USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Máster

Unha introdución á teoría de Iwasawa

Borja Quintela Correa

Curso 2024/2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

MÁSTER UNIVERSITARIO DE MATEMÁTICAS

Traballo Fin de Máster

Unha introdución á teoría de Iwasawa

Borja Quintela Correa

Xullo, 2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Unha introdución á teoría de Iwasawa
Breve descrición do contido
Este traballo pretende realizar unha introdución á teoría de Iwasawa, comezando polo estudo da estrutura dos módulos finitamente xerados sobre $\mathbb{Z}_p[\![T]\!]$ e do teorema de control de Iwasawa para o número de clases dos corpos ciclotómicos. Na segunda parte centrámonos no lado analítico, con énfase nas series de potencias de Coleman. Formulamos tamén a conxectura principal de Iwasawa, para a cal se traballarán algunhas das ideas implicadas na súa demostración.
Recomendacións
Outras observacións

Índice

Resumo **VIII**

Introdución **XI**

1. Preliminares alxébricos **1**

1.1. Números p-ádicos 1

1.2. Factorización de primos en extensións 4

1.3. Corpos de clase 6

1.4. Teoría de corpos de clase 9

2. Estrutura dos módulos sobre $\mathbb{Z}_p[[T]]$ **11**

2.1. Teorema de preparación de Weierstrass 11

2.2. Propiedades do anel $\mathbb{Z}_p[[T]]$ 15

2.3. Teorema de clasificación 19

3. Propiedades das $\mathbb{Z}_p$-extensións **25**

3.1. $\mathbb{Z}_p$-extensións 25

3.2. Conxectura de Leopoldt 28

3.3. Estrutura xeral das $\mathbb{Z}_p$-extensións 29

4. Teorema de control de Iwasawa e ideais característicos **37**

4.1. Demostración do teorema de control 37

4.2. O ideal característico e a conxectura de Kummer–Vandiver 43

4.3. Conxectura principal de Iwasawa 47

5. Series de potencias de Coleman **51**

5.1. Operadores de Coleman 52

5.2. Interpolación de series de potencias 53

5.3. Proba do teorema de Coleman 57

6. Medidas p-ádicas e a función zeta p-ádica de Riemann **59**

6.1. Medidas p-ádicas 60

6.1.1. Integrais e pseudomedidas 61

6.1.2. A transformada de Mahler 63

6.1.3. Derivada logarítmica 66

6.2. A función zeta p-ádica 70

7. O teorema de Iwasawa e a conxectura principal de Iwasawa **77**

7.1. A conxectura principal de Iwasawa 77

7.2. Idea da demostración da conxectura principal de Iwasawa 79

7.3. Extensións da teoría de Iwasawa 80

Bibliografía **83**

Resumo

Este traballo pretende realizar unha introdución á teoría de Iwasawa, comezando polo estudo da estrutura dos módulos finitamente xerados sobre $\mathbb{Z}_p[\![T]\!]$, que se pode entender como unha xeneralización do teorema de clasificación de módulos sobre un dominio de ideais principais. Á súa vez, iso permítenos establecer o teorema de control de Iwasawa para o número de clases dos corpos ciclotómicos.

Na segunda parte, presentamos resultados máis recentes que permiten entender mellor a estrutura alxébrica das $\mathbb{Z}_p$-extensións, formulando a conxectura principal de Iwasawa, que relaciona dita estrutura alxébrica cun obxecto puramente analítico, a función zeta p-ádica.

Finalmente explicamos a estratexia xeral empregada na demostración dese resultado e acabamos ilustrando algunhas tendencias actuais de investigación no tema.

Abstract

This work aims to provide an introduction to Iwasawa theory, beginning with the study of the structure of finitely generated modules over $\mathbb{Z}_p[\![T]\!]$, which can be understood as a generalization of the classification theorem for modules over a principal ideal domain. This, in turn, allows us to establish Iwasawa's control theorem for the class number of cyclotomic fields.

In the second part, we present more recent results that provide a better understanding of the algebraic structure of $\mathbb{Z}_p$-extensions, formulating Iwasawa's main conjecture, which relates this algebraic structure to a purely analytic object: the p-adic zeta function.

Finally, we explain the general strategy used in the proof of this result, and we conclude by illustrating some current research trends in the area.

Introdución

En 1956, o matemático xaponés Kenkichi Iwasawa foi convidado ao encontro de verán da Sociedade Matemática Americana en Seattle. Iwasawa presentou neste evento, baixo o nome de "*A theorem on Abelian groups and its application to algebraic number theory*", a demostración dun teorema (Teorema 4.1 no traballo) que inauguraría o que denominamos actualmente como teoría de Iwasawa.

Foi tres anos máis tarde, en 1959, cando todos os detalles da proba foron publicados en [8]. A partir desta conferencia, Iwasawa escribiu máis de 20 artigos centrándose no que coñecemos hoxe en día como teoría das $\mathbb{Z}_p$-extensións. Neste traballo dedicarémonos a facer unha exposición detallada do que se denomina *teoría de Iwasawa clásica*, que se basea na análise do crecemento da p-parte de Sylow do grupo de clase das $\mathbb{Z}_p$-extensións, ademais de falar da súa conxectura principal e comprender os obxectos matemáticos que conforman a proba para poder dar unha idea da mesma. Por outro lado, consideramos tamén a *teoría de Iwasawa moderna*, da que falaremos no último capítulo, e que abrangue o estudo doutros obxectos matemáticos (por exemplo, o grupo de Shafarevich-Tate) que son de gran interese, por exemplo, para o estudo de funcións L ou curvas elípticas.

Máis concretamente, o obxectivo deste traballo é presentar a conxectura principal da teoría de Iwasawa no caso máis sinxelo, ilustrando tamén as propiedades alxébricas máis relevantes dos módulos implicados. Nunha primeira aproximación, poderiamos dicir que a teoría de Iwasawa se centra no estudo da regularidade que manteñen certos invariantes aritméticos nunha torre de corpos. O caso que máis nos ocupará é a chamada *extensión ciclotómica*. Tomando como corpo base os números racionais, $\mathbb{Q}$, podemos considerar para cada número enteiro positivo n a extensión $\mathbb{Q}_n = \mathbb{Q}(\zeta_{p^n})$, onde ζ_{p^n} é unha raíz primitiva da unidade de orde p^n. Empregando resultados elementais de teoría de Galois tense que

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

Se consideramos a unión de todas estas extensión, temos o que chamaremos $\mathbb{Q}_\infty = \bigcup_{n\geq 1} \mathbb{Q}_n$; o seu grupo de Galois pódese identificar co límite inverso dos correspondentes grupos de Galois,

polo que

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p,$$

onde $\mathbb{Z}_p$ é o anel dos enteiros p-ádicos. Temos tamén que

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_1) \simeq \mathbb{Z}_p,$$

o que supón un exemplo de $\mathbb{Z}_p$-extensión, é dicir, unha extensión que ten por grupo de Galois os enteiros p-ádicos $\mathbb{Z}_p$ e que, en particular, ten un retículo de subcorpos especialmente sinxelo de entender. Á súa vez, entender a estrutura das $\mathbb{Z}_p$-extensións permite comprender tamén outras como $\mathbb{Q}_\infty/\mathbb{Q}$, que teñen por grupo de Galois $\mathbb{Z}_p$ por un grupo finito.

A primeira parte dedícase polo tanto ao estudo das principais propiedades alxébricas e analíticas dos números p-ádicos e, máis en concreto, ás propiedades dos módulos finitamente xerados sobre o anel $\mathbb{Z}_p[\![T]\!]$. No caso dos dominios de ideais principais, hai un teorema de clasificación que permite describir de xeito preciso calquera módulo finitamente xerado. Aquí faremos algo semellante. Para demostralo, cómpre desenvolver primeiro certos resultados, especialmente o coñecido como teorema de preparación de Weierstrass, que é un análogo p-ádico dun resultado de variable complexa sobre factorización de funcións holomorfas. Do mesmo sentido que para os dominios de ideais principais dispomos dun teorema de clasificación que nos permite describir de xeito preciso calquera módulo finitamente xerado, sobre $\mathbb{Z}_p[\![T]\!]$ ocorre algo similar, aínda que neste caso deberemos falar de *pseudoisomorfismos*. Porén, isto será suficiente para asociarlle a calquera módulo finitamente xerado e de torsión un ideal, o chamado *ideal característico*, que terá un papel relevante ao longo do traballo.

Nos Capítulos 3 e 4 introducimos propiamente a teoría de Iwasawa, que parte dun problema relativamente sinxelo: o estudo da variación do número de clases ao longo da extensión ciclotómica. Escribimos p^{e_n} para o cardinal da p-parte correspondente ao grupo de clases de $\mathbb{Q}_n$. Neste contexto, o resultado principal (o coñecido como teorema de Iwasawa), afirma que existen enteiros λ, μ, ν de xeito que, para un n suficientemente grande, cúmprese que

$$e_n = \lambda p^n + \mu n + \nu.$$

A demostración baséase nas seguintes ideas principais:

(a) Unha adaptación do teorema de estrutura para módulos sobre dominios ideais principais, no que imos permitir algunhas operacións adicionais (que reflicte a idea que permitimos pseudoisomorfismos, non só isomorfismos).

(b) Un estudo do comportamento dos primos nas $\mathbb{Z}_p$-extensións, con énfase nas propiedades de ramificación.

(c) Un teorema de control, que permite recuperar información para as extensións $\mathbb{Q}_n$ partindo de resultados sobre $\mathbb{Q}_\infty$.

Por outra banda, este estudo permite introducir o $\mathbb{Z}_p[\![T]\!]$-módulo que intervirá na conxectura principal de Iwasawa, ao que chamamos Y_∞. De xeito informal, é o grupo de Galois correspondente á extensión abeliana non ramificada maximal de $\mathbb{Q}_\infty$. O primeiro resultado que probamos é que é un módulo de torsión, e iso permite demostrar o resultado sobre o crecemento dos e_n. A continuación, asociámoslle ao módulo un obxecto alxébrico que chamaremos *ideal característico*, que é un certo polinomio que codifica información alxébrica sobre o módulo. Porén, Y_∞ non é o obxecto máis axeitado para estudar, e precisamos introducir unha variante del, X_∞, que se corresponde co grupo de Galois da extensión abeliana maximal de $\mathbb{Q}_\infty$ que **só** ramifica en p. A conxectura principal da teoría de Iwasawa relaciona dito ideal característico co ideal xerado por unha serie de potencias, a *serie de potencias de Coleman* correspondente á función zeta p-ádica ζ_p.

Máis en concreto, se $I(G)$ é un certo ideal da álxebra de Iwasawa (o chamado ideal de aumentación), a conxectura principal afirma que

$$\mathrm{ch}_G(X_\infty) = I(G)\zeta_p.$$

Esta serie de potencias, que se introduce nos Capítulos 5 e 6, pódese entender como un avatar p-ádico que interpola certos valores da función zeta complexa, modificados de xeito axeitado para que dean lugar a unha función analítica de variable p-ádica.

Finalmente, no Capítulo 7 discutimos o teorema de Iwasawa, que é un dos ingredientes principais para a demostración da conxectura principal, xa que permite relacionar ζ_p cun obxecto alxébrico, a partir do cal se pode demostrar o resultado central do traballo. Porén, dada a complexidade da proba, omítese a súa demostración nesta memoria. Como apuntamento histórico, subliñamos que hai dous xeitos de proceder. Un deles emprega a teoría dos sistemas de Euler, que aparecen tamén no estudo da conxectura de Birch e Swinnnerton-Dyer, e que son familias de clases de cohomoloxía que cumpren certas propiedades de compatibilidade; o outro, desenvolvido por Mazur e Wiles, emprega a teoría das familias de formas modulares e inspírase en diferentes resultados previos de Ribet.

Por último, gustaríanos facer énfase no feito de que a teoría de Iwasawa aparece en moitos problemas diferentes da teoría de números, que van desde cuestións máis avanzadas relativas ás extensións ciclotómicas a outros contextos diferentes relacionados, por exemplo, coa teoría de curvas elípticas. Nese contexto, existe unha conxectura principal que relaciona un obxecto alxébrico (o ideal característico dun grupo de Selmer) cun obxecto analítico (unha función L p-ádica). A súa demostración, combinando os resultados de Kato e Skinner-Urban, adoita considerarse un dos resultados máis relevantes da teoría de números do que levamos de século XXI.

Capítulo 1

Preliminares alxébricos

Antes de comezar co que propiamente son os conceptos, resultados e teoría que constitúen o núcleo desta memoria, repasaremos certas definicións e ferramentas esenciais necesarias para o desenvolvemento do traballo. En concreto, neste capítulo daremos un contexto adecuado de distintos temas como son os números p-ádicos ou os grupos de corpos de clases co gallo de facilitar as explicacións dos vindeiros capítulos.

1.1. Números p-ádicos

Os números p-ádicos son unha extensión dos números racionais que xurdiron pola necesidade de estudar propiedades aritméticas máis específicas. Nesta sección estudaremos os números p-ádicos tanto dende unha perspectiva alxébrica, como dende unha perspectiva máis analítica, vendo $\mathbb{Q}_p$ coma a completación de $\mathbb{Q}$ con respecto a unha certa norma. Para esta sección seguimos principalmente as referencias [5] e [23].

Consideremos $p \in \mathbb{Z}$ un número primo e sexa $A_n = \mathbb{Z}/p^n\mathbb{Z}$ o anel de clases de equivalencia de enteiros módulo p^n, para $n \geq 1$. Desta forma definimos o homomorfismo

$$\begin{array}{rccc} \phi_n\colon & A_n & \longrightarrow & A_{n-1} \\ & x \text{ mód } p^n & \longmapsto & x \text{ mód } p^{n-1} \end{array}$$

o cal é sobrexectivo e cumpre que $\ker(\phi) = p^{n-1}A_n$. Ademais, temos que a sucesión

$$\ldots \xrightarrow{\phi_{n+1}} A_n \xrightarrow{\phi_n} A_{n-1} \xrightarrow{\phi_{n-1}} \ldots \xrightarrow{\phi_3} A_2 \xrightarrow{\phi_2} A_1$$

forma un sistema proxectivo.

Definición 1.1. Nestas condicións, chamamos **anel dos enteiros p-ádicos**, denotado como $\mathbb{Z}_p$, ao límite proxectivo de (A_n, ϕ_n), é dicir, $\mathbb{Z}_p = \varprojlim(A_n, \phi_n)$.

Polo tanto, se $x = (..., x_n, ..., x_1) \in \mathbb{Z}_p$ temos que $x_i \in A_i$ e $\phi_n(x_n) = x_{n-1}$ se $n \geq 2$. Ademais, $\mathbb{Z}_p$ é un subanel do produto $\prod_{n\geq 1} A_n$. Polo tanto, podemos ver tanto a suma como a multiplicación en $\mathbb{Z}_p$ definidas coordenada a coordenada.

Co gallo de ver as propiedades deste tipo de anel definiremos $\epsilon_n : \mathbb{Z}_p \longrightarrow A_n$ como a función que asocia un elemento $x \in \mathbb{Z}_p$ coa súa compoñente n-ésima, x_n, de A_n.

Proposición 1.2. *A sucesión*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\epsilon_n} A_n \to 0$$

é unha sucesión exacta curta de grupos abelianos.

Demostración. Vexamos que p^n é inxectiva. En efecto, se $x = (x_n)$ é tal que $px = 0$, entón $px_{n+1} = 0$, para todo $n \in \mathbb{N}$. Desta forma podemos expresar $x_{n+1} = p^n y_{n+1}$ con $y_{n+1} \in A_{n+1}$. Como $x_n = \phi_{n+1}(x_{n+1})$, temos que x_n é divisible por p^n e así $x_n = 0$.

Por outra parte, é evidente que $p^n\mathbb{Z}_p \subset \ker(\epsilon_n)$. Probemos que tamén se cumpre a outra inclusión. Se $x = (x_m) \in \ker(\epsilon_m)$, entón $x_m \equiv 0$ (mód p^n), para todo $m \geq n$. Polo tanto, existe $y_{m-n} \in A_{m-n}$ tal que a sua imaxe polo isomorfismo $A_{m-n} \longrightarrow p^n\mathbb{Z}/p^m\mathbb{Z} \subset A_m$ satisfai $x_m = p^n y_{m-n}$. Estes y_i definen un elemento y de $\mathbb{Z}_p$ de tal forma que $p^n y = x$, co que se remata a proba. □

Notación 1.3. Denotaremos por $\mathbb{Z}_p^\times$ ao grupo de elementos de $\mathbb{Z}_p$ invertibles e chamarémolos unidades p-ádicas.

Proposición 1.4. *Un elemento de $\mathbb{Z}_p$ (analogamente de A_n) ten inverso se, e só se non é divisible por p. De feito, todo elemento non nulo de $\mathbb{Z}_p$ pode expresarse de forma única como $p^n u$, con $u \in \mathbb{Z}_p^\times$ e $n \in \mathbb{N}$.*

Demostración. Basta probalo para A_n. Sexa $x \in A_n$ tal que $x \notin pA_n$, entón a súa imaxe en $A_1 = \mathbb{F}_p$ é non nula por ser A_1 un corpo, polo que é invertible. Desta forma existen $y, z \in A_n$ tales que $xy = 1 - pz$, e así, $xy(1 + pz + ... + p^{n-1}z^{n-1}) = 1$, co que x é invertible.

Por outra banda, se $x \in \mathbb{Z}_p$ é non nulo, existe un $n \in \mathbb{N}$ de tal forma que $x_n = \epsilon_n(x) = 0$ e así, $x = p^n u$ con u non divisible por p, polo que $u \in \mathbb{Z}_p^\times$. A unicidade da descomposición é obvia. □

Ademais, cómpre salientar que $\mathbb{Z}_p$ é un anel de valoración discreta. Xa que é un dominio de ideais principais, porque todos os seus ideais son da forma (p^n) con $n \geq 0$, cun único ideal primo non nulo, que é (p). Por outra parte, temos que $\mathbb{Z}_p$ é tamén noetheriano xa que os seus ideais cumpren a condición de cadea descendente e esta implica a súa vez a condición de cadea ascendente:

$$\mathbb{Z}_p = (1) \supset (p) \supset (p^2) \supset ...$$

Definición 1.5. O **corpo dos números p-ádicos** é o corpo de fraccións de $\mathbb{Z}_p$ e denotarémolo como $\mathbb{Q}_p$.

Podemos observar como $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. Ademais, todo elemento $x \in \mathbb{Q}_p \setminus \{0\}$ pode ser escrito de forma única como $x = p^n u$, con $n \in \mathbb{N}$ e $u \in \mathbb{Q}_p^\times$.

Imos presentar agora un acercamento de tipo máis analítico aos números p-ádicos, que será útil para comprender mellor as súas propiedades topolóxicas.

Definición 1.6. Chamaremos **valoración p-ádica** de $x = p^n u \in \mathbb{Z}_p$, con $u \in \mathbb{Z}_p^\times$ e $n \in \mathbb{N}$, á imaxe de x a través da función $v_p : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{R}$ onde $v_p(x) = n$.

Ademais, podemos extender v_p ao corpo dos números racionais como segue: se $x = \dfrac{a}{b} \in \mathbb{Q}^\times$, entón $v_p(x) = v_p(a) - v_p(b)$.

Pola definición dada, adóitase establecer que $v_p(0) = \infty$.

Observación 1.7. Para todo $x, y \in \mathbb{Q}$, temos:

1. $v_p(xy) = v_p(x) + v_p(y)$,
2. $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

Para rematar vexamos dous resultados para poder entender $\mathbb{Q}_p$ coma a completación de $\mathbb{Q}$.

Proposición 1.8. *A topoloxía en $\mathbb{Z}_p$ pódese definir coa métrica*

$$d(x, y) = e^{-v_p(x-y)}.$$

O anel $\mathbb{Z}_p$ é un espazo métrico completo onde $\mathbb{Z}$ é un subespazo denso.

Proposición 1.9. *O corpo $\mathbb{Q}_p$ coa topoloxía definida pola métrica da proposición anterior é localmente compacto, e contén a $\mathbb{Z}_p$ como un subanel aberto. Ademais, $\mathbb{Q}$ é denso en $\mathbb{Q}_p$.*

Como consecuencia, podemos definir $\mathbb{Q}_p$ (respectivamente $\mathbb{Z}_p$) como a completación de $\mathbb{Q}$ (respectivamente $\mathbb{Z}$) coa métrica p-ádica inducida.

1.2. Factorización de primos en extensións

Comezemos recordando que K é un **corpo de números** se é unha extensión finita de $\mathbb{Q}$. Por outra parte, chamaremos **anel de enteiros** de K á clausura enteira de $\mathbb{Z}$ en K e denotarémola por $\mathcal{O}_K$. Ao longo do traballo cando falemos de K estarémonos a referir a un corpo de números.

Consideremos $L \mid K$ unha extensión de corpos de números. Posto que $\mathcal{O}_L$ é un dominio de Dedekind imos estudar o comportamento dos primos de $\mathcal{O}_K$ en $\mathcal{O}_L$ para isto seguiremos como principais referencias [15] e [20].

Definición 1.10. Se $\mathfrak{q}$ é un ideal primo non nulo de $\mathcal{O}_L$ e $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ é un primo, entón diremos que o primo $\mathfrak{q}$ **divide o** primo $\mathfrak{p}$.

Se o primo $\mathfrak{q}$ divide $\mathfrak{p}$, entón temos a seguinte descomposición:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{t} \mathfrak{q}_i^{e_i}, \text{con } e_i \geq 1. \tag{1.1}$$

Os $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ son ideais primos non nulos de $\mathcal{O}_L$ distintos entre si e, en particular, son todos os ideais primos de $\mathcal{O}_L$ que dividen a $\mathfrak{p}$.

Definición 1.11. O enteiro $e_i \geq 1$ da descomposición 1.1 chámase **índice de ramificación** de $\mathfrak{q}_i$ sobre $\mathfrak{p}$. Ademais, chamaremos **grado residual** asociado ao primo $\mathfrak{q}_i$ a:

$$f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}] \geq 1.$$

Proposición 1.12. *Tense a seguinte relación:*

$$[L : K] = \sum_{i=1}^{t} e_i f_i.$$

Xa estamos en condicións de dar as seguintes definicións.

Definición 1.13. Se $\mathfrak{p}$ e $\mathfrak{q}_i$ son primos nas condicións anteriores, entón:

1. Se $e_{\mathfrak{q}_i} = 1$ e $\mathcal{O}_L/\mathfrak{q}_i \mid \mathcal{O}_K/\mathfrak{p}$ é separable, entón diremos que a extensión $L \mid K$ é **non ramificada** en $\mathfrak{q}_i$.

2. Se, ademais, $L \mid K$ é **non ramificada** en $\mathfrak{q}_i$, para todo i, entón diremos que $L \mid K$ é non ramificada en $\mathfrak{p}$.

3. Se existe un único ideal primo de $\mathcal{O}_L$ que divida a $\mathfrak{p}$ tal que o seu grado residual é 1 (ou, equivalentemente, que o seu índice de ramificación sexa igual ao grao de $L \mid K$), diremos que $L \mid K$ é **totalmente ramificado**.

4. O primo $\mathfrak{p}$ **descomponse totalmente** en L se $e_i = f_i = 1$, para todo i.

Se a extensión $L \mid K$ é de Galois, entón tanto o índice de ramificación como o grado residual non dependen do ideal primo $\mathcal{O}_L$ e así

$$[L : K] = efg,$$

onde g denota ao número de ideais primos de $\mathcal{O}_L$ que dividen a $\mathfrak{p}$.

Definición 1.14. Sexa $\mathfrak{q}$ un ideal primo non nulo de $\mathcal{O}_L$. Chamamos **grupo de descomposición** de $\mathfrak{q}$ ao subgrupo

$$D_{\mathfrak{q}} = \{\sigma \in \mathrm{Gal}(L \mid K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

Por outra banda, chámase **corpo de descomposición** de $\mathfrak{q}$ ao corpo de elementos fixados por $D_{\mathfrak{q}}$, isto é,

$$K_D = \{x \in L \mid \sigma(x) = x, \text{ para todo } \sigma \in D_{\mathfrak{q}}\}.$$

Proposición 1.15. *Temos a torre de corpos $K \subset K_D \subset L$, onde $[K_D : K] = g$ e $[L : K_D] = ef$.*

Definición 1.16. Sexa $\mathfrak{q}$ un ideal primo non nulo de $\mathcal{O}_L$. Chamamos **grupo de inercia** de $\mathfrak{q}$ ao subgrupo

$$I_{\mathfrak{q}} = \{\sigma \in \mathrm{Gal}(L \mid K) \mid \sigma(x) \equiv x \pmod{\mathfrak{q}} \text{ para todo } x \in \mathcal{O}_L\}.$$

Por outra parte, chámase **corpo de inercia** de $\mathfrak{q}$ ao corpo de elementos fixados por $I_{\mathfrak{q}}$, é dicir,

$$K_I = \{x \in L \mid \sigma(x) = x, \text{ para todo } \sigma \in I_{\mathfrak{q}}\}.$$

Proposición 1.17. *Temos a torre de corpos $K \subset K_D \subset K_I \subset L$, onde $[L : K_I] = e$, $[K_I : K_D] = f$ e $[K_D : K] = g$.*

Ademais, se $\lambda = \mathcal{O}_L/\mathfrak{q}$ e $\kappa = \mathcal{O}_K/\mathfrak{p}$, tanto o grupo de descomposición como o de inercia inducen o seguinte isomorfismo

$$D_{\mathfrak{q}}/I_{\mathfrak{q}} \longrightarrow \mathrm{Gal}(\lambda/\kappa).$$

En particular, se a extensión é non ramificada en $\mathfrak{p}$, temos que $D_{\mathfrak{q}} \cong \mathrm{Gal}(\lambda/\kappa)$, posto que o grupo de inercia é trivial.

1.3. Corpos de clase

Nesta sección introduciremos o que é o grupo de clases de ideais e daremos ferramentas suficientes para probar, entre outras cousas, que este grupo é finito, explicando a súa conexión coas extensións non ramificadas do corpo. O principal apoio para desenvolver esta sección foi [9].

Definición 1.18. Un **ideal fraccionario** I de K é un $\mathcal{O}_K$-submódulo finitamente xerado non nulo de K. Se I é principal entón dirase que I é un **ideal fraccionario principal**.

