Universidad de Valladolid

Estructura de los Módulos en el Álgebra de Iwasawa

Alejandro Melero Santos

2024/25

COTUTORES: ALBERTO FERNÁNDEZ BOIX
BEATRIZ MOLINA SAMPER

TRABAJO DE FIN DE GRADO
GRADO EN MATEMÁTICAS
FACULTAD DE CIENCIAS

Resumen

El objetivo de este trabajo es demostrar en detalle el Teorema de estructura de los módulos finitamente generados sobre el álgebra de Iwasawa, que no es más que un anillo de series en una variable con coeficientes en los enteros p-ádicos. Este teorema es un resultado importante en la Teoría de Iwasawa, postulada por el matemático japonés Kenkichi Iwasawa, a mediados de la década de 1950.

Se usarán como referencia los resultados recogidos en los capítulos 7 y 12 del libro de Larry Washington; Introduction to Cyclotomic Fields, en el que la Teoría de Iwasawa aparece al estudiar los cuerpos ciclotómicos y su conexión con el último Teorema de Fermat.

Palabras clave

Álgebra, $\mathbb{Z}_p$-módulos, números p-ádicos, anillo de series.

Índice

Introducción

Motivación

Uno de los resultados más básicos del Álgebra Lineal es el hecho de que todo K-espacio vectorial de dimensión finita n es isomorfo a K^n. La técnica empleada para obtener este resultado consiste en realizar transformaciones elementales a una matriz representante del K-espacio vectorial hasta obtener la forma de Gauss.

El Teorema de Estructura de Grupos Abelianos Finitamente Generados nos da un resultado similar, todo grupo de esta forma es isomorfo a la suma directa de un grupo libre (n copias de $\mathbb{Z}$) y un grupo de torsión, éste último isomorfo a $\oplus_{i=1}^{t}(\mathbb{Z}/(p^i))$, donde p es un número primo. Entre las operaciones permitidas que conservan el isomorfismo desaparece la división por elementos distintos de 1 o -1, y la matriz resultante es la llamada forma normal de Smith.

Con esta base nos adentramos en los módulos sobre el Álgebra de Iwasawa, buscando encontrar un resultado similar a los dos anteriores. La dimensión de Krull (que definiremos más adelante), que era 0 y 1 en los casos previos, es ahora de 2, lo que añade dificultad al problema y nos privará de obtener un isomorfismo. En esta ocasión un pseudoisomorfismo (que también definiremos posteriormente) es lo máximo que podremos aspirar a obtener.

Podría decirse que las bases de la teoría de Iwasawa empezaron a formarse con un fallido intento de demostración del conocido último teorema de Fermat por parte del matemático francés Gabriel Lamé (1795-1870). Después de que Joseph Liouville (1809-1882) destacase un detalle que Lamé había pasado por alto en su demostración, esta fue finalmente desacreditada por el matemático alemán Ernst Eduard Kummer (1810-1893). El propio Kummer intentó sortear la laguna en la prueba de Lamé, introduciendo el uso de ideales de un anillo al problema. Acabó demostrando la veracidad del teorema para el caso en el que los exponentes considerados son un conjunto particular de primos, los llamados primos regulares. Más adelante, Martin Eichler (1912-1992) consiguió extender el trabajo de Kummer a algunos de los primos "irregulares". Una de las ramas que se empezó a estudiar en aquel entonces fue el caso de las extensiones de cuerpos de números, y las factorizaciones de algunos de los

ideales de los anillos que surgen en este contexto. A ello le siguió el estudio de cuerpos ciclotómicos, y es en este enfoque en el que Kenkichi Iwasawa (1917-1998) realiza su trabajo. La teoría que desarrolló Iwasawa se centra en el análisis de torres de cuerpos ciclotómicos cuyos grupos de Galois son de una forma concreta. En el centro de la teoría de Iwasawa se encuentra el teorema de estructura cuya prueba detalla esta memoria, resultado que es fundamental para la prueba del teorema que culmina la teoría de Iwasawa.

Estructura

En el Capítulo 1 introducimos el concepto de módulo y repasamos algunos teoremas de estructura más sencillos, con el fin de ayudar a comprender las similitudes y diferencias con el caso de la teoría de Iwasawa.

En el Capítulo 2 hacen su aparición los números p-ádicos y se mencionan sus principales propiedades algebraicas.

El Capítulo 3 está dedicado a la presentación y demostración de resultados concernientes al Álgebra de Iwasawa, entre los cuales destaca el teorema de preparación de Weierstrass.

Finalmente, el Capítulo 4 recoge los últimos detalles necesarios para demostrar el teorema de estructura, así como la prueba del mismo.

1. Módulos. El Teorema de Estructura sobre DIPs.

Nuestro primer objetivo es entender con qué objetos vamos a trabajar. En esta sección veremos uno de dichos objetos, los módulos, y veremos como actúan sobre los Dominios de Ideales Principales.

Empezaremos definiendo el elemento principal de este trabajo, los módulos, que al fin y al cabo son una generalización del concepto de K-espacio vectorial (donde K es un cuerpo) a un anillo A.

Definición 1.1.
Sea A un anillo unitario, y sea e_A su identidad multiplicativa. Un *A-módulo por la izquierda* M es un grupo abeliano $(M, +)$, junto con una operación $\cdot : A \times M \to M$ tal que $\forall\ a, b \in A, \forall\ x, y \in M$, se tiene:

1. $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.
2. $(a + b) \cdot x = a \cdot x + b \cdot x$.
3. $a \cdot (x + y) = a \cdot x + a \cdot y$.
4. $e_A \cdot x = x$.

Una propiedad muy usada, que se deduce de estas cuatro primeras, es:

$$0_A \cdot m = 0_M,\ \ a \cdot 0_M = 0_M \qquad \forall m \in M,\ \ a \in A.$$

Nota: Abusamos de la notación, denominando de la misma forma $(\cdot)$ al producto interno de A y al producto de elementos de M por escalares de A. Ocurre lo mismo con $(+)$, que representa tanto la suma habitual en A como la suma en M.

De forma análoga definimos un módulo por la derecha. Si el anillo es conmutativo, los módulos por la derecha son módulos por la izquierda, y viceversa. Por ello, los denotaremos simplemente como módulos. De aquí en adelante asumimos que todo anillo mencionado es conmutativo.

Ejemplo 1.2.
Dado un anillo A, A^n es un A-módulo para todo $n \in \mathbb{N}$, en los que la suma y el producto por escalares se definen componente a componente.

Ejemplo 1.3.
Todos los grupos abelianos son $\mathbb{Z}$-módulos, considerando que el producto nx (con $n \in \mathbb{Z}$ y $x \in M$) se define como la suma de n sumandos $x + x + \cdots + x$.

Ejemplo 1.4.
Los ideales de un anillo son submódulos sobre dicho anillo.

Definición 1.5.
Un *submódulo* S de un A-módulo M es un subconjunto de M que es, por sí mismo, un A-módulo con las mismas operaciones definidas para M.

Proposición 1.6.
La intersección de submódulos de M es un submódulo de M.

Demostración. Resulta trivial teniendo en cuenta que la intersección de subgrupos abelianos es un subgrupo abeliano. □

Definición 1.7.
Sean M, N dos módulos sobre un anillo A. La *suma directa de M y N,* que denotaremos $M \oplus N$, es el módulo:

$$M \oplus N := \{(a, b) : a \in M, b \in N\}.$$

Y, al igual que mencionábamos en 1.2, la suma y el producto por escalares se realizan componente a componente.

Al tomar un subconjunto cualquiera de un módulo, nos puede interesar el submódulo más pequeño que contiene a dicho subconjunto. Esto motiva la siguiente definición:

Definición 1.8.
Dado un subconjunto B de un A-módulo M, decimos que el *submódulo generado por B*, denotado $\langle\langle B \rangle\rangle$, es la intersección de todos los submódulos $S \subset M$ que contienen a B.

Resulta sencillo comprobar que $\langle\langle B\rangle\rangle$ es, equivalentemente, el menor submódulo de M que contiene a B: de existir un submódulo C de M con $B \subseteq C \subseteq \langle\langle B\rangle\rangle \subseteq M$ tendríamos, por definición de $\langle\langle B\rangle\rangle$, que $\langle\langle B\rangle\rangle \subseteq C$. Y por lo tanto $\langle\langle B\rangle\rangle = C$.

Proposición 1.9.
El submódulo generado por B es igual al conjunto de combinaciones lineales finitas de los elementos de B, con coeficientes en el anillo A:

$$\langle\langle B\rangle\rangle = T := \{a_1b_1 + \cdots + a_nb_n | a_i \in A,\ b_i \in B,\ n \geq 1\}.$$

Demostración. T contiene a B: si $b \in B, b = 1_A \cdot b \in T$. Por tanto, $\langle\langle B\rangle\rangle \subseteq T$. Por las propiedades de módulo, todo A-submódulo que contenga a B contiene a las combinaciones lineales finitas de elementos de B. Es decir, $T \subseteq \langle\langle B\rangle\rangle$, y ya tenemos la igualdad: $\langle\langle B\rangle\rangle = T$. □

1.1. Módulos finitamente generados y finitamente presentados.

De la teoría de grupos abelianos que ya conocemos podemos extraer conceptos que se generalizan para el caso de A-módulos, por ejemplo la ciclicidad o los generadores:

Definición 1.10.
Decimos que un A-módulo M es *finitamente generado* si $M = \langle\langle B\rangle\rangle$, con B un subconjunto finito de A. El conjunto B se dice que es un sistema de generadores de M.

Definición 1.11.
Sea M un A-módulo. Un submódulo se denomina *cíclico* si es el submódulo generado por un sólo elemento de M.

Ejemplo 1.12.
Sea $a \in A$, y consideremos el módulo $A/(a)$. Sus elementos son de la forma $x + (a)$, con $x \in A$. Pero esto se puede reescribir como $x \cdot (1 + (a))$, por lo que $1 + (a)$ es por sí mismo un generador del módulo.

Definición 1.13.
Dado un subconjunto S de un A-módulo M, llamamos *anulador de S sobre A* al conjunto:

$$Ann_A(S) = \{a \in A |\ as = 0\ \forall s \in S\}.$$

Resulta trivial ver que el anulador de un conjunto es un ideal y también un módulo.

Definición 1.14.
Si M admite un sistema de generadores linealmente independiente, a este sistema se le llama *base* y decimos que M es un módulo *libre*. No todos los módulos admiten base, por ejemplo:

- En $\mathbb{Z}/n\mathbb{Z}$ (visto como $\mathbb{Z}$-módulo), cualquier elemento es anulado por n, por lo que $\mathbb{Z}/n\mathbb{Z}$ no tiene base. Lo mismo ocurre, evidentemente, con todo submódulo suyo.

Este tipo de elementos, responsables de que no todo módulo tenga una base, se denominan elementos de *torsión*.

Definición 1.15.
Decimos que un elemento x de un A-módulo M es de *torsión* si $\exists a \in A$ tal que $a \cdot x = 0$. Si esto ocurre para todo elemento de M, decimos que M es un módulo de torsión.

Puede darse el caso en el que el único elemento de torsión sea 0:

Definición 1.16.
Si un módulo no posee elementos de torsión no nulos, se dice que es un módulo *libre de torsión*.

Ejemplo 1.17.
Los elementos de torsión pueden variar según el anillo sobre el cual se considere el módulo. Ya hemos visto que al considerar $\mathbb{Z}/n\mathbb{Z}$ como $\mathbb{Z}$-módulo, todos sus elementos son de torsión, ya que cumplen la relación $n \cdot x = 0$. Sin embargo, $\mathbb{Z}/n\mathbb{Z}$ puede verse también como $\mathbb{Z}/n\mathbb{Z}$-módulo, y en ese caso los elementos de torsión serán aquellos no coprimos con n.

Proposición 1.18.
Si un A-módulo M es finitamente generado, existe un morfismo ψ sobreyectivo de A^k a M, para algún k finito.

Demostración. Construimos el morfismo de la siguiente forma. Como M es f.g, tomamos su conjunto generador $\{m_1, \ldots, m_k\}$. Entonces, a cada k-úpla $(a_1, \ldots, a_k)$ de A^k le asignaremos el sumando $a_1m_1 + \ldots a_km_k \in M$. Como $\{m_1, \ldots, m_k\}$ es generador de M, tenemos que $M = Im(\psi)$. Es decir, ψ es un morfismo sobreyectivo. □

Corolario 1.19.
Si M es un A-módulo libre finitamente generado, entonces es isomorfo a A^k, con $k \in \mathbb{N}$.

Demostración. Basta ver que el morfismo construido en 1.18 es también inyectivo: si dos elementos $(a_1, \ldots, a_k)$, $(b_1, \ldots, b_k) \in A^k$ tienen la misma imagen por ψ, entonces $\psi(a_1 - b_1, \ldots, a_k - b_k) = 0$. Es decir:

$$(a_1 - b_1)m_1 + (a_2 - b_2)m_2 + \cdots + (a_k - b_k)m_k = 0.$$

Sin embargo, al ser M libre, el conjunto de generadores $\{m_1, \ldots, m_k\}$ es linealmente independiente, por lo que deducimos que $a_i - b_i = 0 \Rightarrow a_i = b_i$ para todo i, y tenemos la inyectividad. □

Definición 1.20.
Decimos que un módulo finitamente generado M es finitamente presentado (o que es de presentación finita), si, dado un conjunto generador de M, $\{m_1, \ldots, m_k\}$ de tamaño k, existe un morfismo sobreyectivo:

$$\psi : A^k \to M$$

tal que $\ker(\psi)$ es finitamente generado.
Veamos que significa esto: La aplicación ψ envía elementos de A en el elemento de M que se puede descomponer como suma de esos elementos multiplicados por los generadores. En $\ker(\psi)$ habrá elementos de la forma $(a_1, \ldots, a_k)$, tales que $a_1m_1 + \cdots + a_km_k = 0$.
Si este núcleo es finitamente generado, existe una cantidad finita (por ejemplo, n) de estas relaciones (y por tanto, de las k-úplas) que generan el resto. Esto

significa que podemos representar el módulo de la forma siguiente:

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{k,1} & \cdots & a_{k,n} \end{pmatrix}$$

Donde cada columna son los coeficientes de una relación del conjunto generador de $\ker(\psi)$. Esta matriz se denomina *matriz de presentación* del módulo M.

