriano y $\dim(A) = 1$. □

Corolario 2.28. *Sea A un anillo de valoración. Son equivalentes:*

(1) *A es un* AVD.

(2) *A es un* DIP.

(3) *A es noetheriano.*

Demostración. La implicación (1) $\Rightarrow$ (2) se probó en el Lema 2.26. La implicación (2) $\Rightarrow$ (3) es trivial. Para demostrar (3) $\Rightarrow$ (1), supongamos que A es un anillo de valoración noetheriano y tomemos I un ideal de A. Como A es noetheriano, I será finitamente generado por una familia $\{a_1, \ldots, a_n\} \subset A$. En virtud de la Proposición 2.10, existirá a_{i_0} de modo que $(a_i) \subset (a_{i_0})$ para todo $i \in \{1, \ldots, n\}$. Así pues se deduce que $I = (a_{i_0})$. □

Corolario 2.29. *Sea A un dominio noetheriano íntegramente cerrado. Sea $\mathfrak{p}$ un ideal primo no nulo y minimal, entonces la localización $A_\mathfrak{p}$ es un* AVD.

Demostración. Observemos que $K_A = K_{A_\mathfrak{p}}$ y además $A_\mathfrak{p}$ es un dominio noetheriano e íntegramente cerrado. Además $\dim(A_\mathfrak{p}) = \mathrm{alt}(\mathfrak{p}) = 1$, concluyendo el resultado usando el Teorema 2.27. □

Capítulo 3

Dominios de Dedekind

Comenzaremos este capítulo recordando el concepto de *módulo proyectivo*, una noción que resultará clave para poder definir los «dominios de Dedekind». La clase de los módulos proyectivos generaliza en cierta medida la clase de los módulos libres.

Un A-módulo P es *proyectivo* si verifica las siguientes condiciones equivalentes ([5, Proposition 3.10]):

(1) Si $\pi\colon M \to N$ es un homomorfismo sobreyectivo de A-módulos y $\phi\colon P \to N$ es un homomorfismo, entonces existe al menos un homomorfismo $\psi\colon P \to M$ de modo que $\phi = \pi \circ \psi$.

(2) El functor $\mathrm{Hom}(P, -)$ es exacto.

(3) Si $0 \to N \xrightarrow{\iota} M \xrightarrow{\pi} P \to 0$ es una sucesión exacta corta de A-módulos entonces escinde, es decir, existe un homomorfismo $\sigma\colon P \to M$ de modo que $\mathrm{id}_P = \pi \circ \sigma$ y así se tiene la descomposición $M = \iota(N) \oplus \sigma(P) \cong N \oplus P$.

(4) Existe un A-módulo Q de modo que $P \oplus Q$ es un A-módulo libre.

Una de las propiedades que caracterizan los módulos proyectivos finitamente generados y que utilizaremos en esta memoria es el *Lema de la base dual*, que relaciona el carácter proyectivo de un A-módulo con la existencia de un conjunto finito de generadores junto con su respectiva base dual:

Teorema 3.1 (Lema de la base dual)**.** *Dado P un A-módulo, equivalen:*

(1) *P es un A-módulo proyectivo finitamente generado.*

(2) *Existe un número finito de elementos $x_1, \ldots, x_n \in P$ y $f_1, \ldots, f_n \in \mathrm{Hom}_A(P, A)$ de modo que, para todo $x \in P$, $x = \sum_{i=1}^{n} f_i(x) x_i$.*

Demostración. [5, Proposition 3.12] □

3.1. Dominios de Dedekind: grupo de Picard

Sea A un domino y sea $S_A \subset A$ el conjunto de los elementos no nulos de A. Dado M un A-módulo arbitrario, podemos construir el K_A-espacio vectorial $S_A^{-1}M$. La dimensión de este espacio vectorial se denomina *rango del A-módulo M* y se denotará $\operatorname{rang}_A(M)$, o simplemente $\operatorname{rang}(M)$. Si M es un A-módulo finitamente generado entonces $\operatorname{rang}_A(M)$ es finito.

Teorema 3.2. *Sea A un dominio. Si $\mathfrak{f} \subset K_A$ es un A-submódulo no nulo, entonces se verifica que* $\operatorname{rang}(\mathfrak{f}) = 1$. *Además, $\mathfrak{f}$ es un ideal fraccionario invertible de A si, y solo si, $\mathfrak{f}$ es un A-módulo proyectivo finitamente generado.*

Demostración. Si $\mathfrak{f}$ es un A-submódulo no nulo de K_A, la inclusión $\mathfrak{f} \subset K_A$ induce un isomorfismo canónico de K_A-espacios vectoriales entre $S_A^{-1}\mathfrak{f}$ y K_A (de hecho son el mismo K_A-espacio vectorial). De este modo, podemos deducir que el rango de $\mathfrak{f}$ es 1. Utilizando la Observación 1.11, sabemos que la aplicación $\boldsymbol{\mu}\colon (A :_{K_A} \mathfrak{f}) \to \operatorname{Hom}_A(\mathfrak{f}, A)$ dada por $y \mapsto \mu_y$ es un isomorfismo de A-módulos. De esta manera, cada $y \in (A :_{K_A} \mathfrak{f})$ determina un único homomorfismo de A-módulos $\mu_y\colon \mathfrak{f} \to A$ dado por $x \mapsto xy$.
Entonces, el hecho de que $\mathfrak{f}$ verifique la igualdad $A = \mathfrak{f}(A :_{K_A} \mathfrak{f})$, significa que $1 = \sum_{i=1}^{n} x_i y_i$ para ciertos $x_i \in \mathfrak{f}$ e $y_i \in (A :_{K_A} \mathfrak{f})$. Esta expresión equivale a:

$$x = 1 \cdot x = \sum_{i=1}^{n} x_i y_i x = \sum_{i=1}^{n} x_i \mu_{y_i}(x) \qquad (\ \forall\, x \in \mathfrak{f}\ ),$$

es decir, a que $\mathfrak{f}$ es un A-módulo proyectivo finitamente generado (Teorema 3.1). □

Introducimos uno de los conceptos clave de esta memoria:

Definición 3.3. Sea A un dominio. Diremos que A es un *dominio de Dedekind* (DD) si todo ideal fraccionario de A es invertible, es decir, si $(\texttt{Frac}(A), \cdot)$ es un grupo abeliano.

Teorema 3.4. *Para un dominio A equivalen:*

(1) *A es un dominio de Dedekind.*
(2) *Todo ideal fraccionario de A es proyectivo de tipo finito.*
(3) *Todo ideal entero no nulo de A es invertible.*
(4) *Todo ideal entero de A es proyectivo de tipo finito.*

Además, todo dominio A verificando las condiciones anteriores será noetheriano.

Demostración. Por el Teorema 3.2 (1) $\Leftrightarrow$ (2) y (3) $\Leftrightarrow$ (4). De forma clara se tiene que (1) $\Rightarrow$ (3), veamos que (3) $\Rightarrow$ (1). En efecto, sea $\mathfrak{f} \subset K_A$ un ideal fraccionario y $a \in A \setminus \{0\}$ tal que $a\mathfrak{f} \subset A$. Por hipótesis, el ideal entero $a\mathfrak{f}$ es invertible y por tanto $\frac{1}{a}A \cdot a\mathfrak{f} = \mathfrak{f}$ es invertible. Como consecuencia de (3), un dominio verificando esas condiciones es noetheriano. □

Observación 3.5. Se deduce claramente de la condición (3) del Teorema 3.4 que todo DIP es un DD. En particular todo cuerpo K, los anillos de polinomios $K[X]$, el anillo de los enteros $\mathbb{Z}$ y los AVD son ejemplos de DD. Además, en virtud de la propiedad (4) del Teorema 3.4, los DD se podrán caracterizar como dominios hereditarios, es decir, dominios donde todo ideal es proyectivo.

Corolario 3.6. *Si A es un dominio de Dedekind y S es un subconjunto multiplicativo de A entonces $S^{-1}A$ es un dominio de Dedekind.*

Demostración. Para cada ideal no nulo J de $S^{-1}A$, existe un ideal no nulo I de A de modo que $J = S^{-1}I$. Así pues, I será un ideal fraccionario del dominio de Dedekind A y por lo tanto será invertible, entonces J será un ideal invertible de $S^{-1}A$ (Proposición 1.17). □

El siguiente Teorema, probado por la matemática alemana Emmy Noether, nos da una de las caracterizaciones más famosas y útiles que tienen los DD.

Teorema 3.7 (E. Noether)**.** *Para un dominio A que no es un cuerpo, equivalen:*

(1) *A es un dominio de Dedekind.*

(2) *A es noetheriano y $A_{\mathfrak{m}}$ es un* AVD*, $\forall \mathfrak{m} \in \mathrm{Spm}(A)$.*

(3) *A es noetheriano, íntegramente cerrado y todo ideal primo no nulo de A es maximal, es decir, $dim(A) = 1$.*

(4) *A es noetheriano, $dim(A) = 1$ y $A_{\mathfrak{m}}$ es íntegramente cerrado, $\forall \mathfrak{m} \in \mathrm{Spm}(A)$.*

(5) *Todo ideal primo no nulo de A es invertible.*

Demostración.

(1) $\Rightarrow$ (2) Si A es un DD, en virtud del Teorema 3.4, A es noetheriano y por el Corolario 3.6 tendremos que $A_{\mathfrak{m}}$ es un DD, para cualquier $\mathfrak{m} \in \mathrm{Spm}(A)$. De los Teoremas 3.4 y 2.27 se deduce (2).

(2) $\Rightarrow$ (1) Si A es noetheriano, por la Proposición 1.20, «ser invertible» para los ideales fraccionarios de A es una propiedad local. Por lo tanto, si A verifica (2) entonces es un DD.

(3) $\Leftrightarrow$ (4) Es consecuencia directa de que para dominios, «ser íntegramente cerrado» es una propiedad local (Proposición 2.8).

(2) $\Leftrightarrow$ (3) Esta equivalencia se deduce como consecuencia del Teoremas 3.4, del Teorema 2.27 y de la Proposición 1.20.

(1) $\Rightarrow$ (5) Es consecuencia directa de la caracterización (3) del Teorema 3.4.

(5) $\Rightarrow$ (1) Demostraremos esta implicación por reducción al absurdo. Supongamos que se verifica (4) y que (1) es falso, equivalentemente, que el conjunto $\mathcal{P}$ de ideales (enteros) de A no invertibles es no vacío (utilizando para los DD la caracterización (3) del Teorema 3.4). Consideremos $\mathcal{P}$ ordenado mediante la inclusión. Sea $\{I_\lambda\}_{\lambda\in\Lambda}$ una cadena totalmente ordenada de $\mathcal{P}$; entonces $I := \cup_{\lambda\in\Lambda} I_\lambda \in \mathcal{P}$, ya que en otro caso si $I \notin \mathcal{P}$, el ideal I sería invertible y en particular finitamente generado como A-módulo. Entonces $I = I_{\lambda_0}$ para algún $\lambda_0 \in \Lambda$, pero entonces $I = I_{\lambda_0} \in \mathcal{P}$, lo que es contradictorio. De esta manera toda cadena en $\mathcal{P}$ está acotada superiormente y, por el Lema de Zorn, se deduce que $\mathcal{P}$ posee un elemento maximal $\mathfrak{m}$. El ideal $\mathfrak{m}$ no es invertible; entonces, por (4), $\mathfrak{m}$ no es un ideal primo de A. Sean $a, b \in A$ elementos tales que $a, b \notin \mathfrak{m}$ y $ab \in \mathfrak{m}$. Por ser $\mathfrak{m}$ maximal del conjunto $\mathcal{P}$, el ideal $\mathfrak{m} + (a)$ es invertible y entonces es invertible el ideal $bA \cdot (\mathfrak{m} + aA)$. Como $ab \in \mathfrak{m}$, se tiene que $bA \cdot (\mathfrak{m} + aA) = bA \cdot \mathfrak{m}$ y por lo tanto $\mathfrak{m}$ es invertible. Esto contradice el hecho de que $\mathfrak{m} \in \mathcal{P}$. □

Observación 3.8. Tal como vimos en la Definición 3.3, los DD son exactamente los dominios para los que $(\mathtt{Frac}(A), \cdot)$ es un grupo. Por lo tanto para un dominio de Dedekind A, tenemos que

$$\mathtt{Pic}(A) = \mathtt{Frac}(A)/\mathtt{P}_A$$

es el grupo de clases de isomorfía de sus ideales fraccionarios. Diremos además que el «número de clase» de un DD es el cardinal de su grupo de Picard. Está claro por la propia definición del grupo de Picard y por la Observación 1.7 que un DD es un DIP si y solo si su número de clases es uno, es decir, si todos los ideales fraccionarios son principales. Podemos utilizar el concepto de número de clase como una especie de medida que explica lo «alejado» que un dominio de Dedekind está de ser un DIP. El matemático norteamericano Luther Claborn demostró en [4] que todo grupo abeliano es isomorfo al grupo de Picard de un dominio de Dedekind. De este modo, existen dominios de Dedekind de cualquier número de clase.

Veamos a continuación dos familias de ejemplos que están en el origen del concepto de dominio de Dedekind.

3.2. Dominios de Dedekind: anillos de números

La principal ventaja que poseen los dominios de Dedekind frente a los DFUs es que presentan un buen comportamiento frente a las extensiones enteras; mientras que éstos últimos no lo hacen en general. Vamos a utilizar la caracterización de los dominios de

Dedekind dada en el Teorema 3.7 para probar que, dada una extensión finita y separable L del cuerpo de fracciones K_A de un dominio de Dedekind A, la clausura integra $\overline{A}^L$ de A en L es a su vez un dominio de Dedekind. En particular, los anillos de enteros algebraicos son dominios de Dedekind.