Xa introducidos estes conceptos imos denotar por I_K ao **conxunto de ideais fraccionarios** de $\mathcal{O}_K$. Da mesma forma, denotaremos por P_K ao **conxunto de ideais fraccionarios principais** de $\mathcal{O}_K$, polo tanto, P_K é un subgrupo de I_K. Notemos que I_K forma un grupo abeliano coa multiplicación de ideais.

Definición 1.19. O **grupo de clases de ideais** do anel de enteiros $\mathcal{O}_K$ defínese como o conxunto cociente da seguinte relación de equivalencia

$$I \sim J \text{ se, e só se } \alpha I = \beta J \text{ para algún } \alpha, \beta \in \mathcal{O}_K \setminus \{0\}.$$

Denotarémolo por $\mathrm{Cl}(K)$. Ao seu cardinal, $|\mathrm{Cl}(K)|$, chamarémolo **número de clase** de K.

É dicir, o grupo de clases de ideais dun anel de enteiros K é o seguinte conxunto cociente

$$\mathrm{Cl}(K) = I_K / P_K.$$

De aquí deducimos o seguinte resultado:

Proposición 1.20. *Se $\mathcal{O}_K$ é un dominio de ideais principais, entón $\mathrm{Cl}(K)$ é o grupo trivial.*

Vexamos agora outros conceptos que serán de gran importancia no que segue.

Definición 1.21. Sexa K un corpo de números e sexan $\sigma_1, \dots, \sigma_n$ os embebementos de K en $\mathbb{C}$, onde $n = [K : \mathbb{Q}]$. Para cada elemento $\alpha \in K$ definimos a súa **norma** como

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Por outra banda, se consideramos L outro corpo de números con $K \subset L$ e sexan $\sigma_1, \dots, \sigma_m$ os $m = [L : K]$ embebementos de L en $\mathbb{C}$ que fixan K de forma puntual. Para cada elemento $\beta \in L$ definimos a súa norma relativa como

$$N_K^L(\beta) = \prod_{i=1}^{m} \sigma_i(\beta).$$

Definición 1.22. Sexa I un ideal non nulo de $\mathcal{O}_K$. Defínese a **norma do ideal** I como

$$\|I\| = |\mathcal{O}_K/I|.$$

A norma dun elemento e a norma dun ideal están relacionadas mediante a seguinte proposición.

Lema 1.23. *Sexan K un corpo de números e $\alpha \in \mathcal{O}_K$ non nulo. Entón dáse a seguinte igualdade*

$$|N_{\mathbb{Q}}^K(\alpha)| = \|(\alpha)\|.$$

A proba deste lema pódese atopar en [15, Teorema 3.22].

Definición 1.24. Sexa I un ideal de $\mathcal{O}_K$, defínese a súa **norma** como

$$\|I\| = |\mathcal{O}_K/I|.$$

O seguinte resultado dános finalmente a desigualdade que precisamos.

Teorema 1.25. *Sexa K un corpo de números. Entón existe $\lambda \in \mathbb{R}^+$ de forma que todo ideal non nulo I de $\mathcal{O}_K$ contén un elemento non nulo α tal que*

$$|N_{\mathbb{Q}}^K(\alpha)| \leq \lambda \|I\|.$$

Demostración. Consideremos $\{\alpha_1, \dots, \alpha_n\}$ unha base enteira de $\mathcal{O}_K$ e sexan $\sigma_1, \dots, \sigma_n$ os embebementos de K en $\mathbb{C}$. Vexamos que podemos tomar como λ a

$$\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i \alpha_j|.$$

Para calquera ideal I, tomemos m como o único enteiro positivo que cumpre que $m^n \leq \|I\| < (m+1)^n$ e consideremos os $(m+1)^n$ elementos de $\mathcal{O}_K$

$$\sum_{j=1}^{n} m_j \alpha_j,\ m_j \in \mathbb{Z},\ 0 \leq m_j \leq m.$$

Dous deses elementos son congruentes módulo I xa que hai máis de $\|I\|$ deles, se tomamos a súa diferencia obtemos un elemento non nulo de I que é da forma

$$\alpha = \sum_{j=1}^{n} m_j \alpha_j,\ m_j \in \mathbb{Z},\ |m_j| \leq m.$$

A súa norma satisfai

$$|N_{\mathbb{Q}}^{K}(\alpha)| = \prod_{i=1}^{n} |\sigma_i \alpha| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} m_j |\sigma_i \alpha_j| \leq m^n \lambda \leq \lambda \|I\|.$$

□

Observación 1.26. O λ considerado non depende do ideal elixido, senón que é independente del.

Corolario 1.27. $\mathrm{Cl}(K)$ *contén a un ideal* J *cumprindo que* $\|J\| \leq \lambda$*, sendo* λ *o mesmo que o do anterior teorema.*

Demostración. Dada unha clase de ideais C, consideremos a súa clase inversa, isto é, C^{-1}. Fixemos un ideal $I \in C^{-1}$ e obteñamos un elemento α de dito ideal da mesma forma que na proba anterior. O ideal principal (α) está contido en I, polo tanto, $(\alpha) = IJ$ para algún ideal $J \in C$. Aplicando o Lema 1.23 temos que

$$|N_{\mathbb{Q}}^{K}| = \|(\alpha)\| = \|I\| \cdot \|J\|,$$

de onde obtemos que

$$\|J\| = \frac{|N_{\mathbb{Q}}^{K}(\alpha)|}{\|I\|} \leq \frac{\lambda \|I\|}{\|I\|} = \lambda.$$

□

Corolario 1.28. *O grupo de clases* $\mathrm{Cl}(K)$ *é finito.*

Demostración. Só hai un número finito de ideais J que cumpren que $\|J\| \leq \lambda$ xa que esta desigualdade restrinxe a un conxunto finito os posibles divisores primos de J e desta forma limita as potencias nas que poden ocorrer. □

Definición 1.29. Chámase **corpo de clase de Hilbert** de K, denotado por H, á extensión abeliana non ramificada maximal de K.

Teorema 1.30. *Se* H *é o corpo de clase de Hilbert de* K*, entón a extensión* $H \mid K$ *é finita.*

Sexa $H \mid K$ unha extensión abeliana finita de K onde H é o seu corpo de clase de Hilbert. Para cada ideal primo $\mathfrak{p}$ de K que non ramifica en H, sexa $\mathfrak{q}$ un primo de H sobre K. Entón se denotamos por $\kappa = \mathcal{O}_K/\mathfrak{p}$ e $\lambda = \mathcal{O}_H/\mathfrak{q}$, temos que a extensión $\lambda \mid \kappa$ é unha extensión de corpos

finitos, polo tanto, ten un xerador canónico, o automorfismo de Frobenius e denotarémolo por σ. En particular, como $\mathfrak{p}$ non ramifica o grupo de descomposición $D_{\mathfrak{q}}$ é isomorfo a $\mathrm{Gal}(\lambda \mid \kappa)$, polo que temos un elemento canónico de $D_{\mathfrak{q}}$, chamado Frobenius de $\mathfrak{q}$.

Como a extensión é de Galois existe $\sigma \in \mathrm{Gal}(H \mid K)$ de tal forma que para dous primos distintos $\mathfrak{q}_1, \mathfrak{q}_2$ de H sobre o ideal primo $\mathfrak{p}$ temos a seguinte relación

$$\sigma \,\mathrm{Frob}_{\mathfrak{q}_1}\, \sigma^{-1} = \mathrm{Frob}_{\mathfrak{q}_2}.$$

Ademais, como a extensión é abeliana obtemos que $\mathrm{Frob}_{\mathfrak{q}_1} = \mathrm{Frob}_{\mathfrak{q}_2}$, polo que podemos falar do Frobenius de $\mathfrak{p}$ sen ambigüidade. De feito, temos o chamado **isomorfismo de Artin**,

$$\begin{array}{rccc} \varphi\colon & I_K & \longrightarrow & \mathrm{Gal}(H \mid K) \\ & \mathfrak{p} & \longmapsto & \mathrm{Frob}_{\mathfrak{p}} \end{array}$$

o cal é sobrexectivo e ademais o seu núcleo correspóndese con P_K. Desta forma temos o seguinte corolario, a partir do primeiro teorema de isomorfía.

Corolario 1.31. *O grupo de clases de ideais dun anel de enteiros arbitrario, $\mathcal{O}_K$, é isomorfo ao grupo de Galois da extensión do corpo de clase de Hilbert de K respecto a K, é dicir,*

$$\mathrm{Cl}(K) = I_K/P_K \cong \mathrm{Gal}(H \mid K).$$

1.4. Teoría de corpos de clase

A teoría de corpos de clase é o estudo das relacións entre a aritmética dun corpo e as súas extensións abelianas. O isomorfismo de Artin pódese entender como un primeiro resultado nesa relación: o grupo de clases un corpo de números K é un obxecto que se define en termos da aritmética do corpo (os seus ideais); por outra banda, $\mathrm{Gal}(H \mid K)$ é o grupo de Galois dunha extensión abeliana sobre a que se impoñen unhas condicións de non ramificación.

Ao longo deste traballo precisaremos algún resultado máis sobre a teoría de corpos de clase no caso local. Para iso, sexa K unha extensión finita de $\mathbb{Q}_p$ e sexa K^{ab} a súa extensión abeliana maximal, é dicir, a composición de todas as extensións abelianas de K. Escribimos $\mathcal{O}_K$ para o anel de enteiros de K e dicimos que π é un uniformizador de $\mathcal{O}_K$ se é un xerador do seu único ideal maximal. Para o desenvolvemento desta sección seguimos [18], aínda que aquí ímonos limitar a dous resultados que aparecerán con posterioridade.

O primeiro resultado importante sobre a teoría de corpos de clase local é o seguinte. Para a demostración, referimos ao terceiro capítulo de [18].

Proposición 1.32. *Sexa K unha extensión finita de $\mathbb{Q}_p$. Existe un único homomorfismo continuo*

$$\theta_K \colon K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}} \mid K)$$

coa propiedade de que, para calquera extensión abeliana finita $L \mid K$, o homomorfismo

$$\theta_{L|K} \colon K^\times \longrightarrow \mathrm{Gal}(L \mid K)$$

dado pola composición de θ_K coa proxección ao cociente cumpre a seguinte propiedade:

- *se $L \mid K$ non ramifica, entón $\theta_{L|K}(\pi) = \mathrm{Frob}_{L|K}$ para calquera uniformizador π de $\mathcal{O}_K$;*
- *o morfismo $\theta_{L|K}$ é sobrexectivo e o seu núcleo é $N_{L|K}(L^\times)$.*

Sexa $I \subset \mathrm{Gal}(K^{\mathrm{ab}} \mid K)$ o subgrupo de inercia. Do resultado anterior, pódese deducir o seguinte corolario.

Corolario 1.33. *O homomorfismo anterior induce un homomorfismo sobrexectivo e continuo*

$$\theta_K \colon \mathcal{O}_K^\times \longrightarrow I$$

que herda as propiedades da aplicación anterior.

Capítulo 2

Estrutura dos módulos sobre $\mathbb{Z}_p[[T]]$

Fixado p un número primo, neste capítulo veremos as principais características do anel de series de potencias con coeficientes en $\mathbb{Z}_p$, isto é,

$$\mathbb{Z}_p[\![T]\!] = \left\{ \sum_{i=0}^{\infty} a_i T^i \text{ con } a_i \in \mathbb{Z}_p \right\}.$$

Por comodidade de notación chamaremos a este anel Λ. Comezaremos probando un dos resultados máis importantes do capítulo, o teorema de preparación de Weierstrass, que nos ofrece unha descomposición dos elementos de Λ para concluír que este é un dominio de factorización única. Continuaremos vendo outras propiedades deste anel e remataremos probando o teorema de clasificación, que nos permite descompoñer os Λ-módulos finitamente xerados. A principal fonte para escribir este capítulo foi [26]. Un tratamento similar podémolo atopar en [11].

2.1. Teorema de preparación de Weierstrass

Lema 2.1. *Sexan os polinomios $f(T), g(T) \in \Lambda$, onde $f(T) = a_0 + a_1 T + \ldots$ con $p \mid a_i$ para $0 \leq i \leq n-1$, pero $a_n \in \mathbb{Z}_p^\times$. Entón podemos escribir de forma única:*

$$g(T) = q(T)f(T) + r(T),$$

onde $q(T) \in \Lambda$ e $r(T) \in \mathbb{Z}_p[T]$ é un polinomio de grao como moito $n-1$.

Demostración. Comezaremos probando a unicidade da descomposición. Supoñamos que temos dúas expresións coa forma anterior, isto é, $g = q_1 f + r_1 = q_2 f + r_2$. Definamos $Q = q_1 + q_2$ e $R = r_1 - r_2$, entón temos que $Qf + R = 0$, polo que basta ver que $Q = R = 0$.

Supoñamos que $Q, R \neq 0$ entón $p \nmid Q$ ou $p \nmid R$. Reducindo módulo p temos que $p \mid R$ xa que $R(T) \in \mathbb{Z}_p[T]$ e, polo tanto, $p \mid Qf$.

Posto que $a_n \in \mathbb{Z}_p^\times$, $p \nmid a_n$ e temos que $p \nmid f$, polo tanto, $p \mid Q$ chegando a unha contradición, polo que $Q = R = 0$.

Pasamos agora á demostración da existencia. Sexa o polinomio $h(T) = \sum_{i=0}^{\infty} b_i T^i \in \Lambda$, definimos $\tau = \tau_n : \Lambda \longrightarrow \Lambda$ onde $\tau(h(T)) = \sum_{i=n}^{\infty} b_i T^{i-n}$. Tense que τ é $\mathbb{Z}_p$-linear e, ademais, satisfai as seguintes propiedades:

1. $\tau(T^n h(T)) = h(T)$ para todo $h(T) \in \Lambda$,
2. $\tau(h(T)) = 0$ se, e só se, $h(T) \in \mathbb{Z}_p[T]$ onde o grao de h é menor ou igual a $n-1$.

En efecto, consideremos $h(T) \in \Lambda$, entón $\tau(T^n h(T)) = \tau(\sum_{i=0}^{\infty} b_i T^{i+n}) = \sum_{i=0}^{\infty} b_i T^i = h(T)$.

Por outra banda, $\tau(h(T)) = 0$ se, e só se, $b_i = 0$ para todo $i \geq n$ se, e só se, $h(T) \in \mathbb{Z}_p[T]$ onde o grao de h é menor ou igual a $n-1$.

Podemos expresar f da seguinte forma:

$$f(T) = pP(T) + T^n U(T),$$

onde $P(T) \in \Lambda$ é un polinomio de grao menor que n e $U(T) = a_n + a_{n+1}T + ... = \tau(f(T))$. Como $a_n \in \mathbb{Z}_p^\times$, tense que $p \nmid a_n$ e así $U(T)$ é unha unidade de Λ xa que este é un anel local.

Consideremos agora o polinomio

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j p^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g). \tag{2.1}$$

Para $j = 2$ temos que,

$$\left(\tau \circ \frac{P}{U}\right)^2 \circ \tau(g) = \tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(g)\right)\right).$$

O feito de que p^j apareza na suma 2.1 fai que a serie converxa, polo que $q(T)$ está ben definida en Λ. Agora, se lle aplicamos τ a

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

obtemos

$$\tau(qf) = p\tau(qP) + \tau(T^n qU) = p\tau(qP) + qU,$$

onde a última igualdade se segue da propiedade 1.

Por outra parte,

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

Polo tanto,

$$\tau(qf) = \tau(g).$$

Desta forma, pola propiedade 2, temos que $g(T) = q(T)f(T)+r(T)$, onde o grao de $r(T)$ é menor que $n-1$ co que remata a proba. □

Agora daremos nome a un tipo de polinomio que será de gran importancia no que resta de capítulo, os polinomios mónicos en Λ con coeficientes divisibles por p.

Definición 2.2. Un polinomio non constante $P(T) \in \Lambda$ é **distinguible** se $P(T) = T^n + a_{n-1}T^{n-1} + ... + a_0$, con $p \mid a_i$ para $0 \leq i \leq n-1$.

Polo tanto, acabamos de describir no Lema 2.1 un algoritmo de división para polinomios distinguibles.

Teorema 2.3 (Preparación de Weierstrass)**.** *Sexa a serie de potencias non nula* $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$. *Entón existe un único polinomio distinguible* $P(T)$*, unha única unidade* $U(T) \in \Lambda^\times$ *e un único* $m \in \mathbb{N}$ *de tal forma que*

$$f(T) = p^m U(T)P(T).$$

Demostración. Consideremos $g(T) = T^n$ no Lema 2.1. Nesas condicións temos a seguinte descomposición: $T^n = q(T)f(T) + r(T)$. Posto que

$$q(T)f(T) \equiv q(T)(a_n T^n + \text{termos maiores}) \pmod{p},$$

tense que $r(T) \equiv 0 \pmod{p}$, é dicir, $p \mid r$ e así, $P(T) = T^n - r(T)$ é un polinomio distinguible de grao n. Sexa q_0 o termo constante de $q(T)$, entón $1 \equiv q_0 a_n \pmod{p}$ polo que $q_0 \in \mathbb{Z}_p^\times$ e, consecuentemente, $q(T) \in \Lambda^\times$. Consideremos agora $U(T) = q(T)^{-1} \in \Lambda^\times$. Entón, podemos expresar

$f(T) = U(T)P(T)$. Ademais, como calquera polinomio distinguible de grao n pode escribirse como $P(T) = T^n - r(T)$, podemos transformar $f(T) = U(T)P(T)$ en $T^n = U(T)^{-1}f(T) + r(T)$.

A unicidade séguese da unicidade do Lema 2.1. □

Observación 2.4. O teorema de preparación de Weierstrass xorde a partir da súa versión complexa. Esta afirma que dado $(z, z_2, \dots, z_n) \in \mathbb{C}^n$ se temos unha función analítica f tal que a imaxe na orixe é cero e $f(z, z_2, \dots, z_n)$ ten algún termo que involucre a z (vendo f como unha serie de potencias), entón nunha veciñanza da orixe temos que

$$f(z, z_2, \dots, z_n) = W(z)g(z, z_2, \dots, z_n),$$

onde $W(z)$ sería un análogo ao polinomio distinguible $P(T)$ e $g(z, z_2, \dots, z_n)$ o sería de $U(T)$.

De feito, a versión do teorema que acabamos de ver non é máis ca un caso particular, xa que este pódese extender a calquera anel de series de potencias sobre aneis locais completos.

Corolario 2.5. *Sexa $f(T) \in \Lambda$. Entón, ou ben $f(T)$ é nulo, ou ben $f(T)$ ten unha cantidade finita de ceros.*

Demostración. Supoñamos que $f(T)$ é non nulo e que ten unha cantidade infinita de ceros. Pola descomposición do Teorema 2.3 temos que $f(T) = p^m U(T)P(T)$. Desta forma, $U(T)$ non pode ter unha cantidade infinita de ceros xa que é unha unidade de Λ. Por outra parte, $P(T)$ ten unha cantidade finita de ceros xa que é un polinomio, co que chegamos a unha contradición. □

Posto que Λ é un dominio onde os seus elementos poden descompoñerse de forma única como produto de irredutibles temos, como adiantabamos ao principio do capítulo, o seguinte resultado.

Corolario 2.6. *Λ é un dominio de factorización única onde os elementos irredutibles son p e os polinomios distinguibles irredutibles. Ademais, as unidades de Λ son as series de potencias con termo constante en $\mathbb{Z}_p^\times$.*

Demostración. Grazas ao teorema de preparación de Weiestrass (Teorema 2.3), se consideramos un polinomio non nulo $f(T) \in \Lambda$, entón este pode ser descomposto de forma única como

$$f(T) = p^m U(T)P(T),$$

con $m \in \mathbb{N}$, $U(T) \in \Lambda^\times$ e $P(T)$ un polinomio distinguible. Posto que $\mathbb{Z}_p$ é un dominio de factorización única, entón Λ tamén o é. Desta forma, só falta ver que nesta devandita factorización os irredutibles son, en particular, distinguibles. Consideremos o polinomio distinguible

$$P(T) = P_1(T) \cdots P_n(T),$$

onde para cada $1 \leq i \leq n$, $P_i(T) \in \Lambda$ é irredutible. Necesariamente cada irredutible $P_i(T)$ é distinguible. En efecto, por unha parte, se algún coeficiente non principal asociado a algún $P_i(T)$ non está en $p\mathbb{Z}_p$ entón tampouco o estaría en $P(T)$ o que nos levaría a unha contradición. Por outra parte, sexa a_i o coeficiente principal asociado ao polinomio irredutible $P_i(T)$, basta considerar como irredutible distinguible a $\widetilde{P}_i = a_i^{-1} P_i$, co que quedaría probado. □

2.2. Propiedades do anel $\mathbb{Z}_p[[T]]$

Probado que Λ é un dominio de factorización única, vexamos outras propiedades interesantes deste anel.

Proposición 2.7. *Λ é un anel noetheriano.*

Demostración. Como $\mathbb{Z}_p$ é noetheriano, polo teorema da base de Hilbert (véxase [1, Teorema 7.5]), sabemos que $\mathbb{Z}_p[T]$ é tamén noetheriano. Como todo ideal I de Λ está contido en $\mathbb{Z}_p[T]$, I está finitamente xerado e así Λ é noetheriano. □

Definición 2.8. Dous polinomios dinse que son **primos relativos** se non teñen factores comúns.

Notación 2.9. Sexan $f, g \in \Lambda$, denotaremos por (f, g) ao ideal xerado polas combinacións lineares de f e g con coeficientes en Λ, é dicir,

$$(f, g) = \{af + bg, \text{ con } a, b \in \Lambda\}.$$

Lema 2.10. *Sexan $f, g \in \Lambda$ primos relativos. Entón $[\Lambda : (f, g)] < \infty$.*

Demostración. Sexa $h \in (f, g)$ con grao minimal. Entón temos que $h = p^s H$ con $H = 1$ ou H distinguible. Supoñamos que $H \neq 1$. Como f e g son coprimos, podemos asumir que $H \nmid f$. Pero,

$$f = Hq + r, \text{ grao}(r) < \text{grao}(H) = \text{grao}(h),$$

co que

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

Como $p^s f, hq \in (f, g)$, temos que $p^s r \in (f, g)$ contradicindo a minimalidade de h. Polo tanto, $H = 1$ e $h = p^s$. Sen perda de xeneralidade, podemos asumir que $p \nmid f$ e que f é distinguible. Entón temos que

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

Polo algoritmo da división tense que $\Lambda|(p^s, f)$ é finito xa que cada elemento de Λ é congruente módulo f a un polinomio de grao menor que o grao de f. A cantidade deste tipo de polinomios con coeficientes módulo p^s é finita. □

Lema 2.11. *Sexan $f, g \in \Lambda$ primos relativos, entón:*

1. *A aplicación*

$$\begin{array}{rccc} \phi\colon & \Lambda/(fg) & \longrightarrow & \Lambda/(f) \bigoplus \Lambda/(g) \\ & x \pmod{fg} & \longmapsto & (x \pmod{f}, x \pmod{g}) \end{array}$$

   é inxectiva con conúcleo finito.

2. *Existe unha aplicación inxectiva*

$$\varphi : \Lambda/(f) \bigoplus \Lambda/(g) \longrightarrow \Lambda/(fg),$$

   con conúcleo finito.

Demostración. 1. Por unha parte, consideremos $a \in \Lambda/(fg)$ de tal forma que $\phi(a) = (0 \pmod{f}, 0 \pmod{g})$. Entón, $f \mid a$ e $g \mid a$, pero do feito de ser relativamente primos f e g séguese que $fg \mid a$ e así $a \equiv 0 \pmod{fg}$. Polo tanto, ϕ é inxectivo.

Por outra banda, vexamos que $\operatorname{coker}(\phi) = (\Lambda/(f) \oplus \Lambda/(g))/\phi(\Lambda/(fg))$ é finito. Consideremos $(a \pmod{f}, b \pmod{g})$. Primeiro probaremos que se $a - b \in (f,g)$ entón (a,b) está na imaxe. En efecto, podemos expresar $a - b = fA + gB$ con $A, B \in \Lambda$. Consideremos agora $c = a - \alpha f = b + \beta g$, entón

$$\begin{cases} c \equiv a \pmod{f}, \\ c \equiv b \pmod{g}. \end{cases}$$

Agora, posto que $(a,b) \in \Lambda/(f) \oplus \Lambda/(g)$, podemos tomar un c tal que $(a,b) \equiv (0,c) \pmod{(f,g)}$ e así, polo Lema 2.10, $\{r_1, \ldots, r_n\}$ é un conxunto finito de representantes de $\Lambda/(f,g)$. Desta maneira,

$$\{(0 \pmod{f}, r_i \pmod{g}), 1 \leq i \leq n\}$$

é un conxunto finito de representantes para o conúcleo.

2. Consideremos $M = \phi(\Lambda/(fg))$ e $N = \Lambda/(f) \oplus \Lambda/(g)$. Polo apartado anterior, como ϕ é inxectivo temos que $M \cong \Lambda/(fg)$, así $M \subseteq N$ e N/M é finito.

   Sexa P un polinomio distinguible en Λ relativamente primo con fg definido da seguinte forma:

$$\begin{array}{rccc} P\colon & N & \longrightarrow & N \\ & (x,y) & \longmapsto & (P\cdot x, P\cdot y) \end{array}$$

   Como N/M é finito tense que

$$P^i(x,y) \equiv P^j(x,y) \pmod{M},$$

   para algúns enteiros i, j tales que $j > i$. Disto deducimos que $P^i(1-P^{j-i})(x,y) \in M$ e como $1 - P^{j-i} \in \Lambda^\times$, temos que $P^i(x,y) \in M$. Como N é finitamente xerado como Λ-módulo, temos que existe un k de tal forma que $P^k N \subseteq M$. Supoñamos agora que $P^K(x,y) = 0$ en N, entón $f \mid P^k x$ e $g \mid P^k y$. Como P e fg son relativamente primos $f \mid x$ e $g \mid y$ e así $(x,y) = 0$ en N. Polo tanto,

$$P^k : N \longrightarrow M \cong \Lambda/(fg)$$

   é inxectivo. Por outra parte, $(P^k, fg) \subseteq P^k(N)$ e como polo Lema 2.10 $\Lambda/(P^k, fg)$ é finito entón o conúcleo de p^k tamén o será.