Los módulos poseen ciertas propiedades según las características del anillo base. Como ya hemos mencionado, los módulos sobre cuerpos dan lugar a los ya conocidos $\mathbb{K}$-espacios vectoriales. Nos centraremos ahora en los Dominios de Ideales Principales, y en los módulos finitamente generados sobre los mismos. Recordamos las siguientes definiciones:

Definición 1.21 (Dominio de Factorización Única)**.**
Decimos que un anillo Conmutativo A es un Dominio de Factorización Única si todo elemento $x \in A$ verifica:

$$x = u \cdot i_1 \cdots i_n \qquad n \geq 0, u \in A^{\times}, i_1 \cdots i_n \text{ irreducibles}$$

y de forma que esta factorización es única si no se puede factorizar ninguna unidad distinta de e_A de los i_k.

Definición 1.22 (Dominio de Ideales Principales)**.**
Un Dominio de Ideales Principales , abreviado DIP, es un anillo conmutativo, sin divisores de 0, en el que todo ideal es principal (es decir, está generado por un único elemento).

Algunos ejemplos de DIPs son:

- $\mathbb{Z}$. En $\mathbb{Z}$, si consideramos el ideal $\mathrm{I} = (p_1, \ldots, p_n, \ldots)$, es sencillo ver que $\mathrm{I} = (p)$, con $p = \gcd(p_1, \ldots, p_n, \ldots)$.
- $\mathbb{K}[\mathrm{X}]$, los polinomios con coeficientes en un cuerpo $\mathbb{K}$.

En ambos casos, la identidad de Bézout y la existencia de máximo común divisor permiten hallar el generador único del ideal. Ahora que tenemos definidos los DIPs, podemos dar el siguiente resultado sobre módulos cíclicos:

Proposición 1.23.
Todo módulo cíclico $V = (m)$ sobre un DIP A es isomorfo al cociente $A/(a)$, donde $(a) = Ann_A(V)$.

Demostración. Sea V un módulo cíclico generado por m. Sea $\varphi : A \to V$ el homomorfismo dado por $\varphi(a) = am$. El núcleo de φ es precisamente $Ann_A(V)$, luego por el primer teorema de isomorfía, $A/Ann_A(V) \simeq V$. Por otra parte, como A es un DIP, el anulador de V estará generado por un único elemento $a \in A$, lo que completa la prueba. □

Un resultado importante que relaciona presentación finita y generación finita se puede encontrar en [8][Corollary 23.3]:

Proposición 1.24.
Si A es un DIP, todo módulo finitamente generado es también finitamente presentado.

En la referencia dada se ve que este resultado es cierto para anillos más generales que los DIPs: los llamados anillos noetherianos. Estos anillos los definiremos en el tercer capítulo de la memoria.

1.2. Forma Normal de Smith.

Tener una matriz con la que representar el módulo es un gran paso, pero el mismo módulo puede ser representado por matrices distintas. Con el fin de dar un cierto nivel de unicidad a estas representaciones, recordamos la llamada *Forma Normal de Smith*.

Definición 1.25.
Decimos que una matriz $m \times n$ está en *Forma Normal de Smith* si sus únicos elementos no nulos son los elementos diagonales $\alpha_{i,i}$ y además, $\alpha_{i,i} | \alpha_{i+1,i+1}$ para todo i.

Como hemos visto en el grado, las matrices con elementos en un Dominio de Ideales Principales tienen asignada una "única" *Forma Normal de Smith* (los elementos diagonales pueden diferir en productos por unidades del DIP,

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Matriz en forma normal de Smith, con elementos en $\mathbb{Z}$.

como se prueba en [1][Theorem 3.9]). Es decir, para toda matriz $A(m \times n)$ existen matrices invertibles $L(m \times m)$ y $R(n \times n)$ tal que el producto $S = L \cdot A \cdot R$ está en *Forma Normal de Smith*.
Esto da pie al siguiente teorema:

1.3. El teorema de estructura sobre DIPs.

Teorema 1.26 (Teorema de Estructura de Módulos f.g sobre DIPs)**.**
Sea M un módulo sobre A, un DIP. Entonces

$$M \cong A^r \oplus \bigoplus_i^n A/(a_i)$$

con $a_1|a_2|\cdots|a_n$.

El esquema de la prueba consiste en tomar la presentación matricial del módulo y llevarla a la forma de Smith. Como las matrices por las que multiplicamos en este proceso son invertibles, tendremos isomorfismo entre ambas expresiones. La matriz final tendrá r filas nulas, correspondientes a la parte A^r de la expresión superior, y n filas con un unico elemento no nulo, situado en la diagonal principal. Como cada elemento será divisor del elemento de la fila siguiente, cada una de estas filas corresponderá a un $A/(a_i)$, con la condición de divisibilidad antes mencionada.
Nota: Las operaciones admisibles para llevar a una matriz a su forma normal de Smith se denominan operaciones elementales. Cada una de estas operaciones tienen asociada una matriz. Multiplicar por la izquierda la matriz original por una de estas matrices corresponderá a realizar la operación en cuestión por filas, mientras que multiplicar por la derecha realizará la operación en cuestión a las columnas. Las operaciones elementales son las siguientes:

Operación A Podemos permutar filas/columnas entre sí. La matriz que permuta las filas i y j es:

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix},$$

que es la matriz identidad con las filas i y j intercambiadas.
Operación B Podemos sumar múltiplos de una fila/columna a otra. La matriz correspondiente es:

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & m & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix},$$

la matriz identidad con la fila i sumada m veces a la fila j.
Operación C Podemos multiplicar una fila/columna por un elemento de $A^\times$. Su matriz asociada será, siguiendo el mismo proceso de las operaciones anteriores:

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & m & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix},$$

donde el elemento m es una unidad de $A^\times$.

1.4. Aplicaciones.

El teorema 1.26, aplicado a los módulos sobre $\mathbb{Z}$, da lugar a dos resultados importantes vistos en el grado:

Teorema de Estructura de Grupos Abelianos Finitamente Generados.
Todo grupo abeliano finitamente generado G es isomorfo a:

$$\mathbb{Z}^{\oplus n} \oplus \mathbb{Z}/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_k), \qquad n_1 | \cdots | n_k$$

con $n, n_1, \cdots, n_k$ enteros dependientes del propio G.

Teorema de clasificación de endomorfismos en espacios vectoriales de dimensión finita.
Sea V un $\mathbb{K}$-espacio vectorial de dimensión $n \geq 1$. Un endomorfismo en V es una aplicación lineal $\phi : V \to V$. Dada una base $u = \{u_1, \ldots, u_n\}$ de V, esta aplicación tendrá una representación matricial dada por la matriz B, de forma que $\phi(u) = Bu$.
El objetivo es encontrar una base adecuada para la cual la matriz de la aplicación tenga una forma lo más diagonal posible. Para ello consideramos el *polinomio característico* de la matriz B, $f(\lambda) = \lambda I - B$, siendo λ una indeterminada. En el caso en el que dicho polinomio tenga todas sus raíces en $\mathbb{K}$, se puede escribir

$$f(\lambda) = \prod_{i=1}^{m} (\lambda - \lambda_i)^{e_i}.$$

Se puede dotar a V de estructura de $\mathbb{K}[\lambda]$-módulo de torsión. Aplicando el teorema de estructura, deducimos que V se puede descomponer como suma directa de los sumandos cíclicos $\mathbb{K}[\lambda]w_i$, donde el anulador de w_i es el elemento $Ann(w_i) = (\lambda - \lambda_i)^{e_i}$. Tomando la base $\{w_i, (\lambda - \lambda_i)w_i, \ldots, (\lambda - \lambda_i)^{e_i - 1} w_i\}$, la matriz de cada sumando es:

$$B_i = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix}.$$

Por lo tanto, podemos "pegar" todas estas bases y obtener la llamada forma canónica de Jordan del endomorfismo:

$$\begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_k \end{pmatrix}.$$

2. Los números p-ádicos

En lo posterior, p hará referencia a un número primo *fijo* sin determinar. A continuación describiremos los números p-ádicos y el anillo de enteros p-ádicos, la base del álgebra de Iwasawa.

2.1. La métrica p-ádica.

Los números p-ádicos, $\mathbb{Q}_p$ son una complección de los racionales, $\mathbb{Q}$, cuando se toma en cuenta la métrica especial dada por una norma que denominaremos $\|\cdot\|_p$, la norma p-ádica. No sólo se trata de una complección de $\mathbb{Q}$ diferente de los números reales, si no que al estar diferenciada por la elección del número primo p, tenemos que cada $\mathbb{Q}_p$ es una complección distinta.

Notemos que dados $m \in \mathbb{Z} \setminus \{0\}$ y p primo, podemos factorizar m de forma única como:

$$m = \pm p^n p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$$

donde $p, p_1 \ldots, p_r$ son primos distintos y $n, n_1 \ldots, n_r$ son los exponentes correspondientes a dichos primos al factorizar m, considerando $n \geq 0$ y $n_i > 0$ para $i \in \{1, \ldots, r\}$.

Definición 2.1.
Una **valoración** es una aplicación $v : A \to G \cup \{\infty\}$, dónde $(A, +, \cdot)$ es un anillo conmutativo unitario y $(G, +, <)$ es un grupo abeliano completamente ordenado, que cumple:

- $\forall x \in A$, $v(x) = \infty \Leftrightarrow x = 0$;
- $\forall x, y \in A$, $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \text{mín}\{v(x), v(y)\}$.

Definición 2.2.
Llamamos valoración p-ádica (sobre $\mathbb{Z}$) a la aplicación $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}_{>0}$ que

asigna a cada entero no nulo m el exponente del primo p en su factorización, es decir, el máximo natural n tal que p^n divide a m. Es decir:

$$\begin{array}{rccl} v_p: & \mathbb{Z} & \longrightarrow & \mathbb{N}\cup\{\infty\} \\ & n & \longmapsto & \begin{cases} \infty & n=0 \\ \text{máx}\{k\in\mathbb{N};\ p^k|n\} & n\neq 0 \end{cases} \end{array}$$

Proposición 2.3.
La valoración p-ádica es, de hecho, una valoración.

Demostración. La única de las 3 propiedades de las valoraciones que merece la pena comprobar es la última, y resulta bastante sencilla. Suponemos que $x, y \neq 0$. Podemos asumir sin pérdida de generalidad $v(x) = m \geq v(y) = n$, eso significa que $x = x_1 \cdot p^m$ e $y = y_1 \cdot p^n$. Factorizamos p^n en x y obtenemos:

$$x + y = p^m x_1 + p^n y_1 = p^n(p^{m-n}x_1 + y_1),$$

por lo que $v(x+y) \geq n = \text{mín}\{v(x), v(y)\}$, como queríamos probar. □

Extender el dominio de esta valoración a los racionales no nulos es un proceso sencillo, que se basa en que todo número racional se puede escribir como cociente de dos enteros coprimos:

Definición 2.4.
Sea q un racional no nulo, con $q = m/n$, con $\gcd(m, n) = 1$. Definimos la valoración p-ádica de q como:

$$v_p(q) = v_p(m) - v_p(n).$$

Es sencillo comprobar que v_p constituye una forma natural de extender la valoración p-ádica a los racionales, pues se construye mediante la segunda propiedad de las valoraciones.

Proposición 2.5.
La aplicación $\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}_{>0}$ dada por:

$$\|q\|_p := p^{-v_p(q)}, \qquad \|0\|_p := 0,$$

es una norma en $\mathbb{Q}$.

Demostración. Veamos que se cumplen todas las propiedades de una norma:

1. $\|u\|_p = 0$ *si y solo si* $u = 0$: Por definición, $||0||_p = 0$, y si existe $q \in \mathbb{Q} \setminus \{0\}$ tal que $||q||_p = 0$, entonces la factorización de q es de la forma $q = p^n(u/v)$, con $p^{-n} = 0$. Pero esto es absurdo, por lo que el único racional con norma p-ádica 0 es 0.

2. $\|q_1 q_2\|_p = \|q_1\|_p \|q_2\|_p$, $\forall q_1, q_2 \in \mathbb{Q}$: Si alguno de los dos factores es 0, el producto también lo es, y por 1) tenemos la igualdad. Suponemos ahora que ambos factores son distintos de 0. Podemos reescribir el producto de la forma siguiente:

$$q_1 \cdot q_2 = p^{n_1}(u_1/v_1) \cdot p^{n_2}(u_2/v_2) = p^{n_1+n_2}\left(\frac{u_1 u_2}{v_1 v_2}\right)$$

   Como ningún u_i o v_j tiene a p de factor, deducimos que $||q_1 q_2||_p = p^{-(n_1+n_2)}$. Por otra parte, de la factorización de q_1 y q_2 deducimos que sus normas son p^{-n_1} y p^{-n_2}, respectivamente. Por lo tanto el producto de las mismas será $p^{-n_1} \cdot p^{-n_2} = p^{-(n_1+n_2)}$, y tenemos la igualdad.
   Nota: Esto implica que también se da la igualdad: $v_p(q_1 q_2) = v_p(q_1) + v_p(q_2)$.