Lema 3.9. *Sean $A \subset B$ dominios y supongamos que A es íntegramente cerrado. Si $x \in B$ es entero sobre un ideal I de A entonces x es algebraico sobre K_A y su polinomio irreducible $X^n + c_1X^{n-1} + \cdots + c_n$ es tal que $c_1, \ldots, c_n \in \mathrm{rad}(I)$.*

Demostración. [1, Proposición 5.15]. □

Lema 3.10. *Sea A un dominio íntegramente cerrado, $K = K_A$ su cuerpo de fracciones, L una extensión algebraica finita separable de K y $\overline{A}^L$ la clausura íntegra de A en L. Entonces existe una base $\{v_1, \ldots, v_n\}$ de L como K-espacio vectorial de modo que $\overline{A}^L \subset \sum_{j=1}^n Av_j$.*

Demostración. Si $x \in L$, entonces x es algebraico sobre K_A y por tanto satisface una ecuación de la forma

$$c_0x^t + \cdots + c_{t-1}x + c_t = 0$$

donde para cada $i \in \{1, \ldots, t\}$, $c_i \in A$ y $c_0 \neq 0$. Multiplicando la ecuación por c_0^{t-1}, se ve que c_0x es un elemento entero sobre A y así, $c_0x \in \overline{A}^L$. De este modo, una base de L cualquiera se puede convertir en una base de elementos enteros sobre A simplemente multiplicando por elementos convenientes de A. Consideremos ahora $\mathcal{B} = \{u_1, \ldots, u_n\}$ una de esas bases. Sea $T\colon L \to K$ la aplicación traza de L sobre K. Dado que la extensión es separable, la aplicación K-bilineal $(x, y) \mapsto T(xy)$ es no degenerada. De este modo, existirá una base dual $\{v_1, \ldots, v_n\}$ de la base $\mathcal{B}$, es decir tal que $T(u_iv_j) = \delta_{ij}$. Sea $x \in \overline{A}^L$ un elemento arbitrario. Luego $x = \sum_{j=1}^n x_jv_j$ con $x_j \in K$ y además como $xu_i \in \overline{A}^L$, por el Lema 3.9, se tiene que $x_i = \sum_{j=1}^n x_jT(u_iv_j) = T(xu_i) \in A$. En consecuencia, $\overline{A}^L \subset \sum_{j=1}^n Av_j$. □

Teorema 3.11. *Sea A un dominio de Dedekind con cuerpo de fracciones K_A. Dada una extensión finita y separable L de K_A, la clausura integral $\overline{A}^L$ de A en L es a su vez un dominio de Dedekind.*

Demostración. El anillo $\overline{A}^L$ es íntegramente cerrado por construcción. Por el Lema 3.10, existe una base $\{v_1, \ldots, v_n\}$ de L sobre K_A de modo que $\overline{A}^L \subset \sum_{j=1}^n Av_j$. Como A es noetheriano y $\sum_{j=1}^n Av_j$ es un A-módulo finitamente generado, entonces $\overline{A}^L$ es un anillo noetheriano. Consideremos $\mathfrak{p}$ un ideal primo no nulo de $\overline{A}^L$. Entonces $\mathfrak{p} \cap A$ es un ideal primo de A y a su vez no nulo. En efecto, el coeficiente constante de una ecuación de dependecia entera de grado mínimo sobre A de un elemento no nulo $x \in \mathfrak{p}$ está en $\mathfrak{p}$, y en

particular, en $\mathfrak{p} \cap A$. De este modo, si $\mathfrak{p}$ y $\mathfrak{p}'$ son ideales primos no nulos de $\overline{A}^L$ tales que $\mathfrak{p} \subsetneq \mathfrak{p}'$, entonces se deduce que $\mathfrak{p} \cap A \subsetneq \mathfrak{p}' \cap A$, lo que no es posible en A ($\dim(A) \leq 1$). □

Definición 3.12. Si $K \mid \mathbb{Q}$ es una extensión finita de cuerpos, diremos que K es un *cuerpo de números*. La clausura íntegra de $\mathbb{Z}$ en K se denomina *anillo de enteros,anillo de números* de K, o simplemente *anillo de enteros algebraicos*. Se denotará por $\mathfrak{O}_K = \overline{\mathbb{Z}}^K$.

Corolario 3.13. *Sea K un cuerpo de números y sea $\mathfrak{O}_K$ su anillo de enteros. Entonces $\mathfrak{O}_K$ es un dominio de Dedekind.*

Demostración. Consecuencia directa del Teorema 3.11, ya que $\mathbb{Z}$ es un dominio de Dedekind. □

Ejemplo 3.14. Los anillos de números son uno de los ejemplos clásicos de dominios íntegramente cerrados (Proposición 2.7) que son de dimensión 1. Los ejemplos arquetípicos de cuerpos de números son los cuerpos cuadráticos $\mathbb{Q}(\sqrt{m})$ y los cuerpos ciclotómicos $\mathbb{Q}(\xi_n)$ donde m es un entero libre de cuadrados, n un entero positivo y ξ_n es una raíz n-ésima primitiva de la unidad. Los anillos de números asociados a esas extensiones son $\mathbb{Z}[\sqrt{m}]$ cuando $m \not\equiv 1(4)$ y $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ cuando $m \equiv 1(4)$ para los cuerpos cuadráticos y $\mathbb{Z}[\xi_n]$ para las extensiones ciclotómicas (véase [12, Theorem 3.2 and 3.5]). Por otra parte, el grupo de Picard de un anillo de números es siempre un grupo abeliano finito (véase [12, Theorem 9.7]). Un ejemplo de un cálculo concreto de un grupo de Picard no trivial de un anillo de números se puede consultar en [9, Example 13.28].

3.3. Dominios de Dedekind: curvas regulares

En geometría algebraica aparecen frecuentemente ejemplos de dominios de Dedekind.

Sea K a un cuerpo, que supondremos algebraicamente cerrado. Un polinomio $f \in K[X_1, \ldots, X_n]$ define una función (una función polinómica) $f\colon \mathbf{A}^n(K) \to K$. Dados $X \subset \mathbf{A}^n(K)$, una colección de puntos, y $S \subset K[X_1, \ldots, X_n]$, una colección de polinomios, denotamos:

$$I(X) := \{\, f \in K[X_1, \ldots, X_n] \mid f(\mathbf{x}) = 0,\ \forall \mathbf{x} = (x_1, \ldots, x_n) \in X \,\} \text{ y}$$
$$V(S) := \{\, \mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{A}^n(K) \mid f(\mathbf{x}) = 0,\ \forall f \in S \,\}.$$

Un subconjunto $X \subset \mathbf{A}^n(K)$ es un subconjunto algebraico si existe $S \subset K[X_1, \ldots, X_n]$ tal que $X = V(S)$. Los subconjuntos algebraicos de $\mathbf{A}^n(K)$ conforman la familia de los cerrados de una topología, la topología de Zariski.

Definición 3.15. Sea X un subconjunto algebraico de $\mathbf{A}^n(K)$. Decimos que X es una variedad algebraica de $\mathbf{A}^n(K)$ si es un cerrado irreducible para la topología de Zariski, es decir, no existen X_1, X_2 subconjuntos algebraicos de $\mathbf{A}^n(K)$ distintos a X tales que $X = X_1 \cup X_2$.

Proposición 3.16. *Un subconjunto algebraico $X \subset \mathbf{A}^n(K)$ es una variedad algebraica si, y solo si, $I(X)$ es un ideal primo de $K[X_1, \ldots, X_n]$.*

Demostración. [8, 1.5, Proposition 1] □

Definición 3.17. Dado un conjunto algebraico $X \subset \mathbf{A}^n(K)$, el anillo cociente

$$\Gamma(X) := K[X_1, \ldots, X_n]/I(X)$$

se denomina el anillo de funciones polinómicas definidas sobre X, o anillo de (funciones) coordenadas de X. Si X es una variedad algebraica, $\Gamma(X)$ es un dominio.

Definición 3.18. Sea $X \subset \mathbf{A}^n(K)$ una variedad algebraica. Definimos la dimensión de X como la dimensión de Krull del anillo coordenado $\Gamma(X)$ y se denotará por $\dim(X)$. Diremos que una variedad algebraica $X \subset \mathbf{A}^n(K)$ es una curva algebraica si $\dim(X) = 1$.

Definición 3.19. Sea A un anillo local y noetheriano. Diremos que A es regular si el número mínimo de generadores de su ideal maximal coindide con su dimensión de Krull.

Definición 3.20. Sea A un anillo noetheriano. Diremos que A es un anillo regular si $A_{\mathfrak{p}}$ es un anillo local regular para todo ideal primo $\mathfrak{p}$ de A.

Definición 3.21. Sea $X \subset \mathbf{A}^n(K)$ una variedad algebraica. Diremos que X es una variedad algebraica regular si $\Gamma(X)$ es un anillo regular.

Proposición 3.22. *Una variedad algebraica $X \subset \mathbf{A}^n(K)$ es una curva algebraica regular si, y solo si, su anillo de coordenadas $\Gamma(X)$ es un dominio de Dedekind.*

Demostración. Como $\Gamma(X)$ es regular, entonces para todo ideal maximal $\mathfrak{m} \subset \Gamma(X)$, el anillo $\Gamma(X)_{\mathfrak{m}}$ es un dominio local regular tal que $\dim(\Gamma(X)_{\mathfrak{m}}) = 1$. Es decir, $\Gamma(X)_{\mathfrak{m}}$ es un anillo noetheriano local cuyo maximal es principal, o en otras palabras (por el Teorema 2.27) el anillo $\Gamma(X)_{\mathfrak{m}}$ es un AVD. Equivalentemente (por el Teorema 3.7) $\Gamma(X)$ es un dominio de Dedekind. □

Ejemplo 3.23. Las rectas y las cónicas no degeneradas son curvas planas regulares. Mencionaremos el caso de las cúbicas regulares de género uno como otra familia de ejemplos interesantes en Geometría Algebraica, Teoría de Números y Criptografía. Fijado

$\lambda \in \mathbb{C}\setminus\{0,1\}$, consideremos la curva plana $X = V(F)$, donde $F = Y^2 + X(X-1)(X-\lambda) \in \mathbb{C}[X,Y]$. La curva X es lisa en el sentido de [8, 3.1], es decir, las parciales ∂F_X y ∂F_Y no se anulan simultánemente en ningún punto de X. De este modo, usando [8, Section 3.2, Theorem 1], deducimos que la curva X es regular en el sentido de la Definición 3.21. Denotemos $A = \Gamma(X)$ el anillo de coordenadas de la cúbica X. El anillo A es un DD empleando el Teorema 3.22. En este caso, el grupo $\texttt{Pic}(A)$ tiene infinitos elementos: existe una correspondencia biyectiva entre los puntos de X y los elementos de $\texttt{Pic}(A)$ distintos del neutro. Podemos consultar [9, Example 13.29] para la prueba completa de este hecho. En esta demostración, podemos ver que añadiendo a la curva X un punto en el infinito, el conjunto $X \cup \{\infty\}$ adquiere estructura de grupo abeliano inducida por la de $\texttt{Pic}(A)$.

Capítulo 4

Factorización en primos

Un dominio A tiene la propiedad de «*factorización única en ideales primos*», si para cada ideal no trivial $0 \subsetneq I \subsetneq A$ existe una única colección $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ de primos no nulos de A distintos dos a dos y una única colección de enteros positivos $a_1, \ldots, a_n$ tales que

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i}.$$

Dedicamos este capítulo a la caracterización de los dominios de Dedekind como aquellos dominios que poseen la propiedad de «*factorización única en ideales primos*».

4.1. Dominios de Dedekind: factorización única de ideales

En esta sección, vamos a comprobar que si A es un DD, entonces A verifica la propiedad de «factorización única en ideales primos».

Proposición 4.1. *Si es A es un dominio de Dedekind y $x \in A$ es un elemento no nulo, el conjunto de ideales primos de A que contienen a x es finito.*

Demostración. Sean $\mathtt{S}, \mathtt{T} \subset \mathtt{Frac}(A)$ los subconjuntos

$$\mathtt{S} := \{\ \mathfrak{f} \in \mathtt{Frac}(A) \mid xA \subset \mathfrak{f} \subset A\ \}$$
$$\mathtt{T} := \{\ \mathfrak{f} \in \mathtt{Frac}(A) \mid A \subset \mathfrak{f} \subset \frac{1}{x}A\ \},$$

Consideremos en $\mathtt{S}$ y $\mathtt{T}$ la relación de orden dada por la inclusión. La aplicación $\phi_1 \colon \mathtt{S} \to \mathtt{T}$, que asigna al ideal $\mathfrak{f} \in \mathtt{S}$ el ideal fraccionario $\phi_1(\mathfrak{f}) = \mathfrak{f}^{-1}$, es una aplicación biyectiva antítona, es decir, que invierte el orden. Por otro lado, la aplicación $\phi_2 \colon \mathtt{T} \to \mathtt{S}$, definida por $\phi_1(\mathfrak{f}) = x\mathfrak{f}$, es una aplicación biyectiva que conserva el orden. Por tanto $\phi := \phi_2 \circ \phi_1 \colon \mathtt{S} \longrightarrow \mathtt{S}$ es una aplicación biyectiva antítona. Entonces ϕ establece una correspondencia biyectiva

entre las cadenas descendentes y las cadenas ascendentes de $\mathtt{S}$. Dado que A es un anillo noetheriano y $\mathtt{S}$ es un conjunto de ideales enteros de A, toda cadena ascendente de $\mathtt{S}$ es estacionaria, equivalentemente toda cadena descendente de $\mathtt{S}$ es estacionaria.

Supongamos ahora que en $\mathtt{S}$ hay una cantidad infinita de ideales primos de A. Entonces existirá una colección numerable $\{\,\mathfrak{p}_i \mid i \in \mathbb{N}\,\}$ de primos de A distintos dos a dos que contienen a x. La cadena $\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supseteq \cdots$ es una cadena descendente de $\mathtt{S}$ y por lo tanto es estacionaria. Sea $n \in \mathbb{N}$ tal que $\cap_{i=i}^{n}\mathfrak{p}_i = \cap_{i=1}^{n+1}\mathfrak{p}_i$. Entonces $\cap_{i=1}^{n}\mathfrak{p}_1 \subset \mathfrak{p}_{n+1}$ y (por [1, Proposition 1.11]) necesariamente se tiene que $0 \subsetneq \mathfrak{p}_i \subsetneq \mathfrak{p}_{n+1}$ para algún $i \in \{1, \ldots, n\}$; lo cual contradice que $\dim(A) \leq 1$. □

Corolario 4.2. *Si A es un dominio de Dedekind e $I \subset A$ es un ideal no nulo, entonces el conjunto de ideales primos de A que contienen a I es finito y todos ellos son maximales.*

Demostración. En este caso $\dim(A) \leq 1$, entonces el resultado es consecuencia inmediata de la Proposición 4.1. □

Sea A un dominio de Dedekind y $K = K_A$ su cuerpo de fracciones. Dado $\mathfrak{p} \subset A$ un primo no nulo, $A_\mathfrak{p}$ es un AVD cuyo cuerpo de fracciones es K. Sea t un PU de $A_\mathfrak{p}$ y sea $\nu_\mathfrak{p}\colon K^\times \to \mathbb{Z}$ la valoración correspondiente. Dado un ideal fraccionario $\mathfrak{f} \in \mathtt{Frac}(A)$, su localización $\mathfrak{f}_\mathfrak{p}$ es un ideal fraccionario de $A_\mathfrak{p}$ y por lo tanto, será de la forma $\mathfrak{f}_\mathfrak{p} = (t^n)$ para un único $n \in \mathbb{Z}$. Definimos entonces $\hat{\nu}_\mathfrak{p}(\mathfrak{f}) := n$. La aplicación $\hat{\nu}_\mathfrak{p}\colon \mathtt{Frac}(A) \to \mathbb{Z}$ es un homomorfismo de grupos: dados $\mathfrak{f}, \mathfrak{g} \in \mathtt{Frac}(A)$, si $\hat{\nu}_\mathfrak{p}(\mathfrak{f}) = n$ y $\hat{\nu}_\mathfrak{p}(\mathfrak{g}) = m$ entonces $(\mathfrak{fg})_\mathfrak{p} = \mathfrak{f}_\mathfrak{p}\mathfrak{g}_\mathfrak{p} = (t^n)(t^m) = (t^{m+n})$ y en consecuencia, $\hat{\nu}_\mathfrak{p}(\mathfrak{fg}) = m + n = \hat{\nu}_\mathfrak{p}(\mathfrak{f}) + \hat{\nu}_\mathfrak{p}(\mathfrak{g})$.