□

Proposición 2.12. *Os ideais primos de Λ son 0, (p,T), (p) e os ideais $(P(T))$ onde $P(T)$ é irredutible e distinguible. O ideal (p,T) é o único ideal maximal e, polo tanto, Λ é un anel local.*

Demostración. Está claro que todos estes ideais son primos xa que nos dominios de factorización única hai unha correspondecia biunívoca entre primos e irredutibles. Para demostrar que Λ é un anel local probaremos primeiro que (p,T) é un ideal maximal e, posteriormente, que é o único ideal maximal.

Definimos a aplicación

$$\begin{array}{rccc} \phi\colon & \Lambda & \longrightarrow & \mathbb{Z}_p/p\mathbb{Z}_p \\ & f & \longmapsto & f(0) \pmod{p} \end{array}$$

Temos que $\ker(\phi) = (p,T)$ e, polo primeiro teorema de isomorfía, $\Lambda/\ker(\phi) \cong \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. Como $\mathbb{Z}/p\mathbb{Z}$ é un corpo, temos que (p,T) é maximal. Vexamos agora que é único. Sexa $\mathfrak{p} \neq 0$ primo, probemos que $\mathfrak{p} \subseteq (p,T)$. Sexa $h \in \mathfrak{p}$ de grao minimal, entón $h = p^s H$ con $H = 1$ ou H distinguible. Posto que $\mathfrak{p}$ é primo, $p \in \mathfrak{p}$ ou $H \in \mathfrak{p}$.

Ben, se $1 \neq H \in \mathfrak{p}$, temos que H é irredutible pola minimalidade do grao de h. Se $H = 1$, entón $h = p^s$. En ambos casos, $(f) \subseteq \mathfrak{p}$, onde $f = p$ ou f é irredutible e distinguible. Se $(f) = \mathfrak{p}$, entón $\mathfrak{p} = (p)$ ou $\mathfrak{p} = (f)$, con f irredutible e distinguible co que xa estaría posto que $\mathfrak{p} \subseteq (p, T)$. Se pola contra, $(f) \subsetneq \mathfrak{p}$, entón existe un $g \in \mathfrak{p}$ tal que $f \nmid g$. Como f é irredutible entón f é primo relativo con g e así temos, polo Lema 2.10, que $[\Lambda : (f, g)] < \infty$. Como $(f, g) \subseteq \mathfrak{p}$, entón $[\Lambda : \mathfrak{p}] < \infty$. Desta forma, $\Lambda/\mathfrak{p}$ é un $\mathbb{Z}_p$-módulo finito e así $p^n \in \mathfrak{p}$ para un n suficientemente grande. Polo tanto, $p \in \mathfrak{p}$ xa que $\mathfrak{p}$ é primo. Ademais, $T^i \equiv T^j \pmod{p}$ para algún $i < j$, pero $1 - T^{j-i} \in \Lambda^\times$, polo que $T^i \in \mathfrak{p}$. Desta forma, $T \in \mathfrak{p}$ e $(p, T) \subseteq \mathfrak{p}$. Pero, pola maximalidade de (p, T), chegamos a que $(p, T) = \mathfrak{p}$.

Como todos os ideais primos están contidos en (p, T) temos que o único ideal maximal e así Λ é un anel local. □

Corolario 2.13. Λ *non é un dominio de ideais principais.*

Demostración. Vexamos que o ideal (p, T) non é principal. En efecto, supoñamos que existe $f \in \Lambda$ de tal forma que $(f) = (p, T)$, entón $f \mid p$ e $f \mid T$. Como $f \mid p$, $f = \pm 1$ ou $f = \pm p$. Se $f = \pm 1$, $(f) = \Lambda$, contradición coa maximalidade de (p, T) (como vimos na Proposición 2.12). Se $f = \pm p$, $(f) = p\Lambda$ non pode conter T. □

Observación 2.14. Sexa A un anel local onde $\mathfrak{m}$ é o seu ideal maximal. Se consideramos o conxunto de potencias do ideal maximal, isto é, $\mathfrak{m}^n$ con $n \geq 0$, estas determinan unha base de veciñanzas abertas de 0:

$$0 \subset ... \subset \mathfrak{m}^n \subset \mathfrak{m}^{n-1} \subset ... \subset \mathfrak{m}^2 \subset \mathfrak{m} \subset \mathfrak{m}^0 = A.$$

Entón podemos dotar a dito anel dunha topoloxía, a chamada **topoloxía $\mathfrak{m}$-ádica**. De feito, se o anel local A é noetheriano entón todos os ideais de A son pechados.

Polo tanto, cando falemos da topoloxía do anel Λ estaremos facendo referencia á topoloxía (p, T)-ádica.

Proposición 2.15. *Sexa $f \in \Lambda$ con $f \notin \Lambda^\times$. Entón $\Lambda/(f)$ é infinito.*

Demostración. Se f é nulo entón $\Lambda/(f) = \Lambda$ que é infinito. Supoñamos agora que f é non nulo, polo que basta considerar $f = p$ e f distinguible. Se $f = p$, $\Lambda/(f) \cong \mathbb{Z}/p\mathbb{Z}[\![T]\!]$. Se f distinguible, o algoritmo da división proporciona un límite no grao dos polinomios no cociente. □

2.3. Teorema de clasificación

Comezaremos esta sección definindo un concepto clave para poder clasificar os Λ-módulos finitamente xerados.

Definición 2.16. Diremos que dous Λ-módulos M e M' son **pseudoisomorfos**, se existe un homomorfismo $M \longrightarrow M'$ con núcleo e conúcleo finitos. Denótase como $M \sim M'$.

A definición anterior equivale á existencia dunha sucesión exacta de Λ-módulos

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

onde A e B son Λ-módulos finitos.

Observación 2.17. A relación "ser pseudoisomorfos" non é simétrica. Para ver isto consideremos, por exemplo, (p, T) e Λ. É evidente que $(p, T) \sim \Lambda$ xa que basta considerar a inclusión e temos que $\ker(i) = \{0\}$ e $\operatorname{coker}(i) = \Lambda/(p, T) \cong \mathbb{Z}/p\mathbb{Z}$.

Por outra banda, tense que $\Lambda \nsim (p, T)$. Consideremos $\phi : \Lambda \to (p, T)$ definida de forma que $\phi(1) = f$. Polo tanto, temos que $\phi(\Lambda) = (f) \subseteq (p, T)$. Pola Proposición 2.15, $\Lambda/(f)$ é infinito e da relación de inclusións $(f) \subseteq (p, T) \subseteq \Lambda$, xunto con

$$\Lambda/(f) \Big/ (p, T)/(f) \cong \Lambda/(p, T),$$

deducimos que $(p, T)/(f)$ é infinito, xa que $\Lambda/(p, T)$ é finita polo Lema 2.10. Desta forma, o conúcleo de ϕ é infinito.

Con este novo concepto, decatámonos de que o Lema 2.11 móstranos que se f e g son primos relativos entón:

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

O teorema de clasificación foi probado inicialmente por Iwasawa traballando sobre o anel $\mathbb{Z}_p[\![\Gamma]\!]$, onde Γ é un grupo topolóxico multiplicativo isomorfo ao grupo aditivo $\mathbb{Z}_p$. Máis tarde, Serre [24] observou que $\mathbb{Z}_p[\![\Gamma]\!]$ era isomorfo a Λ e deu unha proba alternativa á dada por Iwasawa utilizando resultados máis xerais de álxebra conmutativa. Cohen [12] aportou outra proba utilizando operacións en filas e columnas como no caso de dominios de ideais principais. Para probar dito teorema seguiremos a interpretación de Lang [11] á proba dada por Cohen.

Teorema 2.18 (Teorema de clasificación)**.** *Se M é un Λ-módulo finitamente xerado, entón temos que:*

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

onde $r, s, t, n_i, m_j \in \mathbb{Z}$ e os f_j son distinguibles e irredutibles.

Demostración. Antes de comezar co que propiamente é a demostración do teorema supoñamos que o Λ-módulo M está xerado por $u_1, \dots, u_n$, con varias relacións $\sum_{i=1}^{n} \lambda_i u_i = 0$ onde $\lambda_i \in \Lambda$.

Denotemos por R a estas relacións. R é un submódulo de Λ^n e como Λ é noetheriano (pola Proposición 2.7), estas relacións están finitamente xeradas. Polo tanto, M pode ser representado por unha matriz de dimensión finita onde as súas filas son da forma $(\lambda_1, \dots, \lambda_n)$ e seguen a relación descrita anteriormente. Aínda que fagamos abuso de notación denotaremos esta matriz por R.

Como adiantabamos anteriormente imos necesitar unha serie de operacións para aplicar á nosa matriz R. Estas operacións preservan o tamaño da matriz e son:

Operación 1. Podemos permutar filas ou columnas.

Operación 2. Podemos engadir un múltiplo dunha fila ou columna a outra fila ou columna, respectivamente. Temos o caso especial de se $\lambda' = q\lambda + r$, entón

$$\begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & \lambda' & \cdots \\ \vdots & & \vdots & \end{pmatrix} \longrightarrow \begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & r & \cdots \\ \vdots & & \vdots & \end{pmatrix}.$$

Operación 3. Podemos multiplicar unha fila ou columna por unha unidade de Λ.

Estas operacións utilízanse para dominios de ideais principais e preservan a clase de isomorfía. Malia isto, imos necesitar tres operacións máis, é aquí onde traballamos cos pseudoisomorfismos (e, evidentemente, preservan a clase de pseudoisomorfía).

Operación 4. Se a matriz R contén unha fila da forma $(\lambda_1, p\lambda_2, \dots, p\lambda_n)$ con $p \nmid \lambda_1$, entón R muda á matriz R' onde a súa primeira fila é $(\lambda_1, p\lambda_2, \dots, p\lambda_n)$ e o resto de filas son as mesmas filas de R só que os seus primeiros elementos están multiplicados por p, é dicir,

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

No caso especial de que $\lambda_2 = \dots = \lambda_n = 0$, podemos multiplicar os primeiros elementos do resto de filas por unha potencia calquera de p.

Operación 5. Se todos os elementos da primeira columna de R son divisibles por p^k e se hai unha fila $(p^k\lambda_1, \dots, p^k\lambda_n)$, con $p \nmid \lambda_1$, entón podemos cambiar á matriz R' que é a mesma que R só que $(p^k\lambda_1, \dots, p^k\lambda_n)$ muda a $(\lambda_1, \dots, \lambda_n)$, isto é,

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix}.$$

Operación 6. Se R contén unha fila da forma $(p^k\lambda_1, \dots, p^k\lambda_n)$ e para algún λ non divisible por p, $(\lambda\lambda_1, \dots, \lambda\lambda_n)$ é tamén unha relación (non necesariamente explícita contida en R), entón podemos cambiar a matriz R por R', onde R' é a mesma matriz ca R só que cambiamos a fila $(p^k\lambda_1, \dots, p^k\lambda_n)$ por $(\lambda_1, \dots, \lambda_n)$.

Xa descritas todas as operacións que imos utilizar, que chamaremos operacións admisibles, definamos algúns conceptos clave para comezar a demostración.

Sexa $f \in \Lambda$ non nulo, entón, polo Teorema 2.3, podemos descompoñer f en

$$f(T) = p^m U(T) P(T),$$

onde U é unha unidade de Λ e P é distinguible.

Definición 2.19. Chamaremos **grao de Weierstrass** de $f(T)$ a

$$\operatorname{grao}_w f(T) = \begin{cases} \infty, & m > 0, \\ \operatorname{grao}(P(T)), & m = 0. \end{cases}$$

Definición 2.20. Sexa unha matriz R, definimos

$$\operatorname{grao}^{(k)}(R) = \text{mín}\, \operatorname{grao}_w(a'_{ij}) \text{ para } i, j \geq k,$$

onde (a'_{ij}) recorre todas as relacións de matrices obtidas de R mediante operacións admisibles que non modifican as primeiras $k-1$ filas.

Definición 2.21. Dicimos que a matriz R está en **forma** $(r-1)$**-normal** se ten a forma

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

onde cada λ_{kk} é distinguible e

$$\operatorname{grao}(\lambda_{kk}) = \operatorname{grao}_w(\lambda_{kk}) = \operatorname{grao}^{(k)}(R), \text{ para } 1 \leq k \leq r-1.$$

Xa definida a forma r-normal dunha matriz imos probar un resultado para aplicalo posteriormente á demostración.

Lema 2.22. *Sexa R' unha matriz en forma r-normal onde os primeiros $r-1$ elementos diagonais son iguais aos de R. Se a submatriz B é non nula, entón R pode transformarse en R' mediante operacións admisibles.*

Demostración. O caso especial da Operación 4 permítenos asumir, cando sexa necesario, que unha potencia de p suficientemente grande divide cada λ_{ij} con $i \geq r$ e $j \leq r-1$, isto é, $p^N \mid A$ onde N é suficientemente grande para que $p^n \nmid B$. Se empregamos a Operación 5 podemos asumir que $p \nmid B$. Podemos asumir tamén que a submatriz B contén un elemento λ_{ij} de tal maneira que

$$\operatorname{grao}_w(\lambda_{ij}) = \operatorname{grao}^{(r)}(R) < \infty.$$

Se $\lambda_{ij} = U(T)P(T)$, entón multiplicamos a columna j-ésima por $U^{-1}(T)$. Polo tanto, podemos asumir que λ_{ij} é distinguible, e tamén que $\lambda_{ij} = \lambda_{rr}$ pola Operación 1.

Empregando o algoritmo da división, podemos utilizar a Operación 2 para asumir que λ_{rj} é un polinomio con grao estritamente menor ao grao de λ_{rr} con $j \neq r$ e tamén ao grao de λ_{jj} con $j < r$.

Como λ_{rr} ten grao de Weierstrass minimal en B, temos que $p \mid \lambda_{rj}$ para $j > r$. Pola Operación 4 podemos asumir que $p^N \mid \lambda_{rj}$ con $j < r$ para un N suficientemente grande. Supoñamos que $\lambda_{rj} \neq 0$ para algún $j > r$. De novo, pola Operación 4 podemos eliminar a potencia de p dalgún λ_{rj} non nulo. Desta forma,

$$\operatorname{grao}_w \lambda_{rj} = \operatorname{grao} \lambda_{rj} < \operatorname{grao} \lambda_{rr} = \operatorname{grao}_w \lambda_{rr},$$

o que é imposible e así, $\lambda_{rj} = 0$ para $j > r$.

Por outra banda, se algún λ_{rj} é non nulo para $j < r$, usamos a Operación 4 para obter $p \nmid \lambda_{rj}$ para algún j. Pero temos,

$$\operatorname{grao}_w \lambda_{rj} \leq \operatorname{grao} \lambda_{rj} < \operatorname{grao} \lambda_{jj} = \operatorname{grao}_w \lambda_{jj}.$$

Como $\operatorname{grao}_w \lambda_{jj} = \operatorname{grao}^{(j)}(R)$, chegamos a unha contradición pola definición de $\operatorname{grao}^{(j)}(R)$. Desta forma $\lambda_{rj} = 0$ para todo $j \neq r$, co que queda probada a afirmación. □

Se comezamos cunha matriz R e $r = 1$, podemos cambiar R ata obter unha matriz do tipo

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

onde os λ_{jj} son distinguibles e $\operatorname{grao} \lambda_{jj} = \operatorname{grao}^{(j)}(R)$ para $j \leq r$. Polo algoritmo da división podemos asumir que λ_{ij} é un polinomio con grao estritamente menor ao grao de λ_{jj} para $i \neq j$.

Supoñamos que λ_{ij} é non nulo para algún $i \neq j$. Posto que $\operatorname{grao}_w \lambda_{jj}$ é minimal, $p \mid \lambda_{ij}$, polo que temos unha relación non nula que é divisible por p, $(\lambda_{i1}, \dots, \lambda_{ir}, 0, \dots, 0)$. Sexa $\lambda = \prod_{i=1}^{r} \lambda_{ii}$. Entón, $p \nmid \lambda$ porque os λ_{jj} son distinguibles e

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

é tamén unha relación, xa que $\lambda_{jj} u_j = 0$. Pola Operación 6 podemos asumir que $p \nmid \lambda_{ij}$ para algún j, polo que

$$\operatorname{grao}_w \lambda_{ij} \leq \operatorname{grao} \lambda_{ij} < \operatorname{grao} \lambda_{jj} = \operatorname{grao}^{(j)}(R).$$

Isto non é posible, polo que $\lambda_{ij} = 0$ para todo i e j con $i \neq j$. Isto quere dicir que $A = 0$. Polo tanto, en termos de Λ-módulos temos

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

Agora falta engadir os factores $\Lambda/(p^k)$ que foron eliminados coa Operación 5, mais o Lema 2.11 permite asegurar que todos os λ_{ij} son irredutibles. Desta maneira queda probado o resultado. □

Capítulo 3

Propiedades das $\mathbb{Z}_p$-extensións

O obxectivo deste capítulo é introducir a noción de $\mathbb{Z}_p$-extensión e establecer as súas propiedades principais. En particular, introduciremos un $\mathbb{Z}_p[\![T]\!]$-módulo e probaremos que é finitamente xerado. Iso permitiranos, no seguinte capítulo, empregar o teorema de clasificación para deducir información sobre o número de clases dos corpos intermedios dunha $\mathbb{Z}_p$-extensión. Para desenvolver estes resultados precisamos entender de xeito preciso o comportamento dos primos nas $\mathbb{Z}_p$-extensións. Para escribir este capítulo guiámonos, principalmente, por [6], [13] e [26].

3.1. $\mathbb{Z}_p$-extensións

De agora en adiante asumiremos que K é un corpo de números. Consideremos a torre de corpos

$$K = K_0 \subset K_1 \subset K_2 \subset ... \subset K_\infty = \bigcup_{i=1}^{n} K_n. \tag{3.1}$$

Definición 3.1. Definimos a **$\mathbb{Z}_p$-extensión** de K como a extensión $K_\infty \mid K$ cuxo grupo de Galois é isomorfo a $\mathbb{Z}_p$, é dicir, $\mathrm{Gal}(K_\infty \mid K) \cong \mathbb{Z}_p$.

Proposición 3.2. *Sexa $K_\infty \mid K$ unha $\mathbb{Z}_p$-extensión. Entón para cada $n \geq 0$ existe unha única subextensión K_n cumprindo que $[K_n : K] = p^n$. De feito, as subextensións K_n xunto con K_∞ son as únicas subextensións intermedias entre K e K_∞.*

Demostración. Polo teorema de Correspondencia de Galois para extensións infinitas (véxase [18, Teorema 7.13]) sabemos que hai unha correspondencia biunívoca entre as subextensións de $K_\infty \mid K$ e os subgrupos pechados de $\mathrm{Gal}(K_\infty \mid K) \cong \mathbb{Z}_p$. Polo tanto, vexamos quen son os subgrupos pechados de $\mathbb{Z}_p$.

Sexa S un subgrupo pechado de $\mathbb{Z}_p$ e sexa $x \in S$ de tal forma que $v_p(x)$ sexa minimal. Entón temos que $x\mathbb{Z} \in S$ e, como S é pechado, $x\mathbb{Z}_p \in S$. Polo tanto, $S = x\mathbb{Z}_p = p^n\mathbb{Z}_p$ para algún $n \geq 0$.

Desta forma, obtemos que a extensión $K_n \mid K$ ten grao p^n. A unicidade provén do feito de que estes subgrupos pechados son únicos. □

En particular, para a extensión (3.1) temos que $\mathrm{Gal}(K_n \mid K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

Proposición 3.3. *Consideremos a $\mathbb{Z}_p$-extensión $K_\infty \mid K$ e sexa ℓ un primo de K que non está sobre p. Entón $K_\infty \mid K$ non ramifica en ℓ, é dicir, as $\mathbb{Z}_p$-extensións son non ramificadas fóra de p.*

Demostración. Consideremos o grupo de inercia do primo ℓ, $I_\ell \subseteq \mathrm{Gal}(K_\infty \mid K) \cong \mathbb{Z}_p$. Como o grupo de inercia é pechado, podemos diferenciar dous casos:

1. $I_\ell = 0$, é dicir, o grupo de inercia é trivial co que a extensión é non ramificada en ℓ.
2. $I_\ell = p^n\mathbb{Z}_p$ para algún enteiro $n \geq 0$.

Imos estudar este último caso, no que I_ℓ é infinito. Como I_ℓ ten orde 1 ou 2 para os primos infinitos, podemos supor que ℓ é un primo finito. Para cada n, sexa ℓ_n un primo de K_n que divida ℓ_{n-1}, onde consideramos que $\ell_0 = \ell$. Pomos $\overline{K_n}$ para a completación de K_n no primo ℓ_n e definimos $\overline{K_\infty} = \bigcup_{n\geq 0} \overline{K_n}$. Sexa I_ℓ o subgrupo de inercia de $\mathrm{Gal}(\overline{K_\infty} \mid \overline{K})$. Por último, sexa U o grupo de unidades de $\overline{K}$. Polos resultados presentados no primeiro capítulo, hai un homomorfismo sobrexectivo e continuo $U \to I_\ell \cong p^n\mathbb{Z}_p$.

Por outra banda, unha comprobación rutineira amosa que $U \cong G \times \mathbb{Z}_\ell^k$, onde G é un grupo finito e $k \geq 0$ é un número enteiro. Como $\mathbb{Z}_\ell^k$ non ten subgrupos pechados de índice p, chegamos a unha contradición. □

Lema 3.4. *Consideremos a $\mathbb{Z}_p$-extensión $K_\infty \mid K$. Entón, polo menos, un primo ramifica nesta extensión e, ademais, existe un enteiro $n \geq 0$ de tal forma que cada primo que ramifica en $K_\infty \mid K_n$ é totalmente ramificado.*

Demostración. Polo Teorema 1.30 sabemos que a extensión abeliana maximal non ramificada de K é finita, polo que algún primo debe ramificar en $K_\infty \mid K$. Ademais, pola Proposición 3.3 sabemos que só van a ramificar en $K_\infty \mid K$ un número finito de primos de K. Sexan ditos primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ con $I_{\mathfrak{p}_1}, \ldots, I_{\mathfrak{p}_t}$ os seus correspondentes grupos de inercia. Entón

$$\bigcap_{j=1}^{t} I_{\mathfrak{p}_j}, \text{ para algún enteiro } n \geq 0.$$

Polo tanto, o corpo fixo de $p^n\mathbb{Z}_p$ é K_n, desta forma, $\mathrm{Gal}(K_\infty \mid K)$ está contido en cada grupo de inercia. Polo que todos os primos sobre cada $\mathfrak{p}_j$ son totalmente ramificados en $K_\infty \mid K_n$. □

Neste punto é natural preguntarnos se para calquera corpo de números K, existe polo menos unha $\mathbb{Z}_p$-extensión. Vexamos que a resposta a esta pregunta é afirmativa.

Para $n \geq 1$, consideremos $\mathbb{Q}(\zeta_{p^n})$ onde $\zeta_{p^n} = e^{2\pi i/p^n}$ é a raíz p^n-ésima primitiva da unidade. Entón temos a seguinte torre de corpos

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^n}) \subset \cdots.$$

Esta torre ten moitas características. Por exemplo, $\mathbb{Q}(\zeta_{p^n}) \mid \mathbb{Q}$ é unha extensión de Galois isomorfa a $(\mathbb{Z}/p^n\mathbb{Z})^\times$ e así $[\mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}] = \varphi(p^n) = p^{n-1}(p-1)$. Por outra banda, $\mathbb{Q}(\zeta_{p^{n+1}}) \mid \mathbb{Q}(\zeta_{p^n})$ tamén é unha extensión de Galois de grao p.

Consideremos agora $G_2 = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2}) \mid \mathbb{Q})$ que é un grupo abeliano isomorfo a $(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p\mathbb{Z}$. Polo tanto, o grupo de Galois de dita extensión ten un único subgrupo H_2 de orde $p-1$ tal que $G_2 \cong \mathbb{Z}/p\mathbb{Z}$. Sexa $\mathbb{Q}_1 = \mathbb{Q}(\zeta_{p^2})^{H_2}$, entón $\mathbb{Q}_1 \mid \mathbb{Q}$ é unha extensión de Galois, abeliana e de grao p.

Razoando da mesma forma, para cada $n \geq 1$, consideremos $G_{n+1} = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}}) \mid \mathbb{Q})$ que é un grupo abeliano tal que $G_{n+1} \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^n\mathbb{Z}$. Así, G_{n+1} ten un único subgrupo H_{n+1} de orde $p-1$ con $G_{n+1}/H_{n+1} \cong \mathbb{Z}/p^n\mathbb{Z}$. Sexa $\mathbb{Q}_n = \mathbb{Q}(\zeta_{p^{n+1}})^{H_{n+1}}$, entón $\mathbb{Q}_n \mid \mathbb{Q}$ é unha extensión abeliana, con grao p^n de forma que o seu grupo de Galois é isomorfo a $\mathbb{Z}/p^n\mathbb{Z}$ e temos a torre

$$\mathbb{Q} \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \ldots \subset \mathbb{Q}_n \subset \ldots \subset \bigcup_{n\geq 1} \mathbb{Q}_n = \mathbb{Q}_\infty.$$

A extensión $\mathbb{Q}_\infty \mid \mathbb{Q}$ é unha $\mathbb{Z}_p$-extensión de $\mathbb{Q}$, chamada a **$\mathbb{Z}_p$-extensión ciclotómica de $\mathbb{Q}$**. De feito, podemos extender este concepto de forma xeral a un corpo de números arbitrario K. Sexa $m \geq 1$ o maior enteiro tal que $\mathbb{Q}_m \subset K$, entón $K_1 = K\mathbb{Q}_{m+1} \mid K$ é unha extensión abeliana con grao p e se $K_n = K\mathbb{Q}_{m+n}$, $\mathrm{Gal}(K_n \mid K) \cong \mathbb{Z}/p^n\mathbb{Z}$, para todo $n \geq 1$. Desta forma, $K_\infty = K\mathbb{Q}_\infty$ é a $\mathbb{Z}_p$-extensión de K e chamarémola **$\mathbb{Z}_p$-extensión ciclotómica de K**.

Polo tanto, enunciamos o seguinte corolario a modo de resposta da pregunta plantexada inicialmente.

Corolario 3.5. *Toda extensión dun corpo de números K ten polo menos unha $\mathbb{Z}_p$-extensión, a $\mathbb{Z}_p$-extensión ciclotómica.*

3.2. Conxectura de Leopoldt

Acabamos de ver que todo corpo de números K ten como mínimo unha $\mathbb{Z}_p$-extensión polo que outra pregunta que xorde é cantas $\mathbb{Z}_p$-extensións independentes pode ter K. Pois ben, foi Heinrich-Wolfgang Leopoldt quen, coa axuda de técnicas avanzadas de teoría de corpos de clase, deu unha resposta que aínda non está probada en xeral.

