

# **Torres infinitas sorprendentes**

**Una introducción a la Teoría de Iwasawa**

MICHAEL FÜTTERER & JOSÉ VILLANUEVA

26 de julio de 2019



# Introducción

En un sentido amplio, el objetivo de la teoría de números es estudiar como se comportan los números enteros o algebraicos y ecuaciones entre ellos en diferentes situaciones. Muchas veces esta conducta puede ser descrita por estructuras algebraicas. Por ejemplo, el grupo de clases de ideales de un campo de números describe la descomposición en factores primos únicos en su anillo de enteros (o más bien su ausencia). Otro ejemplo es el grupo de Selmer de una curva elíptica sobre un campo de números, que tiene que ver con la discrepancia entre la existencia de puntos globales en la curva (es decir, definidos sobre el campo de números) y locales (es decir, definidos sobre una completación). Estos grupos por eso son de mucho interés, pero naturalmente son intrincados de captar.

Este patrón se puede extender a otras situaciones, la más general siendo la de un *motivo* – un término que no vamos a explicar en este texto, pero es quizás el objeto de interés más general de la geometría aritmética, y un campo de números o una curva elíptica son ejemplos de motivos.

La idea pionera de KENKICHI IWASAWA (1917–1998) era estudiar estas conductas no sobre un solo campo de números  $K$ , sino sobre todos los campos de una torre infinita  $K_1 \subseteq K_2 \subseteq \dots$  de estos. Aunque esto parece hacer todo aún más complicado, en realidad lleva a una teoría rica y fecunda. Este proceso analiza los grupos que uno quiere entender como módulos sobre un cierto anillo, el *álgebra de Iwasawa*  $\Lambda$ , y así los hace más manejables – de manera similar a como el dominio íntegro de enteros  $p$ -ádicos  $\mathbb{Z}_p$  se comporta mejor que los anillos finitos  $\mathbb{Z}/p^r\mathbb{Z}$ . Con estos métodos, Iwasawa consiguió demostrar teoremas importantes sobre los grupos de clases de campos de números, como por ejemplo el siguiente.

**Teorema I (Iwasawa, 1959):** *Sea  $K$  un campo de números y  $p$  un primo. Para cada  $r \in \mathbb{N}_{\geq 1}$  sea  $K_r/K$  una extensión tal que  $\text{Gal}(K_r/K) \simeq \mathbb{Z}/p^r\mathbb{Z}$  y  $K_r \subseteq K_{r+1}$ . Escribimos  $p^{e_r}$  como la máxima potencia de  $p$  que divide el orden del grupo de clases de  $K_r$ . Entonces existen constantes  $\mu, \lambda \in \mathbb{N}_{\geq 0}$  y  $\nu \in \mathbb{Z}$  tal que*

$$e_r = \mu p^r + \lambda r + \nu \quad \text{para } r \gg 0.$$

Otro objeto en el centro de interés de la teoría de números moderna son las funciones  $L$ , por ejemplo la función zeta de Riemann, la función zeta de Dedekind de un campo de números o la función  $L$  de Hasse y Weil de una curva elíptica (en general, se puede definir una tal función para cualquier motivo). Desde hace mucho tiempo existía evidencia de que estas funciones tienen alguna conexión con los grupos que mencionamos anteriormente. Por ejemplo, la fórmula analítica de números de clases conecta los grupos de clases de un campo de números a su función zeta de Dedekind, o la conjetura de Birch y Swinnerton-Dyer conecta el grupo de Selmer de una curva elíptica a la función  $L$  de Hasse y Weil. Otro resultado en este estilo es el *criterio de Kummer*:

**Teorema II (Kummer, 1850):** *Sea  $h_p$  el número de clases del campo ciclotómico  $\mathbb{Q}(\mu_p)$ . Entonces*

$$\begin{aligned} p \mid h_p &\iff p \mid \zeta(1-n) \text{ para algún } n \geq 1 \text{ par} \\ &\iff p \text{ divide uno de } \zeta(-1), \zeta(-3), \dots, \zeta(4-p). \end{aligned}$$

Aquí,  $\zeta$  es la función zeta de Riemann.<sup>1</sup>

<sup>1</sup> De hecho se sabe que los valores en los enteros negativos de la función zeta de Riemann son racionales, que

La razón por la cual ERNST EDUARD KUMMER (1810–1893) se interesó en esto es que fue capaz de demostrar el Último Teorema de Fermat para exponentes  $p$  con  $p \nmid h_p$ . Su demostración bonita es muy instructiva para entender la teoría básica de campos ciclotómicos, que juegan un papel importante en la teoría de Iwasawa, y remitimos a [Was97, Cap. 1] para ella.