Considerando en $\mathtt{Frac}(A)$ el orden dado por la inclusión y en $\mathbb{Z}$ el orden habitual, la aplicación $\hat{\nu}_\mathfrak{p}\colon \mathtt{Frac}(A) \to \mathbb{Z}$ es antítona. Dados $\mathfrak{f}, \mathfrak{g} \in \mathtt{Frac}(A)$, si $\hat{\nu}_\mathfrak{p}(\mathfrak{f}) = n$, $\hat{\nu}_\mathfrak{p}(\mathfrak{g}) = m$ y $\mathfrak{f} \subset \mathfrak{g}$ entonces $\mathfrak{f}_\mathfrak{p} = (t^n) \subset \mathfrak{g}_\mathfrak{p} = (t^m)$ y por lo tanto $n \geq m$, es decir, $\hat{\nu}_\mathfrak{p}(\mathfrak{f}) \geq \hat{\nu}_\mathfrak{p}(\mathfrak{g})$.

La aplicación $\hat{\nu}_\mathfrak{p}\colon \mathtt{Frac}(A) \to \mathbb{Z}$ es una extensión de la valoración de $A_\mathfrak{p}$ ya que, para cada $x \in K^\times$, se tiene que $(xA)_\mathfrak{p} = xA_\mathfrak{p} = (t^{\nu_\mathfrak{p}(x)})$ y de este modo $\hat{\nu}_\mathfrak{p}(xA) = \nu_\mathfrak{p}(x)$. Por esa razón, de aquí en adelante utilizaremos por comodidad la notación $\nu_\mathfrak{p}(\mathfrak{f})$ en lugar de $\hat{\nu}_\mathfrak{p}(\mathfrak{f})$.

Lema 4.3. *Sea A un dominio de Dedekind, $I \subset A$ un ideal y $\mathfrak{p} \subset A$ un ideal primo no nulo. Entonces $\nu_\mathfrak{p}(I) = 0$ si, y solo si, $\mathfrak{p}$ no contiene a I. En particular, si $\mathfrak{q}$ es un ideal primo no nulo de A distinto de $\mathfrak{p}$, se tiene que $\nu_\mathfrak{q}(\mathfrak{p}) = \nu_\mathfrak{p}(\mathfrak{q}) = 0$.*

Demostración. Si $I \subset \mathfrak{p}$, tendremos que $\nu_\mathfrak{p}(I) \geq \nu_\mathfrak{p}(\mathfrak{p}) = 1$. Supongamos que $I \not\subset \mathfrak{p}$. entonces existirá un elemento $x \in I - \mathfrak{p}$ que será una unidad en $A_\mathfrak{p}$. De este modo, dado que $xA \subset I \subset A$, tendremos que $0 = \nu_\mathfrak{p}(x) = \nu_\mathfrak{p}(xA) \geq \nu_\mathfrak{p}(I) \geq \nu_\mathfrak{p}(A) = \nu_\mathfrak{p}(1) = 0$. Por otra parte, dado que los ideales $\mathfrak{p}$ y $\mathfrak{q}$ son ideales primos no nulos, ambos son maximales ($\dim(A) = 1$). De este modo, ninguno está contenido en el otro y así $\nu_\mathfrak{q}(\mathfrak{p}) = \nu_\mathfrak{p}(\mathfrak{q}) = 0$. □

Corolario 4.4. *Sea A un dominio de Dedekind con cuerpo de fracciones K_A. Si $\mathfrak{f}$ es un ideal fraccionario de A entonces $\nu_{\mathfrak{p}}(\mathfrak{f}) = 0$ para todo ideal primo no nulo $\mathfrak{p}$ de A salvo a lo sumo para un número finito de ellos. En particular, si $x \in K_A^{\times}$, $\nu_{\mathfrak{p}}(x) = 0$ para casi todo ideal primo no nulo $\mathfrak{p}$ de A.*

Demostración. Si $\mathfrak{f} \subset A$ es un ideal entero de A, aplicando el Corolario 4.2 y el Lema 4.3 se deduce el resultado. Si $\mathfrak{f}$ es un ideal tendremos que $\mathfrak{f} = \frac{1}{a}I$, siendo $a \in A$ un elemento no nulo e $I \subset A$ un ideal entero de A. Tendremos entonces que, para todo ideal primo no nulo $\mathfrak{p}$ de A, $\nu_{\mathfrak{p}}(\mathfrak{f}) = \nu_{\mathfrak{p}}(\frac{1}{a}I) = \nu_{\mathfrak{p}}(I) - \nu_{\mathfrak{p}}(a)$ que será cero salvo para un número finito de primos no nulos. □

Teorema 4.5. *Sea A un dominio de Dedekind. Entonces $\texttt{Frac}(A)$ es isomorfo al grupo abeliano libre $\bigoplus_{\mathfrak{p}\neq 0}\mathbb{Z}$, cuya base canónica está indicada por el conjunto de los ideales primos no nulos de A. El isomorfismo asigna a cada ideal fraccionario $\mathfrak{f} \in \texttt{Frac}(A)$ el elemento de $\bigoplus_{\mathfrak{p}\neq 0}\mathbb{Z}$ definido por $(\,\nu_{\mathfrak{p}}(\mathfrak{f})\,)_{\mathfrak{p}\neq 0}$.*

Demostración. Por el Corolario 4.4, la aplicación $\Psi\colon \texttt{Frac}(A) \longrightarrow \bigoplus_{\mathfrak{p}\neq 0}\mathbb{Z}$ que asigna a un ideal fraccionario $\mathfrak{f}$ de A el elemento $\Psi(\mathfrak{f}) = (\,\nu_{\mathfrak{p}}(\mathfrak{f})\,)_{\mathfrak{p}\neq 0}$ es una aplicación bien definida y es trivialmente un homomorfismo de grupos. Veamos que es biyectiva. Sean $\mathfrak{f}, \mathfrak{g} \in \texttt{Frac}(A)$ de modo que $(\,\nu_{\mathfrak{p}}(\mathfrak{f})\,)_{\mathfrak{p}\neq 0} = (\,\nu_{\mathfrak{p}}(\mathfrak{g})\,)_{\mathfrak{p}\neq 0}$, es decir, tales que $\mathfrak{f}_{\mathfrak{p}} = \mathfrak{g}_{\mathfrak{p}}$ para todo ideal primo no nulo $\mathfrak{p} \subset A$. Empleando el Lema 1.19 se deduce que $\mathfrak{f} = \cap_{\mathfrak{p}\neq 0}\mathfrak{f}_{\mathfrak{p}} = \cap_{\mathfrak{p}\neq 0}\mathfrak{g}_{\mathfrak{p}} = \mathfrak{g}$. Para ver que la aplicación es sobreyectiva, observemos que para cualquier vector $v = (n_{\mathfrak{p}})_{\mathfrak{p}\neq 0}$ se tiene que $\mathfrak{f}_v = \prod_{\mathfrak{p}\neq 0}\mathfrak{p}^{n_{\mathfrak{p}}} \in \texttt{Frac}(A)$ es un ideal fraccionario tal que

$$\nu_{\mathfrak{q}}(\,\mathfrak{f}_v\,) = \sum_{\mathfrak{p}\neq 0} n_{\mathfrak{p}}\nu_{\mathfrak{q}}(\mathfrak{p}) = n_{\mathfrak{q}}.$$

De este modo, el producto $\mathfrak{f}_v = \prod_{\mathfrak{p}\neq 0}\mathfrak{p}^{n_{\mathfrak{p}}}$ es la preimagen de $v = (n_{\mathfrak{p}})_{\mathfrak{p}\neq 0}$. □

Observación 4.6. Si A es un AVD, el isomorfismo establecido en el Teorema 4.5 no es más que la valoración discreta $\nu_{\mathfrak{p}}\colon \texttt{Frac}(A) \to \mathbb{Z}$, donde $\mathfrak{p}$ es el único ideal maximal de A.

Corolario 4.7. *Si A es un* DD*, todo ideal entero no nulo $I \subsetneq A$ posee una única factorización como producto finito de ideales primos no nulos de A.*

4.2. Factorización única de ideales implica Dedekind.

La propiedad establecida en el Corolario 4.7 caracteriza aquellos dominios que son DD:

Teorema 4.8 (Matusita)**.** *Si A es un dominio con la propiedad de que todo ideal entero no nulo $I \subsetneq A$ se puede escribir como un producto finito de ideales primos no nulos, entonces A es un dominio de Dedekind.*

Demostración. Como consecuencia del Teorema 3.4, es suficiente demostrar que todo ideal primo no nulo de A es invertible. Dividiremos la demostración en dos pasos:

Paso 1: Veamos que si $\mathfrak{p}$ es un ideal primo no nulo de A que es invertible entonces $\mathfrak{p}$ es necesariamente un ideal maximal de A.

Supongamos que $\mathfrak{p}$ no es maximal. Existirá un elemento $a \in A \setminus \mathfrak{p}$ tal que $aA + \mathfrak{p} \subsetneq A$. Por hipótesis, los ideales $I_1 := aA + \mathfrak{p}$ e $I_2 := a^2A + \mathfrak{p}$, admiten descomposición en producto de ideales primos no nulos de A, escribiremos estas descomposiciones de la forma

$$I_1 := \mathfrak{p}_1 \cdots \mathfrak{p}_s, \qquad I_2 := \mathfrak{q}_1 \cdots \mathfrak{q}_t,$$

permitiendo repeticiones entre los ideales $\mathfrak{p}_i$ y entre los ideales $\mathfrak{q}_j$. Por construcción $\mathfrak{p} \subset I_1 \cap I_2$, por tanto $\mathfrak{p}$ está contenido en cada uno de los ideales $\mathfrak{p}_i$ y $\mathfrak{q}_j$, entonces sus imágenes $\bar{\mathfrak{p}}_i$, $\bar{\mathfrak{q}}_j$ en el dominio $\bar{A} := A/\mathfrak{p}$ son ideales primos. Además, los elementos $\bar{a}, \bar{a}^2 \in \bar{A}$ son no nulos, entonces $\bar{I}_1 = \bar{a}\bar{A}$ e $\bar{I}_2 = \bar{a}^2\bar{A}$ son distintos de cero y principales; por tanto son ideales invertibles de $\bar{A}$. De las descomposiciones

$$\bar{I}_1 = \bar{a}\bar{A} = \bar{\mathfrak{p}}_1 \cdots \bar{\mathfrak{p}}_s, \qquad \bar{I}_2 = \bar{a}^2\bar{A} = \bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_t$$

se deduce que los ideales primos $\bar{\mathfrak{p}}_i$ y $\bar{\mathfrak{q}}_j$ son invertibles. Como $\bar{I}_1^2 = \bar{I}_2$, se tiene que

$$\bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_t = \bar{\mathfrak{p}}_1^2 \cdots \bar{\mathfrak{p}}_s^2,$$

y como los ideales $\bar{\mathfrak{p}}_i$ y $\bar{\mathfrak{q}}_j$ son invertibles necesariamente salvo el orden la colección $\bar{\mathfrak{q}}_1, \ldots, \bar{\mathfrak{q}}_t$ coincide con la colección $\bar{\mathfrak{p}}_1, \bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_s, \bar{\mathfrak{p}}_s$. Por tanto en A se verifica que

$$(aA + \mathfrak{p})^2 = I_1^2 = \mathfrak{p}_1^2 \cdots \mathfrak{p}_s^2 = \mathfrak{q}_1 \cdots \mathfrak{q}_t = a^2A + \mathfrak{p}.$$

Entonces se tiene que $\mathfrak{p} \subset (aA + \mathfrak{p})^2 = a^2A + a\mathfrak{p} + \mathfrak{p}^2 \subset aA + \mathfrak{p}^2$. Además si $p \in \mathfrak{p}$ y $p = ax + y$ con $x \in A$ e $y \in \mathfrak{p}^2$, se tiene que $ax \in \mathfrak{p}$, y utilizando que $\mathfrak{p}$ es primo y que $a \in A - \mathfrak{p}$ se deduce que $x \in \mathfrak{p}$. Por tanto $\mathfrak{p} \subset a\mathfrak{p} + \mathfrak{p}^2 \subset \mathfrak{p}$, es decir $\mathfrak{p} = a\mathfrak{p} + \mathfrak{p}^2 = \mathfrak{p}(aA + \mathfrak{p})$. Multiplicando por $\mathfrak{p}^{-1}$ esta última igualdad concluiremos que $A = aA + \mathfrak{p}$, lo que es contrario a la hipótesis. De este modo deducimos que $\mathfrak{p}$ es maximal.

Paso 2: Sea $\mathfrak{p}$ un ideal primo no nulo de A y sea $b \in \mathfrak{p}$ un elemento no nulo. Por hipótesis, el ideal entero $bA \subset A$ admite una descomposición en producto un número finito de ideales primos no nulos de A

$$bA = \mathfrak{p}_1 \cdots \mathfrak{p}_m,$$

y como bA es invertible cada uno de los ideales primos $\mathfrak{p}_i$ es invertible. Ahora, usando el **Paso 1**, se deduce que éstos son ideales maximales de A. Como $bA = \mathfrak{p}_1 \cdots \mathfrak{p}_m \subset \mathfrak{p}$ y $\mathfrak{p}$ es primo, se deduce al menos uno de estos primos es tal que $\mathfrak{p}_i \subset \mathfrak{p}$. Como $\mathfrak{p}_i$ es maximal se tiene que $\mathfrak{p} = \mathfrak{p}_i$ y por tanto $\mathfrak{p}$ será invertible. □

El siguiente Teorema recoge la caracterización de los dominios de Dedekind en términos de la existencia y unicidad de la factorización de ideales fraccionarios como producto de ideales primos y maximales:

Teorema 4.9. *Sea A un dominio. Son equivalentes:*

(1) *A es un dominio de Dedekind.*

(2) *Todo ideal entero no nulo de A es producto de ideales maximales.*

(3) *Todo ideal entero no nulo de A es producto de ideales primos.*

Además, en virtud del Teorema 4.5 si se verifica cualquiera de las condiciones, la factorización será única.

Demostración. Consecuencia inmediata del Corolario 4.7 y del Teorema 4.8 teniendo en cuenta que todo ideal primo no nulo de un dominio de Dedekind es maximal. □

A pesar de la propiedad de factorización única en ideales que poseen estos dominios, no todos los DFUs serán dominios de Dedekind. Recíprocamente no todos los dominios de Dedekind serán DFUs, tal como percibió Ernst Kummer. Los ejemplos típicos son los siguientes:

Ejemplo 4.10. (DFU $\not\Rightarrow$ DD)
Sea K un cuerpo. El anillo de polinomios en dos variables $A = K[X, Y]$ es un DFU pero no es un DD ya que $\dim(A) > 1$ (la cadena de ideales primos $0 \subsetneq (X) \subsetneq (X, Y)$ tiene longitud 2).