Recordemos que o grao da extensión $K \mid \mathbb{Q}$ podémolo expresar como $[K : \mathbb{Q}] = r_1 + 2r_2$, onde r_1 representa o número de embebementos de K en $\mathbb{R}$ e $2r_2$ o número de embebementos de K en $\mathbb{C}$.

Teorema 3.6. *Consideremos un corpo de números K. Sexa K' a composición de todas as $\mathbb{Z}_p$-extensións de K. Entón existe un enteiro $c \geq 1$ tal que* $\mathrm{Gal}(K' \mid K) \cong \mathbb{Z}_p^c$ *e*

$$r_2 + 1 \leq c \leq r_1 + 2r_2 = [K : \mathbb{Q}].$$

O enteiro c é entón o número de $\mathbb{Z}_p$-extensións independentes de K. Podemos expresalo como $c = r_2 + 1 + \delta$ onde δ é un enteiro positivo chamado **defecto de Leopoldt**. O que afirma a conxectura de Leopoldt é que $\delta = 0$, é dicir:

Conxectura 3.7 (Leopoldt)**.** *Nas condicións do Teorema 3.6, $c = r_2 + 1$.*

En particular, esta conxectura foi probada en 1967 por Brumer no caso no que K é unha extensión abeliana de $\mathbb{Q}$ [2]. A día de hoxe, foron publicadas numerosas probas sobre que a conxectura de Leopoldt é certa, tanto en casos particulares como no caso xeral. De feito, o coñecido matemático rumano Preda Mihăilescu (que probou en 2002 a conxectura de Catalan) deu unha proba de dita conxectura en 2009 [17] que aínda se está a estudar se é correcta.

Exemplo 3.8. Se $K = \mathbb{Q}$, é inmediato que $r_1 = 1$ e $r_2 = 0$, polo que $c = 1$. Isto é, só existe unha $\mathbb{Z}_p$-extensión independente de $\mathbb{Q}$ (a ciclotómica).

Exemplo 3.9. Sexa K unha extensión cadrática real de $\mathbb{Q}$, isto é, $K = \mathbb{Q}(\sqrt{d})$ onde $d > 0$ é libre de cadrados. Os embebementos posibles son aqueles onde $\sqrt{d}$ vai ata unha raíz de $Irr(\sqrt{d}, \mathbb{Q}) = x^2 - d$, que son, $\sqrt{d}$ e $-\sqrt{d}$. Polo tanto, $r_1 = 2$ e $r_2 = 0$. Desta forma, polo Teorema 3.6 temos que $c = 1$, é dicir, só existe unha $\mathbb{Z}_p$-extensión independente de K (a $\mathbb{Z}_p$-extensión ciclotómica), se este é unha extensión cadrática real de $\mathbb{Q}$.

Por outra banda, se K é unha extensión cadrática imaxinaria de $\mathbb{Q}$, é dicir, $K = \mathbb{Q}(\sqrt{-d})$ con $d > 0$ e libre de cadrados, entón temos que as raíces de $Irr(\sqrt{-d}, \mathbb{Q}) = x^2 + d$ son $\pm i\sqrt{d}$, polo que $r_1 = 0$ e $r_2 = 1$. Así, $c = 2$. Unha destas $\mathbb{Z}_p$-extensións é a ciclotómica e á outra chámaselle **$\mathbb{Z}_p$-extensión anticiclotómica**.

3.3. Estrutura xeral das $\mathbb{Z}_p$-extensións

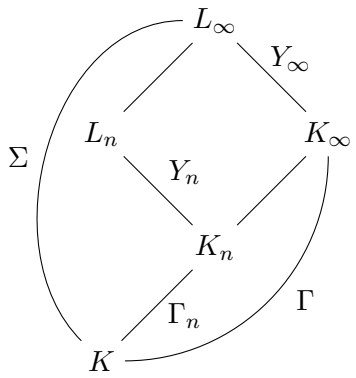
Consideremos Γ un grupo topolóxico multiplicativo isomorfo a $(\mathbb{Z}_p, +)$ e sexa γ_0 o seu xerador topolóxico (isto é, o subgrupo cíclico xerado por γ_0 é denso en Γ). De xeito máis ilustrativo, podemos relacionar γ_0 con $1 \in \mathbb{Z}_p$ xa que $\mathbb{Z} = (1)$, que é denso en $\mathbb{Z}_p$. Posto que os subgrupos pechados de $\mathbb{Z}_p$ son da forma $p^n\mathbb{Z}_p$ con $n \geq 0$, os subgrupos pechados de Γ adoptan a forma Γ^{p^n} con $n \geq 0$.

A continuación explicaremos a notación que utilizaremos no que segue.

Notación 3.10. Consideraremos como ata agora un corpo de números K.

- $\Gamma = \mathrm{Gal}(K_\infty \mid K) \cong \mathbb{Z}_p$.
- $\Sigma = \mathrm{Gal}(L_\infty \mid K)$.
- H_n: corpo de clase de Hilbert de K_n. Polo tanto, $\mathrm{Gal}(H_n \mid K_n) \cong \mathrm{Cl}(K_n)$.
- A_n: p-Sylow de $\mathrm{Cl}(K_n)$.
- L_n: p-Hilbert corpo de clase. Polo tanto, $\mathrm{Gal}(L_n \mid K_n) \cong A_n$. Ademais, é de Galois sobre K xa que K_n o é sobre K.
- $L_\infty = \bigcup_{n \geq 0} L_n$.
- $Y_n = \mathrm{Gal}(L_n \mid K_n) \cong A_n$.
- $Y_\infty = \mathrm{Gal}(L_\infty \mid K_\infty)$.

No seguinte diagrama podemos ver de forma máis clara toda esta terminoloxía.



Definición 3.11. Definimos $\Lambda(\Gamma)$ como o límite proxectivo de $\mathbb{Z}_p[\mathrm{Gal}(K_n \mid K)]$, é dicir,

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(K_n \mid K)].$$

Se dotamos a Λ coa topoloxía (p,T)-ádica temos que Λ é un anel topolóxico. Consideremos $p_n(T) = (1+T)^{p^n} - 1$ para $n \geq 0$, entón $\{p_n(T)\}_{n\geq 0}$ é unha base de veciñanzas abertas de 0.

Lema 3.12. *Existe un isomorfismo*

$$\Lambda(\Gamma) \cong \Lambda$$

de $\mathbb{Z}_p$-álxebras topolóxicas.

Demostración. Denotemos por $\gamma_0^{(n)}$ á imaxe de γ_0 en $\mathrm{Gal}(K_n \mid K)$. Entón temos que

$$\begin{array}{ccc} \mathbb{Z}_p[\mathrm{Gal}(K_n \mid K)] & \longrightarrow & \mathbb{Z}_p[T]/p_n(T) \\ \gamma_0^{(n)} & \longmapsto & 1+T \end{array}$$

é un isomorfismo de $\mathbb{Z}_p$-álxebras. Polo tanto, se tomamos límites proxectivos temos que:

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(K_n \mid K)] \cong \varprojlim \mathbb{Z}_p[T]/(p_n(T)) \cong \Lambda.$$

□

No que resta de capítulo imos supor a seguinte afirmación. Iso permite simplificar varios dos argumentos e presentar de forma máis clara as ideas principais.

Suposición 3.13. Todos os primos ramificados en $K_\infty \mid K$ son totalmente ramificados.

Consideremos a torre de corpos $K_n \subseteq L_n \cap K_{n+1} \subseteq K_{n+1}$. Posto que $[K_{n+1} : K_n] = p$, podemos diferenciar dous casos:

1. $[L_n \cap K_{n+1} : K_n] = 1$, polo que $L_n \cap K_{n+1} = K_n$.
2. $[L_n \cap K_{n+1} : K_n] = p$, co que $L_n \cap K_{n+1} = K_{n+1}$.

Grazas ao Lema 3.4, sabemos que existe polo menos un primo en K_n que ramifica en K_{n+1}, e pola Suposición 3.13 vai ramificar totalmente. Malia isto, L_n é unha extensión non ramificada de K_n por definición, co que o primo p non ramifica en $L_n \cap K_{n+1}$. Desta forma, atopámonos no primeiro caso, é dicir, $L_n \cap K_{n+1} = K_n$. Polo tanto,

$$Y_n = \mathrm{Gal}(L_n \mid K_n) \cong \mathrm{Gal}(L_n K_{n+1} \mid K_{n+1}),$$

que é un cociente de Y_{n+1}. En efecto,

$$\begin{aligned} Y_n &\cong \mathrm{Gal}(L_nK_{n+1} \mid K_{n+1}) \cong \mathrm{Gal}(L_{n+1} \mid K_{n+1}) / \mathrm{Gal}(L_{n+1} \mid L_nK_{n+1}) \\ &= Y_{n+1} / \mathrm{Gal}(L_{n+1} \mid L_nK_{n+1}). \end{aligned}$$

Analogamente temos que

$$Y_n \cong \mathrm{Gal}(L_nK_\infty \mid K_\infty).$$

Polo tanto,

$$\varprojlim Y_n \cong \mathrm{Gal}(\bigcup_{n\geq 1} L_nK_\infty \mid K_\infty) = \mathrm{Gal}(L_\infty \mid K_\infty) = Y_\infty.$$

Sexa agora $\gamma \in \Gamma_n = \Gamma/\Gamma^{p^n}$, se consideramos unha extensión $\gamma' \in \mathrm{Gal}(L_n \mid K)$ de γ e $y \in Y_n$. Temos que γ actúa sobre y mediante

$$y^\gamma = \gamma' y (\gamma')^{-1}.$$

Como Y_n é abeliano, y^γ está ben definida. En efecto, sexa $\widehat{\gamma}$ outra extensión de γ, temos que:

$$(\widehat{\gamma})^{-1}\gamma' y (\gamma')^{-1}\widehat{\gamma} = ((\widehat{\gamma})^{-1}\gamma')((\gamma')^{-1}\widehat{\gamma})y = ((\gamma')^{-1}\widehat{\gamma})^{-1}((\gamma')^{-1}\widehat{\gamma})y = y.$$

Polo que deducimos que $\gamma' y (\gamma')^{-1} = \widehat{\gamma} y (\widehat{\gamma})^{-1}$, e así vemos como a acción non depende da extensión de γ escollida. Desta forma acabamos de ver como Y_n é un $\mathbb{Z}_p[\Gamma_n]$-módulo.

Corolario 3.14. *Y_∞ é un Λ-módulo.*

Demostración. Basta con ver que é un Γ-módulo. Sexa $\gamma \in \Gamma$, tomemos $\gamma' \in \Sigma = \mathrm{Gal}(L_\infty \mid K)$ unha extensión de γ. Entón se $y \in Y_\infty$, γ actúa en y:

$$y^\gamma = \gamma' y (\gamma')^{-1}.$$

Posto que Y_∞ é abeliano, seguindo o mesmo razoamento que fixemos anteriormente temos que a acción está ben definida. □

O noso obxectivo agora é, como adiantabamos ao principio do capítulo, probar que Y_∞ é un Λ-módulo finitamente xerado. Para isto, introduciremos 4 lemas que farán que a proba sexa máis sinxela.

Lema 3.15. *Consideremos $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ os primos que ramifican en $K_\infty \mid K$ e denotemos por $\overline{\mathfrak{p}}_i$ o primo de L sobre $\mathfrak{p}_i$. Sexa $I_{\overline{\mathfrak{q}}_i} \subset \Sigma$ o grupo de inercia asociado ao primo $\overline{\mathfrak{q}}_i$. Nestas condicións tense que*

$$\Sigma = I_{\overline{\mathfrak{q}}_i} Y_\infty = Y_\infty I_{\overline{\mathfrak{q}}_i}, \text{ para } i = 1, \dots, s.$$

Demostración. Nas hipóteses anteriores, como a extensión $L_\infty \mid K_\infty$ é non ramificada, temos que $I_{\overline{\mathfrak{p}}_i} \cap Y_\infty = \{1\}$. Polo tanto, deducimos que o homomorfismo

$$\begin{array}{rccc} \varphi\colon & I_{\overline{\mathfrak{p}}_i} & \longrightarrow & \Sigma/Y_\infty \cong \Gamma = \mathrm{Gal}(K_\infty \mid K) \\ & \Sigma & \longmapsto & \Sigma|_{K_\infty} \end{array}$$

é inxectivo, xa que $\ker(\varphi) = I_{\overline{\mathfrak{p}}_i} \cap Y_\infty = \{1\}$. Por outra banda, sabemos pola Suposición 3.13 que $K_\infty \mid K$ é totalmente ramificada en $\mathfrak{p}_i$ co que temos que φ é sobrexectiva e, desta forma, concluímos que $I_{\overline{\mathfrak{p}}_i} \cong \Sigma/Y_\infty = \Gamma$. Polo tanto, podemos expresar Σ como

$$\Sigma = I_{\overline{\mathfrak{p}}_i} Y_\infty = Y_\infty I_{\overline{\mathfrak{p}}_i},$$

como queriamos probar. □

Observación 3.16. Sexa o elemento $\epsilon_i \in I_{\overline{\mathfrak{p}}_i}$ tal que $\varphi(\epsilon_i) = \gamma_0$, entón ϵ_i é o xerador topolóxico de $I_{\overline{\mathfrak{p}}_i}$. Ademais, como $I_{\overline{\mathfrak{p}}_i} \subseteq Y_\infty I_{\overline{\mathfrak{p}}_1}$, temos que

$$\epsilon_i = a_i \epsilon_1$$

para algún $a_i \in Y_\infty$ (é evidente que $a_1 = 1$).

Lema 3.17. *Sexa Σ' a clausura do conmutador de Σ. Entón,*

$$\Sigma' = Y_\infty^{\gamma_0 - 1} = T Y_\infty.$$

Demostración. O conmutador de Σ é $\{[a,b] = aba^{-1}b^{-1} \mid a, b \in \Sigma\}$. Temos que $I_{\overline{\mathfrak{p}}_i} \cong \Gamma$, polo que, en particular, $I_{\overline{\mathfrak{p}}_1} \cong \Gamma \subseteq \Sigma$. Desta forma, podemos identificar $\gamma \in \Gamma$ co seu elemento correspondente en $I_{\overline{\mathfrak{p}}_1}$ co gallo de definir a acción de Γ sobre Y_∞. Esta acción é $x^\gamma = \gamma x \gamma^{-1}$.

Sexan $a = \alpha x$, $b = \beta y$ con $\alpha, \beta \in \Gamma$ e $x, y \in Y_\infty$ elementos arbitrarios de $\Sigma = I_{\overline{\mathfrak{p}}_1} X \cong \Gamma X$.

Entón temos que

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x\beta y x^{-1}\alpha^{-1}y^{-1}\beta^{-1} \\ &= x^{\alpha}\alpha\beta y x^{-1}\alpha^{-1}y^{-1}\beta^{-1} = \\ &= x^{\alpha}(yx^{-1})^{\alpha\beta}(\alpha\beta)\alpha^{-1}y^{-1}\beta^{-1} \\ &= x^{\alpha}(yx^{-1})^{\alpha\beta}(y^{-1})^{\beta} \\ &= (x^{\alpha})^{1-\beta}(y^{\beta})^{\alpha-1}. \end{aligned}$$

Se consideramos $\beta = 1$, $\alpha = \gamma_0$, obtemos que $y^{\gamma_0-1} \in \Sigma'$, polo que $Y_\infty^{\gamma_0-1} \subseteq \Sigma'$. Ademais, para un β escollido de forma arbitraria temos que existe un $v \in \mathbb{Z}_p$ de maneira que $\beta = \gamma_0^v$. Polo tanto,

$$1-\beta = 1-\gamma_0^v = 1-(1+T)^v = 1-\sum_{n=0}^{\infty}\binom{v}{n}T^n = \sum_{n=1}^{\infty}\binom{v}{n}T^n \in T\Lambda.$$

Como $T = \gamma_0 - 1$, $(x^{\alpha})^{1-\beta} \in Y_\infty^{\gamma_0-1}$. De forma análoga, $(y^{\beta})^{1-\alpha} \in Y_\infty^{\gamma_0-1}$. Ademais, $Y_\infty^{\gamma_0-1} = TY_\infty$ é pechado xa que é a imaxe do compacto Y_∞. Polo tanto, $\Sigma' \subseteq Y_\infty^{\gamma_0-1}$, co que queda probado o lema. □

O seguinte resultado é moi importante posto que permítenos saber información de cada Y_n a partir de Y_∞.

Lema 3.18. *Sexa $Z_0 \subseteq Y_\infty$ xerado por $\{a_2, \dots, a_s\}$ e TY_∞. Consideremos $Z_n = \nu_n Z_0$, onde*

$$\nu_n = 1+\gamma_0+\gamma_0^2+\dots+\gamma_0^{p^n-1} = \frac{(1+T)^{p^n}-1}{T}.$$

Entón temos que

$$Y_n \cong Y_\infty/Z_n, \text{ para } n \geq 0.$$

Demostración. Comezaremos co caso $n = 0$. Temos a seguinte torre de corpos

$$K \subseteq L_0 \subseteq L.$$

Posto que L_0 é a p-extensión abeliana non ramificada maximal de K e $L \mid K$ é unha p-extensión, temos que $L_0 \mid K$ é a subextensión abeliana non ramificada maximal de $L \mid K$. Polo tanto, $\mathrm{Gal}(L \mid L_0)$ ten que ser o subgrupo pechado de Σ xerado por Σ' e todos os grupos de inercia. Desta forma, $\mathrm{Gal}(L \mid L_0)$ é a clausura do grupo xerado por $Y_\infty^{\gamma_0-1}$, $I_{\bar{\mathfrak{p}}_1}$ e $\{a_2, \dots, a_s\}$, polo que

$$Y_0 = \mathrm{Gal}(L_0 \mid K) = \Sigma/\mathrm{Gal}(L \mid L_0) = Y_\infty I_{\bar{\mathfrak{p}}_1}/\mathrm{Gal}(L \mid L_0) \cong Y_\infty/\overline{\langle Y_\infty^{\gamma_0-1}, a_2, \dots, a_s\rangle} = Y_\infty/Z_0,$$

como queriamos probar. Supoñamos agora que $n \geq 1$ e reemplacemos K por K_n e γ_0 por $\gamma_0^{p^n}$, entón ϵ_i muda a $\epsilon_i^{p^n}$. Observemos que

$$\epsilon_i^{k+1} = (a_i\epsilon_1)^{k+1} = a_i\epsilon_1 a_i\epsilon_1^{-1}\epsilon_1^2 a_i\epsilon_1^{-2}\cdots\epsilon_1^k a_i\epsilon_1^{-k}\epsilon_1^{k+1} = a_i^{1+\epsilon_1+\cdots+\epsilon_1^k}\epsilon_1^{k+1}.$$

Polo tanto,

$$\epsilon_i^{p^n} = (\nu_n a_i)\epsilon_1^{p^n}.$$

Polo que a_i é reemplazado por $\nu_n a_i$. Ademais, $Y_\infty^{\gamma_0-1}$ muda a $(\gamma_0^{p^n}-1)Y_\infty = \nu_n Y_\infty^{\gamma_0-1}$. Desta forma, Z_0 convértese en $\nu_n Z_0$ co que chegamos ao resultado desexado. □

Enunciamos agora unha versión do lema de Nakayama que nos permitirá concluír a demostración. Como é habitual, buscamos obter información de X a partir do seu cociente por un ideal maximal.

Lema 3.19 (Nakayama)**.** *Consideremos X un Λ-módulo compacto. Entón*

$$X \text{ é finitamente xerado sobre } \Lambda \text{ se, e só se } X/(p,T)X \text{ é finito.}$$

Ademais, se $X/(p,T)X = \langle x_1,\dots,x_n\rangle_{\mathbb{Z}}$, entón $X = \langle x_1,\dots,x_n\rangle_\Lambda$. En particular,

$$X/(p,T)X = 0 \text{ se, e só se } X = 0.$$

Demostración. Denotemos por U a unha veciñanza de 0 en X. Posto que $(p,T)^n \longrightarrow 0$ en Λ (por ser (p,T) o maximal de Λ), cada $z \in X$ ten unha veciñanza, U_z, cumprindo $(p,T)^n U_z \subseteq U$ para un n suficientemente grande. Ademais, como X é compacto por hipótese, unha colección finita de U_z recobren X. Desta forma, $(p,T)^n X \subseteq U$ para un n suficientemente grande, co que $\bigcap_n((p,T)^n X) = 0$ para calquera Λ-módulo compacto X.

Supoñamos agora que $x_1,\dots,x_n$ xeran a $X/(p,T)X$. Sexa $Y = \Lambda x_1 + \dots + \Lambda x_n \subseteq X$, entón Y é compacto (por ser a imaxe de Λ^n) e, en particular, pechado. Entón X/Y é un Λ-módulo compacto. Por hipótese, $X = Y + (p,T)X$ co que

$$X/Y = (Y + (p,T)X)/Y = (p,T)X/Y,$$

e, en consecuencia,

$$(p,T)^n X/Y = X/Y, \text{ para todo } n \geq 0.$$

Séguese que $X/Y = 0$ polo que $X = Y$ e $x_1, \dots, x_n$ xeran a X. □

Xa temos todas as ferramentas necesarias para probar o resultado fundamental do capítulo.

Teorema 3.20. *Y_∞ é un Λ-módulo finitamente xerado.*

Demostración. No Corolario 3.14 probamos que Y_∞ é un Λ-módulo, vexamos agora que é finitamente xerado. Temos que $\nu_1 = 1+\gamma_0+\gamma_0^2+\cdots+\gamma_0^{p-1} = \dfrac{(1-T)^p-1}{T} \in (p,T)$, entón $Z_0/(p,T)Z_0$ é un cociente de $Z_0/\nu_1 Z_0 = Z_0/Z_1$. En efecto,

$$Z_0/(p,T)Z_0 \cong (Z_0/\nu_1 Z_0)/((p,T)Z_0/\nu_1 Z_0).$$

Ademais, grazas ao Lema 3.18, $Z_0/Z_1 \subseteq Y_\infty/Z_1 \cong Y_1$ que é finito (xa que como vimos $Y_1 = \mathrm{Gal}(L_1 \mid K) \cong A_1$ que é finito). Polo tanto, polo Lema 3.19 temos que Z_0 é finitamente xerado. Como $Y_\infty/Z_0 \cong Y_0$ é finito e Z_0 é finitamente xerado, concluímos que Y_∞ é finitamente xerado. □

Olvidemos agora a Suposición 3.13. Sexan unha $\mathbb{Z}_p$-extensión $K_\infty \mid K$ e un enteiro $e \geq 0$ de tal maneira que todos os primos que ramifican en $K_\infty \mid K_e$ sexan totalmente ramificados. Entón apliquemos os Lemas 3.18 e 3.20. Desta forma, Y_∞, que é o mesmo para a extensión $K_\infty \mid K_e$ como para $K_\infty \mid K$, é un Λ-módulo finitamente xerado. Para $n \geq e$ imos definir $\nu_{n,e}$ como segue,

$$\nu_{n,e} = \frac{\nu_n}{\nu_e} = 1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \cdots + \gamma_0^{p^n - p^e}.$$

Posto que $\gamma_0^{p^e}$ xera $\mathrm{Gal}(K_\infty \mid K_e)$, podemos reemplazar no Lema 3.18 ν_n por $\nu_{n,e}$ en $K_\infty \mid K_e$ e Z_0 por Z_e. Polo que

$$Z_n = \nu_{n,e} Z_e \text{ e } Y_n \cong Y_\infty/Z_n \text{ para } n \geq e.$$

Basicamente acabamos de probar o seguinte teorema.

Teorema 3.21. *Dada unha $\mathbb{Z}_p$-extensión $K_\infty \mid K$, entón Y_∞ é un Λ-módulo finitamente xerado e existe un enteiro $e \geq 0$ satisfacendo*

$$Y_n \cong Y_\infty/\nu_{n,e} Z_e \text{ para todo } n \geq e.$$

Capítulo 4

Teorema de control de Iwasawa e ideais característicos

No capítulo anterior vimos ferramentas suficientes para probar que Y_∞ é un Λ-módulo finitamente xerado. É agora onde unindo estes procedementos cuns resultados previos, poderemos probar un dos teoremas fundamentais da teoría de Iwasawa, o teorema de control de Iwasawa. Nesta parte do capítulo seguimos [26].

Na segunda sección trataremos un obxecto que aporta información sobre certos módulos, o ideal característico. Ademais, trataremos a conxectura de Kummer-Vandiver. As fontes utilizadas para a elaboración desta parte foron [3] e [13].

É xa na terceira sección onde faremos unha pequena introdución á conxectura principal de Iwasawa para dar un esbozo no capítulo 7 de como é a súa proba. Nesta sección a nosa principal referencia foi [3].

4.1. Demostración do teorema de control

Comezamos a sección enunciando o teorema de control de Iwasawa que xa anticiparamos na introdución.

Teorema 4.1 (Teorema de control de Iwasawa)**.** *Sexan $K_\infty \mid K$ unha $\mathbb{Z}_p$-extensión e p^{e_n} a potencia exacta de p que divide á orde do grupo de clases de K_n. Entón existen enteiros $\lambda \geq 0$, $\mu \geq 0$ e ν (que non dependen de n) e un enteiro n' de tal forma que*

$$e_n = \lambda n + \mu p^n + \nu \text{ para todo } n \geq n'.$$

Definición 4.2. Aos enteiros λ, μ e ν definidos no teorema anterior denomínaselles **invariantes de Iwasawa**.

Como adiantabamos ao principio do capítulo, xa probamos que Y_∞ é un Λ-módulo finitamente xerado. Polo tanto, podemos aplicarlle o teorema de clasificación (Teorema 2.18). Do mesmo xeito, sabemos que Y_∞/Z_e é finito, polo que Z_e é pseudoisomorfo a Y_∞ e así podemos volver a empregar o teorema para obter información. É dicir, temos que

$$Z_e \sim Y_\infty \sim \Lambda^r \oplus \big(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\big) \bigoplus \big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\big),$$

onde, como de costume, estamos a tomar pseudoisomorfismos.

