Universidad de Valladolid

El Teorema de Estructura de Módulos Finitamente Generados sobre el Álgebra de Iwasawa

Alejandro Melero Santos

2023/24

TUTOR: ALBERTO FERNÁNDEZ BOIX
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 capitulos 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 en 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-e.v. 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.

Estructura

En el Capítulo 1 introducimos los conceptos básicos para la comprensión de este trabajo y los primeros resultados en el álgebra de Iwasawa, incluyendo el Teorema de Preparación p-ádica de Weierstrass, una pieza fundamental de buena parte de las posteriores demostraciones.

En el Capítulo 2 abordamos los lemas y proposiciones que concluyen en la prueba del Teorema, echando un vistazo al Teorema de la Base de Hilbert como herramienta para probar que el álgebra de Iwasawa es un anillo noetheriano.

1. Conceptos

1.1. Álgebra Lineal

Del siguiente teorema, que se prueba en la asignatura de Estructuras Algebraicas, surge la motivación de este trabajo.

Teorema 1.1 (Teorema de Estructura de Grupos Abelianos Finitamente Generados)**.**
Todo grupo abeliano finitamente generado G es (isomorficamente equivalente a) la suma directa de grupos cíclicos finitos e infinitos, y el número de sumandos de cada clase depende únicamente de G. Dicho de otra forma, todo grupo abeliano finitamente generado puede expresarse como

$$\mathbb{Z}^{\oplus n} \oplus \mathbb{Z}/(p^1) \oplus \cdots \oplus \mathbb{Z}/(p^k),$$

donde p es un número primo.

Definición 1.2.
La **dimensión de Krull** de un anillo A es el supremo de las longitudes de las cadenas (por inclusión estricta) de sus ideales primos.

Ejemplo: Si K es un cuerpo, su dimensión de Krull es 0. Los dominios de ideales principales tienen dimensión de Krull igual a 1. En el anillo que trataremos, la dimensión de Krull es 2, como veremos más adelante.

Definición 1.3.
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. $e_A \cdot x = x$

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 nos referimos a ellos simplemente cómo modulos.

Los módulos son una generalización del concepto de K-espacio vectorial (donde K es un cuerpo) a un anillo A.

En este trabajo trataremos con módulos finitamente generados, es decir, aquellos en los que cada elemento puede ser representado como una combinación lineal de un subconjunto finito (fijo) que llamamos *base*, con coeficientes elementos del anillo escalar.

Definición 1.4.
Sea M un módulo sobre el anillo A. Un elemento $g \in M$ es **de torsión** si existe $r \in A$ tal que $r\ m = 0$ y r no es divisor de 0 (no existe un elemento no nulo $a \in A$ tal que $r\ a = 0$).

De forma análoga, los elementos de torsión de un grupo son aquellos que tienen orden finito. Es sencillo ver que todo grupo se puede descomponer como suma directa del grupo de elementos de torsión (el subgrupo de torsión), y por otra, el subgrupo de elementos que no son de torsión (el subgrupo libre).

Definición 1.5.
Una secuencia de grupos y homomorfismos de grupos, representada como:

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

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

Definición 1.6.
Llamamos **conúcleo** de un homomorfismo de grupos $f : G \to H$ al grupo $H/f(G)$.

1.2. Los números p-ádicos

Dado un número primo p, denominamos números p-ádicos a las series:

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

en la cuál k es un entero y a_i es entero con $0 \leq a_i < p$. Si $k \geq 0$, decimos que s es un *entero p-ádico.*

Definición 1.7.
La valoración p-ádica de s asociada al primo p, denotada $\nu_p(s)$, se define como:

$$\nu_p(s) = \max\{e \in \mathbb{Z} | p^e \text{ divide a } s\}$$

Asociada a esta definición encontramos la de valor absoluto p-ádico de s:

$$|s|_p = p^{-\nu_p(s)}$$

Definición 1.8.
Llamamos **Álgebra de Iwasawa** al anillo de series formales con coeficientes en los enteros p-ádicos. De ahora en adelante la denotaremos:

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

Lema 1.9.
Sean $f, g \in \Lambda$. Supongamos que $f = a_0 + a_1 T + \cdots$, 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 de forma única g de la forma siguiente:

$$g = qf + r$$

Donde $q \in \Lambda$ y $r \in \mathbb{Z}_p$ 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 $0 = qf + r$. Si q, $r \neq 0$, podemos asumir que o bien $\pi \not| q$ o bien $\pi \not| r$. Reduciendo mód π vemos que $\pi | r$, (ya que $r = -qf$, $r = \sum_{i+j=0}^{i+j=n-1} a_i q_i T^i$, con $\pi | a_i$), por lo que $\pi | qf$. Por hipótesis, $\pi \not| f$. Como

luego $\pi|q$, y tenemos una contradicción. Así, $q = r = 0$.
Para probar la existencia, definimos el operador $\tau = \tau_n : \Lambda \to \Lambda$ como:

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

τ es esencialmente un operador de traslación. Además, es $\mathbb{Z}_p$-lineal y cumple:

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

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

Podemos escribir

$$f(T) = \pi P(T) + T^n U(T)$$

Donde $P(T)$ es un polinomio de grado menor que n y $U(T) = a_n + a_{n+1}T + \cdots = \tau(f(T))$. Ya que $a_n \in \mathbb{Z}_p^{\times}$, $U(T)$ es una unidad en el anillo de series de potencias. Sea

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

La contribución de cada π^j resulta en que la serie converja, luego $q(T)$ está bien definida en Λ. Ya que

$$qf = \pi q P + T^n q U,$$

Tenemos

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

Pero

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

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

De ahora en adelante, nos referiremos a este último resultado como: "algoritmo de división".

1.3. Preparación P-ádica de Weierstrass

Definición 1.10.
Decimos que un polinomio $P(T) \in \mathbb{Z}_p$ es *distinguido* si $P(T) = T^n + a_{n-1}T^{n-1}\cdots + a_1T + a_0$, con $a_i \in \mathfrak{p},\ 0 \leq i \leq n-1$.

El teorema siguiente se puede encontrar en [1, Página 115, Teorema 7.3]. En sus términos originiales se enuncia para grupos más generales que $\mathbb{Z}_p$, pero este caso es suficiente para el tema a tratar.

Teorema 1.11 (Teorema de preparación p-ádica de Weierstrass)**.**
Sea

$$f(t) = \sum_{i=0}^{\infty} a_iT^i \in \Lambda$$

Supongamos que para algún n, $a_i \in \mathfrak{p}$, $0 \leq a_i \leq n-1$, 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: $f(T) = P(T)U(T)$, donde $U(T) \in \Lambda$ es una unidad y $P(T)$ es un polinomio distinguido de grado n. De forma más general, si f es no nula, se puede escribir de forma única como:

$$f(T) = \pi^\mu P(T)U(T)$$

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

Demostración. Aplicamos el lema anterior a $g(T) = T^n$. Entonces, podemos escribir:

$$T^n = q(T)f(T) + r(T), \qquad \text{donde } \deg r \leq n-1$$

Como

$$q(T)f(T) \equiv q(T)(a_n T^n + \text{términos de mayor grado}) \mod \pi$$

Debe darse que $r(T) \equiv 0 \mod \pi$. Luego $P(T) = T^n - r(T)$ es un polinomio distinguido de grado n. Sea q_0 el término constante de $q(T)$. Comparando los coeficientes de T^n, vemos que $1 \equiv q_0 a_n \mod \pi$. Luego $q_0 \in \mathbb{Z}_p^\times$, por lo que $q(T)$ es una unidad. Ahora, sea $U(T) = 1/q(T)$. Reordenando términos, vemos que $f(T) = U(T)P(T)$, como deseabamos. Ya que cualquier polinomio distinguido de grado n se puede escribir en la forma $P(T) = T^n - r(T)$, podemos transformar de nuevo la ecuación $f(T) = U(T)P(T)$ como:

$$T^n = U(T)^{-1}f(T) + r(T).$$

La unicidad probada en el lema anterior garantiza la unicidad de $P(T)$ y $U(T)$. La generalización es consecuencia de factorizar la mayor potencia de π posible en $f(T)$. □

2. El álgebra de Iwasawa

2.1. Resultados previos

Los resultados siguientes se corresponden con [1, Lema 13.7] y posteriores.