Ejemplo 4.11. (DD $\not\Rightarrow$ DFU)
Consideremos el cuerpo de números $K := \mathbb{Q}(\sqrt{-5})$ y $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$ su anillo de números correspondiente. En virtud del Corolario 3.13 sabemos que $\mathfrak{O}_K$ es un dominio de Dedekind pero no es DFU. En efecto, veamos que el número 6 se puede factorizar de forma distinta como producto de elementos irreducibles de $\mathfrak{O}_K$. En efecto:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

Veamos ahora que 2, 3, $1 + \sqrt{-5}$ y $1 - \sqrt{-5}$ son elementos irreducibles. Para ello, vamos a emplear la norma de la extensión $K \mid \mathbb{Q}$. Sea $\alpha + \beta\sqrt{-5} \in K$ arbitrario. Tenemos que $N_K(\alpha + \beta\sqrt{-5}) = \alpha^2 + 5\beta^2$ por lo que se puede ver fácilmente que no hay elementos de norma 2. Supongamos que $2 = xy$ con $x, y \in \mathfrak{O}_K$. Empleando propiedades elementales de la norma, podemos ver que $4 = N_K(2) = N_K(x) \cdot N_K(y)$ lo que implica que x o y son unidades (porque no hay elementos de norma 2). De este modo deducimos que 2 es un elemento irreducible. Lo mismo ocurre con con 3, $1 + \sqrt{-5}$ y $1 - \sqrt{-5}$, por lo que la factorización en irreducibles no es única en $\mathfrak{O}_K$.

4.3. DIP si, y solo si, DFU

Veamos que en los dominios de Dedekind, «ser DIP» y «ser DFU» son propiedades equivalentes.

Lema 4.12. *Si A es un* DFU*, todo ideal primo no nulo minimal de A es principal.*

Demostración. Sea $\mathfrak{p}$ un ideal primo minimal no nulo. Sea $0 \neq a \in \mathfrak{p}$ y consideremos su factorización en elementos primos $a = up_1 \dots p_r$, donde $r \geq 1$, $p_1, \dots, p_r$ son primos y $u \in A^\times$. Como $\mathfrak{p}$ es primo, al menos uno de sus factores primos p_i de a es tal que $p_i \in \mathfrak{p}$. Entonces tendremos que $0 \subsetneq (p_i) \subset \mathfrak{p}$. Como $\mathfrak{p}$ es minimal deducimos que $\mathfrak{p} = (p_i)$. □

Proposición 4.13. *Un anillo A es un* DIP *si, y solo si, es un* DFU *y todos los ideales primos no nulos de A son maximales.*

Demostración. Si A es un DIP, en particular será un DFU y un DD. De este modo empleando que $\dim(A) \leq 1$, deducimos que todos los ideales primos no nulos de A son maximales. Para el recíproco, empleando el Lema 4.12 tendremos que todo ideal primo minimal no nulo de A es principal y por lo tanto, invertible. Empleando el Teorema 3.7 se deduce que A es un DD. Por el Teorema 4.9, todo ideal se podrá escribir como producto de ideales primos (principales) y de este modo A será un DIP. □

Corolario 4.14. *Sea A un* DD*. Entonces A es un* DFU *si y solo si A es un* DIP*.*

Demostración. Inmediato de la Proposición 4.13. □

4.4. Aritmética de ideales en un dominio de Dedekind.

El isomorfismo esplicitado en el Teorema 4.5 nos permite trabajar con los ideales fraccionarios de un DD de modo análogo a como trabajamos con los números enteros.

Definición 4.15. Dado un dominio A e ideales fraccionarios $\mathfrak{f}, \mathfrak{g} \in \texttt{Frac}(A)$, diremos que $\mathfrak{f}$ *divide a* $\mathfrak{g}$, y se denotará $\mathfrak{f} \mid \mathfrak{g}$, si existe $I \subset A$ un ideal entero tal que $\mathfrak{f}I = \mathfrak{g}$.

Trivialmente si $\mathfrak{f} \mid \mathfrak{g}$, entonces $\mathfrak{g} \subset \mathfrak{f}$. Esta afirmación se resume mediante el eslogan «si divide, contiene». No obstante, el recíproco «si contiene, divide» no siempre es cierto:

Ejemplo 4.16. Consideremos el dominio $\mathbb{Z}[X]$ y los ideales $(2) \subsetneq (2, X)$. Supongamos que $(2, X) \mid (2)$, es decir, existe $I \subseteq \mathbb{Z}[X]$ un ideal entero tal que $(2) = (2, X)I$. En particular, para cada $f \in I$, el producto $Xf \in (2)$. De este modo, todos los coeficientes de f serán enteros pares y así, $f \in (2)$. De esta manera, deducimos que $I \subseteq (2)$ y dado que el otro

contenido es trivial, obtenemos la igualdad. No obstante, esto es contradictorio ya que si multiplicásemos la igualdad $(2) = (2, X)(2)$ por $(2)^{-1}$ deduciríamos que $\mathbb{Z}[X] = (2, X)$, lo que es falso $(1 \notin (2, X))$.

Aunque el eslogan «si contiene, divide» no se verifique para cualquier dominio A, sí se verifica si A es un DD.

Proposición 4.17 (Contener es dividir)**.** *Si A es un dominio de Dedekind y $\mathfrak{f}$ y $\mathfrak{g}$ son ideales fraccionarios de A, entonces:*

$$\mathfrak{f} \mid \mathfrak{g} \iff \mathfrak{g} \subset \mathfrak{f}$$

Demostración. Únicamente hay que justificar la implicación «$\Leftarrow$». Supongamos que $\mathfrak{g} \subset \mathfrak{f}$. Entonces $\mathfrak{f}^{-1}\mathfrak{g} \subset \mathfrak{f}^{-1}\mathfrak{f} = A$. Entonces $I = \mathfrak{f}^{-1}\mathfrak{g} \subset A$ es un ideal tal que $\mathfrak{f}I = \mathfrak{g}$. (Se comprueba fácilmente que $I = (\mathfrak{g} :_{K_A} \mathfrak{f})$.) □

Los dominios para los que se verifica la equivalencia de la Proposición 4.17 se denominan CDR por su denominación en inglés *containment-division ring*. Esta propiedad caracteriza a los dominios noetherianos que son dominios de Dedekind:

Teorema 4.18. *Para un dominio A, son equivalentes:*

(1) *A es un* DD.

(2) *A es un* CDR *noetheriano.*

Demostración. En la Proposición 4.17 se probó (1) $\Rightarrow$ (2). Supongamos que A es un CDR noetheriano; por el Teorema 4.8, A es un DD si cualquier ideal no nulo A se puede escribir como producto de ideales primos no nulos. Denotemos por $\mathcal{P}$ el conjunto de ideales no nulos de A tales que no se puede obtener como producto de ideales primos no nulos de A. Supongamos que $\mathcal{P}$ es no vacío. Sea $I \in \mathcal{P}$. En particular $I \subsetneq A$; entonces existirá un ideal primo $\mathfrak{p}_1 \subset A$ de modo que $I \subset \mathfrak{p}_1$. Como A es un CDR, existirá un ideal $I_1 \subset A$ tal que $I = I_1\mathfrak{p}_1$. Por el Lema de Nakayama ([1, Proposition 2.6]) $I \subsetneq I_1$. Además $I_1 \in \mathcal{P}$ no es primo e $I_1 \subsetneq A$. Argumentando análogamente para $I_1 \in \mathcal{P}$ se obtiene $I_1 = I_2\mathfrak{p}_2$ con $\mathfrak{p}_2$ un ideal primo no nulo de A e $I_2 \in \mathcal{P}$ tal que $I_1 \subsetneq I_2$. De forma inductiva se construye una cadena ascendente de ideales $I \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$, lo cual contradice que A sea noetheriano. Por tanto necesariamente $\mathcal{P} = \varnothing$. □

Observación 4.19. En un dominio de Dedekind, la relación «divide a» entre ideales fraccionarios es la relación «contiene a». Entonces $\texttt{Frac}(A)$ con la relación «divide a» es un retículo. Introducimos la siguiente notación para dos ideales fraccionarios $\mathfrak{f}$ y $\mathfrak{g}$:

- $\mathrm{mcd}(\mathfrak{f},\mathfrak{g}) := \mathfrak{f}+\mathfrak{g}$ es el menor ideal fraccionario de A que contiene a $\mathfrak{f}\cup\mathfrak{g}$.
- $\mathrm{mcm}(\mathfrak{f},\mathfrak{g}) := \mathfrak{f}\cap\mathfrak{g}$ es el mayor ideal fraccionario de A contenido en $\mathfrak{f}\cup\mathfrak{g}$.

La propiedad asociativa de la suma y la intersección de A-módulos nos permite extender esta notación a una familia finita de ideales fraccionarios $\mathfrak{f}_1,\ldots,\mathfrak{f}_n$:

- $\mathrm{mcd}(\mathfrak{f}_1,\ldots,\mathfrak{f}_n) := \mathfrak{f}_1+\cdots+\mathfrak{f}_n$.
- $\mathrm{mcm}(\mathfrak{f}_1,\ldots,\mathfrak{f}_n) := \mathfrak{f}_1\cap\cdots\cap\mathfrak{f}_n$.

Obsérvese que si $\mathfrak{f},\,\mathfrak{g}\in\mathtt{Frac}(A)$, entonces

$$\mathfrak{f}\,|\,\mathfrak{g} \quad\Longleftrightarrow\quad \nu_{\mathfrak{p}}(\mathfrak{f})\le\nu_{\mathfrak{p}}(\mathfrak{g}),\ \forall\mathfrak{p}\in\mathrm{Spec}(A),\ \mathfrak{p}\neq 0.$$

es decir, la aplicación biyectiva

$$\Psi\colon \mathtt{Frac}(A)\longrightarrow\bigoplus_{\mathfrak{p}\neq 0}\mathbb{Z}$$

definida en el Teorema 4.5 es un isomorfismo de grupos ordenados, considerando en $\bigoplus_{\mathfrak{p}\neq0}\mathbb{Z}$ el orden inducido por el de $\mathbb{Z}$ componente a componente.

Proposición 4.20. *Sea A un dominio de Dedekind y sean $\mathfrak{f}=\prod_{\mathfrak{p}\neq0}\mathfrak{p}^{a_{\mathfrak{p}}}$ y $\mathfrak{g}=\prod_{\mathfrak{p}\neq0}\mathfrak{p}^{b_{\mathfrak{p}}}$ ideales fraccionarios de A junto con sus respectivas descomposiciones en producto de primos no nulos de A. Entonces se tiene que:*

$$\mathrm{mcd}(\mathfrak{f},\mathfrak{g})=\prod_{\mathfrak{p}\neq0}\mathfrak{p}^{\min\{a_{\mathfrak{p}},b_{\mathfrak{p}}\}}\ ,\qquad\qquad \mathrm{mcm}(\mathfrak{f},\mathfrak{g})=\prod_{\mathfrak{p}\neq0}\mathfrak{p}^{\max\{a_{\mathfrak{p}},b_{\mathfrak{p}}\}};$$

además $\mathfrak{f}\mathfrak{g}=\prod_{\mathfrak{p}\neq0}\mathfrak{p}^{a_{\mathfrak{p}}+b_{\mathfrak{p}}}$ *y* $(\mathfrak{f}:_{K_A}\mathfrak{g})=\prod_{\mathfrak{p}\neq0}\mathfrak{p}^{a_{\mathfrak{p}}-b_{\mathfrak{p}}}$.

Demostración. Probaremos la primera, la tercera y la cuarta afirmaciones.

Sea $\mathfrak{h}$ un ideal fraccionario de A tal que $\mathfrak{f}\cup\mathfrak{g}\subset\mathfrak{h}$. Entonces para cada ideal primo no nulo $\mathfrak{p}$, tendremos que $a_{\mathfrak{p}}=\nu_{\mathfrak{p}}(\mathfrak{f})\le\nu_{\mathfrak{p}}(\mathfrak{h})$ y $b_{\mathfrak{p}}=\nu_{\mathfrak{p}}(\mathfrak{g})\le\nu_{\mathfrak{p}}(\mathfrak{h})$ y así $\min\{a_{\mathfrak{p}},b_{\mathfrak{p}}\}\le\nu_{\mathfrak{p}}(\mathfrak{h})$. Así pues $\prod_{\mathfrak{p}\neq0}\mathfrak{p}^{\min\{a_{\mathfrak{p}},b_{\mathfrak{p}}\}}$ es el menor ideal fraccionario que contiene a $\mathfrak{f}\cup\mathfrak{g}$.

La tercera expresión se deduce de que $\Psi\colon\mathtt{Frac}(A)\to\bigoplus_{\mathfrak{p}\neq0}\mathbb{Z}$ es un isomorfismo de grupos y la cuarta se sigue de este hecho teniendo además en cuenta que $(\mathfrak{f}:_{K_A}\mathfrak{g})=\mathfrak{f}\mathfrak{g}^{-1}$:

$$\Psi((\mathfrak{f}:_{K_A}\mathfrak{g}))=\Psi(\mathfrak{f}\mathfrak{g}^{-1})=\Psi(\mathfrak{f})+\Psi(\mathfrak{g}^{-1})=\Psi(\mathfrak{f})-\Psi(\mathfrak{g}).\qquad\square$$

Observación 4.21. Del resultado anterior se deduce que para todo par de ideales $\mathfrak{f}$ y $\mathfrak{g}$ de un dominio de Dedekind se verifica que $\mathfrak{f}\mathfrak{g}=(\mathfrak{f}\mathfrak{g})(\mathfrak{f}+\mathfrak{g})$ y que $\mathfrak{g}(\mathfrak{f}:_{K_A}\mathfrak{g})=\mathfrak{f}$, tal como sugiere la intuición.

Definición 4.22. Sea A un dominio de Dedekind y $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ una familia de ideales enteros de A. Diremos que $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ son coprimos si $\text{mcd}(\mathfrak{f}_1, \ldots, \mathfrak{f}_n) = A$. Obsérvese que si una familia finita de ideales fraccionarios es tal que sus elementos son coprimos, entonces la familia está formada por ideales enteros.

Lema 4.23. *Sea $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ una familia de ideales enteros de un dominio de Dedekind A. Las siguientes afirmaciones son equivalentes*

(1) *Los ideales $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ son coprimos.*

(2) *Para cada ideal primo $\mathfrak{p}$ no nulo de A, $\text{mín}\{\nu_{\mathfrak{p}}(\mathfrak{f}_i) \,|\, 1 \leq i \leq n\} = 0$.*

(3) *Ningún ideal primo no nulo de A divide simultáneamente a todos los $\mathfrak{f}_i$.*

Demostración.