Proposición 4.3. *Consideremos*

$$E = \Lambda^r \oplus \big(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\big) \bigoplus \big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\big).$$

Definamos $\mu = \sum_{i=1}^{s} n_i$ *e* $\lambda = \sum_{j=1}^{t} m_j \operatorname{grao}(f_j)$. *Se* $E/\nu_{n,e}E$ *é finito para todo* n, *entón temos que:*

1. $r = 0$,
2. *existen constantes* n' *e* v *tales que* $|E/\nu_{n,e}E| = p^{\mu p^n + \lambda n + v}$, *para todo* $n > n'$.

Demostración. Imos calcular $V/\nu_{n,e}V$ para cada un dos sumandos da suma directa.

Caso $V = \Lambda$: Como $\nu_{n,e} \notin \Lambda^\times$, entón, en virtude da Proposición 2.15, $\Lambda/(\nu_{n,e})$ é infinito. Polo tanto, Λ non pode ser un sumando.

Caso $V = \Lambda/(p^k)$: Temos que

$$V/\nu_{n,e}V \cong \Lambda/(\nu_{n,e}, p^k).$$

Polo teorema de preparación de Weierstrass (Teorema 2.3), o cociente de dous polinomios distinguibles é distinguible ou constante. Como

$$\nu_{n,e} = \frac{\nu_n}{\nu_e} = \frac{((1+T)^{p^n}-1)/T}{((1+T)^{p^e}-1)/T}$$

deducimos que $\nu_{n,e}$ é un polinomio distinguible. Ademais, polo algoritmo da división, todo elemento de $\Lambda/(p^k, \nu_{n,e})$ está representado de maneira única por un polinomio mód p^k de grao menor ao grao de $\nu_{n,e}$, é dicir, grao menor a $p^n - p^e$. Polo tanto,

$$|V/\nu_{n,e}V| = p^{k(p^n-p^e)} = p^{kp^n+c}, \text{ sendo } c \text{ unha constante.}$$

Caso $V = \Lambda/(f(T)^m)$: Consideremos $g = f(T)^m$, así g é un polinomio distinguible e denotemos por δ ao seu grao. Como g é distinguible podemos expresalo da forma

$$T^\delta \equiv pQ(T) \pmod{g},$$

polo que

$$T^k \equiv p(\text{polinomio}) \pmod{g}, \quad \text{para } k \geq \delta.$$

Se $p^n \geq \delta$, temos que

$$(1+T)^{p^n} = 1 + p(\text{polinomio}) + T^{p^n} \equiv 1 + p(\text{polinomio}) \pmod{g}.$$

Polo tanto,

$$(1+T)^{p^{n+1}} \equiv 1 + p^2(\text{polinomio}) \pmod{g}.$$

Entón

$$\begin{aligned} P_{n+2}(T) =& (1+T)^{p^{n+2}} - 1 = \left(\sum_{i=0}^{p-1}(1+T)^{ip^{n+1}}\right)((1+T)^{p^{n+1}} - 1) \\ \equiv& (1 + ... + 1 + p^2(\text{polinomio}))(P_{n+1}(T)) \equiv p(1 + p(\text{polinomio}))P_{n+1}(T) \pmod{g}. \end{aligned}$$

Posto que $1 + p(\text{polinomio})$ é unha unidade de Λ,

$$\frac{P_{n+2}}{P_{n+1}} \text{ actúa como } p(\text{unidade}) \text{ en } V = \Lambda/(g),$$

para $p^n \geq \delta$. Asumamos agora que $n' > e$, $p^{n'} \geq \delta$ e $n \geq n'$, entón

$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}}{P_{n+1}},$$

e

$$\nu_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(\nu_{n+1,e}V) = p\nu_{n+1,e}V.$$

Polo tanto,

$$|V/\nu_{n+2,e}V| = |V/pV| \cdot |pV/p\nu_{n+1,e}V| \text{ para } n \geq n'.$$

Como $(g,p)=1$, a multiplicación por p é inxectiva co que

$$|pV/p\nu_{n+1,e}V| = |V/\nu_{n+1,e}V|.$$

Ademais, posto que $V/pV \cong \Lambda/(p,g) = \Lambda/(p,T^\delta)$, temos que a orde de V/pV é p^δ. Por indución,

$$|V/\nu_{n,e}V| = p^{\delta(n-n'-1)}|V/\nu_{n'+1,e}V|, \text{ para } n \geq n'+1.$$

Se $V/\nu_{n,e}V$ é finito, entón

$$|V/\nu_{n,e}V| = p^{\delta n+c},$$

para $n \geq n'+1$ e algunha constante c. Se $V/\nu_{n,e}V$ é infinito entón V non pode ocorrer (é dicir, cando f e $\nu_{n,e}$ non son coprimos polo Lema 2.10). Por último, xuntando todo temos o resultado probado. □

Como

$$Y_\infty \sim \big(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\big) \bigoplus \big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\big),$$

é dicir, $r=0$, dicimos que Y_∞ é un módulo de Λ-torsión.

Consideremos agora a sucesión exacta curta

$$0 \longrightarrow A \longrightarrow Z_e \longrightarrow E \longrightarrow B \longrightarrow 0,$$

onde A e B son finitos e E é o definido na proposición anterior. Ata o momento sabemos a orde de $E/\nu_{n,e}E$ para todo $n > n'$, polo que quédanos obter información semellante de Z_e. Ata agora, vimos que $e_n = \mu p^n + \lambda n + c_n$ con c_n acoutado.

Lema 4.4. *Supoñamos que tanto Z como E son Λ-módulos con $Z \sim E$ de tal forma que $Z/\nu_{n,e}Z$ é finito para todo $n \geq e$. Entón, existen constantes c e n' tales que*

$$|Z/\nu_{n,e}Z| = p^c|E/\nu_{n,e}E|, \text{ para todo } n \geq n'.$$

Demostración. Consideremos o seguinte diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{n,e}Z & \longrightarrow & Z & \longrightarrow & Z/\nu_{n,e}Z & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi'_n} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi''_n} & & \\ 0 & \longrightarrow & \nu_{n,e}E & \longrightarrow & E & \longrightarrow & E/\nu_{n,e}E & \longrightarrow & 0 \end{array}$$

Expliquemos os morfismos que aparecen. φ é o homomorfismo que define o pseudoisomorfismo entre Z e E, φ'_n é a restricción de φ a $\nu_{n,e}Z$ e φ''_n e de tal forma que se $\overline{y} \in Z/\nu_{n,e}Z$, entón $\varphi''_n(\overline{y}) = \overline{\varphi(y)} \in E/\nu_{n,e}E$.

Polo tanto, podemos afirmar o seguinte:

1. $|\ker(\varphi'_n)| \leq |\ker(\varphi)|$,
2. $|\operatorname{coker}(\varphi'_n)| \leq |\operatorname{coker}(\varphi)|$,
3. $|\operatorname{coker}(\varphi''_n)| \leq |\operatorname{coker}(\varphi)|$,
4. $|\ker(\varphi''_n)| \leq |\ker(\varphi)| \cdot |\operatorname{coker}(\varphi)|$.

A primeira afirmación é evidente posto que como φ'_n é a restricción de φ a $\nu_{n,e}Z$, tense que $\ker(\varphi'_n) = \ker(\varphi_n) \cap \nu_{n,e}Z$. A segunda débese ao feito de que $\operatorname{coker}(\varphi'_n) \subseteq \nu_{n,e}\operatorname{coker}(\varphi) \subseteq \operatorname{coker}(\varphi)$. A terceira desigualdade séguese da sobrexectividade de $\operatorname{coker}(\varphi) \longrightarrow \operatorname{coker}(\varphi''_n)$. Probemos agora a última desigualdade.

Polo lema da serpe (véxase [10, Lema 9.1]), temos a seguinte sucesión exacta longa respecto do diagrama anterior

$$0 \longrightarrow \ker(\varphi'_n) \longrightarrow \ker(\varphi) \longrightarrow \ker(\varphi''_n) \longrightarrow \operatorname{coker}(\varphi'_n) \longrightarrow \operatorname{coker}(\varphi) \longrightarrow \operatorname{coker}(\varphi''_n) \longrightarrow 0.$$

Deducimos que o núcleo de $\ker(\varphi) \longrightarrow \ker(\varphi''_n)$ é $\ker(\varphi'_n) = \ker(\varphi) \cap \nu_{n,e}Z$, o que induce a seguinte cadea exacta

$$0 \longrightarrow \frac{\ker(\varphi)}{\ker(\varphi'_n)} \xrightarrow{\alpha} \ker(\varphi''_n) \xrightarrow{\beta} \operatorname{coker}(\varphi'_n).$$

Onde deducimos, grazas ao primeiro teorema de isomorfía, que $\dfrac{\ker(\varphi''_n)}{\ker(\beta)} \cong \operatorname{Im}(\beta) \subseteq \operatorname{coker}(\varphi'_n)$, polo que

$$\frac{|\ker(\varphi''_n)|}{|\ker(\beta)|} \leq |\operatorname{coker}(\varphi'_n)|,$$

e así,

$$|\ker(\varphi''_n)| \leq |\operatorname{coker}(\varphi''_n)| \cdot |\ker(\beta)| = |\operatorname{coker}(\varphi''_n)| \cdot \frac{|\ker(\varphi)|}{|\ker(\varphi'_n)|} \leq |\operatorname{coker}(\varphi''_n)| \cdot |\ker(\varphi)|,$$

como queriamos probar. A igualdade anterior séguese do feito de que α é inxectivo e así

$$\ker(\alpha) \cong \frac{\ker(\varphi)}{\ker(\varphi'_n)} \cong \ker(\beta),$$

e a última igualdade provén da segunda afirmación.

Supoñamos agora que $0 \leq n \leq m$, entón podemos afirmar que:

1. $|\ker(\varphi'_m)| \leq |\ker(\varphi'_n)|$,
2. $|\operatorname{coker}(\varphi'_m)| \leq |\operatorname{coker}(\varphi'_n)|$,
3. $|\operatorname{coker}(\varphi''_n)| \leq |\operatorname{coker}(\varphi''_n)|$.

Como $\nu_{m,e} = \left(\frac{\nu_{m,e}}{\nu_{n,e}}\right)\nu_{n,e}$, temos que $\nu_{m,e}Z \subseteq \nu_{n,e}Z$ e así $\ker(\varphi'_m) \subseteq \ker(\varphi'_n)$ co que a primeira afirmación queda probada. En canto á segunda, consideremos $\nu_{m,e}y \in \nu_{m,e}E$, se $z \in \nu_{m,e}E$ é un representante de $\nu_{m,e}y$ en $\operatorname{coker}(\varphi'_n)$, temos que

$$\nu_{n,e}y - z = \varphi(\nu_{n,e}x) \text{ para algún } x \in Z.$$

Se multiplicamos por $\nu_{m,e}/\nu_{n,e}$ obtemos

$$\nu_{m,e}y - \frac{\nu_{m,e}}{\nu_{n,e}}z = \varphi(\nu_{m,e}x) = \varphi'_m(\nu_{m,e}x).$$

Desta forma, $\nu_{m,e}/\nu_{n,e}$ multiplicado polos representantes de $\operatorname{coker}(\varphi'_n)$ da lugar a representantes de $\operatorname{coker}(\varphi'_m)$, entón $\operatorname{coker}(\varphi'_m) \subseteq \operatorname{coker}(\varphi'_n)$. Por último, a terceira desigualdade dedúcese do feito de que $\nu_{m,e}E \subseteq \nu_{n,e}E$ xa que así $E/\nu_{n,e} \subseteq E/\nu_{m,e}E$, polo que $\operatorname{coker}(\varphi''_n) \subseteq \operatorname{coker}(\varphi''_m)$.

Polas afirmacións anteriores sabemos que as ordes de $\ker(\varphi'_n)$, $\operatorname{coker}(\varphi'_n)$ e $\operatorname{coker}(\varphi''_n)$ son constantes a partir dun $n \geq n'$ con n' fixado. Para rematar a proba queda probar que $\ker(\varphi''_n)$ é constante. Polo lema da serpe temos

$$|\ker(\varphi'_n)| \cdot |\ker(\varphi''_n)| \cdot |\operatorname{coker}(\varphi)| = |\ker(\varphi)| \cdot |\operatorname{coker}(\varphi'_n)| \cdot |\operatorname{coker}(\varphi''_n)|.$$

Polo que é evidente que $\ker(\varphi''_n)$ ten orde constante (pois φ é un pseudoisomorfismo). □

Desta forma, temos E como o definimos anteriormente (con $Z_e/\nu_{n,e}Z_e$ finito e $Z_e \sim E$). Polo tanto, existen λ e μ constantes enteiras positivas, un enteiro v e un enteiro n' tal que

$$p^{e_n} = |Y_n| = |Y_\infty/Z_e| \cdot |Z_e/\nu_{n,e}Z_e| = p^c|E/\nu_{n,e}E| = p^{\lambda n + \mu p^n + v}, \text{ para todo } n > n'.$$

Co que o teorema de control de Iwasawa (Teorema 4.1) queda probado.

Polo tanto, tanto μ como λ controlan o crecemento da p-parte do grupo de clase da $\mathbb{Z}_p$-extensión $K_\infty \mid K$. Con todo, sábese moi pouco sobre o comportamento destes invariantes. A

continuación, enunciaremos dous resultados que apórtannos algo de información relevante sobre estes invariantes.

O primeiro deles é o coñecido como teorema de Ferrero-Washington, que aporta información sobre o μ-invariante da extensión ciclotómica.

Teorema 4.5 (Ferrero-Washington)**.** *Sexa K unha extensión abeliana de $\mathbb{Q}$, entón tense que $\mu(K_\infty \mid K) = 0$, onde $K_\infty \mid K$ é a $\mathbb{Z}_p$-extensión ciclotómica.*

O segundo resultado que queremos comentar é a chamada conxectura de Greenberg, que considera o caso de corpos de números totalmente reais. Máis en concreto, dicimos que un corpo de números K é totalmente real se, para cada inmersión de K nos números complexos, a imaxe está contida nos números reais. É unha condición equivalente que K estea xerado sobre $\mathbb{Q}$ por unha raíz dun polinomio con coeficientes enteiros cuxas raíces sexan todas reais.

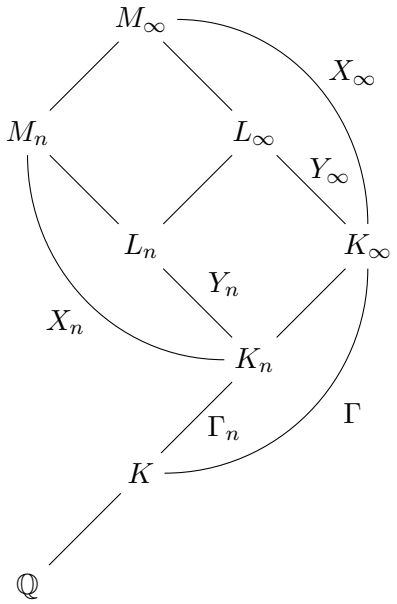
Conxectura 4.6 (Greenberg)**.** *Supoñamos que K é totalmente real, entón $\lambda(K_\infty \mid K) = 0$, onde $K_\infty \mid K$ é a $\mathbb{Z}_p$-extensión ciclotómica.*

4.2. O ideal característico e a conxectura de Kummer–Vandiver

Como anticipamos con anterioridade, nesta última sección do capítulo definiremos un obxecto fundamental que recompila información alxébrica sobre certos módulos de torsión, o ideal característico. Veremos que implicacións ten sobre o módulo de torsión estudado nas seccións anteriores e definiremos un novo módulo de torsión para poder introducir a segunda parte do traballo na seguinte sección: a conxectura principal de Iwasawa. Ademais, veremos unha conxectura relacionada co último teorema de Fermat que xorde neste contexto.

A partir de agora consideraremos un caso menos xeral do estudado ata agora, o caso ciclotómico no que o corpo base é $\mathbb{Q}$. Máis en concreto, sexa p un primo impar e sexa $K = \mathbb{Q}(\zeta_p)$, onde ζ_p é unha raíz p-ésima primitiva da unidade. Este caso é o que consideraremos no que resta de traballo.

Imos definir os novos obxectos cos que imos a traballar. Chamaremos M_∞ á p-extensión abeliana maximal de K_∞ non ramificada fóra do primo sobre p. Do mesmo xeito, X_∞ denotará o grupo de Galois da extensión $M_\infty \mid K_\infty$, isto é, $X_\infty = \mathrm{Gal}(M_\infty \mid K_\infty)$.



Consideremos $G = \mathrm{Gal}(K_\infty \mid \mathbb{Q})$. A partir de agora traballaremos no anel $\Lambda(G)$, que se define como

$$\Lambda(G) := \varprojlim \mathbb{Z}_p[G/H],$$

onde H recorre os subgrupos abertos de G. Desta forma, temos resultados similares aos do Capítulo 3. En primeiro lugar, podemos asegurar que os dous módulos que estamos a considerar teñen unha acción de $\Lambda(G)$.

Proposición 4.7. *Tanto Y_∞ como X_∞ son $\Lambda(G)$-módulos.*

O seguinte resultado é fundamental para o desenvolvemento posterior dos resultados.

Proposición 4.8. *Tense que X_∞ é finitamente xerado e de torsión como $\Lambda(G)$-módulo.*

As demostracións atópanse ao longo de [26, Sección 13.5]. As ideas no caso de X_∞ son parecidas ás probas xa vistas sobre Y_∞, pero son máis técnicas xa que usan teoría de Kummer.

Xa podemos, entón, introducir o concepto de ideal característico. Para isto, vexamos primeiro o seguinte teorema.

Teorema 4.9. *Sexa M un $\Lambda(G)$-módulo de torsión finitamente xerado. Nese caso, existe unha sucesión exacta curta de $\Lambda(G)$-módulos*

$$0 \longrightarrow \bigoplus_{j=1}^{n} \Lambda(G)/\Lambda(G) f_j \longrightarrow M \longrightarrow N \longrightarrow 0,$$

onde os f_j son divisores non nulos en $\Lambda(G)$, para $1 \leq j \leq n$, e N é un $\Lambda(G)$-módulo finito.

Demostración. Véxase [3, Teorema 2 (apéndice)]. □

Definición 4.10. Nas condicións do teorema anterior, chamamos **ideal característico** do módulo M a

$$\mathrm{ch}(M) := \prod_{j=1}^{n} f_j \Lambda(G).$$

De feito, unha comprobación rutineira amosa que o ideal característico depende só do módulo M e non da sucesión exacta curta escollida no Teorema 4.9.

Proposición 4.11. *O ideal característico é multiplicativo en sucesións exactas, é dicir, se M_1, M_2 e M_3 son $\Lambda(G)$-módulos de torsión finitamente xerados e temos a sucesión exacta*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0.$$

Entón

$$\mathrm{ch}(M_2) = \mathrm{ch}(M_1)\,\mathrm{ch}(M_3).$$

Corolario 4.12. *O ideal característico de Y_∞ é*

$$\mathrm{ch}(Y_\infty) = p^\mu \prod_{j=1}^{t} f_j^{m_j}.$$

Demostración. Véxase [3, Proposición 1 (apéndice)]. □

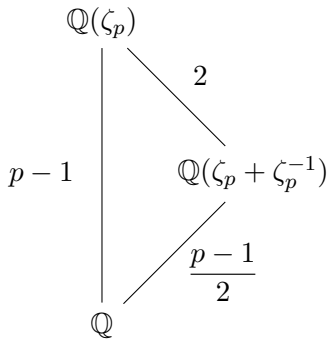
A partir de agora denotaremos por ζ_p unha raíz p-ésima primitiva da unidade (con p un primo impar). Consideremos

$$K = \mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\cos(2\pi/p)) \subseteq \mathbb{R},$$

é dicir, K é o subcorpo maximal real de $\mathbb{Q}(\zeta_p)$. Ademais, como ζ_p é unha raíz do polinomio

$$X^2 - (\zeta_p + \zeta_p^{-1})X + 1 = 0,$$

temos que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$, obtendo o seguinte diagrama:



Ademais, como sabemos, o número de clase dun corpo intermedio da extensión $\mathbb{Q}(\zeta_p) \mid \mathbb{Q}$, que denotaremos por N, divide o número de clase de $\mathbb{Q}(\zeta_p)$, isto é, $|\operatorname{Cl}(N)| \mid |\operatorname{Cl}(\mathbb{Q}(\zeta_p))|$. Polo tanto, $|\operatorname{Cl}(\mathbb{Q}(\zeta_p)^+)|$ divide a $|\operatorname{Cl}(\mathbb{Q}(\zeta_p))|$. De feito, sábese que o número de clase de $\mathbb{Q}(\zeta_p)$ pode ser expresado como $|\operatorname{Cl}(\mathbb{Q}(\zeta_p))| = h \cdot |\operatorname{Cl}(\mathbb{Q}(\zeta_p)^+)|$ onde h pode calcularse, de forma sinxela, en termos de números de Bernoulli, mentres que $|\operatorname{Cl}(\mathbb{Q}(\zeta_p)^+)|$ é máis difícil de calcular explicitamente.

Kummer probou que se $p \nmid |\operatorname{Cl}(\mathbb{Q}(\zeta_p))|$, isto é, se p é un primo regular, entón o último teorema de Fermat é certo para o expoñente p. A partires deste feito, xurdiu a seguinte conxectura.

Conxectura 4.13 (Kummer–Vandiver)**.** *O número de clase de $\mathbb{Q}(\zeta_p)^+$ non é divisible por p, é dicir, $p \nmid |\operatorname{Cl}(\mathbb{Q}(\zeta_p)^+)|$.*

Na seguinte táboa mostramos os primos que foron comprobados ata agora. Os últimos en aumentar dita extensión foron W. Hart, D. Harvey e W. Ong, en 2016, comprobándoo para todo primo $p < 2^{31}$ (véxase [7]).

Táboa cos primos verificados ata a actualidade		
Ano	Primos ata	Autores
1850	43	Kummer
1851	97	Kummer
1874	163	Kummer
1930	199	Stafford e Vandiver
1937	613	Vandiver
1951	2000	Lehmer, Lehmer e Vandiver
...	...	...
2016	2 147 483 648	Hart, Harvey e Ong

4.3. Conxectura principal de Iwasawa

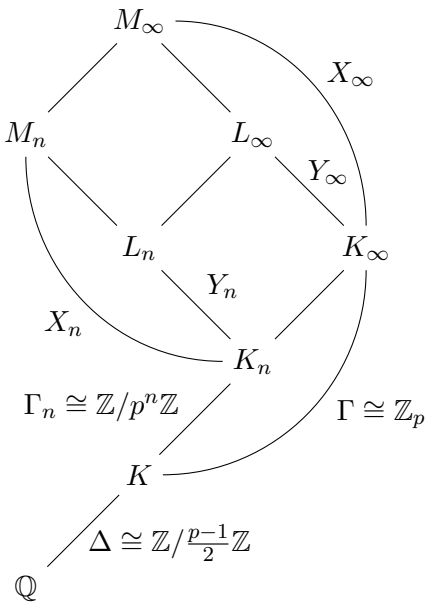
Agora podemos preguntarnos cal é o ideal característico de X_∞: é a conxectura principal de Iwasawa quen responde esta cuestión. Nesta sección faremos unha breve andaina de dita conxectura xa que a veremos máis polo miúdo nos seguintes tres capítulos.

Denotaremos por K_n ao corpo local $\mathbb{Q}_p(\mu_{p^{n+1}})^+$ e por F_n ao corpo global $\mathbb{Q}(\mu_{p^{n+1}})^+$. Por outra banda, Δ será o grupo de Galois da extensión $K \mid \mathbb{Q}$ que é de grao $\dfrac{p-1}{2}$.

Da mesma maneira, temos que

$$\Lambda[\Delta] \cong \mathbb{Z}_p[\![T]\!][\Delta] \cong \varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})^+ \mid \mathbb{Q})] =: \Lambda(G).$$

Vexamos todo isto no diagrama anterior adaptado ao caso ciclotómico.



Hai un xerador do ideal característico de X_∞ que está intimamente ligado á función zeta de Riemann. Iwasawa descubriu que hai un análogo p-ádico a esta función, a cal denotou por ζ_p, que ten unha interpretación natural en termos da álxebra de Iwasawa $\Lambda(G)$. Pero antes de falar desta función p-ádica vexamos uns conceptos previos.

Definición 4.14. Unha **pseudomedida** μ é un elemento no anel de fraccións de $\Lambda(G)$ tal que $(g-1)\mu \in \Lambda(G)$, para todo $g \in G$. Defínese como

$$\begin{array}{rccc} \mu\colon & C(G,\mathbb{C}_p) & \longrightarrow & \mathbb{C}_p \\ & \nu & \longmapsto & \displaystyle\int_G \nu d\mu, \end{array}$$

onde $C(G, \mathbb{C}_p)$ é o espazo de funcións continuas de G en $\mathbb{C}_p$.

Definición 4.15. Defínese o **carácter ciclotómico** como

$$\begin{array}{rccc} \chi\colon & \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}) \mid \mathbb{Q}) & \longrightarrow & \mathbb{Z}_p^\times \\ & g & \longmapsto & \chi(g), \end{array}$$

de xeito que $\zeta_n^{\chi(g)} = g(\zeta_n)$, para todo $g \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}) \mid \mathbb{Q})$.

Vistos estes termos temos o seguinte resultado, onde ζ_p xa é o análogo p-ádico da función zeta de Riemann.

Teorema 4.16. *Existe unha única pseudomedida ζ_p en G de tal forma que*

$$\int_G \chi(g)^k d\zeta_p = (1 - p^{k-1})\zeta(1-k),$$

para todos os enteiros pares $k \geq 2$.

Por outra banda, defínese o **homomorfismo de aumentación** como

$$\begin{array}{rccc} \mathrm{aum}\colon & \Lambda(G) & \longrightarrow & \mathbb{Z}_p \\ & \displaystyle\sum_{g \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)^+ \mid \mathbb{Q})} a_g \cdot g & \longmapsto & \displaystyle\sum_{g \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)^+ \mid \mathbb{Q})} a_g. \end{array}$$

Denotaremos ao seu núcleo como $I(G)$, é dicir, $I(G) = \ker(\mathrm{aum})$ e chamarémolo **ideal de aumentación**.

Observación 4.17. Para cada pseudomedida μ temos que $I(G)\mu$ é un ideal de $\Lambda(G)$. En particular, $I(G)\zeta_p$ é un ideal de $\Lambda(G)$.

Desta forma xa podemos enunciar a conxectura principal de Iwasawa.