3. $\|q_1 + q_2\|_p \leq \|q_1\|_p + \|q_2\|_p$: Si q_1, q_2 o $q_1 + q_2$ son iguales a 0, el resultado es trivial. Suponemos que este no es el caso, y consideramos primero el caso en que tanto q_1 como q_2 son enteros. Entonces, suponemos sin pérdida de generalidad que $p^{n_1}|q_1$ y $p^{n_2}|q_2$, con $n_1 \geq n_2$. Se da por lo tanto la igualdad: $q_1 + q_2 = p^{n_2}\,(p^{n_2-n_1}q_2 + q_1) \Rightarrow p^{n_2}|(q_1 + q_2)$. Y por lo tanto:

$$\begin{aligned} v_p(q_1 + q_2) &\geq \text{mín}\{v_p(q_1), v_p(q_2)\} \\ p^{-v_p(q_1+q_2)} &\leq p^{-(\text{mín}\{v_p(q_1), v_p(q_2)\})} \\ \|q_1 + q_2\|_p &\leq \text{máx}\{\|q_1\|_p, \|q_2\|_p\} \\ &\leq \|q_1\|_p + \|q_2\|_p. \end{aligned}$$

   Suponemos ahora que $q_1 = a/b$ y $q_2 = c/d$, con $a, b, c, d \in \mathbb{Z}$. Tenemos

entonces:

$$\begin{aligned} v_p\left(\frac{a}{b}+\frac{c}{d}\right) &= v_p\left(\frac{ad+cb}{bd}\right) = v_p\left(ad+cb\right) - v_p\left(bd\right) \\ &\geq \text{mín}\{v_p(ad), v_p(cb)\} - (v_p(b)+v_p(d)) \\ &= \text{mín}\{v_p(a)+v_p(d), v_p(c)+v_p(b)\} - (v_p(b)+v_p(d)) \\ &= \text{mín}\{v_p(a)-v_p(b), v_p(c)-v_p(d)\} \\ &= \text{mín}\{v_p\left(\frac{a}{b}\right), v_p\left(\frac{c}{d}\right)\} \end{aligned}$$

Y por lo tanto:

$$\begin{aligned} \|q_1+q_2\|_p = p^{-v_p\left(\frac{a}{b}+\frac{c}{d}\right)} &\leq p^{-\text{mín}\{v_p\left(\frac{a}{b}\right), v_p\left(\frac{c}{d}\right)\}} \\ &= \text{máx}\{\|q_1\|_p, \|q_2\|_p\} \\ &\leq \|q_1\|_p + \|q_2\|_p. \end{aligned}$$

□

Llamamos métrica p-ádica a la distancia inducida por esta norma;

$$d_p(u,v) = \|u-v\|_p.$$

2.2. Series p-ádicas.

Definición 2.6.
Dado un número primo p, denominamos series p-ádicas a las series:

$$s = \sum_{i=k}^{\infty} q_i p^i$$

en la cuál k es un entero y q_i es 0 o un racional no negativo con denominador no divisible por p.

Una serie p-ádica es *normalizada* si todos los coeficientes q_i son enteros menores que p o 0.

Dada una serie p-ádica $s = \sum_{i=k}^{\infty} q_i p^i$, denotamos expansión p-aria de s a la expresión: $\ldots q_n q_{n-1} \ldots q_1 q_0 . q_{-1} q_{-2} \ldots q_{k+1} q_k$, dónde el punto juega un

papel análogo al del separador decimal. (Si $k \geq 0$, denotamos $q_i = 0$ para todo $i < k$ y no se escribe el punto ni los q_j con $j < 0$).

Dos series p-ádicas son *equivalentes* si existe N tal que, $\forall n > N$, la diferencia de sus sumas parciales hasta n es igual a 0 o tiene valoración p-ádica superior a n.

Veamos ahora que cada serie p-ádica es equivalente a tan sólo una serie normalizada. En particular una serie normalizada no es equivalente a más series normalizadas que ella misma. Es decir, las series normalizadas son representantes canónicos de las clases de equivalencia. Para probarlo nos ayudamos del siguiente lema:

Lema 2.7.
Todo número racional q se puede escribir de forma única como:

$$q = ap^{v_p(q)} + r,$$

donde a es un entero con $0 < a < p$ y $v_p(r) > v_p(q)$.

Demostración. Ya hemos visto que podemos escribir $q = p^{v_p(q)} \frac{m}{n}$, donde m y n son enteros, coprimos y no divisibles por p. Por el Lema de Bézout, existen enteros a y b, con $0 \leq a < p$, tales que $m = an + bp$, es decir:

$$\frac{m}{n} = a + p\frac{b}{n} \Rightarrow q = p^{v_p(q)}\frac{m}{n} = ap^{v_p(q)} + p^{v_p(q)+1}\frac{b}{n},$$

que es la representación que queremos (nótese que si se diese $a = 0$, entonces m sería múltiplo de p, lo cual es absurdo). La unicidad se obtiene al considerar que la diferencia de dos representaciones debe ser igual a 0, luego:

$$0 = (a - a')p^{v_p(q)} + (r - r') = p^{v_p(q)}((a - a') + p(s - s')).$$

La segunda igualdad se justifica al ser r y r', (y por lo tanto también su diferencia), de valoración p-ádica estrictamente mayor que la de q. Entonces, $(s - s')$ es de valoración mayor o igual que 0, lo que permite sustituirlo por c/d, siendo d coprimo con p. Multiplicando la ecuación por p, obtenemos: $0 = (a - a')d + pc$. Por un lado $d \not| p$, y por otro $|a - a'| < p$, luego la única solución es $c = a - a' = 0$, y deducimos que $a = a'$ y $r = r'$. □

Proposición 2.8.
Toda serie p-ádica es equivalente a exactamente una serie normalizada.

Demostración. Sea $\sum_{i=k}^{\infty} q_i p^i$ una serie p-ádica. En primer lugar, esta serie es equivalente a otra cuyo término inicial es de valoración 0. Esto es sencillo de probar: En primer lugar, inicializamos la serie (es decir, escogemos el primer índice k) de forma que q_k no sea nulo. Si $v_p(q_k) = 0$, ya hemos terminado. Si no, llamamos l a la valoración de q_k, y escribimos $q_k = p^l s_k$, y realizamos las sustituciones: $q_k \to 0$ y $q_{k+l} \to q_{k+l} + s_k$. Repitiendo este proceso obtendremos o bien la serie 0 o bien una con término inicial de valoración 0.
Ahora, partiendo de esta nueva serie, tomamos el primer coeficiente q_i no nulo y que no sea un entero de $[1, \dots, p-1]$. Por el lema anterior, lo podemos escribir en la forma: $q_i = a_i + p s_i$. Realizamos las sustituciones $q_i \to a_i$, $q_{i+1} \to q_{i+1} + s_i$. Iterando este proceso obtenemos la serie normalizada que buscamos. La unicidad es consecuencia de que la única serie normalizada equivalente a 0 es la serie nula. □

Proposición 2.9.
Toda serie p-ádica normalizada converge en la norma $\|\cdot\|_p$.

Demostración. Sea $s = \sum_{i=k}^{\infty} q_i p^i$ una serie p-ádica normalizada. Es decir, $0 \leq q_i < p$ para todo $i > k$. Consideramos la sucesión de sumas parciales $\{s_m\} = \{\sum_{i=k}^{m} q_i p^i\}$. La norma p-ádica de la diferencia de dos de estas sumas parciales consecutivas es:

$$\|s_m - s_{m-1}\|_p = \|\sum_{i=k}^{m} q_i p^i - \sum_{i=k}^{m-1} q_i p^i\|_p = \|q_m p^m\|_p = 1/p^m$$

Sabemos que s se puede escribir como la suma telescópica

$$s = \sum_{i=k}^{\infty} (s_i - s_{i-1}),$$

considerando $s_{k-1} = 0$. Por lo tanto, tomando normas y aplicando la desigualdad triangular:

$$\|s\|_p = \|\sum_{i=k}^{\infty} (s_i - s_{i-1})\|_p \leq \sum_{i=k}^{\infty} \|(s_i - s_{i-1})\|_p =$$
$$= \sum_{i=k}^{\infty} \frac{1}{p^i} = \frac{p^{1-k}}{p-1} < \infty.$$

□

Ejemplo 2.10.
Es un hecho conocido que bajo la métrica euclídea, la serie geométrica $\sum_{i=0}^{\infty} t^i$ converge al valor $\frac{1}{1-t}$ si y sólo si $|t| < 1$, y diverge en caso contrario. Ahora bien, si tomamos $t = p$, nos encontramos con la serie normalizada con todos los coeficientes idénticos e iguales a 1. Como hemos probado, esta serie converge en la norma $\|\cdot\|_p$, y es la serie p-ádica normalizada correspondiente al número racional $1/(1-p)$.

2.3. El cuerpo de los números p-ádicos.

Cuando consideramos las sucesiones de Cauchy en $\mathbb{Q}$ bajo la norma p-ádica, ocurre algo notable: sea $(r_0, r_1, \dots)$ una sucesión de Cauchy para $\|\cdot\|_p$, esto es, para cada $n > 0$ existe un N tal que si $k, m > N$, entonces $\|r_k - r_m\|_p < p^{-n}$. Es decir, existen puntos fijos a partir de los cuales las expansiones p-arias de los elementos de la serie son idénticas "de derecha a izquierda".

Al completar $\mathbb{Q}$ en base a $\|\cdot\|_p$, lo que hacemos es tomar todos los límites de las sucesiones de Cauchy. Estos límites poseen una expresión p-aria bien definida; ya sea esta finita o infinita; gracias a que, como mencionábamos antes, todos los elementos de las sucesiones de Cauchy a partir de cierto índice n_i coinciden en todos sus coeficientes de potencias con exponentes menores o iguales que i.

Establecidas las series p-ádicas y la norma p-ádica, pasamos a definir los números p-ádicos de las siguientes dos formas:

Definición 2.11 ($\mathbb{Q}_p$, primera definición.)**.**
Los números p-ádicos, $\mathbb{Q}_p$, se definen como el conjunto de las clases de equivalencia de las series p-ádicas, o, lo que es lo mismo, las series p-ádicas normalizadas. Dado un número racional q, la expansión p-ádica de q es la expansión p-ádica de la serie normalizada asociada a q.

Definición 2.12 ($\mathbb{Q}_p$, segunda definición.)**.**
$\mathbb{Q}_p$ denota la complección de los números racionales, $\mathbb{Q}$, respecto de la norma p-ádica, $\|\cdot\|_p$.

Teorema 2.13.
Las dos definiciones anteriores son equivalentes.

Demostración. Como hemos visto, toda serie normalizada converge en la norma $\|\cdot\|_p$, por lo que es un representante de algún elemento de la complección de $\mathbb{Q}$ para dicha norma. Asimismo, dada una sucesión de números racionales $\{y_n\}_{n=1}^{\infty}$ cuya norma p-ádica converja, podemos considerar la expansión p-ádica de cada elemento, y por la condición de Cauchy, deducimos que el límite también es una serie normalizada. Esto prueba la equivalencia de ambas definiciones. □

Proposición 2.14.
$\mathbb{Q}_p$ posee estructura de cuerpo, y $\mathbb{Q}$ es un subcuerpo suyo.

Demostración. Sea $s \in \mathbb{Q}_p \setminus \{0\}$, $s = \sum_{i=k}^{\infty} s_i p^i$. Supongamos que $k \neq 0$. Entonces, si s es invertible, y su inverso es r, tenemos que:

$$\begin{aligned} s \cdot r = 1 \Rightarrow \|s \cdot r\|_p = 1 \Rightarrow \|s\|_p^{-1} = \|r\|_p \\ \Rightarrow (s \cdot p^{-k}) \cdot (p^k \cdot r) = 1 \end{aligned}$$

Es decir, la invertibilidad de s es equivalente a la de $s \cdot p^{-k}$, elemento cuya expansión p-ádica comienza en 0. Así pues, podemos suponer sin pérdida de generalidad que s es un elemento de $\mathbb{Q}_p$ de norma 1, por lo que su expansión p-ádica es de la forma $\sum_{i=0}^{\infty} s_i p^i$. Sea $r \in \mathbb{Q}_p$, $r = \sum_{i=0}^{\infty} r_i p^i$.

$$\begin{aligned} s \cdot r = 1 \Leftrightarrow \left(\sum_{i=0}^{\infty} s_i p^i\right) \cdot \left(\sum_{j=0}^{\infty} r_j p^j\right) = 1 \\ \sum_{\substack{i+j=0 \\ i,j \geq 0}}^{\infty} s_i r_j p^{i+j} = 1 \end{aligned}$$

La serie anterior no está normalizada, luego al despejar los términos r_j hay que tener en cuenta los resultados de operaciones anteriores. Las ecuaciones

resultantes son:

$$\begin{aligned} s_0 r_0 = 1 + k_0 p \equiv 1 \quad \text{mód } p \\ s_1 r_0 + s_0 r_1 = k_0 + k_1 p \equiv k_0 \quad \text{mód } p \\ s_2 r_0 + s_1 r_1 + s_0 r_2 = k_1 + k_2 p \equiv k_1 \quad \text{mód } p \\ \sum_{i=0}^{n} s_{n-i} r_i = k_{n-1} + k_n p \equiv k_{n-1} \quad \text{mód } p \end{aligned}$$

Los valores r_j se despejan de forma inductiva, obteniendo en su cálculo el valor k_{j-1}. Como todas estas ecuaciones de una incógnita en congruencias tienen solución en $\mathbb{Z}/p\mathbb{Z}$, el elemento r es sin duda una serie normalizada, y constituye el inverso de s. Por la arbitrariedad de s, deducimos que todo elemento no nulo de $\mathbb{Q}_p$ es invertible, por lo que $\mathbb{Q}_p$ es un cuerpo. Para la segunda afirmación, basta con observar que $\mathbb{Q} \subset \mathbb{Q}_p$: si $q \in \mathbb{Q}$, entonces consideramos la sucesión constante $(q)_{n=1}^{\infty}$. Es trivial ver que converge en la norma $\|\cdot\|_p$ y que el límite es q, por lo que $q \in \mathbb{Q}_p$. Como sabemos que $\mathbb{Q}$ es un cuerpo, deducimos que es subcuerpo de $\mathbb{Q}_p$. □

Veamos ahora como se relaciona un número racional con su serie p-ádica normalizada correspondiente.

Tomemos $r \in \mathbb{Q}$. Factorizamos r obteniendo $r = p^{n_r} \cdot a/b$, a y b coprimos. Consideraremos la serie correspondiente a a/b. Sea $\sum_{i=k}^{\infty} s_i p^i$ dicha serie. Consideramos $a/b = s_0 + s_1 \cdot p \cdots$ y pasamos el primer término a la izquierda para obtener:$a/b - s_0 = p(s_1 + s_2 \cdot p \cdots)$.
Al multiplicar por b, obtenemos: $a - bs_0 = p(\cdots)$. Así, s_0 será el entero menor que p (o 0) tal que $a - bs_0$ es múltiplo de p. Una vez tenemos s_0, computamos $(a/b - s_0)/p$ y repetimos el proceso. Eventualmente encontraremos un ciclo y podremos terminar el proceso. El último paso es reconsiderar p^{n_r} y modificar la serie como corresponda, añadiendo n_r ceros si $n_r > 0$ o añadiendo la separación decimal n_r posiciones a la izquierda si $n_r < 0$.