Consideramos $\Lambda = \mathbb{Z}_p[[T]]$, las series formales cuyos coeficientes son enteros p-ádicos.

Lema 2.1.
Sean $f, g \in \Lambda$, relativamente primos. Entonces el ideal (f, g) es de índice finito en Λ.

Demostración. Sea $h \in (f, g)$ de grado mínimo. Entonces $h = p^s H$ con $H = 1$ o H distinguido. Supongamos $H \neq 1$. Ya que f y g son relativamente primos, asumimos sin pérdida de generalidad que H no divide a f. Pero

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

Luego

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

Ya que $\deg(p^s r) < \deg h$ y $p^s r \in (f, g)$, tenemos una contradicción. Luego $H = 1$ y $h = p^s$. Asumimos sin pérdida de generalidad que f no es divisible por p y que es distinguido. Tenemos

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

Por el algoritmo de división, todo elemento de Λ es congruente mód f con un polinomio de grado menor que $\deg f$. Como la cantidad de polinomios de dicho tipo es finita mód p^s, el ideal (p^s, f) es de índice finito, lo que completa la prueba. □

Lema 2.2.
Sean $f,\ g \in \Lambda$ relativamente primos. Entonces

(1) La aplicación

$$\Lambda/(fg) \to \Lambda/(f) \oplus \Lambda/(g)$$

es inyectiva y con connúcleo finito.

(2) Existe una aplicación inyectiva

$$\Lambda/(f) \oplus \Lambda/(g) \to \Lambda/(fg)$$

de connúcleo finito.

Demostración. (1) Cómo Λ es Dominio de Factorización Única, la aplicación es inyectiva. Consideramos el elemento $(a \mod f,\ b \mod g)$. Si $a-b \in (f,g)$, entonces $a-b=(fA+gB)$, para algún A y B. Sea

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

Entonces

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

por lo que (a,b) está en la imagen. Ahora, sean $(r_1,\ldots,r_n) \in \Lambda$ representantes de $\Lambda/(f,g)$. Deducimos que

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

Es un sistema de representantes del connúcleo del mapa, por lo que dicho connúcleo es finito.
(2) De (1):

$$\Lambda/(fg) \simeq M \subseteq \Lambda/(f) \oplus \Lambda/(g) =: N$$

siendo M de indice finito en N. Sea P un polinomio distinguido en Λ que sea primo relativo con fg. Si $(x,y) \in N$, entonces:

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

Para algún $i < j$. Como $1 - P^{j-i} \in \Lambda^\times$, tenemos que $P^i(x,y) \in M$. Luego $P^k N \subseteq M$ para algún k. Supongamos $P^k(x,y) = 0$ 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. Deducimos que

$$N \xrightarrow{p^k} M \xrightarrow{\sim} \Lambda/(fg)$$

es inyectiva. La imagen contiene al ideal (P^k, fg), el cual es de índice finito por el Lema 2.1, lo que commpleta la prueba. □

Proposición 2.3.
Los ideales primos de Λ son 0, (p,T), p, y los ideales del tipo $(P(T))$, con $P(T)$ 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 2.1 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 $(p,T) \subseteq \mathfrak{p}$. Pero $\Lambda/(p,T) \simeq \mathbb{Z}/p\mathbb{Z}$, por lo que (p,T) es maximal e igual a $\mathfrak{p}$.
Como todos los ideales primos están contenidos em (p,T), éste es el único ideal maximal, lo que completa la prueba. □

Lema 2.4.
Sea $f \in \Lambda$ con $f \in \Lambda^\times$. Entonces $\Lambda/(f)$ es infinito.

Demostración. Podemos suponer que $f \neq 0$. Entonces basta considerar los casos $f = p$ y f distinguido. Si $f = p$, $\Lambda/(f) \simeq \mathbb{Z}/p\mathbb{Z}[[T]]$, 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. □

Definición 2.5.
Decimos que un Anillo A es Noetheriano si toda cadena de ideales es finita, 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.

2.2. Teorema de la Base de Hilbert

El siguiente resultado no lo probaremos, pero nos será útil para el lema posterior.

Proposición 2.6 (**Teorema de la Base de Hilbert**).
Sea A un anillo Noetheriano. Entonces $A[T]$ es un Anillo Noetheriano.