Teorema 4.18 (Conxectura principal de Iwasawa)**.** *Tense que*

$$\mathrm{ch}_G(X_\infty) = I(G)\zeta_p.$$

Porén, en moitos casos convén dispor dunha formulación equivalente que non involucre á función L p-ádica. A modo de notación, para cada $n \geq 0$, consideremos $K_n = \mathbb{Q}_p(\mu_{p^{n+1}})^+$. Denotaremos por U_n^1 o grupo de unidades de K_n que son congruentes con 1 módulo $\mathfrak{p}_n$, onde por $\mathfrak{p}_n$ referímonos ao ideal maximal de K_n. Por outro lado, D_n será o grupo de unidades ciclotómicas de K_n, así D_n virá xerado por

$$\pm\frac{\zeta_n^{-e/2}-\zeta_n^{e/2}}{\zeta_n^{-1/2}-\zeta_n^{1/2}},$$

onde ζ_n denota a p^{n+1}-ésima raíz da unidade e e é unha raíz primitiva módulo p tal que verifica que $e^{p-1}\not\equiv 1 \pmod{p^2}$. Definimos D_n^1 como o subgrupo de todos os elementos de D_n que son congruentes con 1 módulo $\mathfrak{p}_n$. Ademais, C_n^1 denotará a clausura de D_n^1 en U_n^1 respecto á topoloxía $\mathfrak{p}_n$-ádica. Por último, definimos

$$U_\infty^1=\varprojlim U_n^1 \quad \text{e} \quad C_\infty^1=\varprojlim C_n^1.$$

O seguinte teorema, que moitas veces aparece co nome de teorema de Iwasawa, é o que nos dá a ponte entre as dúas formulacións equivalentes que imos estudar da conxectura principal.

Teorema 4.19. *O $\Lambda(G)$-módulo U_∞^1/C_∞^1 é canonicamente isomorfo a $\Lambda(G)/I(G)\zeta_p$, onde ζ_p denota a función zeta p-ádica.*

Sexa V_n^1 o grupo de unidades de K_n que son congruentes con 1 módulo $\mathfrak{p}_n$, definimos E_n^1 como a clausura de V_n^1 en U_n^1 respecto á topoloxía $\mathfrak{p}_n$-ádica e

$$E_\infty^1=\varprojlim E_n^1.$$

Temos a seguinte sucesión exacta de $\Lambda(G)$-módulos

$$1\longrightarrow \mathrm{Gal}(M_\infty \mid L_\infty)\longrightarrow \mathrm{Gal}(M_\infty \mid K_\infty)\longrightarrow \mathrm{Gal}(L_\infty \mid K_\infty)\longrightarrow 1.$$

Grazas á teoría de corpos de clase temos que

$$\mathrm{Gal}(M_\infty \mid L_\infty)\cong U_\infty^1/E_\infty^1,$$

polo que a anterior sucesión exacta pode ser reescrita como

$$1\longrightarrow U_\infty^1/E_\infty^1\longrightarrow X_\infty\longrightarrow Y_\infty\longrightarrow 1.$$

Ademais, posto que

$$U_\infty^1/E_\infty^1\cong\frac{U_\infty^1/C_\infty^1}{E_\infty^1/C_\infty^1},$$

temos que

$$1\longrightarrow E_\infty^1/C_\infty^1\longrightarrow U_\infty^1/C_\infty^1\longrightarrow X_\infty\longrightarrow Y_\infty\longrightarrow 1.$$

Así, pola Proposición 4.11, temos que

$$\mathrm{ch}(E_\infty^1/C_\infty^1)\,\mathrm{ch}(X_\infty) = \mathrm{ch}(U_\infty^1/C_\infty^1)\,\mathrm{ch}(Y_\infty),$$

é dicir,

$$\mathrm{ch}(E_\infty^1/C_\infty^1)\,\mathrm{ch}(U_\infty^1/C_\infty^1)^{-1}\,\mathrm{ch}(X_\infty)\,\mathrm{ch}(Y_\infty)^{-1} = 1.$$

Polo tanto, polo Teorema 4.19 teriamos que

$$\mathrm{ch}(E_\infty^1/C_\infty^1)\,\mathrm{ch}(\Lambda(G)/I(G)\zeta_p)^{-1}\,\mathrm{ch}(X_\infty)\,\mathrm{ch}(Y_\infty)^{-1} = 1.$$

Co que para demostrar a conxectura principal de Iwasawa (Teorema 4.18) basta con probar o seguinte teorema.

Teorema 4.20. *Tense que a conxectura principal de Iwasawa (Teorema 4.18) é certa se, e só se*

$$\mathrm{ch}(Y_\infty) = \mathrm{ch}(E_\infty^1/C_\infty^1).$$

Desta forma, reducimos o problema posto que xa non está involucadra a función zeta p-ádica de Riemann ζ_p.

Capítulo 5

Series de potencias de Coleman

Comezando co desenvolvemento dos resultados precisos para a formulación e demostración da conxectura principal de Iwasawa, o primeiro paso deste capítulo será expoñer certos resultados xerais para poder presentar un tipo de serie de potencias especial a través dun resultado clave, o teorema de Coleman (Teorema 5.2). Esta serie de potencias terá gran importancia no que resta de traballo. Para o desenvolvemento do capítulo guiámonos, principalmente, pola referencia [3].

En canto á notación que utilizaremos, denotemos por $\mu_{p^{n+1}}$ ao grupo das raíces p^{n+1}-ésimas da unidade. Deste modo, definimos $\mathcal{K}_n = \mathbb{Q}_p(\mu_{p^{n+1}})$. Por outro lado, $\mathcal{U}_n$ representará o grupo multiplicativo das unidades do anel de enteiros de $\mathcal{K}_n$, é dicir, $\mathcal{O}_{\mathcal{K}_n}^{\times}$. Chamaremos ξ_n ao xerador de $\mu_{p^{n+1}}$, o cal satisfai $\xi_{n+1}^p = \xi_n$ para todo $n \geq 0$, e definiremos $\pi_n = \xi_n - 1$. Polo tanto, (ξ_n) é un xerador do límite proxectivo $\varprojlim \mu_{p^{n+1}}$, que denotaremos por $T_p(\mu)$,e que é un $\mathbb{Z}_p$-módulo libre de rango 1.

Definición 5.1. Definimos

$$\mathcal{U}_\infty = \varprojlim \mathcal{U}_n,$$

onde o límite proxectivo tómase a partir das aplicacións norma $\mathrm{N}_{n,m} : \mathcal{K}_n \longrightarrow \mathcal{K}_m$ cando $n \geq m$, e $\mathrm{N}_{n,n-1} : \mathcal{U}_n \longrightarrow \mathcal{U}_{n-1}$.

O resultado clave deste capítulo é o seguinte. Afirma que cando temos unidades en cada un dos $\mathcal{K}_n$ que son compatibles mediante as aplicacións de norma estas poden interpolarse nunha serie de potencias.

Teorema 5.2 (Coleman)**.** *Para cada $u = (u_n) \in \mathcal{U}_\infty$, existe unha única serie de potencias $f_u(T) \in \Lambda$ tal que $f_u(\pi_n) = u_n$ para todo $n \geq 0$. A serie $f_u(T)$ denomínase* ***serie de potencias de Coleman****.*

Co gallo de demostrar dito teorema imos dar un contexto adecuado para, posteriormente, ver a súa proba mediante as ferramentas que describiremos a continuación. Algunhas das ideas que aparecerán

5.1. Operadores de Coleman

Na proba do Teorema 5.2, Coleman introduciu novos operadores definidos no anel Λ.

Definición 5.3. Dado un polinomio $f \in \Lambda$, definimos o **operador** φ como

$$\varphi(f)(T) := f((1+T)^p - 1).$$

Proposición 5.4. *O operador φ é inxectivo.*

Demostración. Se $h(T) = a_n T^n + a_{n-1}T^{n-1} + ...$ con $a_n \neq 0$, entón $\varphi(h)(T) = p^n a_n T^n + ...$ que evidentemente é non nulo. □

Vexamos agora cal é a imaxe de φ.

Lema 5.5. *Tense que $Im(\varphi) = \{h(T) \in \Lambda \mid h(\zeta(1+T)-1) = h(T)$, para todo $\zeta \in \mu_p\}$.*

Demostración. Por unha parte, consideremos $h(T) = \varphi(f)(T)$. Entón

$$h(T) = \varphi(f(T)) = f((1+T)^p - 1) = f((\zeta(1+T))^p - 1) = h(\zeta(1+T) - 1).$$

Por outro lado, consideremos $h(T) \in \Lambda$ cumprindo $h(\zeta(1+T)) = h(T)$. Como $h(\zeta - 1) = h(0)$ para todo $\zeta \in \mu_p$, polo teorema de preparación de Weierstrass (Teorema 2.3) temos que

$$h(T) - h(0) = \varphi(T)\widetilde{h}(T),$$

para algún $\widetilde{h}(T) \in \Lambda$. Supoñamos que atopamos coeficientes $\alpha_i \in \mathbb{Z}_p$, con $1 \leq i \leq n-1$ satisfacendo

$$h(T) = \sum_{i=0}^{n-1} \alpha_i \varphi(T)^i + \varphi(T)^n \widetilde{h}_n(T)$$

con $\widetilde{h}_n(T) \in \Lambda$. Entón $\widetilde{h}_n(\zeta(1+T)-1) = \widetilde{h}_n(T)$ e por indución queda probado. □

Imos introducir agora dous homomorfismos en Λ, que podemos pensar como operadores norma e traza, e que precisaremos para os desenvolvementos posteriores.

Proposición 5.6. *Existen homomorfismos continuos únicos $\mathcal{N}, \psi : \Lambda \longrightarrow \Lambda$ tales que*

$$(\varphi \circ \mathcal{N})(f)(T) = \prod_{\zeta \in \mu_p} f(\zeta(1+T)-1) \quad e$$
$$(\varphi \circ \psi)(f)(T) = \frac{1}{p} \cdot \sum_{\zeta \in \mu_p} f(\zeta(1+T)-1).$$

De feito, ψ é un homomorfismo de $\mathbb{Z}_p$-módulos que cumpre que $\psi \circ \varphi = id_\Lambda$, $\mathcal{N}$ preserva produtos e, ademais, leva $\Lambda^\times$ en si mesmo.

Demostración. A unicidade séguese da inxectividade de φ. Por outra parte, vexamos a existencia de $\mathcal{N}$. Dado un polinomio $f \in \Lambda$, definamos

$$h(T) = \prod_{\zeta \in \mu_p} f(\zeta(1+T)-1) \in \Lambda.$$

Temos que $h(T) = h(\zeta(1+T)-1)$ para todo $\zeta \in \mu_p$ e polo Lema 5.5, $h(T) = \varphi(g(T))$ para algún polinomio $g(T) \in \Lambda$. Desta forma, basta definir $\mathcal{N}(f) := g$. En canto á existencia de ψ, definamos

$$v(T) = \sum_{\zeta \in \mu_p} f(\zeta(1+T)-1) \in \Lambda.$$

Temos que ver que $v(T) = p \cdot w(T)$ para algún polinomio $w(T) \in \Lambda$. Sexa $\mathfrak{p}_0$ o ideal maximal do anel de enteiros de $\mathbb{Q}_p(\mu_p)$. Posto que para todo $\zeta \in \mu_p$ cúmprese que

$$\zeta(1+T) - 1 \equiv T \pmod{\mathfrak{p}_0\Lambda},$$

entón $v(T) \in p\Lambda$. Ademais, posto que $w(\zeta(1+T)-1) = w(T)$ para todo $\zeta \in \mu_p$, temos que $w(T) = \varphi(q(T))$ para algún polinomio $q(T) \in \Lambda$. Desta forma podemos definir $\psi(f) := q$. A igualdade $\psi \circ \varphi = id_\Lambda$ séguese das consideracións anteriores. □

5.2. Interpolación de series de potencias

A idea básica do teorema de Coleman é fixarnos nas unidades de Λ que quedan fixas a través de $\mathcal{N}$. Posto que se $f \in \Lambda^\times$, entón para todo $n \geq 0$ tense que $f(\pi_n) \in \mathcal{U}_n$. Como ademais, $\mathcal{N}(f) = f$, estos valores son compatibles coa norma polo seguinte motivo. A ecuación mínima de ξ_n sobre $\mathcal{K}_{n-1}$ é $X^p - \xi_{n-1} = 0$, así

$$\mathrm{N}_{n,n-1} f(\xi_n - 1) = \prod_{\zeta \in \mu_p} f(\zeta\xi_n - 1). \tag{5.1}$$

Por outra banda, podemos reescribir $\mathrm{N}(f) = f$ como

$$\varphi(f)(T) = \prod_{\zeta \in \mu_p} f(\zeta(1+T) - 1).$$

Ademais, por definición temos que $\varphi(f)(\pi_n) = f(\pi_{n-1})$ polo que a parte dereita da ecuación (5.1) é igual a $f(\pi_{n-1})$. Agora trataremos de ver o máis difícil da proba, isto é, que todos os elementos de $\mathcal{U}_\infty$ se obteñen da mesma forma.

Veremos que a forma máis natural de atopar puntos fixos de $\mathcal{N}$ actuando en $\Lambda^\times$ é que, se $f \in \Lambda^\times$, sempre existe o límite de $\mathcal{N}^k(f)$ cando $k \longrightarrow \infty$ e este pertence a Λ.

Lema 5.7. *Sexa $f \in \Lambda$ un polinomio. Se $\varphi(f)(T) \equiv 1 \pmod{p^m\Lambda}$ para algún enteiro positivo m, entón $f(T) \equiv 1 \pmod{p^m\Lambda}$.*

Demostración. Consideremos

$$f(T) - 1 = \Big(\sum_{n=0}^{\infty} \alpha_n T^n\Big) p^k,$$

onde non se cumpre sempre que os α_n son divisibles por p e $k \geq 0$. Sexa l o menor enteiro tal que p non divide α_l, entón

$$\varphi(f)(T) - 1 = p^k g(T), \quad \text{onde} \quad g(T) = \sum_{n=0}^{\infty} \alpha_n \varphi(T)^n.$$

Nese caso $\varphi(T) \equiv T^p \pmod{p\Lambda}$ e temos

$$g(T) \equiv \alpha_l T^{pl} + \ldots \pmod{p\Lambda}.$$

Polo tanto, como p non divide α_r, $g(T) \notin p\Lambda$, polo que $k \geq m$. □

Lema 5.8. *Sexa un polinomio $f \in \Lambda^\times$, entón $\mathcal{N}(f) \equiv f \pmod{p\Lambda}$. Se, ademais, asumimos que $f \equiv 1 \pmod{p^m\Lambda}$ para algún enteiro $m \geq 1$, entón $\mathcal{N}(f) \equiv 1 \pmod{p^{m+1}\Lambda}$.*

Demostración. Consideremos $\mathfrak{p}_0$ o ideal maximal do anel de enteiros de $\mathbb{Q}_p(\mu_p)$. Se temos que $f \equiv 1 \pmod{p^k\Lambda}$ para algún enteiro $k \geq 0$, isto é, se

$$f(T) = \sum_{n=0}^{\infty} \alpha_n T^n,$$

entón $\alpha_0 \equiv 1 \pmod{p^k}$ e $\alpha_n \equiv 0 \pmod{p^k}$ para $n \geq 1$. Como para cada $\zeta \in \mu_p$ temos que

$$\zeta(1+T) - 1 \equiv T \pmod{\mathfrak{p}_0\Lambda},$$

entón

$$f(\zeta(1+T)-1) \equiv f(T) \pmod{\mathfrak{p}_0 p^k \Lambda}.$$

Desta forma,

$$\varphi(\mathcal{N}(f)) = \prod_{\zeta \in \mu_p} f(\zeta(1+T)-1) \equiv f(T)^p \pmod{p^{k+1}\Lambda}.$$

Asumamos que $k \geq 1$, entón $f(T)^p \equiv 1 \pmod{p^{k+1}\Lambda}$ e o resultado séguese do Lema 5.7. No caso de $k = 0$, temos que

$$f(T)^p \equiv f(T^p) \equiv \varphi(f)(T) \pmod{p\Lambda}$$

e, como no anterior caso, o resultado séguese a partir do Lema 5.7. □

Corolario 5.9. *Sexa un polinomio $f \in \Lambda^\times$ e sexan α e β enteiros tales que $\beta \geq \alpha \geq 0$, entón*

$$\mathcal{N}^\beta(f) \equiv \mathcal{N}^\alpha(f) \pmod{p^{\alpha+1}\Lambda}.$$

Demostración. Decatémonos de que polo Lema 5.8 temos que

$$\mathcal{N}^{\beta-\alpha}(f)/f \equiv 1 \pmod{p\Lambda}.$$

Polo que se aplicamos $\mathcal{N}^\alpha$ en ámbalas partes o resultado quedaría probado grazas á segunda afirmación do mesmo lema. □

Corolario 5.10. *Sexa $f \in \Lambda^\times$, entón $g = \lim_{k \longrightarrow +\infty} \mathcal{N}^k(f)$ existe en $\Lambda^\times$ e g é un punto fixo de $\mathcal{N}$.*

Demostración. Como sabemos Λ vén dotado pola topoloxía (p,T)-ádica (posto que é un anel local), ademais, nesta topoloxía Λ é completo, polo que o resultado séguese deste feito. □

Lema 5.11. *Temos que $(1-\varphi)\Lambda = T\Lambda$.*

Demostración. A inclusión cara a dereita é inmediata. Sexa agora $g \in T\Lambda$, vexamos que se cumpre que $g \in (1-\varphi)\Lambda$. Definamos

$$w_n(T) = (1+T)^{p^n} - 1,$$

para $n \geq 0$. Como w_n é un polinomio distinguible de grao p^n, polo algoritmo da división (Lema 2.1) temos a descomposición

$$g = g_n + w_n r_n,$$

onde g_n denota un polinomio en Λ de grao menor que p^n e $r_n \in \Lambda$. Definamos agora

$$k_n = \sum_{i=0}^{n-1} \varphi^i(g_{n-i}).$$

Temos que $k_{n+1} - \varphi(k_n) = g_{n+1}$. Posto que g_{n+1} converxe a g en Λ, basta con probar que k_n converxe a algún $k \in \Lambda$ xa que así teriamos $g = (1-\varphi)k$. Para $l = 1, \dots, n$ temos

$$\varphi^{n-l}(g) = \varphi^{n-l}(g_l) + w_n \varphi^{n-l}(r_l).$$

Se sumamos estas ecuacións para $l = 1, \dots, n$ temos

$$\sum_{i=0}^{n} \varphi^i(g) = k_n + w_n s_n,$$

con $s_n \in \Lambda$. Posto que $g \in T\Lambda$ é evidente que a suma do lado esquerdo vai converxer xa que n tende a infinito, polo que remata a proba. □

Definición 5.12. Temos os seguintes subconxuntos de Λ:

$$\Lambda^{\psi=1} = \{f \in \Lambda \mid \psi(f) = f\} \quad \text{e}$$
$$\Lambda^{\psi=0} = \{f \in \Lambda \mid \psi(f) = 0\}.$$

Proposición 5.13. *Existe una sucesión exacta*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{i} \Lambda^{\psi=1} \xrightarrow{\theta} \Lambda^{\psi=0} \xrightarrow{\alpha} \mathbb{Z}_p \longrightarrow 0,$$

onde $\theta(f) = (1-\varphi)(f)$, i é a inclusión e α é a avaliación en $T = 0$.

Demostración. Posto que $\psi \circ \varphi = 1_\Lambda$ temos que θ está ben definido. Agora temos que ver que i é inxectiva, $\mathrm{Im}(i) = \ker(\theta)$, $\mathrm{Im}(\theta) = \ker(\alpha)$ e α é sobrexectiva.

A inxectividade de i vén dada por ser esta a inclusión. A sobrexectividade de α séguese de que $1 + T \in \Lambda^{\psi=0}$. Por outra parte, polo Lema 5.11, temos que $\mathrm{Im}(\theta) = T\Lambda = \ker(\alpha)$. Por último, vexamos que $\mathrm{Im}(i) = \ker(\theta)$ e que, precisamente, é $\mathbb{Z}_p$. A inclusión cara á dereita é clara. Supoñamos agora que $f(T) \notin \mathbb{Z}_p$, entón $f(T)$ é da forma

$$f(T) = a_0 + a_r T^r + \dots, \quad \text{onde} \quad a_r \neq 0.$$

Pero aplicando φ obtemos

$$\varphi(f(T)) = a_0 + p^r a_r T^r + ...,$$

polo que $\varphi(f) \neq f$. Desta forma, quedaría a igualdade probada e remata a proba. □

5.3. Proba do teorema de Coleman

Xa estamos en condicións de probar o Teorema 5.2.

Demostración. Vexamos a existencia. Consideremos $u \in \mathcal{U}_\infty$ e para cada $n \geq 0$ sexa $f_n \in \Lambda^\times$ tal que $f_n(\pi_n) = u_n$. Sexa agora a sucesión $\{g_n\} \in \Lambda$ onde $g_n(T) = \mathcal{N}^n f_{2n}(T)$. Para todo $m \geq n$, $g_m(\pi_n) \equiv u_n \pmod{p^{m+1}}$. En particular, tense que $\lim_{m \longrightarrow \infty} g_m(\pi_n) = u_n$. Repetindo k veces para $1 \leq k \leq n$,

$$u_{n-l} = N_{n,n-l}(f_n(\pi_n)) = (\mathcal{N}^l f_n)(\pi_{n-l}).$$

Se $m \geq n$, entón

$$u_n = (\mathcal{N}^{2m-n} f_{2m})(\pi_n).$$

Polo Corolario 5.9, temos que

$$\mathcal{N}^{2m-n} f_{2m} \equiv \mathcal{N}^m f_{2m} \pmod{p^{m+1}\Lambda}.$$

Evaluando en π_n obtemos que

$$u_n \equiv g_m(\pi_n) \pmod{p^{m+1}\Lambda}.$$

Posto que Λ é compacto, $\{g_n\}$ ten polo menos un punto límite que denotaremos por $h(T)$. Desta forma, para todo $n \geq 0$, $h(T)$ verifica que $h(\pi_n) = u_n$, polo que podemos tomar $h(T) = f_u(T)$.

Por outra parte, a unicidade de $f_u(T)$ séguese do teorema de preparación de Weierstrass (Teorema 2.3). □

Exemplo 5.14. Sexan $a, b \in \mathbb{Z}^+$ relativamente primos a p, é dicir, $(a, p) = (b, p) = 1$, definamos

$$u = (u_n), \text{ onde } u_n = \frac{\xi_n^{-a/2} - \xi_n^{a/2}}{\xi_n^{-b/2} - \xi_n^{b/2}}.$$

Tense que $u_n \in \mathcal{F}_n^\times$ de tal forma que $N_{n,m}(u_n) = u_m$ para $n \geq m$. Ademais, a serie de potencias

$$v_l(T) = \frac{(1+T)^{-l/2} - (1+T)^{l/2}}{T},$$

cumpre que $v_l(T) \in \Lambda$ cando $(l,p) = 1$. Polo que a serie de potencias

$$f_u(T) = \frac{v_a(T)}{v_b(T)} \in \Lambda$$

e verifica que $f_u(\pi_n) = u_n$ para todo n.

Sexa $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_\infty \mid \mathbb{Q}_p)$, onde $\mathcal{K}_\infty = \mathbb{Q}_p(\mu_{p^\infty})$. Se denotamos por W ao conxunto de $f \in \Lambda^\times$ satisfacendo que $\mathcal{N}(f) = f$, temos o seguinte resultado inmediato a partir do Teorema 5.2.

Corolario 5.15. *Sexa*

$$\begin{array}{rccc} \phi\colon & \mathcal{U}_\infty & \longrightarrow & W \\ & u & \longmapsto & f_u(T) \end{array}$$

entón ϕ é un $\mathcal{G}$-isomorfismo.

Capítulo 6

Medidas p-ádicas e a función zeta p-ádica de Riemann

O obxectivo deste capítulo é introducir tanto o concepto de medida como o de pseudomedida p-ádica para, posteriormente, introducir a función zeta p-ádica de Riemann. Desta forma xa teriamos os ingredientes necesarios para, no seguinte capítulo, poder explicar de maneira máis detallada a conxectura principal de Iwasawa e dar unha idea da súa proba. A referencia fundamental para este capítulo foi [3].

Recordemos que a función zeta de Riemann vén dada pola serie de potencias

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}, \quad \Re(s) > 1.$$

É dicir, a suma unicamente converxe cando a parte real de s é maior ca 1. A función zeta de Riemann admite unha continuación analítica a todo o plano complexo e anúlase nos enteiros negativos pares, mentres que se satisfai que

$$\zeta(1-2k) = -\frac{B_{2k}}{2k},$$

onde $k \geq 1$ é un enteiro e B_{2k} é o $(2k)$-ésimo número de Bernoulli.

Observación 6.1. Recordemos que os números de Bernoulli son números racionais definidos a partir de

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Poden ser calculados mediante

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0.$$

De feito, se $k \geq 3$ é impar temos que $B_k = 0$.

Neste capítulo, construímos unha función de variable p-ádica que interpola os valores da función zeta de Riemann nos enteiros negativos, é dicir, que ao avaliala en $-1, -3, -5, ...$ recupera (salvo un factor axeitado) o valor da función zeta neses puntos e que ademais cumpre boas propiedades analíticas.

Observación 6.2. A través da ecuación funcional, en vez de considerar os valores da función zeta nos enteiros negativos impares, podemos considerar os valores nos enteiros positivos pares, nos que, despois de normalizar polas potencias de π axeitadas, a función tamén toma valores racionais que se poden expresar en termos dos números de Bernoulli; por exemplo,

$$\frac{\zeta(2)}{\pi^2} = \frac{1}{6}, \quad \frac{\zeta(4)}{\pi^4} = \frac{1}{90}, \quad \frac{\zeta(6)}{\pi^6} = \frac{1}{945}.$$

6.1. Medidas p-ádicas

Como adiantabamos ao comezo do capítulo, nesta sección definiremos o concepto tanto de medida p-ádica como o de pseudomedida, para logo poder tratar cun tipo especial de pseudomedida que é clave no que respecta á proba da conxectura principal de Iwasawa. Para ese obxectivo necesitaremos a serie de Coleman descrita no anterior capítulo, xa que será necesaria para poder falar do denominado homomorfismo derivada logarítmica.