Veamos un ejemplo práctico: Calculemos la expresión 5-ádica de 20/7:

- $20/7 = 5 \cdot 4/7$
- $4/7 - a_0 = 5k \Rightarrow \quad 4 - 7a_0 = 5k' \Rightarrow a_0 = 2,\ k = -2/7$
- $-2/7 - a_1 = 5k \Rightarrow -2 - 7a_1 = 5k' \Rightarrow a_1 = 4,\ k = -6/7$

- $-6/7 - a_2 = 5k \Rightarrow -6 - 7a_2 = 5k' \Rightarrow a_2 = 2,\ k = -4/7$
- $-4/7 - a_3 = 5k \Rightarrow -4 - 7a_3 = 5k' \Rightarrow a_3 = 3,\ k = -5/7$
- $-5/7 - a_4 = 5k \Rightarrow -5 - 7a_4 = 5k' \Rightarrow a_4 = 0,\ k = -1/7$
- $-1/7 - a_5 = 5k \Rightarrow -1 - 7a_5 = 5k' \Rightarrow a_5 = 2,\ k = -3/7$
- $-3/7 - a_6 = 5k \Rightarrow -3 - 7a_6 = 5k' \Rightarrow a_6 = 1,\ k = -2/7$
- Como volvemos a obtener $k - 2/7$, el ciclo llega a su fin. Tenemos que: $4/7 = \ldots\overline{1203242}_5$ y por tanto $20/7 = \cdots\overline{1203242}0_5$. (La notación $\ldots\overline{x}y$ denota periodicidad de x hacia la izquierda, de forma simétrica a la notación habitual.)

Para calcular la expansión 5-ádica de $4/35$, en el paso final habríamos obtenido: $4/35 = \cdots\overline{120324}.2_5$, pues la separación decimal se movería una posición hacia la izquierda.

La norma p-ádica en $\mathbb{Q}_p$ se define de forma natural: La norma de un elemento que es límite de una sucesión de Cauchy (bajo la norma $\|\cdot\|_p$) de racionales será el limite de la sucesión de normas correspondiente.

2.4. Los enteros p-ádicos.

Definición 2.15.
Si $s = \sum_{i=k}^{\infty} q_i p^i \in \mathbb{Q}_p$, con $k \geq 0$, decimos que s es un *entero p-ádico*, y el conjunto de enteros p-ádicos se denota por $\mathbb{Z}_p$. El conjunto $\mathbb{Z}_p$, junto con la suma y el producto clásicos, posee estructura de anillo conmutativo.

Lema 2.16.
Los enteros p-ádicos son exactamente los elementos de $\mathbb{Q}_p$ que tienen norma p-ádica $\|\cdot\|_p$ menor o igual a 1.

Demostración.
Sea $a \in \mathbb{Z}_p$. Entonces, al no tener decimales en su expansión p-ádica, su valoración p-ádica es como mínimo 0, luego: $\|a\|_p = p^{-v_p(a)} \leq p^0 = 1$.
En el otro sentido, si $\|a\|_p \leq 1$, $p^{-v_p(a)} \leq p^0 \Rightarrow v_p(a) \geq 0$. Es decir, en la expansión p-ádica de a no hay ningún decimal, luego $a \in \mathbb{Z}_p$. □

Definición 2.17.
Decimos que un anillo conmutativo A es local si cumple una de las siguientes condiciones equivalentes:

- A posee un único ideal maximal $\mathfrak{m}$.
- $1 \neq 0$ y si $x, y \in A$ no son unidades, $x + y$ tampoco es una unidad. (El conjunto de no unidades es un ideal y, de hecho, es el maximal.)
- $1 \neq 0$ y $\forall x \in A$, o bien x o bien $1 - x$ es una unidad.

Denotaremos $(A, \mathfrak{m})$ al anillo local.

Proposición 2.18.
$x \in \mathbb{Z}_p$ es una unidad si y solo si $\|x\|_p = 1$.

Demostración. Veamos ambas implicaciones:

- Sea x una unidad en $\mathbb{Z}_p$. Entonces $x^{-1} \in \mathbb{Z}_p$ y, por el Lema anterior, $\|(x)\|_p \leq 1$ y $\|(x^{-1})\|_p \leq 1$. Como $x \cdot x^{-1} = 1$, entonces por las propiedades de la norma: $\|x \cdot x^{-1}\| = \|1\| = 1$, lo cual sólo es cierto si $\|x\| = \|x^{-1}\| = 1$.
- Sea ahora $x \in \mathbb{Z}_p$ tal que $\|x\| = 1$. Por las propiedades de la norma, $\|x^{-1}\| = 1$, y por el Lema anterior, $x^{-1} \in \mathbb{Z}_p$. Concluimos que x es una unidad. □

Definición 2.19.
Denotamos por $\mathfrak{p}$ al ideal generado por p en $\mathbb{Z}_p$, es decir, a los elementos de $\mathbb{Z}_p \setminus \mathbb{Z}_p^{\times}$.

Tenemos el corolario siguiente:

Corolario 2.20.
$(\mathbb{Z}_p, \mathfrak{p})$ es un anillo local.

Demostración. Se deduce de la segunda caracterización dada en 2.17. □

Nota: Las unidades de $\mathbb{Z}_p$ se pueden identificar como aquellos elementos cuya expansión p-ádica tiene un 0 como elemento de las "unidades". Un ejemplo, para $p = 3$, son los elementos $\ldots\overline{0}10_3 = 10_3 = 3$ o $\ldots\overline{2}0_3 = -3$.
Por último, tenemos el siguiente resultado:

Proposición 2.21.
$\mathbb{Z}_p$ es un DIP.

Demostración. Veamos que los únicos ideales propios posibles son de la forma $(\mathfrak{p}^n)$, con $n \in \mathbb{N}$.
Sea I un ideal. Si I posee un elemento q tal que $v_p(q) = n$, podemos factorizar p^n y escribir $q = up^n$, donde u es unidad de $\mathbb{Z}_p$. Esto implica que, multiplicando por u^{-1}, el elemento $p^n \in I$ y por tanto $\mathfrak{p}^n \subset I$. Ahora bien, esto se cumple para cada $q \in I$, y como $\mathfrak{p}^n \supset \mathfrak{p}^{n+1}$ para todo n, tenemos que:

$$I = \mathfrak{p}^{\text{mín}\{v_p(q)\}}, \qquad \text{cuando } q \in I,$$

donde la existencia del mínimo se debe a que las cadenas descendientes de números naturales acaban estabilizándose. □

3. Introducción al Álgebra de Iwasawa

3.1. Anillos de series formales en una variable

Repasamos primero la definición de Polinomio y de anillo de Polinomios:

Definición 3.1.
Un *polinomio* en el anillo A es una aplicación $P : \mathbb{N} \to A$ de soporte finito. Representamos cada polinomio como suma de los monomios conformados por el producto $P(m)T^m$, donde T es una indeterminada y m es menor o igual que el elemento más grande del soporte de P. Es decir:

$$P = P_0 + P_1T + P_2T^2 + \cdots + P_nT^n, \quad P_i = P(i) \in A,\ P_i = 0 \text{ si } i > n.$$

Definición 3.2 (Anillo de Polinomios)**.**
El *anillo de polinomios* de un anillo conmutativo A es el anillo formado por todos los polinomios en A. Se representa por $A[T]$. En él, la suma y el producto se definen de manera natural, teniendo en cuenta:

- La distributividad del producto en A sobre la suma.
- La regla de la potencia para T, es decir, $T^i \cdot T^j = T^{i+j}$. Al ser A anillo conmutativo, $A[T]$ también lo es, y sus elementos invertibles son únicamente las constantes invertibles en A.

Si en la definición de polinomio no exigimos que el soporte de la aplicación sea finito, obtenemos las llamadas **series formales**:

Definición 3.3.
Una *serie formal* en A es una aplicación $s : \mathbb{N} \to A$. Si denotamos $a_i := s(i),\ i \in \mathbb{N}$, tenemos que la representación de las series, de forma análoga al caso de los polinomios, es:

$$s = \sum_{i=0}^{\infty} a_iT^i.$$

Definición 3.4 (Anillo de Series formales)**.**
Sea A un anillo conmutativo. El *anillo de series formales* en T con coeficientes en A se denota por $A[[T]]$. La suma y el producto se definen de igual manera que para el anillo de polinomios $A[T]$, y $A[[T]]$ es conmutativo al serlo A.

Si bien $A[[T]]$ no es un cuerpo, pues el elemento T, por ejemplo, no es invertible, podemos categorizar los elementos que si poseen inverso de forma relativamente sencilla, como vemos en la siguiente proposición:

Proposición 3.5.
Los elementos invertibles de $A[[T]]$ son aquellos cuyo coeficiente independiente es invertible en A.

Demostración. Tenemos que comprobar que dada una serie $f = \sum_{i=0}^{\infty} f_i T^i$ en $A[[T]]$, podemos construir su inversa. Si existe esta serie, de la forma $g = \sum_{i=0}^{\infty} g_i T^i$, tenemos que $f \cdot g = 1$. Expandimos el producto:

$$\begin{aligned} f \cdot g &= \left(\sum_{i=0}^{\infty} f_i T^i \right) \left(\sum_{j=0}^{\infty} g_j T^j \right) \\ &= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} f_i g_j T^{i+j} = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} f_i g_{k-i} \right) T^k \end{aligned}$$

Comparando con la ecuación $fg = 1$, vemos que esta igualdad se satisface si y solo si $f_0 g_0 = 1$ y $\sum_{i=0}^{k} f_i g_{k-i} = 0$ para todo $k \geq 1$. Si f_0 no es invertible en A, la primera igualdad no se cumple, luego $f_0 \in A^{\times}$ es una condición necesaria. Ahora bien, si f_0 es invertible, con $f_0^{-1} = g_0$, el resto de ecuaciones se pueden escribir como:

$$\begin{aligned} f_0 g_k &= -\sum_{i=1}^{k} f_i g_{k-i} \\ g_k &= -g_0 \cdot \sum_{i=1}^{k} f_i g_{k-i} \end{aligned}$$

Y podemos despejar uno a uno todos los coeficientes de g. Por lo tanto la condición impuesta es suficiente y g es la inversa de f en $A[[T]]$. □

Proposición 3.6.
Si $(A, \mathfrak{m})$ es un anillo local, $(A[[T]], (\mathfrak{m}, T))$ es un anillo local.

Demostración. Sea $f = a_0 + a_1 T + \cdots + a_n T^n + \cdots$ un elemento de $A[[T]]$ que no sea una unidad. Entonces, por 3,5, a_0 no es una unidad de A. Como

A es local, $1 - a_0$ es unidad. Pero entonces:

$$1 - f = (1 - a_0) + a_1 T + \cdots + a_n T^n + \cdots ,$$

que es una unidad de $A[[T]]$ (Por 3.5). Es decir, $A[[T]]$ es local. De todo lo expuesto deducimos la siguiente cadena de implicaciones:

$$f \notin A[[T]]^\times \Leftrightarrow a_0 \notin A^\times \Leftrightarrow a_0 \in \mathfrak{m} \Leftrightarrow f \in (\mathfrak{m}, T).$$

Por lo tanto, $(\mathfrak{m}, T)$ es el conjunto de no unidades de $A[[T]]$, es decir, su ideal maximal. □

Un caso particular de [4, Corolario 2.2], del cual no presentaremos la prueba, nos permite dar el siguiente resultado:

Proposición 3.7.
Si un anillo A es un DIP, entonces el anillo de series $A[[T]]$ es un DFU (Dominio de Factorización Única), pero no es necesariamente un DIP.

3.2. Preparación p-ádica de Weierstrass

En esta sección se probarán dos de los resultados que más usaremos, la división p-ádica y el teorema de preparación de Weierstrass, en su forma sobre el Álgebra de Iwasawa.

Definición 3.8.
Llamamos **Álgebra de Iwasawa** al anillo de series formales con coeficientes en los enteros p-ádicos. De ahora en adelante la denotaremos:

$$\Lambda = \mathbb{Z}_p[[T]]$$

A continuación prepararemos una serie de resultados que nos permitirán familiarizarnos con los elementos de Λ y entenderlos mejor.

De la Proposición 3.5 deducimos:

Lema 3.9.
Las unidades de Λ son los elementos cuyo coeficiente independiente pertenece a las unidades de $\mathbb{Z}_p$.

Y de 3.6 tenemos que:

Corolario 3.10.
Λ es un anillo local.

Ahora pasamos a probar el primero de los objetivos de esta sección, que emplearemos para identificar y categorizar elementos de Λ, la división p-ádica de Weierstrass. Para ello, definimos primero el siguiente operador:

Definición 3.11.
Se define el operador de traslación de orden $n \geq 0$, $\tau = \tau_n : \Lambda \to \Lambda$ como:

$$\tau\left(\sum_{i=0}^{\infty} b_i T^i\right) = \sum_{i=n}^{\infty} b_i T^{i-n}$$

De ahora en adelante usaremos siempre la notación τ para referirnos a τ_n.

Lema 3.12.
El operador τ es $\mathbb{Z}_p$-lineal y cumple las siguientes propiedades:

a) $\tau(T^n h) = h, \ \forall h \in \Lambda$.

b) $\tau(h) = 0 \iff h \in \mathbb{Z}_p[T]$, con $\deg(h) \leq n-1$.