(1) $\Rightarrow$ (2) Dado un I ideal entero de A, se tiene que, para todo $\mathfrak{p}$ ideal primo no nulo, $\nu_{\mathfrak{p}}(I) \geq \nu_{\mathfrak{p}}(A) = \nu_{\mathfrak{p}}(1) = 0$. Supongamos que existe $\mathfrak{p}$ un ideal primo no nulo tal que $\text{mín}\{\nu_{\mathfrak{p}}(\mathfrak{f}_i) \mid 1 \leq i \leq n\} > 0$. De este modo, para todo $i \in \{1, \ldots, n\}$ se tiene que $\nu_{\mathfrak{p}}(\mathfrak{f}_i) > 0$ y usando el Lema 4.3 se obtiene que $\mathfrak{f}_i \subset \mathfrak{p}$. Así pues $\text{mcd}\{\mathfrak{f}_1, \ldots, \mathfrak{f}_n\} \subset \mathfrak{p} \subsetneq A$.

(2) $\Rightarrow$ (3) Supongamos que $\nu_{\mathfrak{p}}(\mathfrak{f}_i) = 0$ para todo $i \in \{1, \ldots, n\}$ y para todo $\mathfrak{p}$ ideal primo no nulo. Usando el Lema 4.3 y el hecho de que los ideales son enteros, la afirmación anterior equivale a decir que $\mathfrak{f}_i \not\subset \mathfrak{p}$ para todo $i \in \{1, \ldots, n\}$ y para todo $\mathfrak{p}$ ideal primo no nulo. Usando la Proposición 4.17 se deduce el resultado.

(3) $\Rightarrow$ (1) Es inmediato. $\square$

Capítulo 5

Ideales y otras caracterizaciones

Sabemos por el Corolario 4.14 que las propiedades «ser DIP» y «ser DFU» para un dominio de Dedekind son equivalentes. No obstante, existen dominios de Dedekind que no verifican ninguna de estas dos propiedades, tal como nos muestran los ejemplos 4.10 y 4.11. Una propiedad interesante que caracteriza completamente a estos dominios es que, dado un ideal no nulo I arbitrario, existen dos elementos distintos de cero que generan I; pudiendo elegir uno de ellos de forma arbitraria entre los elementos de dicho ideal.

Proposición 5.1. *Sea A un dominio de Dedekind. Si I e I' son ideales enteros y no nulos de A, existe $J \subset A$ un ideal coprimo con I' de modo que IJ es un ideal principal de A.*

Demostración. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos de A que dividen a I' (que serán un número finito por el Corolario 4.7. Para cada $i \in \{1, \ldots, n\}$ tomamos

$$a_i \in (\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_n)I - \mathfrak{p}_i I$$

Esto es claramente posible dado que los dos productos son divisibles por potencias distintas de $\mathfrak{p}_i$. Además se tiene que los a_i son forzosamente elementos no nulos. Definamos ahora $a := \prod_{i=1}^{n} a_i$. Tendremos entonces que $\nu_{\mathfrak{p}_i}(a) = \nu_{\mathfrak{p}_i}(a_i) = \nu_{\mathfrak{p}_i}(I)$. De este modo, $(a) \subset I$ y dado que A es un dominio de Dedekind, I divide a (a). Por lo tanto, existirá $J \subset A$ un ideal tal que $(a) = IJ$. Además, para cada $i \in \{1, \ldots, n\}$ tendremos que $\nu_{\mathfrak{p}_i}(J) = \nu_{\mathfrak{p}_i}(a) - \nu_{\mathfrak{p}_i}(I) = 0$ y así, J es coprimo con I' (Lema 4.23). □

Corolario 5.2. *Un dominio de Dedekind semilocal (es decir, que posea un número finito de ideales maximales) es un* DIP.

Demostración. Consideremos I' el producto de todos los ideales maximales de A. Aplicando la Proposición 5.1 a cualquier ideal I de A deducimos que necesariamente $J = A$ y de este modo $IJ = IA = I$ es un ideal principal de A. □

Corolario 5.3 (Aproximación finita)**.** *Sea $\mathfrak{f}$ un ideal fraccionario de un dominio de Dedekind A y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ un conjunto finito de ideales primos no nulos de A. Entonces existe $x \in \mathfrak{f}$ de manera que $\nu_{\mathfrak{p}_i}(x) = \nu_{\mathfrak{p}_i}(\mathfrak{f})$, para todo $i \in \{1, \ldots, n\}$.*

Demostración. En virtud de la Observación1.7, el ideal fraccionario $\mathfrak{f}$ es de la forma $\mathfrak{f} = \frac{1}{s}I$ con $s \in A$ no nulo e I un ideal entero no nulo de A. Un argumento del tipo utilizado en la prueba de la Proposición 5.1 permite establecer la existencia de un elemento $a \in A$ de manera que $\nu_{\mathfrak{p}_i}(a) = \nu_{\mathfrak{p}_i}(I)$, con $i \in \{1, \ldots, n\}$. El elemento $x := \frac{a}{s} \in \mathfrak{f}$ es tal que, para todo $i \in \{1, \ldots, n\}$:

$$\nu_{\mathfrak{p}_i}(x) = \nu_{\mathfrak{p}_i}(a) - \nu_{\mathfrak{p}_i}(s) = \nu_{\mathfrak{p}_i}(I) - \nu_{\mathfrak{p}_i}(s) = \nu_{\mathfrak{p}_i}(\mathfrak{f}). \qquad \square$$

Proposición 5.4. *Si $I \subset A$ es un ideal entero no nulo del dominio de Dedekind A, entonces A/I es un anillo artiniano cuyos ideales son principales.*

Demostración. Sea $\pi\colon A \to A/I$ el homomorfismo canónico del paso al cociente. Utilizaremos la notación $\pi(x) = \bar{x}$ y para los ideales de A/I, $\bar{J} = J/I \subset A/I$ siendo $J \subset A$ un ideal de A que contiene a I. El anillo A es noetheriano y por lo tanto A/I también lo será. Por el Corolario 4.2 existe un número finito de primos no nulos de A que dividen a I; si $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ son los primos no nulos de A que dividen a I, entonces $\mathrm{Spec}(A/I) = \mathrm{Spm}(A/I) = \{\bar{\mathfrak{p}_1}, \ldots, \bar{\mathfrak{p}_s}\}$ y $\dim(A/I) = 0$. Por otra parte, sea $\bar{J} = J/I \subset A/I$ un ideal de A/I. En virtud del Corolario 5.3, existirá un elemento $a \in J$ de modo que $\nu_{\mathfrak{p}_i}(a) = \nu_{\mathfrak{p}_i}(J)$ para todo $i \in \{1, \ldots, s\}$. Obsévese que si $\mathfrak{p} \subset A$ es un ideal primo no nulo se tiene que:

$$aA \subset aA + I \subset J \implies \nu_{\mathfrak{p}}(J) \leq \nu_{\mathfrak{p}}(aA + I) \leq \nu_{\mathfrak{p}}(a)$$
$$I \subset aA + I \subset J \implies \nu_{\mathfrak{p}}(J) \leq \nu_{\mathfrak{p}}(aA + I) \leq \nu_{\mathfrak{p}}(I).$$

Por tanto, para cualquier $0 \neq \mathfrak{p} \in \mathrm{Spec}(A)$:

$$\nu_{\mathfrak{p}}(aA + I) = \begin{cases} \nu_{\mathfrak{p}}(J) & \text{si } \mathfrak{p} \mid I \\ 0 = \nu_{\mathfrak{p}}(J) & \text{si } \mathfrak{p} \nmid I \end{cases}$$

Así se deduce que $(a) + I = J$, y de este modo, $\bar{J} = (\bar{a})$ es un ideal principal de A/I. $\square$

Proposición 5.5. *Sea $I \subset A$ un ideal de un dominio de Dedekind A. Dado un elemento no nulo $a \in I$, existe un elemento $b \in I$ de modo que $I = (a, b)$.*

Demostración. Como $aA \subset I$, I divide a aA y en virtud de la Proposición 4.17 existirá un ideal $I' \subset A$ de modo que $II' = aA$. Usando la Proposición 5.1, existirá un ideal J coprimo con I' de modo que IJ es principal; pongamos $IJ = bA$ para cierto b que necesariamente debe estar en I. De este modo tendremos que $\mathrm{mcd}(aA, bA) = \mathrm{mcd}(II', IJ) = I$, dado que $\mathrm{mcd}(I', J) = A$. De este modo se sigue que $aA + bA = I$ por la Observación 4.19. $\square$

Un resultado muy curioso sobre los dominios de Dedekind es que pueden ser caracterizados de formas muy variadas. Las propiedades dadas en las Proposiciones 5.4 y 5.5 también caracterizan completamente a estos dominios.

Teorema 5.6 (Asano-Jensen)**.** *Sea A un dominio. Son equivalentes:*

(1) *A es un dominio de Dedekind.*

(2) *Para todo ideal no nulo I de A y cualquier elemento $a \in I$ distinto de cero existe $b \in I$ de modo que $I = (a, b)$.*

Demostración. La Proposición 5.5 demuestra (1) $\Rightarrow$ (2). Demostremos (2) $\Rightarrow$ (1). Un anillo que verifique (2) es noetheriano y por tanto, en virtud de los Teoremas 3.7 y 2.27, es suficiente probar que $A_{\mathfrak{p}}$ es un DIP para cada ideal primo no nulo $\mathfrak{p}$ de A. Un ideal propio del anillo local $A_{\mathfrak{p}}$ será de la forma $J_{\mathfrak{p}} = JA_{\mathfrak{p}}$ siendo $J \subset A$ un ideal no nulo y tal que $J \subset \mathfrak{p}$. Sea $b \in J$ tal que $J = J\mathfrak{p} + bA$ localizando obtendremos que $J_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}} J_{\mathfrak{p}} + bA_{\mathfrak{p}}$. Empleando el Lema de Nakayama tendremos que $J_{\mathfrak{p}} = bA_{\mathfrak{p}}$ y así $A_{\mathfrak{p}}$ es un DIP. □

Corolario 5.7. *Sea A un dominio. Son equivalentes:*

(1) *A es un dominio de Dedekind.*

(2) *Para todo ideal I no nulo de A, A/I es un anillo cuyos ideales son principales.*

Demostración.

(1) $\Rightarrow$ (2) Probado en la Proposición 5.4

(2) $\Rightarrow$ (1) Sea I un ideal no nulo de A y supongamos que no es principal. De este modo tenemos que $(a) \subsetneq I$, para cualquier $a \in I$ no nulo. Consideremos el cociente $I/(a)$ que por hipótesis es principal. Si $\bar{b}$ es un generador de $I/(a)$, trivialmente $(a, b) = I$. Basta aplicar el Teorema 5.6. □

Para concluir, recopilamos todas las caracterizaciones equivalentes que existen para dominios de Dedekind que mencionamos en este trabajo: consideremos A un dominio. Son equivalentes:

(1) A es dominio de Dedekind

(2) Todo ideal primo no nulo de A es invertible.

(3) Todo ideal entero no nulo de A es invertible.

(4) Todo ideal fraccionario de A es invertible.

(5) Todo ideal entero de A es proyectivo de tipo finito.

(6) Todo ideal fraccionario de A es proyectivo de tipo finito.

(7) A es noetheriano y $A_{\mathfrak{m}}$ es un AVD (o un cuerpo) para todo $\mathfrak{m}$ ideal maximal de A.

(8) A es noetheriano, íntegramente cerrado y cada ideal primo no nulo de A es maximal.

(9) A es noetheriano, íntegramente cerrado y $\dim(A) \leq 1$.

(10) Todo ideal entero no nulo de A es producto de ideales maximales.

(11) Todo ideal entero no nulo de A es producto de ideales primos.

(12) A es noetheriano y se verifica la propiedad «si contiene, divide».

(13) Para todo ideal no nulo I de A y cualquier elemento $a \in I$ distinto de cero existe $b \in I$ de modo que $I = (a, b)$.

(14) Para todo ideal I no nulo de A, A/I es un anillo principal.

Capítulo 6

Teorema de Clasificación.

Sea A un anillo y M un A-módulo. Definimos el aniquilador de un elemento $x \in M$ como el ideal $\mathrm{Ann}_A(x) = \{a \in A \mid ax = 0\}$. Se dice que $x \in M$ es un *elemento de torsión* si existe $a \in A \setminus \{0\}$ de modo que $ax = 0$, es decir, si $\mathrm{Ann}_A(x) \neq 0$. El A-submódulo de M definido por

$$\mathrm{Tor}(M) = \{x \in M \mid x \text{ es un elemento de torsión}\}$$

se denomina *torsión de* M, y el ideal

$$\mathrm{Ann}_A(M) = \bigcap_{x \in M} \mathrm{Ann}_A(x),$$

el *aniquilador del* A*-módulo* M. Se dice que M es un A-módulo de torsión si $M = \mathrm{Tor}(M)$ y respectivamente libre de torsión si $\mathrm{Tor}(M) = 0$.

Observación 6.1. Mediante una simple comprobación, es fácil observar que dado un A-módulo M, el cociente $M/\mathrm{Tor}(M)$ es libre de torsión.

En este último capítulo, probaremos el Teorema de Clasificación de los módulos finitamente generados sobre un dominio de Dedekind. Para empezar, comenzaremos estudiando la estructura de los módulos finitamente generados libres de torsión sobre estos dominios. En el Teorema 6.5 se establece la clasificación de esta clase de módulos: dado A un DD y un A-módulo M finitamente generado libre de torsión, éste determina una única clase de isomorfía $[\mathfrak{f}] \in \mathtt{Pic}(A)$ y un único entero $N \geq 0$ tal que $M \cong A^N \oplus \mathfrak{f}$. Consideramos la siguiente sucesión exacta corta:

$$0 \longrightarrow \mathrm{Tor}(M) \longrightarrow M \longrightarrow M/\mathrm{Tor}(M) \longrightarrow 0. \tag{6.1}$$

Dado que $M/\mathrm{Tor}(M)$ es un A-módulo finitamente generado libre de torsión, y en particular proyectivo por la Proposición 6.3, la sucesión (6.1) escinde y así

$$M \cong M/\mathrm{Tor}(M) \oplus \mathrm{Tor}(M).$$

En el Teorema 6.19 se expone la clasificación de los A-módulos de torsión finitamente generados para un DD. Para la clasificación de este tipo de A-módulos utilizaremos un resultado intermedio, la clasificación de los módulos finitamente generados sobre un AVD, recogida en el Teorema 6.11. El resultado final de la memoria es el Teorema 6.21 que establece la clasificación de los módulos finitamente generados sobre un dominio de Dedekind como consecuencia de los resultados anteriores.