Sexa $\mathfrak{G}$ un grupo abeliano profinito, é dicir, un grupo abeliano que é isomorfo ao límite proxectivo dunha colección de grupos finitos. Consideremos $\mathfrak{I}_{\mathfrak{G}}$, que vai denotar o conxunto de subgrupos abertos de $\mathfrak{G}$. Nese caso, podemos definir

$$\Lambda(\mathfrak{G}) = \varprojlim \mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}],$$

onde $\mathfrak{H}$ recorre $\mathfrak{I}_{\mathfrak{G}}$.

Ao longo da sección traballeremos en $C(\mathfrak{G}, \mathbb{C}_p)$, isto é, o espazo normado de funcións continuas de $\mathfrak{G}$ en $\mathbb{C}_p$, onde, como é habitual, $\mathbb{C}_p$ denota a clausura alxébrica de $\mathbb{Q}_p$. A norma asociada ao espazo $C(\mathfrak{G}, \mathbb{C}_p)$ é a norma do supremo, é dicir, se $f \in C(\mathfrak{G}, \mathbb{C}_p)$ entón

$$\|f\| = \sup_{g \in \mathfrak{G}} |f(g)|_p.$$

Desta forma, $C(\mathfrak{G}, \mathbb{C}_p)$ é un $\mathbb{C}_p$-espazo de Banach, é dicir, é un espazo completo respecto á súa norma.

Definición 6.3. Unha **medida p-ádica** en $\mathfrak{G}$ é un funcional linear

$$M : C(\mathfrak{G}, \mathbb{C}_p) \longrightarrow \mathbb{C}_p,$$

que verifica as seguintes propiedades:

1. $|M(f)|_p \leq \|f\|$, onde $\|\cdot\|$ denota a norma do supremo.
2. $M(f) \in \mathbb{Q}_p$ se $f \in C(\mathfrak{G}, \mathbb{C}_p)$.

6.1.1. Integrais e pseudomedidas

O noso obxectivo é explicar como integrar calquera función $\mathbb{C}_p$-avaliada en $\mathfrak{G}$ respecto a un elemento $\lambda \in \Lambda(\mathfrak{G})$.

Definición 6.4. Sexa $f \in C(\mathfrak{G}, \mathbb{C}_p)$, dicimos que f é unha **función localmente constante** se existe un subgrupo aberto $\mathfrak{H}$ de $\mathfrak{G}$ de tal forma que f é constante módulo $\mathfrak{H}$.

Imos introducir agora un obxecto que vén inspirado pola teoría de integración de variable real.

Notación 6.5. Denotaremos por $\mathrm{Step}(\mathfrak{G})$ á subálxebra das funcións localmente constantes.

Proposición 6.6. *A subálxebra* $\mathrm{Step}(\mathfrak{G})$ *é densa en* $C(\mathfrak{G}, \mathbb{C}_p)$.

Pódese atopar en [3, Capítulo 3, sección 2] dita discusión.

Sexa $f \in \mathrm{Step}(\mathfrak{G})$ unha función localmente constante módulo $\mathfrak{H}$ subgrupo de $\mathfrak{G}$. Denotaremos por $\lambda_{\mathfrak{H}}$ a imaxe de λ en $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$, isto é,

$$\lambda_{\mathfrak{H}} = \sum_{x \in \mathfrak{G}/\mathfrak{H}} a_{\mathfrak{H}}(x)x,$$

onde $a_{\mathfrak{H}} \in \mathbb{Z}_p$. Definamos agora

$$\int_{\mathfrak{G}} f d\lambda = \sum_{x \in \mathfrak{G}/\mathfrak{H}} a_{\mathfrak{H}}(x) f(x).$$

Temos que a integral é independente da elección do subgrupo $\mathfrak{H}$. Ademais, como $a_{\mathfrak{H}}(x) \in \mathbb{Z}_p$ cúmprese que

$$\left| \int_{\mathfrak{G}} f d\lambda \right|_p \leq \|f\|.$$

Sexa f unha función continua $\mathbb{C}_p$-avaliada en $\mathfrak{G}$, entón podemos tomar unha sucesión $\{f_n\}$ pertencente a Step($\mathfrak{G}$) que converxa a dita función f. De feito,

$$\left\{\int_{\mathfrak{G}} f_n d\lambda\right\}$$

é unha sucesión de Cauchy e como $C(\mathfrak{G}, \mathbb{C}_p)$ é un $\mathbb{C}_p$-espazo de Banach esta vai converxer en $\mathbb{C}_p$. Polo que podemos definir

$$\int_{\mathfrak{G}} f d\lambda = \lim_{n \longrightarrow \infty} \int_{\mathfrak{G}} f_n d\lambda.$$

Por outra banda, se definimos

$$M_\lambda(f) = \int_{\mathfrak{G}} f d\lambda,$$

temos un funcional linear en $C(\mathfrak{G}, \mathbb{C}_p)$ verificando as hipóteses da Definición 6.3, polo que temos definida unha medida p-ádica nun grupo abeliano profinito $\mathfrak{G}$ arbitrario. Vexamos agora unha serie de afirmacións que serán de axuda no que segue.

Proposición 6.7. *Temos que:*

1. *Se $\lambda = g \in \mathfrak{G}$, entón temos que dg é a medida de Dirac dada por*

$$\int_{\mathfrak{G}} f dg = f(g).$$

2. *Se $\nu : \mathfrak{G} \longrightarrow \mathbb{C}_p^\times$ é un homomorfismo de grupos continuo, entón podemos extendelo a*

$$\begin{array}{rccc} \nu\colon & \Lambda(\mathfrak{G}) & \longrightarrow & \mathbb{C}_p \\ & \lambda & \longmapsto & \nu(\lambda) = \displaystyle\int_{\mathfrak{G}} \nu d\lambda. \end{array}$$

3. *O produto de elementos de $\Lambda(\mathfrak{G})$ vén dado pola convolución de medidas, $*$, isto é,*

$$\int_{\mathfrak{G}} f(x) d(\lambda * \widetilde{\lambda})(x) = \int_{\mathfrak{G}} \left(\int_{\mathfrak{G}} f(x+y) d\lambda(x) \right) d\widetilde{\lambda}(y).$$

Agora introduciremos o concepto de pseudomedida co gallo de amosar que o análogo p-ádico da función zeta de Riemann tamén posee un polo. Denotemos por $Q(\mathfrak{G})$ ao anel de fraccións de $\Lambda(\mathfrak{G})$, isto é,

$$Q(\mathfrak{G}) = \left\{ \frac{a}{b} \mid a, b \in \Lambda(\mathfrak{G}), b \text{ non divisor de } 0 \right\}.$$

Definición 6.8. Nestas condicións, dicimos que $\lambda \in Q(\mathfrak{G})$ é unha **pseudomedida** en $\mathfrak{G}$ se $(g-1)\lambda \in \Lambda(\mathfrak{G})$, para todo $g \in \mathfrak{G}$.

Exemplo 6.9. Supoñamos agora que $\lambda \in \mathfrak{G}$ é unha pseudomedida e sexa $\nu : \mathfrak{G} \longrightarrow \mathbb{C}_p^{\times}$ un homomorfismo que non é identicamente un. Entón podemos definir

$$\int_{\mathfrak{G}} \nu d\lambda = \frac{\int_{\mathfrak{G}} \nu d((g-1)\lambda)}{\nu(g)-1},$$

onde $g \in \mathfrak{G}$ e verifica que $\nu(g) \neq 1$. É independente da escolla de g posto que, como vimos anteriormente, ν exténdese dende $\Lambda(\mathfrak{G})$ a $\mathbb{C}_p$.

6.1.2. A transformada de Mahler

Como de costume, consideremos o binomial

$$\binom{x}{n} = \frac{x!}{n!(x-n)!} = \frac{x(x-1)\cdots(x-n+1)}{n!}, \quad n \geq 1.$$

Pola súa banda, se $n = 0$, entón pomos

$$\binom{x}{n} = 1.$$

A ferramenta clave para relacionar Λ con $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_\infty \mid \mathbb{Q}_p)$ vén dada a partir do seguinte teorema cuxa proba non veremos, pero pode atoparse en [14, Teorema 1].

Teorema 6.10 (Mahler)**.** *Sexa unha función continua $f : \mathbb{Z}_p \longrightarrow \mathbb{C}_p$. Entón temos que f pode ser expresada de maneira única como*

$$f(x) = \sum_{n=0}^{\infty} \alpha_n \binom{x}{n},$$

onde

$$\lim_{n \longrightarrow \infty} \alpha_n = 0.$$

Observación 6.11. A partir do teorema anterior temos que:

1. $\alpha_n = (\nabla^n f)(0)$ con $\nabla f(x) = f(x+1) - f(x)$.
2. Posto que

$$\left| \binom{x}{n} \right|_p \leq 1$$

para todo $x \in \mathbb{Z}_p$, cúmprese que

$$\|f\| = \sup_{a_n \in \mathbb{C}_p} |a_n|_p.$$

3. Se $\lambda \in \Lambda(\mathbb{Z}_p)$, entón

$$a_n(\lambda) = \int_{\mathbb{Z}_p} \binom{x}{n} d\lambda \in \mathbb{Z}_p, \quad \text{para} \quad n \geq 0. \tag{6.1}$$

Definición 6.12. Neste contexto, definimos a **transformada de Mahler** como

$$\begin{array}{rccl} \mathcal{M}\colon & \Lambda(\mathbb{Z}_p) & \longrightarrow & \Lambda \\ & \lambda & \longmapsto & \mathcal{M}(\lambda) = \displaystyle\sum_{n=0}^{\infty} a_n(\lambda) T^n, \end{array}$$

onde, para cada $\lambda \in \Lambda(\mathbb{Z}_p)$, $a_n(\lambda)$ vén dada pola expresión (6.1).

Teorema 6.13. *A transformada de Mahler é un isomorfismo de $\mathbb{Z}_p$-álxebras.*

Demostración. A inxectividade do homomorfismo de $\mathbb{Z}_p$-módulos, $\mathcal{M}$, séguese do teorema de Mahler (Teorema 6.10). Para ver que hai unha bixección imos construir a súa inversa. Consideremos $\gamma : \Lambda \longrightarrow \Lambda(\mathbb{Z}_p)$ definida como segue. Sexa

$$g(T) = \sum_{n=0}^{\infty} a_n T^n \in \Lambda,$$

definimos o funcional linear continuo

$$\begin{array}{rccl} L\colon & \mathbb{Z}_p & \longrightarrow & \mathbb{C}_p \\ & f & \longmapsto & L(f) = \displaystyle\sum_{n=0}^{\infty} \alpha_n a_n, \end{array}$$

onde f ten a expresión de Mahler do Teorema 6.10. Evidentemente a serie vai converxer xa que

$$\lim_{n \longrightarrow \infty} \alpha_n = 0.$$

Por outro lado, como $a_n \in \mathbb{Z}_p$ temos que $|L(f)|_p \leq \|f\|$ para todo f. En consecuencia, existe un $\lambda \in \Lambda(\mathbb{Z}_p)$ cumprindo que $L = M_\lambda$ e, desta forma, definimos a inversa de $\mathcal{M}$, γ, como

$$\begin{array}{rccl} \gamma\colon & \Lambda & \longrightarrow & \Lambda(\mathbb{Z}_p) \\ & g(T) & \longmapsto & \lambda. \end{array}$$

Co que o resultado quedaría probado. □

Vexamos agora un par de resultados que serán de utilidade no que resta de capítulo.

Lema 6.14. *Tense que $\mathcal{M}(id_{\mathbb{Z}_p}) = 1+T$ e así a transformación de Mahler é o único isomorfismo de $\mathbb{Z}_p$-álxebras topolóxicas que manda o xerador topolóxico $id_{\mathbb{Z}_p}$ de $\mathbb{Z}_p$ a $1+T$.*

Demostración. Tomemos $\lambda = 1_{\mathbb{Z}_p}$, entón temos que

$$\mathcal{M}(1_{\mathbb{Z}_p}) = \sum_{n=0}^{\infty} a_n(1_{\mathbb{Z}_p})T^n,$$

onde

$$a_n(1_{\mathbb{Z}_p}) = \int_{\mathbb{Z}_p} \binom{x}{n} d1_{\mathbb{Z}_p} = \binom{1}{n}.$$

Así,

$$\mathcal{M}(1_{\mathbb{Z}_p}) = \binom{1}{0}T^0 + \binom{1}{1}T^1 + \sum_{n=2}^{\infty}\binom{1}{n}T^n = 1+T+0+...=1+T.$$

Por outro lado, basta ter en conta que para cada escolla dun xerador topolóxico γ de $\mathbb{Z}_p$, hai un único isomorfismo topolóxico de $\mathbb{Z}_p$-álxebras que levan γ en $1+T$. □

Lema 6.15. *Para todo $g \in \Lambda$ e todo enteiro positivo $k \in \mathbb{Z}$, temos*

$$\int_{\mathbb{Z}_p} x^k d(\gamma(g(T))) = (D^k g(T))_{T=0},$$

onde $D = (1+T)d/dT$.

Demostración. Fixado $g(T) = \sum_{n=0}^{\infty} a_n T^n \in \Lambda$, consideremos o funcional linear continuo

$$\begin{array}{rccl} L\colon & \mathbb{Z}_p & \longrightarrow & \mathbb{C}_p \\ & f & \longmapsto & L(f) = \displaystyle\int_{\mathbb{Z}_p} xf(x)d\gamma(g(T)). \end{array}$$

Temos que $|L(f)|_p \leq \|f\|$ co que para algún $\lambda \in \Lambda(\mathbb{Z}_p)$ temos que $L = M_\lambda$ e así

$$\int_{\mathbb{Z}_p} xf(x)d\gamma(g(T)) = \int_{\mathbb{Z}_p} f(x)d\lambda.$$

Vexamos primeiro que

$$\mathcal{M}(\lambda) = Dg(T).$$

En efecto, por unha parte temos que

$$Dg(T) = \sum_{n=0}^{\infty} (na_n + (n+1)a_{n+1})T^n.$$

Por outra parte, por definición, $\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} b_n T^n$, onde

$$b_n = \int_{\mathbb{Z}_p} x\binom{x}{n} d\gamma(g(T)).$$

Ademais, para todo $n \geq 0$ temos que

$$x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n},$$

co que obtemos, para todo $n \geq 0$, que $b_n = na_n + (n+1)a_{n+1}$ e así queda probada a devandita igualdade. Por outro lado, para todo $h(T) \in \Lambda$, cúmprese que

$$\int_{\mathbb{Z}_p} d\gamma(h(T)) = h(0).$$

Polo tanto, probar o enunciado do lema equivale a probar que para cada $k \geq 0$ verifícase que

$$\int_{\mathbb{Z}_p} x^k d\gamma(g(T)) = \int_{\mathbb{Z}_p} d\gamma(D^k g(T)).$$

Aplicando indución chégase a que

$$\int_{\mathbb{Z}_p} d\gamma(D^k g(T)) = \int_{\mathbb{Z}_p} x^{k-1} d(\gamma(Dg(T))).$$

Con estas consideracións é inmediata a igualdade que buscabamos probar. □

6.1.3. Derivada logarítmica

Comezaremos a sección discutindo sobre un resultado que será de gran utilidade posteriormente. Intuitivamente podemos pensar que $\Lambda(\mathbb{Z}_p^\times)$ non se pode identificar canonicamente cun subconxunto de $\Lambda(\mathbb{Z}_p)$ xa que o grupo multiplicativo $\mathbb{Z}_p^\times$ non é un subgrupo de $(\mathbb{Z}_p, +)$. Malia isto, si que se pode. Seguindo a discusión dada en [3, Capítulo 3, Sección 4], temos que podemos identificar $\Lambda(\mathbb{Z}_p^\times)$ cun subconxunto A de $\Lambda(\mathbb{Z}_p)$ de forma que

$$A = \{\lambda \in \Lambda(\mathbb{Z}_p) \mid \#(\lambda) = \lambda\}. \tag{6.2}$$

Continuaremos definindo o homomorfismo derivada logarítmica que é crucial para poder definir na seguinte sección o análogo p-ádico da función zeta de Riemann e tamén veremos unha sucesión exacta que será de gran importancia posteriormente.

Definición 6.16. Definimos o **homomorfismo derivada logarítmica** como

$$\begin{array}{rccl} \delta_k\colon & \mathcal{U}_\infty & \longrightarrow & \mathbb{Z}_p \\ & u & \longmapsto & \delta_k(u) = \left(D^{k-1}\left(\dfrac{(1+T)f_u'(T)}{f_u(T)} \right) \right)_{T=0}, \end{array}$$

onde $D = (1+T)d/dT$ e $f_u(T)$ é a serie de potencias asociada no teorema de Coleman (Teorema 5.2).

Notemos que $\mathrm{Im}(\delta_k) \subseteq \mathbb{Z}_p$ posto que $f_u \in \Lambda^\times$. Por outra parte, recordemos a definición de carácter ciclotómico (Definición 4.15). O carácter ciclotómico é o homomorfismo

$$\begin{array}{rccl} \chi\colon & \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}) \mid \mathbb{Q}) & \longrightarrow & \mathbb{Z}_p^\times \\ & g & \longmapsto & \chi(g), \end{array}$$

onde $\zeta_n^{\chi(g)} = g(\zeta_n)$, para todo $g \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}) \mid \mathbb{Q})$.

Lema 6.17. *O homomorfismo derivada logarítmica é un homomorfismo de grupos que satisfai*

$$\delta_k(\sigma(u)) = \chi(\sigma)^k \delta_k(u),$$

para todo $u \in \mathcal{U}_\infty$ e $\sigma \in \mathrm{Gal}(\mathcal{K}_\infty \mid \mathbb{Q}_p)$.

Demostración. É evidente que é δ_k é un homomorfismo de grupos. Por outra parte, a igualdade anterior débese ao feito de que

$$f_{\sigma(u)}(T) = f_u((1+T)^{\chi(\sigma)} - 1)$$

e de que

$$D^k(g(1+T)^\alpha - 1) = \alpha^k (D^k g)((1+T)^\alpha - 1), \tag{6.3}$$

para todo enteiro $k \geq 0$, $\alpha \in \mathbb{Z}_p$ e $g \in \Lambda$. □

Sexan $a, b \in \mathbb{Z}$ coprimos con p, definimos $c(a,b) = (c_n(a,b)) \in \mathcal{U}_\infty$ como

$$c_n(a,b) = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-b/2} - \zeta_n^{b/2}}.$$

Proposición 6.18. *Denotemos por $\zeta(s)$ á función zeta de Riemann complexa. Temos que:*

1. *Se k é un enteiro positivo impar, entón: $\delta_k(c(a,b)) = 0$.*
2. *Se k é un enteiro positivo par, entón: $\delta_k(c(a,b)) = (b^k - a^k)\zeta(1-k)$.*

Demostración. Consideremos

$$f(T) = \frac{(1+T)^{-a/2} - (1+T)^{a/2}}{(1+T)^{-b/2} - (1+T)^{b/2}}$$

de tal forma que para todo $n \geq 0$, $f(\pi_n) = c_n(a,b)$. Facemos o cambio de variable $T = e^z - 1$ e así $D = d/dz$, obtendo

$$\delta_k(c(a,b)) = \left(\left(\frac{d}{dz}\right)^{k-1} \frac{d}{dz} \log f(e^z - 1)\right)_{z=0}.$$

Denotando

$$g(z) = \frac{d}{dz} \log f(e^z - 1),$$

temos que

$$2g(z) = b\left(\frac{1}{e^{-bz}-1} - \frac{1}{e^{bz}-1}\right) - a\left(\frac{1}{e^{-az}-1} - \frac{1}{e^{az}-1}\right).$$

Cada cociente anterior podémolo expresar da seguinte forma

$$\frac{1}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} \cdot t^{n-1},$$

onde B_n é o n-ésimo número de Bernoulli. Posto que $B_m = 0$ cando m é un enteiro positivo impar distinto de un, facendo unhas sinxelas contas obtemos que

$$g(z) = \sum_{k=2}^{\infty} \frac{B_k z^{k-1}}{k!}(a^k - b^k), \quad \text{con } k \text{ par.}$$

Para rematar a proba basta considerar a igualdade

$$\zeta(1-k) = -\frac{B_k}{k},$$

onde k é un enteiro positivo par. □

Consideremos a seguinte acción de $\mathcal{G}$ en $\Lambda(\mathbb{Z}_p)$

$$g \cdot (\alpha_{\mathbb{Z}_p}) = (\chi(g) \cdot \alpha)_{\mathbb{Z}_p},$$

onde $\alpha \in \mathbb{Z}_p$. Coa notación $\alpha_{\mathbb{Z}_p}$ queremos resaltar que vemos α como un elemento de $\mathbb{Z}_p$ na álxebra de Iwasawa $\Lambda(\mathbb{Z}_p)$. Desta forma temos que $\Lambda(\mathbb{Z}_p^\times)$ é un $\mathcal{G}$-submódulo. Ademais, como vimos no Lema 6.14, $\mathcal{M}(id_{\mathbb{Z}_p}) = 1 + T$ polo que temos que $\mathcal{M}$ define un $\mathcal{G}$-isomorfismo entre $\Lambda(\mathbb{Z}_p)$ e Λ cando Λ está dotado pola $\mathcal{G}$-acción definida da seguinte forma

$$(\sigma f)(T) = f((1+T)^{\chi(\sigma)} - 1),$$

con $\sigma \in \mathcal{G}$, $f \in \Lambda$ e $\chi(\sigma)$ denota o carácter ciclotómico de σ. Cómpre resaltar tamén que temos o $\mathcal{G}$-isomorfismo canónico

$$\widetilde{\chi} : \Lambda(\mathcal{G}) \cong \Lambda(\mathbb{Z}_p^\times),$$

que vén inducido polo isomorfismo $\chi : \mathcal{G} \cong \mathbb{Z}_p^\times$ e tamén temos $\widetilde{\mathcal{M}} : \Lambda(\mathcal{G}) \cong \Lambda^{\psi=0}$. Definamos agora o seguinte operador

$$\begin{array}{rccl} \widetilde{\mathcal{L}}\colon & \mathcal{U}_\infty & \longrightarrow & \Lambda(\mathcal{G}) \\ & u & \longmapsto & \widetilde{\mathcal{L}}(u) = \widetilde{\mathcal{M}}^{-1}(\mathcal{L}(f_u)), \end{array}$$

onde f_u é a serie de potencias de Coleman de u e $\mathcal{L}$ defínese como

$$\mathcal{L}(f) = \frac{1}{p} \log \left(\frac{f(T)^p}{\varphi(f)(T)} \right).$$

O seguinte resultado é elemental para, no seguinte capítulo, poder probar o teorema fundamental de Iwasawa. Omitiremos a súa proba, pero pode atoparse en [3, Teorema 3.5.1].

Teorema 6.19. *Temos a seguinte sucesión exacta de $\mathcal{G}$-módulos*

$$0 \longrightarrow \mu_{p-1} \times T_p(\mu) \longrightarrow \mathcal{U}_\infty \xrightarrow{\widetilde{\mathcal{L}}} \Lambda(\mathcal{G}) \xrightarrow{\alpha} T_p(\mu) \longrightarrow 0,$$

onde o núcleo da esquerda é a inclusión e $\alpha(\lambda) = (\zeta_n)^{\int_{\mathcal{G}} \chi d\lambda}$.

Proposición 6.20. *Sexa $u \in \mathcal{U}_\infty$, temos que*

$$\int_{\mathcal{G}} \chi(g)^k d\widetilde{\mathcal{L}}(u) = (1 - p^{k-1})\delta_k(u),$$

para $k \geq 1$.

Demostración. Debido a que existe o $\mathcal{G}$-isomorfismo canónico, $\Lambda(\mathcal{G}) \cong \Lambda(\mathbb{Z}_p^\times)$ temos que

$$\int_{\mathcal{G}} \chi(g)^k d\lambda = \int_{\mathbb{Z}_p^\times} x^k d(\widetilde{\chi}(\lambda)) = \int_{\mathbb{Z}_p} x^k d(\widetilde{\chi}(\lambda)).$$

A segunda igualdade séguese de que identificamos $\Lambda(\mathbb{Z}_p^\times)$ co subconxunto (6.2) de $\Lambda(\mathbb{Z}_p)$. Se tomamos $\lambda = \widetilde{\mathcal{L}}(u)$, entón dáse a igualdade

$$\widetilde{\chi}(\widetilde{\mathcal{L}}(u)) = \gamma(\mathcal{L}(f_u)) \quad \text{con} \quad \mathcal{L}(f_u)(T) = \frac{1}{p}\log\left(\frac{f_u(T)^p}{\varphi(f)(T)}\right).$$

Así, polo Lema 6.15 a integral do enunciado é igual a

$$\big(D^{k-1}(h_u(T) - \varphi(h_u)(T))\big)_{T=0} \quad \text{con} \quad h_u(T) = (1+T)\frac{f_u'(T)}{f_u(T)}.$$

Para rematar, basta aplicar a expresión (6.3) á parte da dereita da igualdade do enunciado. □

6.2. A función zeta p-ádica

Recordemos a notación utilizada:

$$\mathcal{G} = \mathrm{Gal}(\mathcal{F}_\infty \mid \mathbb{Q}) \quad \text{e} \quad G = \mathrm{Gal}(F_\infty \mid \mathbb{Q}),$$

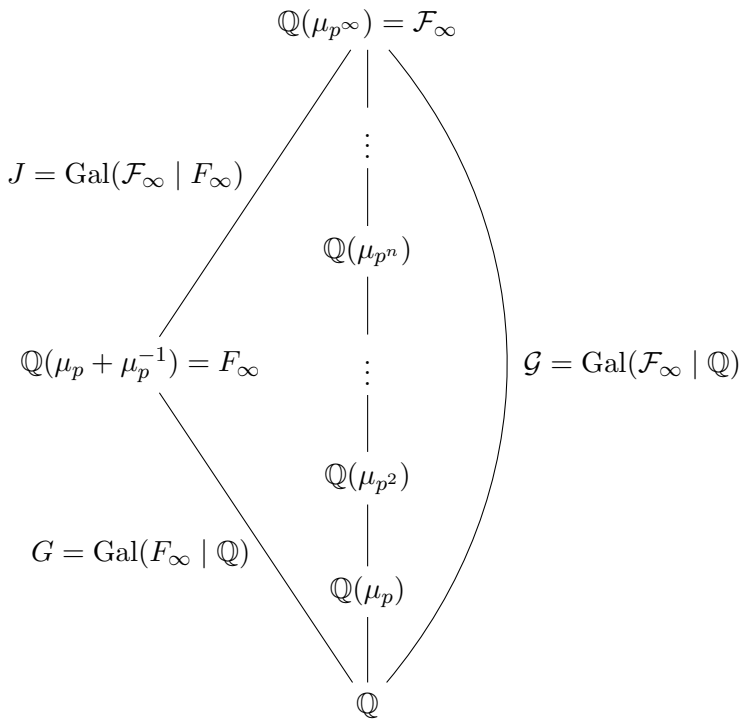
onde $\mathcal{F}_\infty = \mathbb{Q}(\mu_{p^\infty})$ e $F_\infty = \mathcal{F}_\infty^+$ é o seu subcorpo maximal real. Por outro lado, sexa

$$J = \{1, j\} = \mathrm{Gal}(\mathcal{F}_\infty \mid F_\infty), \tag{6.4}$$

onde

$$1: \begin{array}{ccc} \mathcal{F}_\infty & \longrightarrow & \mathcal{F}_\infty \\ \sigma & \mapsto & \sigma \end{array} \qquad \text{e} \qquad j: \begin{array}{ccc} \mathcal{F}_\infty & \longrightarrow & \mathcal{F}_\infty \\ \sigma & \mapsto & \sigma^{-1}. \end{array}$$

Vexamos todo isto nun diagrama.