Demostración. Primero probamos la $\mathbb{Z}_p$-linealidad. Si $\lambda, \mu \in \mathbb{Z}_p$:

$$\begin{aligned}
\tau(\lambda h + \mu g) &= \tau(\lambda \sum_{i=0}^{\infty} h_i T^i + \mu \sum_{i=0}^{\infty} g_i T^i) \\
&= \tau(\sum_{i=0}^{\infty} \lambda h_i T^i + \sum_{i=0}^{\infty} \mu g_i T^i) = \tau(\sum_{i=0}^{\infty} (\lambda h_i + \mu g_i) T^i) \\
&= \sum_{i=n}^{\infty} (\lambda h_i + \mu g_i) T^{i-n} = \sum_{i=n}^{\infty} (\lambda h_i T^{i-n}) + \sum_{i=n}^{\infty} (\mu g_i T^{i-n}) \\
&= (\lambda \sum_{i=n}^{\infty} h_i T^{i-n} + \mu \sum_{i=n}^{\infty} g_i T^{i-n}) = \lambda \tau(h) + \mu \tau(g).
\end{aligned}$$

Propiedad a): Escribimos $h = \sum_{i=0}^{\infty} h_i T^i$, por lo que:

$$\begin{aligned}\tau(T^n h) &= \tau(\sum_{i=0}^{\infty} h_i T^i T^n) = \tau(\sum_{i=0}^{\infty} h_i T^{i+n}) \\ &= \tau(\sum_{j=n}^{\infty} h_{j-n} T^j) = \tau(\sum_{j=0}^{\infty} \tilde{h}_j T^j) \\ &= \sum_{j=n}^{\infty} \tilde{h}_j T^{j-n} = \sum_{i=0}^{\infty} h_i T^i = h.\end{aligned}$$

Propiedad b): Si $\tau(h) = 0$, entonces por definición $h_i = 0$ para todo $i \geq n$, por lo que h es un polinomio de grado estrictamente menor que n. Razonando al revés, si h es un polinomio de grado inferior a n, entonces $h_i = 0$ para todo $i \geq n$, y por lo tanto $\tau(h) = 0$. □

Con el fin de suavizar la demostración de la división p-ádica, introducimos la siguiente notación: para $h, g \in \Lambda = \mathbb{Z}_p[[T]]$, la expresión $(\tau \circ h)^j \circ g$ se define como:

- $j = 0$: $(\tau \circ h)^0 \circ g = \tau(g)$.
- $j = 1$: $(\tau \circ h)^1 \circ g = \sum_{k=n}^{\infty} h_k (g)^{k-n}$.
- $j > 1$: $(\tau \circ h)^j \circ g = \tau(h((\tau \circ h)^{j-1} \circ g))$, el resultado de primero sustituir T por la expresión de $(\tau \circ h)^{j-1} \circ g$ en la expresión de h y aplicar el operador τ al resultado.

La prueba de la división p-ádica pasa por considerar una serie que posee una estructura de la forma $\sum_{j=0}^{\infty} (-1)^j p^j (\tau \circ h)^j \circ \tau(g)$. Que esta serie está bien definida es consecuencia de la aparición de p^j: considerando un $j > 0$ concreto, los términos a la derecha de p^j conforman una serie que pudiera tener términos en T^0, pero no inferiores. Multiplicar por p^j es equivalente a realizar el desplazamiento $T^k \to T^{k+j}$, lo que resulta en una serie cuya potencia más pequeña es, como mucho, T^j. Es decir, la diferencia de sumas parciales consecutivas de $\sum_{j=0}^{\infty} (-1)^j p^j (\tau \circ h)^j \circ \tau(g)$ es inferior a p^{-j} en norma $\| \cdot \|_p$, por lo que esta serie es convergente.

Proposición 3.13 (División p-ádica de Weierstrass)**.**
Sean $f, g \in \Lambda$. Supongamos que $f = a_0 + a_1 T + \cdots + a_n T^n + \cdots$, con $a_i \in \mathfrak{p}$ si $0 \leq i \leq n-1$, pero con $a_n \in \mathbb{Z}_p^\times$. Entonces, podemos escribir g de forma única como:

$$g = qf + r,$$

donde $q \in \Lambda$ y $r \in \mathbb{Z}_p[T]$ es un polinomio de grado a lo sumo $n-1$.

Demostración. Primero probaremos la unicidad. Supongamos que existen dos representaciones con cocientes Q_1 y Q_2, y restos r_1 y r_2. Restando las ecuaciones, obtenemos una nueva ecuación de la forma $0 = qf + r$. Si $q \neq 0$ o $r \neq 0$, reducimos mód p y podemos asumir que: o bien $p \nmid q$ o bien $p \nmid r$. Entonces, escribimos $q = \sum_{i=0}^{\infty} q_i T^i$. Despejando r, tenemos $r = -qf = -\sum_{i+j=0}^{i+j=n-1} a_i q_i T^i$, con $p | a_i \ \forall i$, por lo que $p|r$ y $p|qf$. Por hipótesis, $p \nmid f$. Esto implica que $p|q$ y tenemos una contradicción. Así, $q = r = 0$.

Veamos ahora la existencia. Para ello, podemos escribir:

$$f = pP + T^n U, \tag{1}$$

donde P es un polinomio de grado a lo sumo $n-1$ y

$$U = a_n + a_{n+1} T + \cdots = \tau(f).$$

Ya que $a_n \in \mathbb{Z}_p^\times$, U es una unidad en el anillo Λ. Denotaremos $\tilde{U} = \sum \tilde{u}_i T^i$ a su inverso. Sea

$$q := \frac{1}{U} \cdot \sum_{j=0}^{\infty} (-1)^j p^j \left(\tau \circ \frac{P}{U} \right)^j \circ \tau(g) = \tilde{U} \cdot \sum_{j=0}^{\infty} (-1)^j p^j \left(\tau \circ \frac{P}{U} \right)^j \circ \tau(g).$$

Definiendo $h := P/U = P\tilde{U} = \sum h_i T^i$, podemos escribir:

$$q = \sum_{i=0}^{\infty} \tilde{u}_i T^i \cdot \sum_{j=0}^{\infty} \left[(-1)^j p^j \cdot \left(\tau \circ \sum_{k=0}^{\infty} h_k T^k \right)^j \circ \left(\sum_{l=n}^{\infty} g_l T^{l-n} \right) \right]$$

Ya hemos visto que cada coeficiente q_i de q queda bien definido por la convergencia de la segunda serie. Ahora, multiplicando la ecuación 1 por q obtenemos:

$$qf = pqP + T^n qU,$$

Aplicando el operador τ en ambos lados de la igualdad, y teniendo en cuenta sus propiedades obtenemos:

$$\tau(qf) = p\tau\left(qP\right) + \tau\left(T^n qU\right) = p\tau\left(qP\right) + qU.$$

Y a su vez,

$$\begin{aligned} p\tau\left(qP\right) &= p\left(\tau \circ \frac{P}{U}\right) \circ \left(\sum_{j=0}^{\infty} (-1)^j p^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g)\right) = \\ &= -\sum_{j=0}^{\infty} (-1)^{j+1} p^{j+1} \left(\tau \circ \frac{P}{U}\right)^{j+1} \circ \tau(g) = \\ &= -\sum_{j=1}^{\infty} (-1)^j p^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g) = -(qU - \tau(g)) = \\ &= \tau(g) - qU. \end{aligned}$$

Es decir, $\tau(qf) = p\tau(qP) + qU = \tau(g) - qU + qU = \tau(g)$. Ahora bien, $\tau(qf - g) = \tau(qf) - \tau(g) = 0$. Por b), $qf - g = r$, con $r \in \mathbb{Z}_p[T]$, $\deg(r) \leq n-1$. Esto completa la prueba del lema. □

De ahora en adelante, nos referiremos a este último resultado como: "algoritmo de división". Si en la proposición anterior la condición que hemos impuesto a f sobre sus coeficientes es aplicada a un polinomio de grado exactamente n, tendremos lo que llamaremos *polinomio distinguido*:

Definición 3.14.
Decimos que un polinomio $P \in \mathbb{Z}_p[T]$ es *distinguido* si

$$P = T^n + a_{n-1}T^{n-1} \cdots + a_1 T + a_0,$$

con $a_i \in \mathfrak{p}$, $0 \leq i \leq n-1$.

El teorema siguiente es una consecuencia directa de algoritmo de división cuya formulación general se puede encontrar en [6, Página 115, Teorema 7.3]. En esta referencia se enuncia para anillos más generales que $\mathbb{Z}_p$, pero este caso es suficiente para el tema a tratar.

Teorema 3.15 (Teorema de preparación p-ádica de Weierstrass)**.**
Sea

$$f = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$$

tal que para algún $n \in \mathbb{N}$ se tenga que $a_i \in \mathfrak{p}$, $0 \leq a_i \leq n-1$, pero con $a_n \notin \mathfrak{p}$. (Es decir, $a_n \in \mathbb{Z}_p^{\times}$.) Entonces f se puede escribir de forma única como: $f = PU$, donde $U \in \Lambda$ es una unidad y P es un polinomio distinguido de grado n.

De forma más general, si f es una serie no nula, se puede escribir de forma única como:

$$f = p^{\mu} PU,$$

donde P y U son como hemos expresado antes y μ es un entero no negativo.

Demostración. Aplicamos la división p-ádica a $g = T^n$. Entonces, podemos escribir:

$$T^n = qf + r, \qquad \text{donde } \deg r \leq n-1$$

Como se cumple la congruencia

$$qf \equiv q(a_n T^n + \text{términos de mayor grado}) \mod p,$$

debe darse que $r \equiv 0 \mod p$. Luego $P = qf = T^n - r$ es un polinomio distinguido de grado n. Sea q_0 el término constante de q. Comparando los coeficientes de T^n, vemos que $1 \equiv q_0 a_n \mod p$. Luego $q_0 \in \mathbb{Z}_p^{\times}$, por lo que q es una unidad. Ahora, sea $U = 1/q$. Al dividir por q, vemos que $f = UP$, como deseábamos. Por otra parte, la unicidad probada en el lema anterior garantiza la unicidad de P y de U.
La generalización a series no nulas sin restricciones es consecuencia de factorizar en f la mayor potencia de p posible. □

Nota: Un lema que no probaremos, correspondiente con [6, Lema 7.5] nos indica que cuando f sea un polinomio, la unidad U resultante en la factorización también lo será.

3.3. Propiedades algebraicas del álgebra de Iwasawa.

Nuestra intención ahora es probar ciertas cualidades de Λ: que es un DFU, que es anillo noetheriano, y que su dimensión de Krull es igual a 2.

3.3.1. Factorización Única

Una prueba del siguiente resultado se puede encontrar en: [2][Página 182, Teorema 2.3].

Lema 3.16.
Sea A un anillo conmutativo. Si A es un DFU, A[T] también es un DFU.

Lema 3.17.
Si un polinomio distinguido P es irreducible en $\mathbb{Z}_p[T]$, entonces también es irreducible en Λ.

Demostración. Reducción al absurdo: Supongamos que P es un polinomio distinguido e irreducible en $\mathbb{Z}_p$ tal que $P = h_1 \cdot h_2$, $h_1, h_2 \in \Lambda^\times$. Por el Teorema de Preparación, $h_i = p^{\mu_i} P_i U_i$, con $P_i \in \mathbb{Z}_p[T]$. Es decir, $P = p^{\mu_1+\mu_2} P_1 P_2 U_1 U_2$. Por la unicidad de la descomposición, debemos tener que

$$\mu_1 + \mu_2 = 0, \quad U_1 U_2 = 1, \quad P = P_1 P_2,$$

pero esto es absurdo al ser P irreducible en $\mathbb{Z}_p[T]$. Luego P es también irreducible en Λ. □

Proposición 3.18.
Λ es un Dominio de Factorización Única (DFU).

Demostración. Sea $h \in \Lambda$. Por el Teorema de Preparación de Weierstrass (3.15), podemos descomponer h como: $h = p^m \cdot P \cdot U$ de forma única, con P

distinguido y U unidad de Λ. Ya poseemos dos de los factores, la unidad U y los elementos irreducibles p. Ahora bien, $P \in \mathbb{Z}_p[T]$, que es un DFU (3.16), luego $P = P_1 \cdot P_2 \cdots P_n$, todos ellos polinomios distinguidos e irreducibles. (De no ser distinguido algún factor, podríamos extraer de él una unidad distinta de 1 o un factor p, y reagrupando, la factorización de h perdería su unicidad, dándose el absurdo).
Deducimos que Λ es un DFU, cuyos elementos irreducibles son los polinomios distinguidos irreducibles y p.
Nota: También podemos usar 3.7 directamente, ya que $\mathbb{Z}_p$ es un DIP, lo cual hemos visto en 2.21. □

3.3.2. Noetherianidad.

Definición 3.19.
Decimos que un anillo A es noetheriano si toda cadena creciente de ideales estabiliza, es decir, si todas las cadenas $I_1 \subseteq I_2 \subseteq \cdots \subset I_n \subseteq \cdots$ cumplen que $I_n = I_{n+1} = \cdots$ para algún n (dependiente de la cadena considerada).

Ejemplo 3.20.
Los cuerpos son anillos noetherianos, pues sus únicos ideales son (0) y el total.

Ejemplo 3.21.
El anillo de enteros algebraicos (el conjunto de elementos de $\mathbb{C}$ que son raíz de algún polinomio mónico de coeficientes enteros) no es noetheriano. Por ejemplo, contiene a la cadena infinita

$$(2^{1/2}) \subset (2^{1/4}) \subset (2^{1/8}) \cdots \subset (2^{1/2^{j-1}}) \subset (2^{1/2^j}) \cdots ,$$

que nunca estabiliza. (Los generadores son las raíces reales de los polinomios $x^{(2^j)} - 2$).

Observemos que la condición de anillo noetheriano es una generalización de la de Dominio de Ideales Principales: pasamos de que todos los ideales estén generados por un único elemento a que todos estén generados por un conjunto finito de elementos. (El hecho de que esta condición es equivalente a la Noetherianidad puede verse en [3, p.115, 116; Th 5.7 & Th 5.8]).

El siguiente resultado no lo probaremos, pero nos será útil para probar que Λ es, en efecto, un anillo noetheriano. Una prueba del siguiente teorema se puede encontrar en [3, página 118].

Proposición 3.22 (**Teorema de la Base de Hilbert**)**.**
Sea A un anillo noetheriano. Entonces $A[T]$ es un anillo noetheriano.

Lema 3.23.
Sea I un ideal de Λ. Entonces existe un polinomio de grado mínimo en I.

Demostración. Si $h \in I$, aplicamos el Teorema de Preparación de Weierstrass (3.15) y escribimos $h = p^m \cdot P \cdot U$, donde U es invertible. Es decir, $p^m \cdot P \in I$. El elemento $p^m \cdot P$ es, por definición de P, un polinomio perteneciente a $\mathbb{Z}_p[T]$, luego su grado es finito. Considerando la aplicación $\phi : I \to \mathbb{N}$ definida por $\phi(h) = \deg P$, donde P es el polinomio distinguido resultante al aplicar el Teorema de Preparación a h, deducimos que $\text{ínf}\, \phi(I)$ se alcanza, por lo que $\phi^{-1}(\text{ínf}\, \phi(I)) \neq \emptyset$. Es decir, I posee al menos un elemento de grado mínimo. □

Proposición 3.24.
Λ es un anillo noetheriano.