Una de las ideas revolucionarias de Iwasawa fue usar su teoría de torres de extensiones infinitas y el álgebra de Iwasawa para estudiar estas conexiones sorprendentes entre las funciones  $L$  con grupos de clases o sus análogos y buscar una explicación profunda para ellas. Esto es viabilizado porque no sólo ciertos valores especiales de funciones  $L$  son racionales (o al menos algebraicos), sino además varían de manera  $p$ -ádicamente continua. Estos asombrosos fenómenos llevan a la existencia de un análogo  $p$ -ádico de muchas funciones  $L$ . Este análogo es «más algebraico» en el sentido que puede ser visto como elemento en el álgebra de Iwasawa  $\Lambda$ . Iwasawa intuyó que estas *funciones  $L$   $p$ -ádicas* son como un eslabón intermediario entre las funciones  $L$  clásicas (complejas) y los grupos de origen aritmético ... esto es la *Conjetura Principal de Iwasawa*.

De manera más precisa, en el caso clásico esto significa lo siguiente. El análogo  $p$ -ádico de la función zeta de Riemann fue construido por primera vez por TOMIO KUBOTA (\*1930) y HEINRICH-WOLFGANG LEOPOLDT (1927–2011), y luego con métodos más novedosos por Iwasawa. Estos últimos métodos ven este análogo  $p$ -ádico como un objeto (esencialmente) en el álgebra de Iwasawa que está conectado a la función compleja de Riemann por una *fórmula de interpolación*:

**Teorema III (Kubota/Leopoldt, 1964; Iwasawa, 1969):** *Existe un único elemento  $\mu \in \Lambda[1/h]$ , donde  $\Lambda$  es el álgebra de Iwasawa y  $h \in \Lambda$  es un elemento regular, con la propiedad de que*

$$\kappa^{1-n}(\mu) = (1 - p^{n-1})\zeta(1 - n)$$

para cada  $n \in \mathbb{N}_{\geq 1}$ , donde los  $\kappa^{1-n}: \Lambda \rightarrow \mathbb{Z}_p$  con  $n \in \mathbb{N}_{\geq 1}$  son una familia de morfismos canónicos.

Para  $n \geq 1$  sea  $X_n$  un cierto subgrupo<sup>2</sup> del grupo de clases del campo  $K_n := \mathbb{Q}(\mu_{p^n})$  y sea  $X = \varprojlim_n X_n$ . Entonces  $X$  es un módulo sobre el álgebra de Iwasawa  $\Lambda$ . La Conjetura Principal de Iwasawa, demostrada por BARRY MAZUR (\*1937) y ANDREW WILES (\*1953), conecta la función zeta de Riemann usando su análogo  $p$ -ádico, con estos grupos de clases:

**Teorema IV (Mazur/Wiles, 1984):** *Existe un morfismo de  $\Lambda$ -módulos*

$$\Lambda/(h\mu) \rightarrow X$$

con núcleo y conúcleo finito.

El poder de esta afirmación podría no ser obvio a primera vista. Sin embargo, es una de las relaciones más profundas entre las funciones  $L$  y la aritmética. El criterio de Kummer del teorema II es una consecuencia de la Conjetura Principal, como son otros resultados sobre los grupos de clases como los teoremas de Stickelberger y Herbrand/Ribet.

Este texto invita al lector que conozca los fundamentos de la teoría de números algebraica, al fascinante mundo de la Teoría de Iwasawa. Vamos a conocer el álgebra de Iwasawa (capítulos 2 y 3) y su teoría de torres de extensiones y usar esto para demostrar su teorema I y algunos resultados más sobre grupos de clases (capítulo 4). Luego vamos a construir la función zeta  $p$ -ádica de Riemann del teorema III y las funciones  $L$   $p$ -ádicas de Dirichlet (capítulo 5). Después vamos explicar la Conjetura Principal de Iwasawa y sus implicaciones

es un fenómeno habitual, aunque no trivial, de muchas funciones  $L$ . Decimos que  $p \mid \frac{a}{b}$  para un número racional  $\frac{a}{b}$  con  $(a, b) = 1$  si  $p \mid a$ .

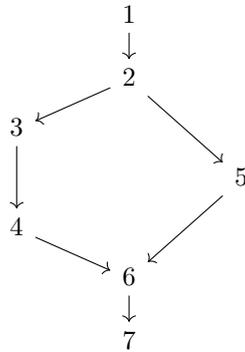
<sup>2</sup> Más precisamente, tomamos el subgrupo de la  $p$ -parte donde la conjugación compleja actúa por  $-1$ .