Se M é un $\mathbb{Z}_p[J]$-módulo, entón p vai ser impar e temos a seguinte descomposición

$$M = M^+ \oplus M^-, \quad \text{con} \quad M^+ = \frac{1+j}{2}M \quad \text{e} \quad M^- = \frac{1-j}{2}M.$$

Desta forma, temos que

$$\Lambda(\mathcal{G}) = \Lambda(\mathcal{G})^+ \oplus \Lambda(\mathcal{G})^-.$$

Lema 6.21. *Temos o seguinte isomorfismo*

$$\Lambda(\mathcal{G})^+ \cong \Lambda(G).$$

Demostración. Posto que

$$\mathcal{G}_n = \mathrm{Gal}(\mathcal{F}_n \mid \mathbb{Q}) \text{ e } G_n = \mathrm{Gal}(F_n \mid \mathbb{Q}),$$

sendo $\mathcal{F}_n = \mathbb{Q}(\mu_{p^{n+1}})$ e $F_n = \mathbb{Q}(\mu_{p^{n+1}})^+$, imos considerar a sobrexección natural

$$\pi_n : \mathbb{Z}_p[\mathcal{G}_n] \longrightarrow \mathbb{Z}_p[G_n].$$

O obxectivo é ver que π_n induce un isomorfismo entre $\mathbb{Z}_p[\mathcal{G}_n]^+$ e $\mathbb{Z}_p[G_n]$. Por unha parte, π_n é sobrexectivo e leva $\mathbb{Z}_p[\mathcal{G}_n]^-$ a cero. Por outra parte, o $\mathbb{Z}_p$-rango de $\mathbb{Z}_p[\mathcal{G}_n]^+$ é

$$\frac{p-1}{2}\cdot p^n$$

debido á seguinte descomposición

$$\mathbb{Z}_p[\mathcal{G}_n]^+ = \bigoplus_{j \text{ par e } j \pmod{p-1}} \mathbb{Z}_p[\mathcal{G}_n]^{(j)}.$$

□

Lema 6.22. *Sexa $\lambda \in \Lambda(\mathcal{G})$ tal que $\chi^k(\lambda) = 0$ para todo $k > 0$, entón $\lambda = 0$.*

Demostración. Recordemos o isomorfismo $\widetilde{\mathcal{M}} : \Lambda(\mathcal{G}) \cong \Lambda^{\psi=0}$. Desta forma temos que

$$\widetilde{\mathcal{M}}(\lambda) = \sum_{n=0}^{\infty} T^n \int_{\mathcal{G}} \binom{\chi(g)}{n} d\lambda.$$

Cando $n > 0$, $\binom{x}{n}$ é un polinomio na variable x con termo constante nulo. Polo que por hipótese temos que

$$\int_{\mathcal{G}} \binom{\chi(g)}{n} d\lambda = 0 \quad \text{para } n > 0.$$

Así $\widetilde{\mathcal{M}}(\lambda)$ é unha constante e debe de ser identicamente cero posto que $\widetilde{\mathcal{M}}(\lambda) \in \Lambda^{\psi=0}$. □

Corolario 6.23. *Nas condicións do lema anterior, se $\lambda \in \Lambda(\mathcal{G})$ cumprindo que $\chi^k(\lambda) \neq 0$, para todo $k > 0$, entón λ non é un divisor de cero.*

Demostración. Sexa $\lambda' \cdot \lambda = 0$, como χ^k é un homomorfismo de aneis de $\Lambda(\mathcal{G})$ entón $\chi^k(\lambda') = 0$ para todo $k > 0$ e así $\lambda' = 0$. □

Observación 6.24. O Lema 6.22 é análogo para pseudomedidas en $\mathcal{G}$.

Demostración. Consideremos ξ unha pseudomedida en $\mathcal{G}$ tal que $\chi^k(\xi) = 0$ para todo $k > 0$. Para cada $v \in \mathbb{Z}_p^\times$, denotemos a σ_v como o único elemento de $\mathcal{G}$ tal que $\chi(\sigma_v) = v$. Agora escollamos $v = 1 + p$, entón

$$\chi^k(\sigma_v - 1) = (1+p)^k - 1$$

que evidentemente é non nulo para todo $k > 0$. Polo tanto, $\sigma_v - 1$ non é un divisor de cero en $\Lambda(\mathcal{G})$ polo corolario anterior. Por outro lado, a hipótese $\chi^k(\xi) = 0$ implica que

$$\chi^k((\sigma_v - 1)\xi) = 0$$

para todo $k > 0$. De novo, polo corolario previo temos que $\xi = 0$ xa que $\sigma_v - 1$ non é un divisor de cero. □

Consideremos $Q(\mathcal{G})$, o anel de cocientes de $\Lambda(\mathcal{G})$, entón temos a seguinte descomposición

$$Q(\mathcal{G}) = Q(\mathcal{G})^+ \oplus Q(\mathcal{G})^-$$

e, desta forma, podemos identificar pseudomedidas en G con pseudomedidas en $\mathcal{G} \in Q(\mathcal{G})^+$.

Corolario 6.25. *Sexa $\lambda \in \Lambda(\mathcal{G})$, entón:*

1. *Se $\int_{\mathcal{G}} \chi^k d\lambda = 0$ para k enteiro positivo impar, entón $\lambda \in \Lambda(\mathcal{G})^+$.*
2. *Se $\int_{\mathcal{G}} \chi^k d\lambda = 0$ para k enteiro positivo par, entón $\lambda \in \Lambda(\mathcal{G})^-$.*

Demostración. Sexa $\lambda \in \Lambda(\mathcal{G})$ e consideremos a súa descomposición $\lambda = \lambda^+ + \lambda^-$. Recordemos a expresión (6.4), entón como $\chi(j) = -1$ é evidente que $\chi^k(1 + j) = 0$ para todos os k enteiros impares, mentres que $\chi^k(1 - j) = 0$ para todos os k enteiros pares. Desta forma, o resultado séguese a partir do Lema 6.22. □

Observación 6.26. Ao igual que antes, o corolario é análogo para pseudomedidas.

A seguinte proposición é fundamental para probar a existencia do análogo p-ádico da función zeta de Riemann, pero antes veremos un lema necesario para poder probar dito resultado.

Lema 6.27. *Sexa e unha raíz primitiva módulo p de tal forma que $e^{p-1} \not\equiv 1 \pmod{p^2}$, entón temos que*

$$I(\mathcal{G}) = (\sigma_e - 1)\Lambda(\mathcal{G}) = \Lambda(\mathcal{G})\theta(e, 1),$$

onde $\theta(a, b) = \sigma_b - \sigma_a$ e $I(\mathcal{G})$ é o ideal de aumentación.

Proposición 6.28. *Existe unha única pseudomedida $\widetilde{\zeta_p}$ en $\mathcal{G}$ de tal forma que*

$$\int_{\mathcal{G}} \chi(g)^k d\widetilde{\zeta_p} = \begin{cases} (1 - p^{k-1})\zeta(1 - k) & \text{se } k \text{ enteiro positivo par,} \\ 0 & \text{se } k \text{ enteiro positivo impar.} \end{cases}$$

Demostración. Comecemos vendo a existencia. Sexan $a, b \in \mathbb{Z}$ relativamente primos con p e tales que $b \neq \pm a$. Definimos, $c(a, b) = \{c_n(a, b)\} \in \mathcal{U}_\infty$ como anteriormente, é dicir,

$$c_n(a,b) = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-b/2} - \zeta_n^{b/2}}.$$

Por outra parte, definimos tamén

$$\lambda(a,b) = \widetilde{\mathcal{L}}(c(a,b)) \in \Lambda(\mathcal{G}).$$

Polas Proposicións 6.18 e 6.20 temos que

$$\int_{\mathcal{G}} \chi^k d\lambda(a,b) = \begin{cases} (b^k - a^k)(1-p^{k-1})\zeta(1-k) & \text{se } k \text{ enteiro positivo par,} \\ 0 & \text{se } k \text{ enteiro positivo impar.} \end{cases} \tag{6.5}$$

Consideremos agora $\theta(a,b) = \sigma_b - \sigma_a \in \Lambda(\mathcal{G})$, onde recordemos que σ_u denota o único elemento de $\mathcal{G}$ tal que $\chi(\sigma_u) = u$ para todo $u \in \mathbb{Z}_p^\times$. Así para todo $k > 0$ temos que

$$\chi^k(\theta(a,b)) = b^k - a^k$$

é non nulo xa que $b \neq \pm a$. En consecuencia, $\theta(a,b)$ non é un divisor de cero en $\Lambda(\mathcal{G})$ e

$$\widetilde{\zeta_p} = \frac{\lambda(a,b)}{\theta(a,b)} \in Q(\mathcal{G}).$$

O seguinte paso é probar que $\widetilde{\zeta_p}$ é independente do par (a,b) escollido. En efecto, sexa (v,w) outra escolla, temos grazas á integral (6.5) que

$$\chi^k(\theta(v,w)\lambda(a,b)) = \chi^k(\theta(a,b)\lambda(v,w)),$$

para todo $k > 0$, e o Lema 6.22 amosa que

$$\theta(v,w)\lambda(a,b) = \theta(a,b)\lambda(v,w),$$

co que temos a independencia. O Lema 6.27 mostra que $\widetilde{\zeta_p}$ é unha pseudomedida. En efecto, tomando $a = e$, $b = 1$ onde e denota unha raíz primitiva módulo p tal que $e^{p-1} \not\equiv 1 \pmod{p^2}$. Polo mesmo lema, o ideal de aumentación de $\Lambda(G)$ está xerado por $\theta(e,1)$. Pero se $\sigma \in \mathcal{G}$, entón $\sigma - 1 \in I(\mathcal{G})$, é dicir, $\sigma - 1 = \theta(e,1)\lambda$ con $\lambda \in \Lambda(\mathcal{G})$. Polo que queda claro que $(\sigma-1)\widetilde{\zeta_p} \in \Lambda(\mathcal{G})$. Para rematar a unicidade séguese dos lemas anteriores. □

Como consecuencia do Corolario 6.25 e da Proposición 6.28 temos o seguinte teorema, onde a pseudomedida ζ_p é o análogo p-ádico desexado da función zeta de Riemann.

Teorema 6.29. *Existe unha única pseudomedida ζ_p en G cumprindo que*

$$\int_G \chi(g)^k d\zeta_p = (1 - p^{k-1})\zeta(1 - k),$$

para todo k enteiro par positivo.

Capítulo 7

O teorema de Iwasawa e a conxectura principal de Iwasawa

Xa construída a función zeta p-ádica de Riemann temos os ingredientes necesarios para poder probar o teorema de Iwasawa, que como veremos é fundamental para comprender a súa conxectura principal. Ademais, trataremos de forma máis divulgativa a idea da proba de dita conxectura debido á súa complexidade. Algunhas boas referencias para os conceptos que exploraremos neste capítulo son os últimos capítulos de [3], o artigo de Greenberg [6] e o texto de Sharifi [25]. Do mesmo xeito, para rematar trataremos a evolución da teoría de Iwasawa en diferentes ramas das matemáticas. Ao igual que nos anteriores capítulos seguiremos a utilizar a mesma notación.

7.1. A conxectura principal de Iwasawa

Como adiantabamos anteriormente, nesta sección veremos un teorema fundamental no que corresponde á demostración da conxectura principal de Iwasawa.

Definición 7.1. Definimos $\mathcal{D}_n$ como a intersección do grupo de unidades globais de $\mathcal{F}_n$ co subgrupo de $\mathcal{F}_n^\times$ xerado por $\sigma(\pi_n)$, onde σ recorre os elementos de $\mathrm{Gal}(\mathcal{F}_n \mid \mathbb{Q})$. Por outra banda, definimos $D_n = \mathcal{D}_n \cap F_n$.

De feito, D_n está xerado por todas as conxugacións de Galois de $\pm c_n(e,1)$ onde recordemos

$$c_n(e,1) = \frac{\zeta_n^{-e/2} - \zeta_n^{e/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}},$$

sendo e a raíz primitiva módulo p cumprindo que $e^{p-1} \not\equiv 1 \pmod{p^2}$. Ademais, D_n ten

índice finito no grupo de todas as unidades de F_n, posto que este correspóndese con $\mathrm{Cl}(F_n)$, que como vimos é finito.

Definición 7.2. Definimos $\mathcal{C}_n$ como a clausura de $\mathcal{D}_n$ respecto a topoloxía p-ádica, é dicir, $\mathcal{C}_n = \overline{\mathcal{D}_n}$. Analogamente temos que $C_n = \overline{D_n}$.

Ademais, denotaremos $\mathcal{U}_n^1 = \{x \in \mathcal{U}_n \mid x \equiv 1 \pmod{\mathfrak{p}_n}\}$. De forma máis xeral, se Y é un subgrupo de $\mathcal{U}_n$ escribiremos $Y^1 = Y \cap \mathcal{U}_n^1$. Por outra banda, temos que

$$U_\infty^1 = \varprojlim U_n^1 \quad \text{e} \quad C_\infty^1 = \varprojlim C_n^1,$$

respecto ás aplicacións norma. De feito, son módulos da álxebra de Iwasawa $\Lambda(G)$.

Vexamos agora un lema que nos axudará a probar o resultado máis importante da sección.

Lema 7.3. *Sexa e unha raíz primitiva arbitraria módulo p tal que $e^{p-1} \not\equiv 1 \pmod{p^2}$, entón*

$$C_\infty^1 = \Lambda(G)b,$$

onde $b = (b_n)$ vén dado por

$$b_n = uc_n(e, 1) \quad \textit{para } n \geq 0,$$

e u é a única raíz $(p-1)$-ésima da unidade en $\mathbb{Q}_p$ satisfacendo que $eu \equiv 1 \pmod{p}$.

O seguinte teorema é fundamental no que corresponde á teoría de Iwasawa, posto que historicamente esta proba levou a Iwasawa ao descubrimento da súa conxectura principal. De feito, hoxe en día é un paso moi importante na demostración de dita conxectura.

Teorema 7.4 (Iwasawa)**.** *U_∞^1/C_∞^1 é canonicamente isomorfo a $\Lambda(G)/I(G) \cdot \zeta_p$ como $\Lambda(G)$-módulo, onde ζ_p denota á función zeta p-ádica de Riemann e $I(G)$ ao ideal de aumentación de $\Lambda(G)$.*

Demostración. Podemos expresar $\mathcal{U}_\infty$ e U_∞ como

$$\mathcal{U}_\infty = \mu_{p-1} \times \mathcal{U}_\infty^1 \quad \text{e} \quad U_\infty = \mu_{p-1} \times U_\infty^1.$$

Polo Teorema 6.19 temos

$$0 \longrightarrow T_p(\mu) \longrightarrow \mathcal{U}_\infty^1 \xrightarrow{\mathcal{L}^1} \Lambda(\mathcal{G}) \longrightarrow T_p(\mu) \longrightarrow 0,$$

onde $\mathcal{L}^1 = \widetilde{\mathcal{L}}\big|_{\mathcal{U}^1_\infty}$. A sucesión é exacta despois de tomar invariantes baixo $J = \{1, j\}$ xa que p é impar. Ademais, como $T_p(\mu)^J = 0$ temos o $\Lambda(G)$-isomorfismo canónico

$$\mathcal{L}^1 : U^1_\infty \cong \Lambda(G).$$

Pero polo Lema 7.3,

$$C^1_\infty = \Lambda(G)b,$$

así

$$\mathcal{L}^1(C^1_\infty) = \Lambda(G)\mathcal{L}^1(b).$$

Pero a proba da Proposición 6.28 amosa que $\mathcal{L}^1(b) = \zeta_p\theta^+(e,1)$, onde $\theta^+(e,1)$ é a imaxe de $\theta(e,1)$ en $\Lambda(G)$. O análogo do Lema 6.27 para G mostra que $\Lambda(G)\theta^+(e,1) = I(G)$, co que remataría a proba. □

7.2. Idea da demostración da conxectura principal de Iwasawa

A demostración da conxectura principal de Iwasawa motivou boa parte dos desenvolvementos que se realizaron na segunda metade do século XX. En primeiro lugar, Iwasawa probara en 1972 o que se coñece como *fórmula analítica para o número de clases*, relacionando os graos dos polinomios que aparecen en ambos lados da conxectura principal. Un corolario do seu traballo é que chegaba con demostrar unha das dúas inclusións de ideais para concluír.

Hai dous acercamentos principais á demostración, que se basean en demostrar as dúas inclusións. Historicamente, o primeiro deles foi desenvolvido por Mazur e Wiles [16] empregando a teoría de formas modulares e representacións de Galois. As formas modulares son funcións holomorfas definidas no semiplano superior complexo e que satisfán boas propiedades relativas ás súas simetrías. Os resultados de Ribet e Mazur–Wiles empregan congruencias entre dous tipos distintos de formas modulares para construír extensións abelianas non ramificadas de corpos ciclotómicos. En particular, Ribet empregou esa idea para demostrar o recíproco dun coñecido teorema de Herbrand, mentres que Mazur e Wiles melloraron o método para demostrar a conxectura principal, estudando para iso a acción de Galois nas xacobianas de formas modulares.

O segundo acercamento, máis relacionado coa teoría que desenvolvemos nesta memoria, emprega os denominados sistemas de Euler, clases de cohomoloxía de Galois que cumpren certas relacións de compatibilidade; este método desenvólvese con detalle na referencia principal que

empregamos para os capítulos anteriores [3]. O método dos sistemas de Euler aparecera xa anteriormente na demostración da conxectura de Birch e Swinnerton-Dyer para rango analítico un desenvolvida por Kolyvagin, e observacións de Thaine e doutros matemáticos daban idea do robusto que era ese método para aplicacións á teoría de Iwasawa.

Rubin [22] empregou o método de Kolyvagin para construír un sistema de Euler sobre $\mathbb{Q}$; dito sistema de elementos emprégase logo para limitar a orde dunha compoñente do grupo de clases en función da orde dunha compoñente do grupo cociente das unidades globais polas ciclotómicas.

As relacións de norma, de xeito informal, permiten relacionar elementos en $\mathbb{Q}(\zeta_{N\ell})$ con outros en $\mathbb{Q}(\zeta_N)$. Máis concretamente, se $\ell \nmid N$, entón

$$\mathbb{N}_{\mathbb{Q}(\zeta_{N\ell})/\mathbb{Q}(\zeta_N)}(1-\zeta_{N\ell}) = \frac{1-\zeta_N}{1-\zeta_N^{\ell-1}},$$

onde $\mathbb{N}$ denota a norma correspondente á extensión de corpos. Con esta relación, pódese empregar un *operador derivada* (que involucra elementos nun grupo de Galois) aos elementos que teñen a forma $1-\zeta_{N\ell}$, para certas eleccións de primos ℓ congruentes con ± 1 módulo unha potencia suficientemente grande do primo p. Deste xeito, obtéñense elementos que son potencias de certos ideais non principais, e pódese así limitar o tamaño do grupo de clases.

7.3. Extensións da teoría de Iwasawa

Para esta última parte, seguimos a referencia de Sharifi [25], na que discute extensións da teoría de Iwasawa. A xeneralización máis directa témola cando substituímos o corpo dos números racionais por un corpo totalmente real, un caso no que tamén temos unha única $\mathbb{Z}_p$-extensión. A función L p-ádica coñécese grazas aos traballos de Deligne-Ribet e Wiles demostrou a conxectura principal baixo certas suposicións. Porén, o método dos sistemas de Euler é difícil de aplicar neste contexto. Aínda que Stark e Rubin conxecturaron que os sistemas de Euler deben existir para extensións abelianas de corpos totalmente reais, polo de agora non hai ningún resultado concluínte.

O caso no que si está ben entendida a teoría de Iwasawa é o dos corpos cadráticos imaxinarios. Nese caso, as extensións abelianas están totalmente descritas grazas á teoría das curvas elípticas con multiplicación complexa, e temos á nosa disposición as chamadas *unidades elípticas*, que son análogos das unidades ciclotómicas. Con estas ferramentas, Coates e Wiles [4] probaron, en 1977, un análogo do teorema de Iwasawa. Rubin, en 1991, demostrou a conxectura principal en termos de sistemas de Euler. Nese caso, a función L p-ádica que se emprega foi construída por Katz.

Un contexto no que a teoría de Iwasawa adquiriu unha dimensión importante ten que ver co estudo das curvas elípticas. Unha curva elíptica sobre os racionais é unha curva plana proxectiva

cun punto no infinito que se pode escribir no plano afín cunha ecuación da forma

$$E\colon y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}, \quad 4a^3 + 27b^2 \neq 0.$$

No conxunto de puntos racionais, $E(\mathbb{Q})$, podemos definir unha estrutura de grupo abeliano; polo teorema de Mordell, o grupo é finitamente xerado. Nese contexto, a conxectura de Birch e Swinnerton-Dyer relaciona o seu rango coa orde de anulación dunha función L asociada á curva elíptica, $L(E, s)$.

A conxectura principal de Iwasawa pode entender como unha versión p-ádica do problema do milenio. O obxecto central deixa de ser a función L complexa e agora éo unha función de variable p-ádica, $L_p(E, s)$, que se pode ver como o análogo da función zeta p-ádica que aparecía na conxectura principal de Iwasawa. Do mesmo xeito, o ideal característico de X_∞ cámbiase agora polo ideal característico doutro módulo, que se chama *grupo de Selmer*.

A diferenza principal neste contexto é que non existe unha fórmula analítica para o número de clases, polo que hai que probar as dúas divisibilidades.

(A) Unha delas séguese da existencia dun sistema de Euler para as curvas elípticas, seguindo o traballo de Kato.

(B) A outra, cuxa demostración é moito máis recente, é consecuencia do traballo de Skinner-Urban sobre formas automorfas para o grupo unitario $\mathrm{GU}(2, 2)$.

Bibliografía

[1] Atiyah, M. F. e Macdonald, I. G. (1978). *Introducción al Álgebra Conmutativa. Reverté.*

[2] Brumer, A. (1967). *On the units of algebraic number fields. Mathematika*, **14**(2).

[3] Coates, J. e Sujatha, R. (2006). *Cyclotomic Fields and Zeta Values. Springer-Verlag.*

[4] Coates, J. e Wiles, A. (1977). *On the Conjecture of Birch and Swinnerton-Dyer. Inventiones Mathematicae*, **39**, 223–251.

[5] Gouvêa, F. Q. (2010). *p-adic Numbers. An Introduction* (3rd ed.). *Springer.*

[6] Greenberg, R. (2001). *Iwasawa Theory – Past and Present.* Manuscrito.

[7] Hart, W., Harvey, D. e Ong, W. (2017). *Irregular primes to two billion.* Manuscrito.

[8] Iwasawa, K. (1959). *On* Γ*-extensions of algebraic number fields. Bulletin of the American Mathematical Society.*

[9] Kedlaya, K. S. (2025). *Notes on Class Field Theory.* Dispoñible en: `https://kskedlaya.org/cft/sec_hilbert.html`

[10] Lang, S. (2002). *Algebra* (3rd ed.). *Springer-Verlag.*

[11] Lang, S. (1978). *Cyclotomic Fields. Springer-Verlag.*

[12] Lang, S. (1976). *Introduction to Modular Forms. Springer-Verlag.*

[13] Lozano-Robledo, A. (2014). *Desde Fermat, Lamé y Kummer hasta Iwasawa: Una introducción a la teoría de Iwasawa. La Gaceta de la RSME.*

[14] Mahler, K. (1958). *An interpolation series for continuous functions of p-adic variable. Journal für die reine und angewandte Mathematik.*

[15] Marcus, D. A. (2018). *Number Fields* (2nd ed.). *Springer.*

[16] Mazur, B. e Wiles, A. (1984). *Class fields of abelian extensions of* $\mathbb{Q}$. *Inventiones Mathematicae*, **76**(2), 179–330.

[17] Mihăilescu, P. (2009). *The* T *and* T^* *components of* Λ*-modules and Leopoldt's conjecture.* Manuscrito.

[18] Milne, J. S. (2022). *Fields and Galois Theory* (Version 5.10). Dispoñible en: `https://www.jmilne.org/math/CourseNotes/FT.pdf`

[19] Milne, J. S. (2020). *Class Field Theory* (Version 4.03). Dispoñible en: `https://www.jmilne.org/math/CourseNotes/CFT.pdf`

[20] Neukirch, J. (1999). *Algebraic Number Theory. Springer.*

[21] Rangel, J. M. C. (2018). *Sobre la p-parte del grupo de clases de ideales: una introducción a la teoría de Iwasawa.* Universidad de los Andes.

[22] Rubin, K. (1991). *The 'main conjectures' of Iwasawa theory for imaginary quadratic fields. Inventiones Mathematicae*, **103**(1), 25–68.

[23] Serre, J. P. (1973). *A Course in Arithmetic. Springer.*

[24] Serre, J. P. (1958). *Classes des corps cyclotomiques, d'après Iwasawa. Séminaire Bourbaki.*

[25] Sharifi, R. (2019). *Iwasawa Theory: A Climb up the Tower. Notices of the AMS.*

[26] Washington, L. C. (1982). *Introduction to Cyclotomic Fields* (2nd ed.). *Springer.*

[27] Zúñiga, J. G. (2017). *Teoría de Iwasawa.* Pontificia Universidad Católica de Valparaíso.