Demostración. Notemos que $A = \mathbb{Z}_p$ es noetheriano, ya que es un DIP. Sea $f \in A[[T]]$, $f = \sum_{i=r}^{\infty} a_r T^r$. Decimos que f es de grado r y coeficiente a_r. Sea I un ideal en $A[[T]]$ y sea f_1 de grado mínimo en I. Supongamos que tenemos $f_1, \ldots, f_i$, con grados $d_1, \ldots, d_i$ y coeficientes $a_1, \ldots, a_i$. Escogemos f_{i+1} de forma que:

1. $f_{i+1} \in I$
2. $a_{i+1} \notin (a_1, \ldots, a_i)$
3. f_{i+1} es de grado mínimo.

Entonces el proceso de escoger nuevos elementos es finito, ya que de no serlo, tendríamos una cadena de ideales infinita $(a_1) \subset (a_1, a_2) \subset \cdots$ en A, lo cual es absurdo al ser A noetheriano.
Supongamos entonces que esta cadena se estabiliza en k, y veamos que

entonces $I = (f_1, \ldots, f_k)$. Sea $g = aT^d + \ldots$ un elemento de I de grado d y coeficiente a Entonces $a \in (a_1, \ldots, a_k)$. Se pueden dar dos casos:

Caso 1: $d \geq d_k$. Como $d_i \leq d_{i+1}$ para todo i, tenemos que $d \geq d_i$ para $i = 1, \ldots, k$. Ahora, $a = \sum_{i=1}^{k} c_{i0} a_i$, con $c_{i0} \in A$. Definimos:

$$g_0 = \sum_{i=1}^{k} c_{i0} T^{d-d_i} f_i$$

de manera que g_0 tiene grado d y coeficiente a, por lo que $g - g_0$ tiene grado superior a d. Definimos de igual forma $g_0, \ldots, g_r \in (f_0, \ldots, f_k)$ para que $g - \sum_{i=0}^{k} g_i$ tenga grado mayor que $d + r$. Sea b el coeficiente de $g - \sum_{i=0}^{k} g_i$. Por construcción, $b \in (a_1, \ldots, a_k)$, luego:

$$b = \sum_{i=1}^{k} c_{i,r+1} a_i$$

con $c_{i,r+1} \in A$. Definimos

$$g_{r+1} = \sum_{i=1}^{k} c_{i,r+1} X^{d+r+1-d_i} f_i$$

de forma que $g - \sum_{i=0}^{r+1} g_i$ tenga grado mayor que $d + r + 1$. Así

$$g = \sum_{r=0}^{\infty} g_r = \sum_{r=0}^{\infty} \sum_{i=1}^{k} c_{i,r+1} X^{d+r+1-d_i} f_i,$$

y al hacer la suma en orden inverso (lo cuál es aceptable al haber finitos terminos de la forma bX^j para cada j) vemos que $g \in (f_1, \cdots, f_k)$.

Caso 2: $d < d_k$. Al igual que en el caso anterior, $a \in (a_1, \cdots, a_k)$. Sea m el mínimo tal que $a \in (a_1, \cdots, a_m)$. Debe cumplirse que $d \geq d_m$. Como en el caso primero, $a = \sum_{i=1}^{m} c_i a_i$ con $c_i \in A$. Definimos

$$h_1 = \sum_{i=1}^{m} c_i X^{d-d_i} f_i \in (f_1, \cdots, f_k) \subseteq I.$$

El coeficiente principal de h es a, luego el grado de $g - h$ es mayor que d. Tras a lo sumo $d_k - d$ iteraciones, nos encontramos con que el elemento $g - \sum h_i$ está en I y tiene grado al menos d_k, y todos los $h_i \in (f_1, \ldots, f_k)$. Nos encontramos de nuevo en el caso 1, por lo que concluimos que I es el ideal $(f_1, \ldots, f_k)$. □

3.3.3. Dimensión de Krull.

Definición 3.25.
La **dimensión de Krull** de un anillo A es el supremo de las longitudes de las cadenas (por inclusión estricta) de sus ideales primos.

Proposición 3.26.
La dimensión de Krull de un cuerpo es 0, y la de un DIP es 1.

Demostración. Sea $\mathbb{K}$ un cuerpo. Como los únicos ideales posibles son el nulo y el total del cuerpo, la única cadena posible es (0), de longitud 0. Por ello, la dimensión de Krull de $\mathbb{K}$ es 0.

Sea A un DIP. Tomemos un ideal primo $(q) \subset A$. Supongamos que existe otro ideal primo (m) tal que $(q) \subseteq (m) \subset A$. Entonces, tenemos que $q = a_0 m$ para algún $a_0 \in A$. Pero como q es primo, o bien $a_0 \in (q)$, o bien $m \in (q)$. En el primer caso, $a_0 = a_1 q$, luego $q = a_1 q m$ y m es una unidad de A, luego $(m) = A$. En el segundo caso, $m = a_1 q$, luego $q = a_0 a_1 q$ y por lo tanto a_1 y a_0 son unidades y deducimos que $(q) = (m)$. De ambas formas, todos los ideales primos son maximales. Las cadenas serán de la forma $(0) \subset (p)$, luego la dimensión de Krull es de 1.

□

Definición 3.27.
Sea I un ideal sobre el anillo A. Definimos el índice de I como el cardinal del cociente A/I.

Ejemplo 3.28.
El cardinal de (n) sobre $\mathbb{Z}$ es n.
El índice del ideal (T) sobre $A[T]$, (los polinomios en una variable con coeficientes en el anillo A), es el cardinal de A.

Lema 3.29.
Sean $T^n + a_{n-1}T^{n-1} + \cdots + a_0 = P \in \mathbb{Z}_p[T]$ un polinomio distinguido y $U = \sum b_i T^i \in \Lambda^\times$ una unidad de Λ. Entonces $\deg(PU) \geq \deg(P)$. (En el caso $f \in \Lambda \smallsetminus \mathbb{Z}_p[T]$, decimos que $\deg(f) = \infty$).

Demostración. Supongamos que $\deg(PU) \leq n-1$. Entonces podemos calcular el n-ésimo coeficiente del producto PU, que debe ser igual a 0:

$$\begin{aligned} PU &= \sum_{i=0}^{\infty} b_i T^i \cdot \sum_{j=0}^{n} a_j T^j \\ &= \sum_{i+j=0}^{\infty} b_i a_j T^{i+j} = \sum_{k=0}^{\infty} \sum_{l=0}^{k} a_l b_{k-l} T^k \end{aligned}$$

El término que acompaña a T^n debe ser 0: $a_n b_0 + a_{n-1} b_1 + \cdots + a_0 b_n = 0$. Como P es distinguido, $\{a_{n-1}, \ldots, a_0\} \subset \mathfrak{p}$. Es decir, $a_n b_0 \in \mathfrak{p}$. Pero esto es absurdo, ya que $a_n = 1$ y $b_0 \in \mathbb{Z}_p^\times = \mathbb{Z}_p \smallsetminus \mathfrak{p}$. Por lo tanto, nuestra hipótesis de que el n-ésimo coeficiente de PU es 0 es falsa, y PU tiene grado por lo menos n. □

Lema 3.30.
Sean $f, g \in \Lambda$, relativamente primos. Entonces el ideal (f, g) es de índice finito en Λ.

Demostración. Sea $h \in (f, g)$ un polinomio de grado mínimo. En virtud de 3.15 y de 3.29, podemos escribir h como $h = p^s H$, donde, o bien $H = 1$, o bien H es distinguido. Veamos que $H = 1$ por reducción al absurdo. Supongamos $H \neq 1$. Ya que f y g son relativamente primos, asumimos sin pérdida de generalidad que H no divide a f. Pero entonces, por el algoritmo de división, existen $q \in \Lambda$, $r \in \mathbb{Z}_p[T]$ tales que:

$$f = Hq + r, \qquad \deg r < \deg H = \deg h.$$

Luego

$$p^s f = hq + p^s r.$$

Ya que $\deg(p^s r) < \deg h$ y $p^s r = p^s f - hq \in (f, g)$, hemos encontrado un nuevo elemento de grado mínimo (estrictamente menor que el grado de h), por lo que hemos llegado a contradicción. Es decir, $H = 1$ y $h = p^s$.
Como f y g son primos entre sí, el factor p no aparece en alguna de sus descomposiciones que nos da el Teorema de Preparación de Weierstrass. Por lo tanto, podemos asumir sin pérdida de generalidad que uno de ellos (por ejemplo f), no es divisible por p y es distinguido. Tenemos entonces:

$$(f, g) \supseteq (p^s, f).$$

Por el algoritmo de división, todo elemento de Λ es congruente módulo f con un polinomio de grado menor que $d = \deg f$. Al hacer ahora módulo p^s, restringimos los coeficientes de dichos polinomios a enteros p-ádicos cuya expansión p-ádica es finita, de longitud menor o igual a s. Es decir, cada polinomio tiene d coeficientes de longitud s. Considerando que cada elemento de la expansión puede tomar p valores, tenemos un total de $d^{(s^p)}$ posibles polinomios. En todo caso, hay una cantidad finita de ellos, por lo que el ideal (p^s, f) es de índice finito. Como $\Lambda/(f, g) \subseteq \Lambda/(p^s, f)$, el ideal (f, g) es también de índice finito. □

Ahora, veamos la forma que tienen los ideales primos de Λ:

Proposición 3.31.
Los ideales primos de Λ son 0, (p, T), $\mathfrak{p} = (p)$, y los ideales del tipo (P), con P un polinomio irreducible y distinguido. El ideal (p, T) es el único ideal maximal.

Demostración. Es fácil ver que todos son ideales primos. Sea $\mathfrak{p} \neq 0$ ideal primo. Sea $h \in \mathfrak{p}$ de grado mínimo. Entonces $h = p^s H$, con $H = 1$ o H distinguido. Como $\mathfrak{p}$ es primo, $p \in \mathfrak{p}$ o $H \in \mathfrak{p}$. Si $1 \neq H \in \mathfrak{p}$, H debe ser irreducible , al ser el grado de h mínimo. En ambos casos, se tiene que $(f) \subseteq \mathfrak{p}$ con $f = p$ o f irreducible y distinguido. Si $(f) = \mathfrak{p}$, $\mathfrak{p}$ es uno de los ideales enunciados antes, y ya habríamos acabado. Por lo tanto, supongamos que $(f) \neq \mathfrak{p}$, luego existe un $g \in \mathfrak{p}$ tal que $f \not| g$. Como f es irreducible,

f y g son relativamente primos. El lema 3.30 implica que $\mathfrak{p}$ es de índice finito en Λ. Como $\Lambda/\mathfrak{p}$ es un $\mathbb{Z}_p$-módulo finito, $p^N \in \mathfrak{p}$ para un N grande, luego $p \in \mathfrak{p}$ ya que $\mathfrak{p}$ es primo. Además $T^i \equiv T^j \mod \mathfrak{p}$ para $i < j$. Pero $1 - T^{j-i} \in \Lambda^\times$, luego $T^i \in \mathfrak{p}$. Por ello, $T \in \mathfrak{p}$, y sigue que $(p, T) \subseteq \mathfrak{p}$. Ahora bien, $\Lambda/(p, T) \simeq \mathbb{Z}/p\mathbb{Z}$, por lo que (p, T) es maximal e igual a $\mathfrak{p}$.
Como todos los ideales primos están contenidos en (p, T), éste es el único ideal maximal, lo que completa la prueba. □

Proposición 3.32.
Λ es un anillo local cuyo único ideal maximal es (p, T).

Demostración. Consecuencia directa de 3.31. □

Como consecuencia de la proposición 3.31, vemos ahora que la dimensión de Krull de Λ es de 2, pues tenemos la cadena de ideales primos:

$$0 \subset (p) \subset (p, T) \subset \Lambda,$$

que es de longitud 2, y no existe ninguna cadena con longitud superior a esta.

4. El Teorema de Estructura

Una vez expuestas las propiedades del Álgebra de Iwasawa, nos adentramos en la prueba del teorema de estructura. Empezaremos por exponer y tratar de mitigar las dificultades que supone el tener una dimensión de Krull de 2, frente al caso de dimensión 1 en los DIPs. Después definiremos algunas aplicaciones útiles entre Λ-módulos y las operaciones entre matrices que resultan de ellas, para culminar con la prueba del teorema.

4.1. Pseudoisomorfía. Enunciado del Teorema

Para conseguir expandir 1.26 al caso de módulos sobre Λ, tendremos ciertas restricciones. En primer lugar, nos tendremos que conformar con conseguir una relación más leve que la de isomorfismo, que llamaremos pseudo-isomorfismo.

Definición 4.1.
Una sucesión de grupos y homomorfismos de grupos, representada como:

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \dots \xrightarrow{f_n} G_n$$

se dice que es *exacta* en G_i si $Im(f_i) = Ker(f_{i-1})$. Si es exacta en todo G_i, se denomina simplemente exacta.

Nota: Las sucesiones finitas de este tipo se suelen representar de forma que $G_0 = 0 = G_n$.

Definición 4.2.
Llamamos *conúcleo* o *cokernel* de un homomorfismo de grupos $\phi : G \to H$ al grupo cociente $H/\phi(G)$.

Ejemplo 4.3.
De forma análoga a la situación en la que el núcleo de una aplicación inyectiva es el grupo trivial, el conúcleo de una aplicación sobreyectiva es también el grupo trivial.

Definición 4.4.
Dos Λ-módulos M y M' son *pseudo-isomorfos*, denotado

$$M \sim M'$$

si existe un homomorfismo $\phi : M \to M'$ con núcleo y conúcleo finitos. En otras palabras, si existe una secuencia exacta de Λ-módulos:

$$0 \to A \to M \to M' \to B \to 0,$$

donde A y B son Λ-módulos finitos.

Estamos listos para enunciar el teorema objetivo de este trabajo:

Teorema 4.5 (Teorema de Estructura de módulos finitamente Generados)**.** Sea M un Λ-módulo finitamente generado. Entonces

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j^{m_j}) \right)$$

Donde $r, s, t, n_i, m_j \in \mathbb{Z}$ y $f_j \in \Lambda$ son polinomios distinguidos e irreducibles.