Una prueba de este teorema se puede encontrar en [4, página 118].

Lema 2.7.
Λ es un anillo Noetheriano.

Demostración. Notemos que $A = \mathbb{Z}_p$ es Noetheriano (Lema 2.3). 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 $A[[T]]$. Sea f_1 de grado mínimo en I. Supongamos que tenemos $f_1, \cdots, f_i$, con grados $d_1, \cdots, d_i$ y coeficientes $a_1, \cdots, a_i$. Escogemos f_{i+1} de forma que:

1. $f_{i+1} \in I$
2. $a_{i+1} \notin (a_1, \cdots, a_i)$
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 $I = (f_1, \cdots, f_k)$. Sea $g = aT^d + \cdots$ un elemento de I de grado d y coeficiente a Entonces $a \in (a_1, \cdots, a_k)$. 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 $i = 1, \cdots, k$. 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 $g_0, \cdots, g_r \in (f_0, \cdots, f_k)$ 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, $b \in (a_1, \cdots, a_k)$, 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 Iy tiene grado al menos d_k, y todos los $h_i \in (f_1, \cdots, f_k)$. Nos encontramos de nuevo en el caso 1, por lo que concluimos que $I = (f1, \cdots, fk)$. □

Definición 2.8.
Dos Λ-módulos M y M' son *pseudo-isomorfos*, denotado

$$M \sim M'$$

si existe un homomorfismo $M \to M'$ con núcleo y connúcleo 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.

Observación. De forma general, $M \sim M'$ no implica $M' \sim M$ pero el lema 2.2 nos dice que, si $(f, g) = 1$, entonces $\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g)$ y $\Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$. Con esto, pasamos al resultado final:

2.3. El Teorema de Estructura

Teorema 2.9 (Teorema de Estructura de módulos finitamente Generados)**.** Sea M un Λ-módulo finitamente generado. Entonces

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

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

Demostración. Sean $u_1, \cdots, u_n$ los generadores de M, junto con las relaciones

$$\lambda_1 u_1 + \cdots + \lambda_n u_n = 0, \qquad \lambda_i \in \Lambda$$

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 $(\lambda_1, \cdots, \lambda_n)$, tales que $\sum \lambda_i u_i = 0$. Abusando de la notación, llamaremos R a esta matriz.

2.3.1. Operaciones Admisibles

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.

Operación 1 Si R contiene una fila $(\lambda_1, p\lambda_2, \cdots, p\lambda_n)$, con $p \not| \lambda_1$, entonces podemos sustituir la matriz R por la matriz R', la cual tiene como primera fila $(\lambda_1, \lambda_2, \cdots, \lambda_n)$, y todos los elementos de la primera columna excepto λ_1 son multiplicados por p.

$$\begin{pmatrix} \lambda_1 & p\lambda_2 & \cdots \\ \alpha_1 & \alpha_2 & \cdots \\ \beta_1 & \beta_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p\alpha_1 & \alpha_2 & \cdots \\ p\beta_1 & \beta_2 & \cdots \end{pmatrix}$$

Como caso especial, si $\lambda_2 = \cdots = \lambda_n = 0$, podemos multiplicar todos los elementos $\alpha_1, \beta_1, \cdots$ por una potencia arbitraria de p.

Demostración. En R tenemos la relación

$$\lambda_1 u_1 + p(\lambda_2 u_2 + \cdots + \lambda_n u_n) = 0$$

Sea $M' = M \oplus v\Lambda$ modulo las relaciones adicionales:

$$(-u_1, pv) = 0, \qquad (\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) = 0$$

Existe un morfismo natural $M \to M'$ ($u \mapsto (u, 0)$ módulo las nuevas relaciones). Supongamos que $m \mapsto 0$. Entonces m está en las relaciones, por lo que

$$(m, 0) = a(-u_1, pv) + b(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v)$$

Con $a, b \in \Lambda$. Tomando los segundos términos vemos que $ap = -b\lambda_1$. Como $p \not| \lambda_1$, deducimos que $p|b$, y por tanto, $\lambda_1|a$. Viendo ahora la otra componente:

$$\begin{aligned} m &= \frac{-a}{\lambda_1}(\lambda_1 u_1) + \frac{-a}{\lambda_1} p(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= \frac{-a}{\lambda_1}(0) = 0. \end{aligned}$$