6.1. Módulos libres de torsión sobre un dominio de Dedekind.

Lema 6.2. *Sea A un dominio y sea M un A-módulo finitamente generado no nulo. Entonces M es libre de torsión si, y solo si, M es isomorfo a un submódulo de un A-módulo libre de rango finito A^n, que puede ser elegido de modo que $n = \operatorname{rang}(M)$.*

Demostración. Si M es isomorfo a un submódulo de A^m, entonces M es libre de torsión. Recíprocamente, asumamos que M es libre de torsión. Sea K_A el cuerpo de fracciones de A y $S_A \subset A$ el subconjunto multiplicativo de los elementos no nulos de A. Si $\{x_1, x_2, \ldots, x_r\} \subset M$ es un conjunto de generadores de M como A-módulo, entonces $\{\frac{x_1}{1}, \frac{x_2}{1}, \ldots, \frac{x_r}{1}\}$ es un conjunto de generadores de $S_A^{-1}M$ como K_A-espacio vectorial. Entonces si $\operatorname{rang}(M) = \dim_{K_A}(S_A^{-1}M) = n \leq r$, podemos suponer sin perder generalidad que $\{\frac{x_1}{1}, \frac{x_2}{1}, \ldots, \frac{x_r}{1}\}$ es una base de $S_A^{-1}M$ como K_A-espacio vectorial. Para cada $n+1 \leq i \leq r$, $\frac{x_i}{1} = \sum_{j=1}^{r} \frac{a_{ij}}{b_{ij}} \frac{x_j}{1}$, para ciertos $a_{ij}, b_{ij} \in A$ con $b_{ij} \neq 0$. Tomemos $b = \prod_{i,j} b_{ij}$ y $a'_{ij} \in A$ tales que $\frac{a_{ij}}{b_{ij}} = \frac{a'_{ij}}{b}$. Dado que M es libre de torsión, la aplicación $M \to S_A^{-1}M$ es inyectiva y de este modo M será isomorfo a su imagen mediante esta aplicación, que es un submódulo del módulo libre $\bigoplus_{j=1}^{n} \frac{x_j}{b} A$. □

Proposición 6.3. *Sea A un dominio de Dedekind. Se verifican las siguientes afirmaciones:*

(1) *Si M es un A-módulo finitamente generado y libre de torsión de rango $n \geq 1$, existirá una familia $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_n$ de ideales fraccionarios de A de modo que*

$$M \cong \mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n.$$

(2) *Todo A-módulo finitamente generado y libre de torsión es proyectivo.*

Demostración. Sea M un A-módulo finitamente generado y libre de torsión. En virtud del Lema 6.2, M será isomorfo a un submódulo de un A-módulo libre de rango $n = \operatorname{rang}(M)$. Podemos suponer sin perdida de generalidad que $M \subset A^n$. Si $n = 1$, M es isomorfo a un ideal entero de A y por lo tanto habríamos terminado. Supongamos que $n > 1$ y razonemos

por inducción. Consideremos la sucesión exacta corta correspondiente a la proyección en la última componente

$$0 \longrightarrow A^{n-1} \xrightarrow{\iota} A^n \xrightarrow{\pi} A \longrightarrow 0.$$

Esta sucesión induce una sucesión exacta corta

$$0 \longrightarrow M \cap A^{n-1} \xrightarrow{\iota} M \xrightarrow{\pi} \pi(M) \longrightarrow 0. \tag{6.2}$$

Trivialmente $\pi(M) \neq \{0\}$ y $\operatorname{rang}(M \cap A^{n-1}) = n-1$. Como A es un DD, el ideal $\pi(M) = \mathfrak{f}_1 \subset A$ es proyectivo. De este modo la sucesión (6.2) escinde, es decir, $M \cong \mathfrak{f}_1 \oplus (M \cap A^{n-1})$. Por hipótesis de inducción existirán $\mathfrak{f}_2, \ldots, \mathfrak{f}_n$ ideales fraccionarios de A de modo que $(M \cap A^{n-1}) \cong \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n$, por lo que $M \cong \mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n$. □

Lema 6.4. *Sea A un dominio de Dedekind y sean $\mathfrak{f}$, $\mathfrak{g} \subset K_A$ ideales fraccionarios de A. Entonces existe $x, y \in K_A^\times$ de modo que $x\mathfrak{f}$ e $y\mathfrak{g}$ son ideales enteros coprimos.*

Demostración. Después de haber multiplicado si es necesario por elementos no nulos de A, podremos asumir que $\mathfrak{f}$, $\mathfrak{g} \subset A$ son ideales enteros. Sea $c \in A$ tal que $c\mathfrak{f}^{-1} \subset A$ es un ideal entero. La Proposición 5.1 aplicada a los ideales $I = c\mathfrak{f}^{-1}$ e $I' = \mathfrak{g}$ garantiza la existencia de un ideal $J \subset A$ coprimo con $\mathfrak{g}$ tal que $JI = aA$ para cierto elemento no nulo a. De este modo, $J = \frac{a}{c}\mathfrak{f}$ es un ideal entero de A coprimo con $\mathfrak{g}$ (Lema 4.23), tal como queríamos probar. □

Teorema 6.5. *Sea A un dominio de Dedekind. Entonces:*

(1) *Si $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_n$ es una familia de ideales fraccionarios de A, entonces:*

$$\mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n \cong A^{n-1} \oplus \mathfrak{f}_1 \mathfrak{f}_2 \ldots \mathfrak{f}_n.$$

(2) *Si $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_n$ y $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_m$ son dos familias de ideales fraccionarios de A, entonces:*

$$\mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n \cong \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_m \iff m = n \ \text{ y } \ \mathfrak{f}_1 \mathfrak{f}_2 \ldots \mathfrak{f}_n \cong \mathfrak{g}_1 \mathfrak{g}_2 \ldots \mathfrak{g}_m.$$

En particular, si $\mathfrak{f}$ y $\mathfrak{g}$ son ideales fraccionarios de A, entonces:

$$A^m \oplus \mathfrak{f} \cong A^n \oplus \mathfrak{g} \Longleftrightarrow m = n \ y \ \mathfrak{f} \cong \mathfrak{g}.$$

Demostración. (1) Tratemos primero el caso $n = 2$. Veamos que para todo par $\mathfrak{f}$ y $\mathfrak{g}$ de ideales fraccionarios de A existe un isomorfismo $\mathfrak{f} \oplus \mathfrak{g} \cong A \oplus \mathfrak{fg}$. Por el Lema 6.4,existirán elementos no nulos x, $y \in K_A^\times$ tales que $x\mathfrak{f}$, $y\mathfrak{g} \subset A$ son ideales enteros coprimos entre sí.

Entonces podemos suponer que $\mathfrak{f}$ y $\mathfrak{g}$ son ideales enteros coprimos, simplemente sustituyendo cada uno de ellos por los ideales enteros e isomorfos $x\mathfrak{f}$ e $y\mathfrak{g}$. De esta manera tendremos que $\mathfrak{fg} = \mathfrak{f} \cap \mathfrak{g}$ y $\mathfrak{f} + \mathfrak{g} = A$. Empleando que A es proyectivo (libre), la siguiente sucesión exacta escinde

$$0 \longrightarrow \mathfrak{f} \cap \mathfrak{g} \longrightarrow \mathfrak{f} \oplus \mathfrak{g} \longrightarrow \mathfrak{f} + \mathfrak{g} \longrightarrow 0$$

y de este modo $\mathfrak{f} \oplus \mathfrak{g} \cong (\mathfrak{f} + \mathfrak{g}) \oplus (\mathfrak{f} \cap \mathfrak{g}) = A \oplus \mathfrak{fg}$.

Si $n > 2$ un sencillo ejercicio de inducción completa la demostración:

$$\begin{aligned} \mathfrak{f}_1 \oplus \cdots \oplus \mathfrak{f}_{n-1} \oplus \mathfrak{f}_n &\cong A^{n-2} \oplus (\,\mathfrak{f}_1 \cdots \mathfrak{f}_{n-1}\,) \oplus \mathfrak{f}_n \;\cong \\ &\cong A^{n-2} \oplus A \oplus \mathfrak{f}_1 \cdots \mathfrak{f}_{n-1}\mathfrak{f}_n \cong A^{n-1} \oplus \mathfrak{f}_1 \cdots \mathfrak{f}_{n-1}\mathfrak{f}_n. \end{aligned}$$

(2) La implicación «$\Longleftarrow$» es un corolario inmediato de (1).

Para demostrar la otra implicación, supongamos que existe

$$\mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n \xrightarrow{\;\gamma\;} \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_n$$

un isomorfismo de A-módulos. Localizando respecto al subconjunto multiplicativo $S_A \subset A$ de los elementos no nulos de A, obtenemos un isomorfismo de K_A-espacios vectoriales

$$S_A^{-1}\,(\,\mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n\,) \xrightarrow{\;S_A^{-1}\gamma\;} S_A^{-1}\,(\,\mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_n\,).$$

Teniendo en cuenta los isomorfismos de K_A-espacios vectoriales

$$\begin{aligned} S_A^{-1}\,(\,\mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_m\,) \;&\cong\; \bigoplus_{i=1}^{m} S_A^{-1}\mathfrak{f}_i \;=\; K_A^m \\ S_A^{-1}\,(\,\mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_n\,) \;&\cong\; \bigoplus_{i=1}^{n} S_A^{-1}\mathfrak{g}_i \;=\; K_A^n \end{aligned}$$

se deduce que $K_A^m \cong K_A^n$, o equivalentemente, que $m = n$.

Probemos ahora que $\mathfrak{f}_1\,\mathfrak{f}_2 \cdots \mathfrak{f}_n \;\cong\; \mathfrak{g}_1\,\mathfrak{g}_2 \cdots \mathfrak{g}_n$. En virtud del Lema 1.1, sabemos que un homomorfismo $\mathfrak{f} \to \mathfrak{g}$ entre ideales fraccionarios de A viene dado por la multiplicación por un elemento de $K_A^\times$. Para cada $1 \leq i,\, j \leq n$, denotemos por $\gamma_{ij}\colon \mathfrak{f}_i \to \mathfrak{g}_j$ la componente ij del homomorfismo

$$\mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n \xrightarrow{\;\gamma\;} \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_n,$$

y sea $c_{ij} \in K_A^\times$ tal que $\gamma_{ij} = \mu_{c_{ij}}\colon \mathfrak{f}_j \to \mathfrak{g}_i$ es el homomorfismo «multiplicar por c_{ij}». De este modo, el isomorfismo γ determina una matriz cuadrada $C = (c_{ij}) \in \mathrm{M}_{n\times n}(K_A)$, tal que, para $(x_1,\, x_2,\, \ldots,\, x_n) \in \mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n$ y $(x'_1,\, x'_2,\, \ldots,\, x'_n) \in \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \cdots \oplus \mathfrak{g}_n$, la

relación $\gamma(x_1, x_2, \ldots, x_n) = (x'_1, x'_2, \ldots, x'_n)$ admite la siguiente expresión matricial:

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}. \tag{6.3}$$

Obsérvese que, para cada $i \in \{1, 2, \ldots, n\}$,

$$c_{ij}\mathfrak{f}_j \subset \mathfrak{g}_i, \quad \forall j \in \{1, 2, \ldots, n\};$$

por tanto para cada permutación $\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ se tiene que

$$(c_{1\sigma(1)}\mathfrak{f}_{\sigma(1)})(c_{2\sigma(2)}\mathfrak{f}_{\sigma(2)}) \cdots (c_{n\sigma(n)}\mathfrak{f}_{\sigma(n)}) \subset \mathfrak{g}_1\,\mathfrak{g}_2 \cdots \mathfrak{g}_n,$$

es decir,

$$(c_{1\sigma(1)}c_{2\sigma(2)} \cdots c_{n\sigma(n)})\,\mathfrak{f}_1\,\mathfrak{f}_2 \cdots \mathfrak{f}_n \subset \mathfrak{g}_1\,\mathfrak{g}_2 \cdots \mathfrak{g}_n;$$

entonces se tiene que

$$\det(C)\,\mathfrak{f}_1\,\mathfrak{f}_2 \cdots \mathfrak{f}_n \subset \mathfrak{g}_1\,\mathfrak{g}_2 \cdots \mathfrak{g}_n \tag{6.4}$$

Dado que γ es un isomorfismo, la matriz C es invertible y entonces $c = \det(C) \in K_A^\times$. Aplicando el argumento anterior al isomorfismo γ^{-1} cuya matriz asociada será C^{-1} se deduce que

$$c^{-1}\,\mathfrak{g}_1\,\mathfrak{g}_2 \cdots \mathfrak{g}_n \subset \mathfrak{f}_1\,\mathfrak{f}_2 \cdots \mathfrak{f}_n. \tag{6.5}$$

De (6.4) y (6.5) se deduce que $c\,\mathfrak{f}_1\,\mathfrak{f}_2 \cdots \mathfrak{f}_n = \mathfrak{g}_1\,\mathfrak{g}_2 \cdots \mathfrak{g}_n$, y por tanto la existencia del isomorfismo buscado. □

Corolario 6.6. *Sea A un dominio de Dedekind y M un A-módulo finitamente generado y libre de torsión de rango $n \geq 1$. Entonces existe un ideal fraccionario $\mathfrak{f}$ de A único salvo isomorfismo de modo que*

$$M \cong A^{n-1} \oplus \mathfrak{f}.$$

Demostración. En virtud de la Proposición 6.3, el A-módulo M será proyectivo y será isomorfo a una suma directa $\mathfrak{f}_1 \oplus \mathfrak{f}_2 \oplus \cdots \oplus \mathfrak{f}_n$ de ideales fraccionarios de A. Definiendo $\mathfrak{f} := \mathfrak{f}_1\,\mathfrak{f}_2 \ldots \mathfrak{f}_n$ y, haciendo uso del Teorema 6.5, deducimos que $M \cong A^{n-1} \oplus \mathfrak{f}$ y que en esta descomposición el ideal fraccionario $\mathfrak{f}$ es único salvo isomorfismo. □

Observación 6.7. La clase de isomorfía $[\mathfrak{f}] \in \mathtt{Pic}(A)$ del ideal fraccionario $\mathfrak{f}$ se llamará *clase de Steinitz* y únicamente dependerá del A-módulo M. Denotaremos a esta clase por $\mathrm{St}(M)$ y así deduciremos que dos módulos M y M' finitamente generados y libres de torsión sobre un dominio de Dedekind serán isomorfos si, y solo si, tienen el mismo rango y la misma clase de Steinitz.

Corolario 6.8. *Sea A un* DIP *y M un A-módulo. Entonces M es un A-módulo finitamente generado libre de torsión si, y solo si, M es un A-módulo libre tal que $M \cong A^n$; siendo $n = \operatorname{rang}(M)$.*

Demostración. Es consecuencia inmediata del Corolario 6.6 y del Lema 1.8. □

6.2. Módulos finitamente generados sobre un AVD

Antes de abordar el Teorema de Clasificación de los módulos finitamente generados sobre un AVD, recordaremos el concepto dual de los módulos proyectivos: los *módulos inyectivos*. Este tipo de módulos serán de utilidad para la demostración de este Teorema. Haremos un breve repaso de sus propiedades más importantes junto con una de sus principales caracterizaciones: el *Criterio de Baer*.