Lema 4.6.
Sea $f \in \Lambda$ con $f \notin \Lambda^\times$. Entonces $\Lambda/(f)$ es infinito.

Demostración. Podemos suponer que $f \neq 0$. Entonces basta considerar los casos $f = p$ y f distinguido. Si $f = p$, $\Lambda/(f)$ es isomorfo a $\mathbb{Z}/p\mathbb{Z}[[T]]$, que es infinito. Si f es distinguido, aplicamos el algoritmo de división. Obtenemos que $\Lambda/(f) \simeq \mathbb{Z}_p[T]_d$, donde d es el grado de f. En este caso el cuerpo sobre el que se consideran los polinomios es infinito, luego $\Lambda/(f)$ también es infinito. □

La relación de pseudo-isomorfía no es necesariamente simétrica, esto se puede ver tomando como módulos el ideal (p, T) y el anillo total Λ. La relación $(p, T) \sim \Lambda$ se deduce, siendo el homomorfismo que los asocia la inclusión $(p, T) \hookrightarrow \Lambda$. En efecto, el núcleo es 0 y el conúcleo es el cociente

$$\Lambda/(p, T) \simeq \mathbb{Z}_p/(p) \simeq \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}.$$

Sin embargo, supongamos que $\Lambda \sim (p, T)$. Denotemos por $f = \Phi(1)$ a la imagen de $1 \in \Lambda$ por el homomorfismo Φ que relaciona estos módulos. Entonces, por ser homomorfismo, $(f) = (\Phi(1)) = \Phi((1)) = \Phi(\Lambda)$. Pero

tenemos $(f) \subseteq (p, T)$, por lo que f no es unidad. En este caso, podemos aplicar 4.6 para deducir que $\Lambda/(f)$ es infinito. Ahora bien, todo elemento de $\Lambda/(f)$ se puede poner como suma de un elemento de $(p, T)/(f)$ y otro de $(\Lambda/(p, T))/(f)$. Pero este último cociente es finito al serlo también $\Lambda/(p, T)$, por lo que $(p, T)/(f)$ debe ser infinito. Es decir, $Coker(\Phi)$ no es finito, y no hay pseudo-isomorfismo.

4.2. Preparación del Teorema.

Los resultados de esta sección nos permitirán construir las operaciones que definiremos en el próximo apartado. Dichas operaciones serán aplicables a la matriz de relaciones de un módulo con el fin de obtener un módulo pseudo-isomorfo.

Lema 4.7.
Sean $f,\ g \in \Lambda$ relativamente primos. Entonces

(1) La aplicación
$$\Phi : \Lambda/(fg) \to \Lambda/(f) \oplus \Lambda/(g)$$
es inyectiva y con conúcleo finito.

(2) Existe una aplicación inyectiva
$$\Lambda/(f) \oplus \Lambda/(g) \to \Lambda/(fg)$$
de conúcleo finito.

Demostración. (1) Veamos que la aplicación Φ (que consiste en dividir por f y g por separado y tomar los restos) es inyectiva. Si $h_1, h_2 \in \Lambda/(fg)$ tienen la misma imagen por Φ, llamémosla (a, b), podemos escribir:

$$h_1 = k_1 f + a = l_1 g + b.$$
$$h_2 = k_2 f + a = l_2 g + b.$$

Restando ambas ecuaciones, obtenemos:

$$h_1 - h_2 = (k_1 - k_2)f + 0 = (l_1 - l_2)g + 0.$$

Deducimos que $h_1 - h_2$ es múltiplo de f y de g, por lo que, al ser estos coprimos, es múltiplo de fg. Como el único múltiplo de fg en el cociente $\Lambda/(fg)$ es 0, deducimos que $h_1 = h_2$ y por lo tanto la aplicación es inyectiva.

Consideramos un elemento $(a,\ b) \in \Lambda/(f) \oplus \Lambda/(g)$. Veamos primero que si $a - b \in (f, g)$, entonces $(a, b) \in Im(\Phi)$. Sea $a - b \in (f, g)$, entonces $a - b = fA + gB$, para algunos $A, B \in \Lambda$. Sea

$$c = a - fA = b + gB,$$

entonces

$$c \equiv a \mod f, \qquad c \equiv b \mod g,$$

por lo que $(a, b) = \Phi(c)$, es decir, pertenece a la imagen.

Ahora, como f y g son coprimos, 3.30 nos dice que $\Lambda/(f, g)$ tiene una cantidad finita de elementos. Así, escojamos $r_1, \ldots, r_n \in \Lambda$ representantes de los elementos en $\Lambda/(f, g)$. Un elemento (no nulo) del conúcleo debe tener un representante de la forma$(a \mod f, b \mod g) \notin Im(\Phi)$. Al no pertenecer a la imagen, debe darse $(a-b) \notin (f, g)$, y por lo tanto $(a-b) \not\equiv 0 \mod (f, g)$. Es decir, $(a-b) \equiv r_i$ para algún i. Además, como $a-b-r_i \in (f, g)$, deducimos que (a, b) y $(0, -r_i)$ pertenecen a la misma clase de $Coker(\Phi)$. Como esto ocurre independientemente del par (a, b), deducimos que

$$\{\ (0 \mod f,\ r_j \mod g)\ | 1 \leq j \leq n\}$$

es un conjunto de representantes del conúcleo de la aplicación, por lo que dicho conúcleo es finito.
(2) Denotemos:

$$M := \Phi(\Lambda/(fg)),$$
$$N := \Lambda/(f) \oplus \Lambda/(g).$$

De (1) se sigue que M es isomorfo a $\Lambda/(fg)$ y que $|N/M| < \infty$.
Sea P un polinomio distinguido en Λ que sea primo relativo con fg. Sea $(x, y) \in N$, entonces:

$$P^i \cdot (x, y) \equiv P^j \cdot (x, y) \mod M$$

para algunos $i < j$, ya que $|N/M| < \infty$. (No puede haber infinitos elementos de N módulo M, luego debe haber dos índices que den el mismo valor).

Nótese que $1 - P^{j-i} \in \Lambda^\times$ (pues el término independiente de P, y por tanto el de cualquier potencia positiva del mismo, es divisible por p). Por lo tanto tenemos que $P^i \cdot (x, y) \in M$.
Veamos que $P^k N \subseteq M$ para algún k. El exponente i cuya existencia acabamos de demostrar debe ser menor que $|N/M|$, pues tenemos que cada $P^j \cdot (x, y)$ pertenece a una clase de N/M, solo hay $|N/M|$ de las mismas. Pero esto significa que podemos tomar este número como exponente, y por lo tanto,

$$P^{|N/M|} N \subseteq M.$$

Probemos ahora que $P^k : N \to M$ es inyectiva. Supongamos $P^k \cdot (x, y) = 0$ en N, luego $f | P^k x$, $g | P^k y$. Como $\gcd(P, fg) = 1$, $f | x$ y $g | y$; luego $(x, y) = 0$ en N. Por lo tanto la aplicación composición de P^k con el homomorfismo entre M y $\Lambda/(fg)$:

$$N \xrightarrow{P^k} M \xrightarrow{\simeq} \Lambda/(fg),$$

es inyectiva. La imagen contiene al ideal (P^k, fg), el cual es de índice finito por el lema 3.30, lo que completa la prueba. □

Nota: De forma general, $M \sim M'$ no implica $M' \sim M$ (lo que implica que la pseudo-isomorfía no es relación de equivalencia), pero el lema 4.7 nos proporciona una condición bajo la cual se dan ambas relaciones: si $(f, g) = 1$, entonces

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g) \qquad \text{y} \qquad \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg).$$

4.3. Operaciones Admisibles.

Además de las operaciones elementales mencionadas en el primer capitulo, las cuales conservan el isomorfismo, ahora disponemos de otras tres operaciones características que conservan el pseudo-isomorfismo.
Consideramos M un Λ-módulo finitamente generado. Sean $u_1, \ldots, u_n$ generadores de M, junto con las relaciones

$$\lambda_{i,1} u_1 + \cdots + \lambda_{i,n} u_n = 0, \qquad \lambda_{i,j} \in \Lambda.$$

Como las relaciones (que denotaremos por R) son un submódulo de Λ^n, y Λ es noetheriano, las relaciones son finitamente generadas. Por ello, podemos

representar M por una matriz cuyas filas son de la forma $(\lambda_{i,1}, \ldots, \lambda_{i,n})$, tales que $\sum \lambda_{i,j} u_j = 0$. Abusando de la notación, llamaremos R a esta matriz.

A continuación describiremos las operaciones a realizar sobre la matriz que conservan pseudo-isomorfismo con el módulo original. Comenzamos con las tres operaciones que mantienen isomorfismo, las usuales en la demostración de la versión de este teorema para dominios de ideales principales.

Operación A Podemos permutar filas/columnas entre sí.
Operación B Podemos sumar múltiplos de una fila/columna a otra.
Operación C Podemos multiplicar una fila/columna por un elemento de $\Lambda^{\times}$.

Además disponemos de otras tres operaciones, las cuáles probaremos que conservan el pseudo-isomorfismo.

Lema 4.8 (Operación 1)**.**
Si R contiene una fila $(\lambda_{i,1}, p\lambda_{i,2}, \cdots, p\lambda_{i,n})$, con $p \not| \lambda_{i,1}$, entonces podemos sustituir la matriz R por una nueva matriz R', la cual tiene como primera fila $(\lambda_{i,1}, \lambda_{i,2}, \cdots, \lambda_{i,n})$, y todos los elementos de la primera columna excepto $\lambda_{i,1}$ son multiplicados por p. Esta operación es un pseudo-isomorfismo. La operación A nos permite asumir sin perdida de generalidad que la fila que consta de esta particularidad es la primera. Visto en forma matricial:

$$\begin{pmatrix} \lambda_{1,1} & p\lambda_{1,2} & \cdots & p\lambda_{1,n} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{t,1} & \lambda_{t,2} & \cdots & \lambda_{t,n} \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,n} \\ p\lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p\lambda_{t,1} & \lambda_{t,2} & \cdots & \lambda_{t,n} \end{pmatrix}.$$

Como caso especial, si $\lambda_{1,2} = \cdots = \lambda_{1,n} = 0$, podemos multiplicar todos los elementos $\lambda_{j,1}$ con $j > 1$ por una potencia arbitraria de p.

Demostración. En R tenemos la relación

$$\lambda_{1,1} u_1 + p(\lambda_{1,2} u_2 + \cdots + \lambda_{1,n} u_n) = 0.$$

Dado $v \in M$, sea $M' = M \oplus v\Lambda$ módulo las relaciones adicionales:

$$(-u_1, pv) = 0, \qquad (\lambda_{1,2}u_2 + \cdots + \lambda_{1,n}u_n, \lambda_{1,1}v) = 0.$$

Existe un morfismo natural $M \to M'$ ($u \mapsto (u, 0)$ módulo las nuevas relaciones). Supongamos que la imagen de m por este morfismo es 0 para algún $m \in M$. Entonces se cumple la ecuación:

$$(m, 0) = a(-u_1, pv) + b(\lambda_{1,2}u_2 + \cdots + \lambda_{1,n}u_n, \lambda_{1,1}v),$$

con $a, b \in \Lambda$. Tomando los segundos términos vemos que $ap = -b\lambda_{1,1}$. Como p no divide a $\lambda_{1,1}$, deducimos que $p|b$, y por tanto, $\lambda_{1,1}|a$. Comparando ahora las primeras componente:

$$\begin{aligned} m &= \frac{-a}{\lambda_{1,1}}(\lambda_{1,1}u_1) + \frac{-a}{\lambda_{1,1}}p(\lambda_{1,2}u_2 + \cdots + \lambda_{1,n}u_n) \\ &= \frac{-a}{\lambda_{1,1}}(0) = 0. \end{aligned}$$

Como las imágenes de pv y $\lambda_{1,1}v$ en M' pertenecen a la imagen de M, el ideal $(p, \lambda_{1,1})$ es un anulador de (M'/M). Haciendo las cuentas, si (r_1, r_2v) es un elemento de M', entonces:

$$\begin{aligned} (ap + b\lambda_{1,1})(r_1, r_2v) &= (q, apr_2v + b\lambda_{1,1}r_2v) \\ &= (q + ar_2u_1 - br_2(\lambda_{1,2}u_2 + \cdots + \lambda_{1,n}u_n), 0) + ar_2(-u_1, pv) \\ &\quad + br_2((\lambda_{1,2}u_2 + \cdots + \lambda_{1,n}u_n), \lambda_{1,1}v) \\ &= (q', 0) + ar_2(0) + br_2(0), \qquad q' \in M \\ &= 0 \mod M \end{aligned}$$

Por el lema 3.30, $\Lambda/(p, \lambda_1)$ es finito. Como además M' es finitamente generado, el cociente (M'/M) es finito. Por ello, la sucesión

$$0 \to \Lambda/(p, \lambda_1) \to M \to M' \to M'/M \to 0$$

es exacta, y concluimos que $M \sim M'$.