Como las imágenes de pv y $\lambda_1 v$ en M' pertenecen a la imagen de M, el ideal (p, λ_1) es un anulador de (M'/M). Haciendo las cuentas, si $(r_1, r_2 v) \in M'$, entonces:

$$\begin{aligned}(ap+b\lambda_1)(r_1,r_2v) &= (q, apr_2v + b\lambda_1 r_2 v)\\ &= (q + ar_2u_1 - br_2(\lambda_2u_2+\cdots+\lambda_nu_n), 0) + ar_2(-u_1, pv)\\ &\quad + br_2((\lambda_2u_2+\cdots+\lambda_nu_n), \lambda_1 v)\\ &= (q', 0) + ar_2(0) + br_2(0), \qquad q' \in M\\ &= 0 \mod M\end{aligned}$$

Por el lema 2.1, $\Lambda/(p,\lambda_1)$ es finito. Como además M' es finitamente generado, el cociente (M'/M) es finito. Por ello, la secuencia

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

es exacta, por lo que $M \sim M'$.

El nuevo módulo M' tiene como generadores a $v, u_2, \cdots, u_n$. Todas las relaciones $\alpha_1u_1 + \cdots + \alpha_nu_n = 0$ se convierten en $p\alpha_1v + \cdots + \alpha_nu_n = 0$, luego toda la primera columna de la matriz de relaciones queda multiplicada por p. Además, tenemos la relación $(\lambda_1v_1 + \cdots + \lambda_nu_n = 0)$, 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. □

Operación 2 Si todos los elementos de la primera columna de R son divisibles por p^k y existe una fila de la forma $(p^k\lambda_1, \cdots, p^k\lambda_n)$ con $p \not| \lambda_1$, reemplazaremos la matriz R con la matriz R', que es idéntica a la original, excepto que $(p^k\lambda_1, \cdots, p^k\lambda_n)$ es reemplazado por $(\lambda_1, \cdots, \lambda_n)$.

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \\ p^k\beta_1 & \beta_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \\ p^k\beta_1 & \beta_2 & \cdots \end{pmatrix}$$

Demostración. Sea $M' = M \oplus \Lambda v$ módulo las relaciones:

$$(p^ku_1, -p^kv) = 0, \qquad (\lambda_2u_2 + \cdots + \lambda_nu_n, \lambda_1 v) = 0$$

Tenemos el mismo resultado que en la operación 1, al darse que $p \not| \lambda_1$, deducimos que $M \hookrightarrow M'$. El ideal (p^k, λ_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 R más la relacion adicional generada por $(\lambda_1, \cdots, \lambda_n)$. 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'. □

Operación 3 Si R contiene una fila de la forma $(p^k\lambda_1, \cdots, p^k\lambda_n)$ y, para algún λ con $p \not| \lambda$, $(\lambda\lambda_1, \cdots, \lambda\lambda_n)$ es también una relación (no explicitamente contenida en R, pero obtenible a partir de R), entonces podemos reemplazar R por R', en la que la fila $(p^k\lambda_1, \cdots, p^k\lambda_n)$ es sustituida por $(\lambda_1, \cdots, \lambda_n)$.

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

Una vez establecidas las operaciones admisibles, y viendo que todas ellas preservan el tamaño de la matriz, podemos comenzar.
Si $0 \neq f \in \Lambda$, entonces

$$f(T) = p^{\mu} P(T) U(T),$$

con P distinguido y $U \in \Lambda^{\times}$. Sea

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

a lo que llamos el grado de Weierstrass de f. Dada una matriz R, definimos

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

donde a'_{ij} recorre todas las matrices de relaciones obtenibles a partir de R mediante operacions admisibles que dejen las primeras $(k-1)$ filas sin modificar.

2.3.2. r-normalidad

Si la matriz R tiene la forma

$$\begin{pmatrix} \lambda_{11} & & 0 & 0 & \cdots & 0 \\ & \ddots & & & & \\ 0 & & \lambda_{r-1,r-1} & 0 & \cdots & 0 \\ * & \cdots & * & * & \cdots & * \\ * & \cdots & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

donde λ_{kk} son distiguidos y

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

Decimos que R está en forma $(r-1)$normal.