Observación 6.9. Un A-módulo E es inyectivo si verifica las condiciones equivalentes [5, Proposition 3.19]:

(1) Si $\iota\colon M \to N$ es un homomorfismo inyectivo de A-módulos y $\phi\colon M \to E$ es un homomorfismo arbitrario, entonces existe al menos una extensión de ϕ a un homomorfismo $\psi\colon N \to E$, es decir, un homomorfismo de A-módulos tal que $\psi \circ \iota = \phi$.

(2) El functor contravariante $\operatorname{Hom}(-, E)$ es exacto.

(3) Cualquier sucesión exacta corta de A-módulos

$$0 \to E \xrightarrow{\iota} M \to N \to 0$$

escinde, es decir, existe un homomorfismo $M \xrightarrow{\pi} E$ de modo que $\mathrm{id}_E = \pi \circ \iota$ y así se tiene la descomposición $M = \iota(E) \oplus \ker(\pi) \cong E \oplus N$.

Teorema (*Criterio de Baer*)**.** ([5, Theorem 3.20]) Dado E un A-módulo, equivalen:

(1) E es un A-módulo inyectivo.

(2) Para cada ideal I no nulo de A y cada homomorfismo $I \xrightarrow{\phi} E$ de A-módulos, existe un homomorfismo $A \xrightarrow{\psi} E$ que extiende ϕ, es decir, un homomorfismo tal que $\psi \circ \iota = \phi$.

Sea A un AVD y $t \in A$ un PU, es decir, tal que $\mathfrak{m} = (t)$ es el ideal maximal de A. Recordemos que los únicos ideales no nulos de A son los ideales de la forma (t^n) con $n \in \mathbb{Z}^+$ (Lema 2.26). De modo que (por el Lema de Nakayama) los ideales no nulos de A forman una cadena descendente

$$\cdots \subsetneq (t^s) \subsetneq (t^{s-1}) \subsetneq \cdots \subsetneq (t^2) \subsetneq (t) \subsetneq A$$

Entonces para cada entero $s > 0$, los ideales del anillo $\bar{A} = A/(t^s)$ forman un cadena finita

$$\{0\} \subsetneq (t^{s-1})/(t^s) \subsetneq \cdots \subsetneq (t^2)/(t^s) \subsetneq (t)/(t^s) \subsetneq A/(t^s)$$

Proposición 6.10. *Sea A un* AVD *y t un* PU. *Entonces, para cualquier entero $s > 0$, $A/(t^s)$ es un anillo auto-inyectivo es decir, $A/(t^s)$ es un $A/(t^s)$-módulo inyectivo.*

Demostración. Para demostrar este resultado, vamos a emplear el *Criterio de Baer*. Sea $\bar{A} = A/(t^s)$ y denotemos $\bar{x} = x + (t^s)$ para cada $x \in A$. Consideremos $I \subset \bar{A}$ un ideal y sea $f\colon I \to \bar{A}$ un homomorfismo de $\bar{A}$-módulos. Sea $J := \mathrm{Im}(f) \subset \bar{A}$. Dado que A es un AVD los ideales I y J serán de la forma $I = (\bar{t}^{r_1})$, $J = (\bar{t}^{r_2})$ para ciertos enteros $s \geq r_1,\, r_2 \geq 0$. Obsérvese que $\bar{t}^{s-r_1} f(\bar{t}^{r_1}) = f(\bar{t}^{s-r_1}\bar{t}^{r_1}) = f(\bar{t}^s) = \bar{0}$. Como $f(\bar{t}^{r_1})$ genera el ideal J, se tiene que $t^{s-r_1}t^{r_2} = 0$, y por lo tanto, $s - r_1 + r_2 \geq s$. Conclusión: $r_2 \geq r_1$. Entonces existirá $\bar{a} \in \bar{A}$ de manera que $f(\bar{t}^{r_1}) = \bar{a}\bar{t}^{r_2}$. Sea $\tilde{f}\colon \bar{A} \to \bar{A}$ la aplicación $\bar{A}$-lineal determinada por $\tilde{f}(\bar{1}) = \bar{a}\bar{t}^{r_2 - r_1}$. Es sencillo comprobar que $\tilde{f}_{|I} = f$. □

Teorema 6.11 (Clasificación de módulos finitamente generados sobre un AVD)**.** *Sea A un* AVD *y sea t un* PU. *Si M es un A-módulo finitamente generado sobre A, entonces:*

(1) *existen naturales $N, n \in \mathbb{N}$ y una cadena de enteros $a_1 \geq \cdots \geq a_n \geq 1$ tales que*

$$M \cong A^N \bigoplus \Big(\bigoplus_{i=1}^{n} \frac{A}{(t^{a_i})} \Big);$$

(2) *además, los enteros $N, n, a_1, \ldots, a_n$ son invariantes de la clase de isomorfía de M, es decir, son siempre los mismos para cualquier descomposición de M como en* (1).

Demostración.

Paso 0: Consideramos la sucesión exacta (6.1)

$$0 \longrightarrow \mathrm{Tor}(M) \longrightarrow M \longrightarrow M/\mathrm{Tor}(M) \longrightarrow 0.$$

Dado que $M/\mathrm{Tor}(M)$ es un A-módulo finitamente generados libre de torsión y que A es un AVD (en particular un DIP por 2.27), entonces por el Corolario 6.6 existirá un único $N \in \mathbb{N}$ tal que

$$M/\mathrm{Tor}(M) \cong A^N.$$

Solamente faltaría estudiar los A-módulos de torsión finitamente generados sobre AVDs. Sea T un A-módulo de estas características.

Paso 1: Supongamos que T es un A-módulo de torsión no nulo. Como A es un AVD, el aniquilador de T será de la forma $\mathrm{Ann}_A(T) = (t^{a_1})$, para un entero $a_1 > 0$. Por el Lema

de Nakayama $(t^{a_1}) \subsetneq (t^{a_1-1})$, por lo que existirá un elemento $x_1 \in T$ tal que $t^{a_1-1}x_1 \neq 0$. Denotemos por comodidad $A_1 := A/(t^{a_1})$. De esta manera T puede pensarse como un módulo sobre A_1; además el homomorfismo de A_1-módulos $\iota_1 \colon A_1 \to T$ determinado por $1 \mapsto \iota_1(1) = x_1$ es claramente una aplicación inyectiva. Tomando el cociente $T_1 := T/xA_1$, obtenemos la sucesión exacta corta de A_1-módulos (de hecho de A-módulos)

$$0 \longrightarrow A_1 \xrightarrow{\iota_1} T \xrightarrow{\pi_1} T_1 \longrightarrow 0.$$

Dado que A_1 es un anillo auto-inyectivo, por la Proposición 6.10, deducimos que esta sucesión de A_1-módulos escinde y escinde también como sucesión de A-módulos. De este modo, existirá un isomorfismo de A-módulos tal que

$$T \cong A_1 \oplus T_1.$$

Paso 2: Si $T_1 \neq 0$, dado que T_1 es un A-módulo finitamente generado de torsión y tal que $\mathrm{Ann}_A(T) \subset \mathrm{Ann}_A(T_1)$, existirá un entero $a_2 \leq a_1$ tal que $\mathrm{Ann}_A(T_1) = (t^{a_2})$. De modo análogo al **Paso 1**, existirá un elemento $x_2 \in T_1$ tal que $t^{a_2-1}x_2 \neq 0$. Denotando $A_2 = A/(t^{a_2})$, el A-módulo T_1 es un módulo sobre A_2, y el homomorfismo de A_2-módulos $\iota_2 \colon A_2 \to T_1$ determinado por $1 \mapsto \iota_2(1) = x_2$ es inyectivo. Utilizando de nuevo que A_2 es auto-inyectivo, se deduce que la sucesión exacta de A_2-módulos (también de A-módulos)

$$0 \longrightarrow A_2 \xrightarrow{\iota_2} T_1 \xrightarrow{\pi_2} T_2 \longrightarrow 0$$

escinde, y se obtiene un isomorfismos de A-módulos

$$T \cong A_1 \oplus T_1 \cong A_1 \oplus A_2 \oplus T_2.$$

Repitiendo este procedimiento en un número finito de pasos habremos terminado, ya que T es noetheriano (por ser un A-módulo finitamente generado y A un anillo noetheriano); concluyendo de este modo que existe un isomorfismo del tipo indicado en el enunciado (1).

Paso 3: El entero N está determinado por M ya que $N = \operatorname{rang} M$. Para demostrar que el submódulo $T = \mathrm{Tor}(M)$ determina n y la familia de enteros $a_1 \geq \cdots \geq a_n \geq 1$, es suficiente comprobarlo para A-módulos del tipo $\bigoplus_{i=1}^n A/(t^{a_i})$.

Dada una la familia de enteros $a_1 \geq \cdots \geq a_n \geq 1$, consideremos el A-módulo $M = \bigoplus_{i=1}^n A/(t^{a_i})$. Sea $s = a_1$. Cada eslabón en la filtración de submódulos

$$\{0\} = t^s M \subset t^{s-1}M \subset \cdots \subset t^{i+1}M \subset t^i M \subset \cdots \subset tM \subset M,$$

es un $A/(t)$-espacio vectorial. Denotemos $d_i = \dim_{A/(t)}(t^i M/t^{i+1}M)$. Entonces, para cada entero $a_1 \geq a \geq 1$ el número de repeticiones de un sumando de la forma $A/(t^a)$ en la cadena $a_1 \geq \cdots \geq a_n \geq 1$ es $d_{a-1} - d_a$. □

Corolario 6.12. *Sea A un* AVD *y sea M un A-módulo libre de torsión finitamente generado. Entonces M es un A-módulo libre, es decir, existe un único $N \in \mathbb{N}$ de modo que $M \cong A^N$.*

Corolario 6.13. *Sea A un* AVD*, t un* PU *y sea T un A-módulo de torsión finitamente generado. Entonces existen únicos enteros $n \geq 0$ y $a_1 \geq \cdots \geq a_n \geq 1$ de modo que*

$$T \cong \bigoplus_{i=1}^{n} A/(t^{a_i}).$$

6.3. Módulos de torsión sobre un dominio de Dedekind

Definición 6.14. Sea M un A-módulo y sea $\mathfrak{p}$ un ideal primo de A. La *componente $\mathfrak{p}$-primaria* de M es el submódulo

$$M(\mathfrak{p}) := \{\, x \in M \mid \mathrm{Ann}_A(x) = \mathfrak{p}^r \text{ para algún } r \in \mathbb{Z}^+ \,\}.$$

Diremos que M es $\mathfrak{p}$-primario si $M = M(\mathfrak{p})$.

Observación 6.15. Está claro que si M es un A-módulo $\mathfrak{p}$-primario y finitamente generado, entonces $\mathrm{Ann}_A(M) = \mathfrak{p}^m$ para cierto $m \in \mathbb{Z}^+$. En efecto, si $x_1, \ldots, x_t$ es un conjunto de generadores no nulos de M, y $m_1, \ldots, m_t$ son enteros positivos tales que $\mathrm{Ann}_A(x_i) = \mathfrak{p}^{m_i}$, entonces $\mathrm{Ann}_A(M) = \mathfrak{p}^m$, con $m = \text{máx}\{m_1, \ldots, m_t\}$.

Teorema 6.16 (Descomposición primaria)**.** *Sea A un dominio de Dedekind y sea T un A-módulo de torsión finitamente generado. Luego existen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ ideales primos no nulos de A distintos dos a dos de modo que*

$$T = T(\mathfrak{p}_1) \oplus T(\mathfrak{p}_2) \oplus \cdots \oplus T(\mathfrak{p}_s).$$

Demostración. Supongamos que T es un A-módulo de torsión no nulo y finitamente generado. Como A es un dominio de Dedekind, su aniquilador $I := \mathrm{Ann}_A(T)$ admite una descomposición de la forma $I = \prod_{i=1}^{s} \mathfrak{p}_i^{r_i}$ donde cada r_i es un entero positivo y $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ son ideales primos distintos no nulos de A, es decir, maximales distintos de A. Entonces, los ideales $\mathfrak{p}_1^{r_1}$, $\mathfrak{p}_2^{r_2}$, $\ldots$, $\mathfrak{p}_s^{r_s}$ son ideales coprimos dos a dos,y en consecuencia se tiene que $I = \prod_{i=1}^{s} \mathfrak{p}_i^{r_i} = \bigcap_{i=1}^{s} \mathfrak{p}_i^{r_i}$.

Por el Teorema Chino de los Restos, los homomorfismos $\pi_i \colon A \to A/\mathfrak{p}_i^{r_i}$ determinan un homomorfismo sobreyectivo de anillos $\pi \colon A \to A/\mathfrak{p}_1^{r_1} \times A/\mathfrak{p}_2^{r_2} \times \cdots \times A/\mathfrak{p}_s^{r_s}$ tal que $\ker(\pi) = \mathrm{Ann}_A(T)$. Para cada $i \in \{1, \ldots, s\}$, sea $e_i \in A$ tal que $\pi_i(e_i) = 1$ y $\pi_j(e_i) = 0$ para todo $j \neq i$. Estos elementos de A verifican las siguientes propiedades:

(1) $ae_i \in \mathrm{Ann}_A(T)$, para cualquier $a \in \mathfrak{p}_i^{r_i}$.

(2) $1 = e_1 + \cdots + e_s + a_0$, para cierto $a_0 \in \mathrm{Ann}_A(T)$.

Como consecuencia de estas propiedades, para cada $x \in M$ se tiene que:

(1) $x_i := e_i x \in T(\mathfrak{p}_i)$.

(2) $x = 1 \cdot x = e_1 x + \cdots + e_s x + a_0 x = x_1 + \cdots + x_s$.