El nuevo módulo M' tiene como generadores a $v, u_2, \cdots, u_n$. Todas las relaciones $\lambda_{i,1}u_1 + \lambda_{i,2}u_2 + \cdots + \lambda_{i,n}u_n = 0$ se convierten en relaciones de la forma $p\lambda_{i,1}v + \lambda_{i,2}u_2 + \cdots + \lambda_{i,n}u_n = 0$, luego toda la primera columna de la matriz de relaciones queda multiplicada por p. Además, tenemos la relación $(\lambda_{1,1}v_1 + \cdots + \lambda_{1,n}u_n = 0)$, por lo que la primera fila es ahora redundante y la sustituimos por ésta nueva relación. La matriz R' tiene, por tanto, la forma que antes mencionábamos. □

Lema 4.9 (Operación 2)**.**
Si todos los elementos de la primera columna de R son divisibles por p^k y existe una fila de la forma $(p^k\lambda_{1,1}, p^k\lambda_{1,2}, \ldots, p^k\lambda_{1,n})$ con $p \not| \lambda_1$, reemplazaremos la matriz R con la matriz R', que es idéntica a la original, excepto que la primera fila es reemplazada por $(\lambda_{1,1}, \lambda_{1,2}, \ldots, \lambda_{1,n})$. Esta operación es también pseudo-isomorfismo.

$$\begin{pmatrix} p^k\lambda_{1,1} & p^k\lambda_{1,2} & \cdots & p^k\lambda_{1,n} \\ p^k\lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p^k\lambda_{t,1} & \lambda_{t,2} & \cdots & \lambda_{t,n} \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,n} \\ p^k\lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p^k\lambda_{t,1} & \lambda_{t,2} & \cdots & \lambda_{t,n} \end{pmatrix}.$$

Demostración. Dado $v \in M$, sea $M' = M \oplus \Lambda v$ módulo las relaciones:

$$(p^k u_1, -p^k v) = 0, \qquad (\lambda_{1,2}u_2 + \cdots + \lambda_{1,n}u_n, \lambda_{1,1}v) = 0.$$

Tenemos el mismo resultado que en la operación 1, al darse que $p \not| \lambda_{1,1}$, deducimos que $M \hookrightarrow M'$. El ideal $(p^k, \lambda_{1,1})$ anula a M/M', por lo que el cociente es finito y $M \sim M'$ Ahora, destacamos en primer lugar que, como $p^k(u_1 - v) = 0$ y p^k divide al primer coeficiente de u_1 en todas las relaciones en las que éste no es nulo, podemos describir M' como

$$M' = M'' \oplus (u_1 - v)\Lambda$$

Donde M'' está generado por $v, u_2, \cdots, u_n$ y sus relaciones son las de R junto con la relacion adicional generada por $(\lambda_{1,1}, \cdots, \lambda_{1,n})$. Luego la matriz de relaciones de M'' es R'. Destaquemos que

$$(u_1 - v)\Lambda \simeq \Lambda/(p^k),$$

que es de la forma que queremos, por lo que nos basta trabajar con M'' y R'. □

Lema 4.10 (Operación 3)**.**
Si R contiene una fila de la forma $(p^k\lambda_{1,1}, p^k\lambda_{1,2}, \ldots, p^k\lambda_{1,n})$ y, para algún α con $p \nmid \alpha$, y un $j \neq 1$ se da que $\alpha\lambda j, i = \lambda 1, i$ para todo i es una relación (no explicitamente contenida en R, pero obtenible a partir de R), entonces podemos reemplazar R por R', en la que la fila $(p^k\lambda_{1,1}, p^k\lambda_{1,2}, \ldots, p^k\lambda_{1,n})$ es sustituida por $(\lambda_{1,1}, \lambda_{1,2}, \ldots, \lambda_{1,n})$. Esta transformación es, al igual que las dos anteriores, un pseudo-isomorfismo.

$$\begin{pmatrix} p^k\lambda_{1,1} & p^k\lambda_{1,2} & \cdots & p^k\lambda_{1,n} \\ \alpha\lambda_{2,1} & \alpha\lambda_{2,2} & \cdots & \alpha\lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{t,1} & \lambda_{t,2} & \cdots & \lambda_{t,n} \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,n} \\ \alpha\lambda_{2,1} & \alpha\lambda_{2,2} & \cdots & \alpha\lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{t,1} & \lambda_{t,2} & \cdots & \lambda_{t,n} \end{pmatrix}.$$

Demostración. Consideramos la aplicacion suprayectiva

$$M \to M' = M/(\lambda_1 u_1 + \cdots + \lambda_n u_n)\Lambda$$

El núcleo es anulado por el ideal (α, p^k). Ya que M, y por lo tanto el núcleo, son finitamente generados, y $\Lambda/(\alpha, p^k)$ es finito, el núcleo es también finito, luego $M \sim M'$. M' tiene a R' como matriz de relaciones. □

4.4. R-normalidad.

En este apartado definiremos el concepto de matriz r-normal, donde r es un número natural. La r-normalidad de una matriz jugará un papel similar al de la forma normal de Smith en los DIPs, pues nos permitirá obtener una estructura diagonal bajo ciertos requerimientos sobre los elementos de la diagonal.
Si $0 \neq f \in \Lambda$, entonces, por 3.15:

$$f = p^\mu PU,$$

con P distinguido y $U \in \Lambda^\times$. Definimos el grado de Weierstrass de f como:

$$\deg_w f = \begin{cases} \infty & \mu > 0 \\ \deg\ P(T) & \mu = 0 \end{cases}$$

Nuestro objetivo es modificar una matriz de relaciones sin perturbar los cambios que ya hayan podido ser realizados. Para ello, necesitamos algún tipo de medición de la complejidad de la matriz que no dependa de las primeras filas/columnas, y que no se vea modificada por operaciones que no afecten a dichas filas/ columnas. Dada una matriz R, definimos

$$\deg^{(k)}(R) := \min \deg_w(a'_{ij}) \quad \text{con } i,j \geq k,$$

donde a'_{ij} es un elemento de cualquier matriz de relaciones obtenible a partir de R mediante operaciones admisibles que dejen las primeras $(k-1)$ filas sin modificar. Decimos que R está en forma $(r-1)$-normal si tiene la forma

$$\begin{pmatrix} \lambda_{1,1} & & 0 & 0 & \cdots & 0 \\ & \ddots & & & & \\ 0 & & \lambda_{r-1,r-1} & 0 & \cdots & 0 \\ * & \cdots & * & * & \cdots & * \\ * & \cdots & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

donde λ_{kk} son distinguidos y cumplen que

$$\deg \lambda_{kk} = \deg_w \lambda_{kk} = \deg^{(k)} R, \quad (1 \leq k \leq r-1).$$

Nótese que los grados de los elementos van descendiendo a medida que bajamos por la diagonal. Naturalmente, nuestro objetivo será ver que podemos aumentar el nivel de normalidad bajo ciertas condiciones:

Proposición. Sea R una matriz en forma $(r-1)$-normal para un cierto $r \geq 2$. Si su submatriz B es no nula, entonces R se puede transformar mediante operaciones admisibles, en una matriz R' que esté en forma r-normal y tenga los mismos $(r-1)$ elementos diagonales.

Demostración. El caso especial de la Operación 1 nos permite asumir cuando sea necesario que una potencia de p lo suficientemente grande divide a cada λ_{ij}, con $i \geq r$ y $j \leq r-1$. Es decir, $p^N | A$, con N lo suficientemente grande para que $p^N \not| B$ (Aplicando el caso especial de la operación 1, vamos multiplicando cada columna de A por una potencia lo suficientemente grande de p). Usando la Operación 2, ahora podemos asumir que $p \not| B$. Por ello,

existe al menos una entrada $\lambda_{i,j}$ de de esta submatriz que no es divisible por p. Por definición de $deg^{(r)}R$ podemos suponer que:

$$\deg_w \lambda_{i,j} = \deg^{(r)} R < \infty.$$

Empleamos ahora 3.15: si $\lambda_{i,j} = PU$, multiplicamos la columna por U^{-1}. Es decir, podemos asumir que $\lambda_{i,j}$ es distinguido. Aplicando ahora la operación A (intercambio de filas y columnas), asumimos $\lambda_{i,j} = \lambda_{r,r}$.

Por el algoritmo de división (3.13), podemos emplear la Operación B para asumir que $\lambda_{r,j}$ es un polinomio de grado menor que el de $\lambda_{r,r}$ para todos los $j \neq r$, y menor que el de $\lambda_{j,j}$ cuando $j < r$. (Dividimos la fila r por el polinomio distinguido $\lambda_{r,r}$ y tomamos el resto, o hacemos lo propio por columnas, siendo el divisor $\lambda_{j,j}$).

Como el grado de Weierstrass de $\lambda_{j,j}$ es mínimo en B, debe darse que $p|\lambda_{r,j}$. Por la operación 1, podemos asumir que $p^N|\lambda_{r,j}, j < r$, para algún N grande. Supongamos que $\lambda_{r,j} \neq 0$ para algún $j > r$. La operación 1 nos permite eliminar la potencia de p de algún $\lambda_{r,j}$ no nulo. Entonces

$$\deg_w \lambda_{r,j} = \deg \lambda_{r,j} < \deg \lambda_{r,r} = \deg_w \lambda_{r,r},$$

Lo cual es absurdo, por lo que deducimos que $\lambda_{r,j} = 0$ siempre que $j > r$.

Si algún $\lambda_{r,j} \neq 0$, para $j < r$, usamos la Operación 1 para obtener $p \nmid \lambda_{r,j}$ para cierto j. Pero entonces

$$\deg_w \lambda_{r,j} \leq \deg \lambda_{r,j} < \deg \lambda_{j,j} = \deg_w \lambda_{j,j}.$$

Pero también sabemos que:

$$\deg_w \lambda_{j,j} = \deg^{(j)}(R),$$

y esto contradice la definición minimal de $\deg^{(j)}(R)$. Luego $\lambda_{r,j} = 0 \quad \forall j \neq r$. Vemos ahora que la nueva matriz está en forma r-normal, lo que concluye la demostración. □

4.5. Prueba del Teorema

Una vez establecidos todos los requisitos, pasamos a demostrar el teorema.

Demostración. Si comenzamos con una matriz R de tamaño $t \times n$, 0-normal, podemos sustituir R de manera progresiva empleando operaciones admisibles hasta obtener una matriz de la forma:

$$\begin{pmatrix} \lambda_{1,1} & & & 0 \\ & \ddots & & \\ & & \lambda_{r,r} & \\ A & & & 0 \end{pmatrix},$$

donde los $\lambda_{j,j} \in \Lambda$ son polinomios distinguidos y $\deg\lambda_{j,j} = \deg^{(j)}(R)$ para $j \leq r$. Por el algoritmo de división, podemos asumir que $\lambda_{i,j}$ es un polinomio de grado menor que dicho $\lambda_{j,j}$.
Supongamos $\lambda_{i,j} \neq 0$ para algún $i \neq j$. Como $\deg_w \lambda_{j,j}$ es mínimo por definición, p divide a $\lambda_{i,j}$; y existe por lo tanto una relación no nula de la forma $(\lambda_{i,1}, \cdots, \lambda_{i,r}, 0, \cdots, 0)$ la cual es divisible por p. Sea

$$\lambda = \prod_{i=1}^{r} \lambda_{i,i}.$$

Entonces $p \nmid \lambda$, ya que los $\lambda_{j,j}$ son distinguidos, y fijándonos en las r primeras filas (y considerando la suma de las mismas), vemos que:

$$\left(\lambda\frac{1}{p}\lambda_{i,1}, \cdots, \lambda\frac{1}{p}\lambda_{i,r}, 0, \cdots, 0\right)$$

es también una relación, ya que $\lambda_{j,j}u_j = 0$. Por la operación 3, podemos asumir que $p \nmid \lambda_{i,j}$ para algún j, por lo cual:

$$\deg_w \lambda_{i,j} \leq \deg\lambda_{i,j} < \deg\lambda_{j,j} = \deg^{(j)}(R).$$

Esto es absurdo por la definición de $\deg^{(j)}(R)$. Luego $\lambda_{i,j} = 0$ para todos los i, j con $i \neq j$. Esto implica que $A = 0$, y en términos de Λ-módulos, esta

matriz es la representación de:

$$\Lambda/(\lambda_{1,1}) \oplus \cdots \oplus \Lambda/(\lambda_{r,r}) \oplus \Lambda^{t-r}.$$

Tenemos que considerar que cada vez que hemos aplicado la operación 2 hemos descartado un sumando de la forma $\Lambda/(p^{n_i})$. Es decir, el módulo M original es pseudo-isomorfo a:

$$\Lambda^{t-r} \oplus \left(\bigoplus_{i=1}^{s} \Lambda/\left(p^{n_i}\right) \right) \oplus \left(\bigoplus_{j=1}^{r} \Lambda/(\lambda_{j,j}) \right)$$

El último paso es aplicar el Lema 4.7 a todos los $\Lambda/(\lambda_{j,j})$ en los que $\lambda_{j,j}$ no sea irreducible, es decir:

$$\Lambda/(\lambda_{j,j}) \sim \bigoplus_{k=1}^{h_j} \Lambda/(f_{j,k}^{m_{j,k}}),$$

donde cada $f_{j,k}$ es irreducible y distinguido, pues cada $\lambda_{j,j}$ se puede suponer distinguido (ya que, por construcción, no son divisibles por p). Si h es el número total de factores extraídos de esta manera, (es decir, $h = \sum_{i=1}^{j} h_j$), podemos escribir:

$$M \sim \Lambda^{t-r} \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{l=1}^{h} \Lambda/(f_l^{m_l}) \right),$$

lo cual podemos reescribir mediante un cambio de índices como:

$$M \sim \Lambda^{r} \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j^{m_j}) \right),$$

y con esto queda completada la prueba del Teorema 4.5 □

Bibliografía

Referencias

[1] N. Jacobson, *Basic Algebra I*, W. H. Freeman, 1985.

[2] S. Lang, *Algebra*, Springer, 2002.

[3] S. Roman, *Advanced Linear Algebra*, Springer, 2008.

[4] P. Samuel, *On unique factorization domains*, Illinois Journal of Mathematics, 5 (1961), pp. 1–17.

[5] P. Torrent i Soler, *Iwasawa theory*, Master's thesis, Universitat Politècnica de Catalunya, 2018.

[6] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1997.

[7] `https://www.math.ntu.edu.tw/~mlhsieh/teaching/L3.pdf`. Visitado el 4 de junio de 2025.

[8] `https://ocw.mit.edu/courses/res-18-012-algebra-ii-student-notes-spring-2022/mit18_702s22_lec23.pdf`. Visitado el 4 de junio de 2025.

[9] `https://www.cut-the-knot.org/blue/p-adicNumbers.shtml`. Visitado el 4 de junio de 2025.

[10] `https://renrenthehamster.wordpress.com/wp-content/uploads/2015/08/notes-on-finite-presentation_latex_3.pdf`. Visitado el 4 de junio de 2025.

[11] `https://www.ma.imperial.ac.uk/~dhelm/M3P8/notes7a.pdf`. Visitado el 4 de junio de 2025.

[12] `https://www.math.uwaterloo.ca/~dgwagner/co430I.pdf`. Visitado el 4 de junio de 2025.

[13] `https://web.archive.org/web/20230608074050/https://faculty.math.illinois.edu/~r-ash/Algebra/Chapter8.pdf`. Visitado el 4 de junio de 2025.