Proposición. Si la submatriz $B \neq 0$ entonces R se puede transformar

mediante operaciones admisibles, en una matriz R' que esté en forma r-normal y tenga las mismas $(r-1)$ 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 $p^n \not| B$. Usando la Operación 2, podemos asumir que $p \not| B$. De igual manera, podemos asumir que la submatriz B contiene una entrada λ_{ij} tal que

$$\deg_w \lambda_{ij} = \deg^{(r)} R < \infty$$

Si $\lambda_{ij} = P(T)U(T)$, multiplicamos la columna por U^{-1}. Es decir, podemos asumir que λ_{ij} es distinguido. Por la operación A, asumimos $\lambda_{ij} = \lambda_{rr}$.

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

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

$$\deg_w \lambda_{rj} = \deg \lambda_{rj} < \deg \lambda_{rr} = \deg_w \lambda_{rr},$$

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

Si algún $\lambda_{rj} \neq 0$, para $j < r$, usamos la Operación 1 para obtener $p \not| \lambda_{rj}$ para cierto j. Pero entonces

$$\deg_w \lambda_{rj} \leq \deg \lambda_{rj} < \deg \lambda_{jj} = \deg_w \lambda_{jj},$$

Como

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

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

2.3.3. Procedimiento

Si comenzamos con una matriz R y $r = 1$, podemos sustituir R de manera progresiva hasta obtener una matriz de la forma

$$\begin{pmatrix} \lambda_{11} & & & 0 \\ & \ddots & & \\ & & \lambda_{rr} & \\ A & & & 0 \end{pmatrix}$$

donde los λ_{jj} son distinguidos y $\deg\lambda_{jj} = \deg^{(j)}(R)$ para $j \leq r$. Por el algoritmo de división, podemos asumir que λ_{ij} es un polinomio de grado menor que dicho λ_{jj}. Supongamos $\lambda_{ij} \neq 0$ para algún $i \neq j$. Como $\deg_w \lambda_{jj}$ es mínimo, $p|\lambda_{ij}$; por lo que hay una relación no nula $(\lambda_{i1}, \cdots, \lambda_{ir}, 0, \cdots, 0)$ que es divisible por p. Sea $\lambda = \lambda_{11} \cdots \lambda_{rr}$. Entonces $p \not| \lambda$, ya que los λ_{jj} son distinguidos, y

$$\left(\lambda\frac{1}{p}\lambda_{i1}, \cdots, \lambda\frac{1}{p}\lambda_{ir}, 0, \cdots, 0\right)$$

es también una relación, ya que $\lambda_{jj} u_j = 0$. Por la operación 3, podemos asumir que $p \not| \lambda_{ij}$ para algún j, por lo cual

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

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

$$\Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r}.$$

A lo cual falta añadir los factores de tipo $\Lambda/(p^k)$, que son eliminados como consecuencia de la operación 2. El último paso es aplicar el Lema 2.2 a todos los $\Lambda/(\lambda_{kk})$ en los que λ_{kk} no sea irreducible, expresándolo como la suma directa de los cocientes de Λ por los factor irreducibles de λ_{kk}.
Con esto queda completada la prueba del Teorema. $\square$

Bibliografía

Referencias

[1] Washington, L. C. (1997). Introduction to Cyclotomic Fields. En *Graduate texts in mathematics*. https://doi.org/10.1007/978-1-4612-1934-7

[2] https://web.archive.org/web/20230608074050/https://faculty.math.illinois.edu/~r-ash/Algebra/Chapter8.pdf Illinois.edu Algebra Ch.8

[3] Torrent i Soler, P. (2018). Iwasawa Theory. [Tesis de Maestría, Universitat Politècnica de Catalunya]. https://upcommons.upc.edu/handle/2117/123479?show=full

[4] Roman, Stephen (2008), Advanced Linear Algebra, Graduate Texts in Mathematics (Third ed.), Springer, ISBN 978-0-387-72828-5http://matematicas.uis.edu.co/sites/default/files/paginas/archivos/Advanced%20Linear%20Algebra%20-%20Steven%20Roman.pdf