Por lo tanto, obtendremos que $T = T(\mathfrak{p}_1) + T(\mathfrak{p}_2) + \cdots + T(\mathfrak{p}_s)$. Para cada $j \in \{1, 2, \ldots, s\}$, los ideales $\mathfrak{p}_j^{r_j}$ e $I_j := \prod_{i \neq j} \mathfrak{p}_i^{r_i}$ son coprimos. De este modo, existirán elementos $a, b \in A$, $u \in \mathfrak{p}_j^{r_j}$ y $v \in I_j$ tales que $1 = au + bv$. Por tanto, si $x \in T(\mathfrak{p}_j) \cap (\Sigma_{i \neq j}^s T(\mathfrak{p}_i))$, se tiene que $x = (au + bv)x = aux + bvx = 0$. Como $T = \Sigma_{i=1}^s T(\mathfrak{p}_i)$, se concluye que:

$$T = T(\mathfrak{p}_1) \oplus T(\mathfrak{p}_2) \oplus \cdots \oplus T(\mathfrak{p}_s). \qquad \square$$

Proposición 6.17. *Sea A un dominio, $\mathfrak{m}$ un ideal maximal de A y sea $n \in \mathbb{Z}^+$ un entero positivo. El homomorfismo canónico $\pi\colon A \to A/\mathfrak{m}^n$ se factoriaza a través de la inclusión $\iota\colon A \hookrightarrow A_{\mathfrak{m}}$.*

Demostración. El anillo $A/\mathfrak{m}^n$ es local con maximal $\mathfrak{m}/\mathfrak{m}^n$. Las imágenes en $A/\mathfrak{m}^n$ de los elementos del subconjunto multiplicativo $S_{\mathfrak{m}} = A \setminus \mathfrak{m} \subset A$ son unidades. Por tanto, existe un único homomorfismo de anillos $\pi'\colon A_{\mathfrak{m}} \to A/\mathfrak{m}^n$ tal que $\pi' \circ \iota = \pi$. $\square$

Corolario 6.18. *Sea A un dominio de Dedekind, $\mathfrak{p}$ un ideal primo no nulo de A y sea M un módulo finitamente generado y $\mathfrak{p}$-primario. Entonces:*

(1) *La estructura de A-módulo de M induce una estructura natural de $A_{\mathfrak{p}}$-módulo.*

(2) *En particular, los $A_{\mathfrak{p}}$-submódulos de M son exactamente los A-submódulos de M.*

Demostración. Como M es un módulo finitamente generado y $\mathfrak{p}$-primario, existirá un entero $m > 0$ tal que $\mathrm{Ann}_A(M) = \mathfrak{p}^m$. De modo que la estructura de A-módulo de M induce una estructura natural de $A/\mathfrak{p}^m$-módulo, y por tanto de $A_{\mathfrak{p}}$-módulo (Proposición 6.17). $\square$

Teorema 6.19 (Descomposición de Jordan)**.** *Sea A un dominio de Dedekind y T un A-módulo de torsión finitamente generado. Se verifica:*

Existe $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_k$ una familia de ideales primos de A y una familia de enteros positivos $a_1, a_2, \ldots, a_k$ únicas salvo permutación de índices tales que:

$$T \cong A/\mathfrak{q}_1^{a_1} \oplus A/\mathfrak{q}_2^{a_2} \oplus \cdots \oplus A/\mathfrak{q}_k^{a_k} \tag{6.6}$$

Demostración.

Existencia: Empleando el Teorema de la Descomposición primaria, tenemos que existen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ ideales primos de A distintos dos a dos de modo que $T = \bigoplus_{i=1}^{s} T(\mathfrak{p}_i)$. Cada $T(\mathfrak{p}_i)$ es un A-módulo $\mathfrak{p}_i$-primario y de este modo, por Corolario 6.18, cada $T(\mathfrak{p}_i)$ es también un $A_{\mathfrak{p}_i}$-módulo con la estructura de A-módulo subyacente. Cada $T(\mathfrak{p}_i)$ es un A-módulo de torsión y en consecuencia un $A_{\mathfrak{p}_i}$-módulo de torsión. Para cada $i \in \{1, \ldots, n\}$, $A_{\mathfrak{p}_i}$ es un AVD y de este modo podremos aplicar el Corolario 6.13. Entonces existirán únicos enteros s_i y $a_{i1} \geq \ldots \geq a_{is_i} > 0$ de modo que :

$$T(\mathfrak{p}_i) \cong \bigoplus_{j=1}^{s_i} A_{\mathfrak{p}_i} \,/\, \mathfrak{p}_i^{a_{ij}} A_{\mathfrak{p}_i} \cong \bigoplus_{j=1}^{s_i} A/\mathfrak{p}_i^{a_{ij}}$$

El último isomorfismo es consecuencia directa de la Proposición 6.17. Concluyendo, entonces, que

$$T = \bigoplus_{i=1}^{s} T(\mathfrak{p}_i) \cong \bigoplus_{i=1}^{s} \Big(\bigoplus_{j=1}^{s_i} A/\mathfrak{p}_i^{a_{ij}} \Big) \tag{6.7}$$

es un isomorfismo de T con una descomposición del tipo (6.6).

Unicidad: Supongamos que existe otra familia $\mathfrak{q}'_1, \mathfrak{q}'_2, \ldots, \mathfrak{q}'_t$ de ideales primos no nulos de A y enteros positivos $a'_1, a'_2, \ldots, a'_t$ tales que:

$$T \cong M := A/{\mathfrak{q}'_1}^{a'_1} \oplus A/{\mathfrak{q}'_2}^{a'_2} \oplus \cdots \oplus A/{\mathfrak{q}'_t}^{a'_t} \tag{6.8}$$

Supongamos que $\{\mathfrak{p}'_1, \mathfrak{p}'_2, \ldots, \mathfrak{p}'_{s'}\}$ son los primos distintos entre todos los $\mathfrak{q}'_i$. Agrupando convenientemente los sumandos asociados a un mismo ideal primo, podemos obtener los siguientes isomorfismos:

$$T = \bigoplus_{i=1}^{s} T(\mathfrak{p}_i) \cong \bigoplus_{i=1}^{s'} M(\mathfrak{p}'_i) = M$$

Por la unicidad de la descomposición de un módulo en sus componentes primarias se deduce que deduce que $s = s'$ y que, salvo permutación de índices, $\mathfrak{p}_i = \mathfrak{q}'_i$ y $T(\mathfrak{p}_i) \cong M(\mathfrak{q}'_i)$. Basta entonces estudiar solamente la unicidad de la descomposición de cada una de las componentes primarias.

Supongamos que $T_i = T(\mathfrak{p}_i)$ para uno de los ideales primos $\mathfrak{p}_i \in \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s\}$. En tal caso, T_i es un $A_{\mathfrak{p}_i}$-módulo de torsión y $A_{\mathfrak{p}_i}$ es un AVD. Así pues, los enteros s_i y $a_{i1} \geq \cdots \geq a_{is_i} > 0$, determinan de forma única T_i salvo isomorfismo (Corolario 6.13). De esta manera concluimos la prueba. □

Teorema 6.20. *(Descomposición por invariantes) Sea A un dominio de Dedekind y sea T un A-módulo finitamente generado de torsión. Entonces existirá una familia única de ideales enteros $\{0\} \subsetneq I_1 \subset I_2 \subset \cdots \subset I_m \subsetneq A$ tales que*

$$T \cong \frac{A}{I_1} \oplus \frac{A}{I_2} \oplus \cdots \oplus \frac{A}{I_m}$$

Demostración.
Existencia: En virtud de (6.8) tenemos que

$$T \cong \bigoplus_{i=1}^{s} \Big(\bigoplus_{j=1}^{s_i} A/\mathfrak{p}_i^{a_{ij}} \Big),$$

siendo $\mathfrak{p}_1, \mathfrak{p}_2 \ldots, \mathfrak{p}_s$ una familia de ideales primos de A no nulos y distintos dos a dos , para cada $i \in \{1, 2, \ldots, n\}$ s_i es un entero y $0 < a_{i1} \leq a_{i2} \leq \cdots \leq a_{is_i}$ es una familia de enteros.

Sea $m := \text{máx}\{\, s_i \,|\, 1 \leq i \leq s \,\}$. Añadiendo los ceros necesarios al principio de la lista de los enteros a_{ij}, y salvo permutación de índices, tendremos que para cada $i \in \{1, 2, \ldots, s\}$ se verifica

$$0 \leq a_{i1} \leq a_{i2} \leq \cdots \leq a_{im}.$$

Definamos para cada $j \in \{1, 2, \ldots, m\}$ los ideales $I_j := \prod_{i=1}^{s} \mathfrak{p}_i^{a_{i,m+1-j}}$. Es de comprobación sencilla que $I_1 \subset I_2 \subset \cdots \subset I_m$. Empleando el Teorema Chino de los Restos se obtiene que para cada $j \in \{1, 2, \ldots, m\}$

$$\bigoplus_{i=1}^{s} A/\mathfrak{p}_i^{a_{i,m+1-j}} \cong A/\,\Pi_{i=1}^{s}\, \mathfrak{p}_i^{a_{i,m+1-j}} = A/I_j.$$

Mediante una permutación de sumandos,

$$T \cong \bigoplus_{i=1}^{s} \Big(\bigoplus_{j=1}^{m} A/\mathfrak{p}_i^{a_{ij}} \Big) \cong \bigoplus_{j=1}^{m} \Big(\bigoplus_{i=1}^{s} A/\mathfrak{p}_i^{a_{i,m+1-j}} \Big) \cong \bigoplus_{j=1}^{m} A/I_j.$$

Unicidad: Supongamos que $\{0\} \subsetneq I_1 \subset I_2 \subset \cdots \subset I_m \subsetneq A$ es una cadena de ideales tal que

$$T \cong \frac{A}{I_1} \oplus \frac{A}{I_2} \oplus \cdots \oplus \frac{A}{I_m}.$$

Dado que A es un dominio de Dedekind (por Teorema 4.5) se tiene que los ideales I_j se descomponen de manera única como producto de primos. En particular, el primer ideal

$$I_1 = \prod_{i=1}^{m} \mathfrak{p}_i^{c_{i1}}.$$

Dado que $I_1 \subset I_2 \subset \cdots \subset I_m$, deduciremos que cada ideal se descompondrá en producto de primos como $I_j = \prod_{i=1}^{m} \mathfrak{p}_i^{c_{ij}}$ donde $c_{i1} \geq c_{i2} \cdots \geq c_{im} \geq 0$ para todo $i \in \{1, 2, \ldots, m\}$. De este modo, aplicando de nuevo el Teorema Chino de los Restos, deducimos que

$$T \cong \bigoplus_{i=1}^{m} A/I_j \cong \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{m_i} A/\mathfrak{p}_i^{c_{ij}} \equiv \bigoplus_{k=1}^{s} A/\mathfrak{p}_k^{a_k}.$$

En virtud de la unicidad dada en el Teorema 6.19, deducimos que la familia c_{ij} está determinada de forma única y de este modo también lo estará la familia de ideales $I_1, I_2, \ldots I_m$; concluyendo la prueba. □

6.4. Teorema de Clasificación

En vista de todos los resultados anteriores podemos enunciar el siguiente Teorema.

Teorema 6.21. *Sea A un dominio de Dedekind y sea M un A-módulo finitamente generado.*

(1) *Existen L y T A-submódulos de M, tales que L es libre de torsión, T es de torsión y se verifica que $M = L \oplus T$.*

(2) *Existe un único $N \in \mathbb{N}$ y un ideal fraccionario $\mathfrak{f}$ de A, único salvo isomorfismos, tal que:*

$$L \cong A^{N-1} \oplus \mathfrak{f}.$$

(3) *Existirán dos descomposiciones para T:*

   (a) *(Jordan) Existe $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ una familia única de ideales primos de A no nulos y distintos dos a dos y $a_1, a_2, \ldots, a_s$ una familia única de enteros positivos tales que:*

$$T \cong \bigoplus_{k=1}^{s} A/\mathfrak{p}_k^{a_k}.$$

   (b) *(Invariantes) Existe una familia única de ideales enteros $I_1, I_2, \ldots, I_m$ de manera que $\{0\} \subsetneq I_1 \subset I_2 \subset \ldots \subset I_m \subsetneq A$ y tal que:*

$$T \cong \bigoplus_{k=1}^{m} A/I_k.$$

Demostración. Consideramos la sucesión exacta (6.1):

$$0 \to \operatorname{Tor}(M) \to M \to M/\operatorname{Tor}(M) \to 0.$$

Por la Observación 6.1 y dado que M es de tipo finito, el A-módulo $M/\operatorname{Tor}(M)$ es finitamente generado y libre de torsión. Empleando la Proposición 6.3 se deduce que $M/\operatorname{Tor}(M)$

es un A-módulo proyectivo. De este modo, la sucesión exacta escinde y se tiene que $M \cong M/\operatorname{Tor}(M) \oplus \operatorname{Tor}(M)$, es decir, existen L y T A-submódulos de M, tales que L es libre de torsión, T es de torsión y $M = L \oplus T$. El resultado se deduce ahora por el Corolario 6.6, el Teorema 6.19 y el Teorema 6.20. □

Corolario 6.22. *Sea A un* DIP *y sea M un A-módulo finitamente generado.*

(1) *Existen L y T A-submódulos de M tales que $M = L \oplus T$.*

(2) *El A-módulo L es libre de tipo finito. De este modo, existirá un único $N \in \mathbb{N}$ tal que:*

$$L \cong A^N.$$

(3) *El A-módulo T es finitamente generado y de torsión. Tendremos dos descomposiciones:*

   (a) *(Jordan) Existe $p_1, p_2, \ldots, p_s$ una familia única de elementos irreducibles de A distintos dos a dos y $a_1, a_2, \ldots, a_s$ una familia única de enteros positivos tales que:*

$$T \cong \bigoplus_{k=1}^{s} A/(p_k^{a_k}).$$

   (b) *(Invariantes) Existe $d_1, d_2, \ldots d_m$ una familia única de enteros mayores positivos tales que $d_m \,|\, d_{m-1} \,|\, \ldots \,|\, d_1$ y tales que:*

$$T \cong \bigoplus_{j=1}^{m} A/(d_j).$$

Demostración. Utilizando que A es un DIP, el resultado se deduce del Corolario 6.8 y del Teorema 6.21 □

Bibliografía

[1] Atiyah, M. F. and Macdonald, I. G.: *Introducción al Álgebra Conmutativa.* Reverté, Barcelona, 1980.

[2] Broué, M.: *Some Topics in Algebra.* An advanced undergraduate course at PKU. Mathematical Lectures from Peking University. Springer, Heidelberg, 2014.

[3] Bourbaki, N.: *Élements de Mathématique, Algèbre*, Chapitres 5 et 6. Hermann, Paris, 1964.

[4] Claborn, L.: Every abelian group is a class group. *Pacific J. Math.* 18 (1966), 219–222.

[5] Clark, P. L.: *Commutative Algebra*, 2015. http://math.uga.edu/ pete/integral.pdf

[6] Cohn, P. M.: *Basic Algebra: Groups, rings and fields.* Springer-Verlag, London, 1980.

[7] Eisenbud, D.: *Commutative algebra with a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[8] Fulton, W.: *Algebraic Curves, an Introduction to Algebraic Geometry.* https://www.math.lsa.umich.edu

[9] Grathmann, A.: Class Notes, «Commutative Algebra» (WS 2013/14) https://www.mathematik.uni-kl.de/ gathmann/de/commalg.php

[10] Kosters, M.: Projective modules over Dedekind domains. http://www.math.leidenuniv.nl/ edix/tag_2009/michiel_3.pdf

[11] May, J.P.: Notes on Dedekind rings. https://www.math.uchicago.edu/ may/MISC/Dedekind.pdf

[12] Stewart, I. and Tall, D.: *Algebraic Number Theory and Fermat's Last Theorem.* (3rd Ed.) A.K. Peters, Massachusetts, 1994.

[13] Sutherland, A.: Number Theory I. Fall 2019. Massachusetts Institute of Technology: MIT OpenCourseWare
https://ocw.mit.edu. License: Creative Commons BY-NC-SA.