(capítulo 6). La demostración de la Conjetura Principal es mucho más difícil y por eso no podemos decir mucho sobre ella en este texto. Finalmente, en el capítulo 7 vamos a describir algunas de las áreas de investigación activa en la Teoría de Iwasawa que muestran como todas estas ideas pueden ser generalizadas a nuevos terrenos.

## Guía

Los conocimientos necesarios para entender este texto son modestos. Asumimos que el lector tiene conocimientos básicos del álgebra conmutativa, la teoría de Galois, la teoría de números algebraica y la topología. En el capítulo 1 recopilamos algunos resultados importantes de dichas áreas y damos referencias. Los capítulos 2–6 constituyen la parte principal de este texto, en el que explicamos en detalle y de la manera más autocontenida posible los aspectos de la Teoría de Iwasawa clásica que nos parecen más importantes. Finalmente, en el último capítulo 7 explicamos generalizaciones. Únicamente en este capítulo suponemos algunos conocimientos adicionales.

El siguiente diagrama muestra la dependencia de los capítulos.



## Otros textos

Aquí queremos mencionar algunos textos importantes que pueden ser útiles para un lector que quiere aprender de la Teoría de Iwasawa y que influyeron a los autores en su camino de conocerla. Por supuesto nuestra presentación de esta área no es ni remotamente completa, y estos otros textos pueden complementarla.

Los libros de Washington [Was97] y Lang [Lang0] sobre campos ciclotómicos son clásicos que cobran mucho material, entre otros la Teoría de Iwasawa clásica y mucho de lo que hacemos aquí, aunque la presentación ya no es la más moderna. Una buena visión conjunta sobre la Teoría de Iwasawa clásica es dada por las notas de Sharifi [Sha], pero él presume más conocimientos previos como por ejemplo cohomología de grupos. Un texto más compendiado que también incluye la Teoría de Iwasawa para curvas elípticas son las notas de Wüthrich [Wut14]. También queremos mencionar el libro [NSW08] de Neukirch, Schmidt y Wingberg que contiene algunos aspectos (más algebraicos) de la Teoría de Iwasawa. Finalmente, el libro [CS06] de Coates y Sujatha explica la Conjetura Principal de Iwasawa y contiene una demostración completa sin pedir muchos conocimientos previos.

El texto corto de Kato [Kat07] de su plática en el ICM de 2006 da un panorama general y bonito de la Teoría de Iwasawa clásica y también la más moderna, incluyendo desarrollos recientes. En un estilo muy leíble explica también mucho sobre las motivaciones, con foco sobre todo en la Conjetura Principal y sus generalizaciones. Otro texto digno de leerse es [Gre01b] de Greenberg, que también incluye mucha información sobre la historia de la teoría.

Por supuesto deberíamos mencionar algunos textos de Iwasawa mismo; aquí solo listamos los que nos parecen los más importantes. En [Iwa59a] demostró su fórmula del teorema I para el orden de los grupos de clases, uno de los primeros resultados importantes en su teoría. Luego en [Iwa69b] reinterpretó los resultados de Kubota y Leopoldt sobre las funciones  $L$   $p$ -ádicas, dando una nueva demostración de su existencia. Esto le permitió formular su Conjetura Principal en [Iwa69a], después de ya haber demostrado un caso muy especial en [Iwa64] (véase [Gre01b, (4.1)]). Finalmente, el texto [Iwa73] contiene un gran panorama en general de los aspectos algebraicos de su trabajo junto con nuevos resultados.

Para literatura más avanzada o más específica remitimos a las referencias que se encuentran durante el texto, sobre todo en el capítulo 7 sobre generalizaciones.

## Agradecimientos

En un inicio este texto consistía de nuestras notas del curso «Introducción a la Teoría de Iwasawa» que impartimos en la Escuela de Otoño de Teoría de Números, en el marco de las actividades del 51 Congreso de la Sociedad Matemática Mexicana (21–26 octubre 2018) en Villahermosa, Tabasco. Agradecemos profundamente a Carlos Castaño la invitación que nos extendió para participar como ponentes y por haber alentado la redacción de este trabajo.

También queremos agradecer a los participantes del curso, especialmente a Tim Gendron, cuyos valiosos comentarios mejoraron la redacción del texto.

Un agradecimiento profundo a nuestros colegas del Instituto de Matemáticas de Heidelberg: Benjamin Kupferer, Pavel Sechin y Oliver Thomas, por su disponibilidad para discutir de matemáticas con nosotros y especialmente a Katharina Hübner quien también leyó una versión preliminar. Las innumerables discusiones que tuvimos con ellos son invaluable para la redacción de este trabajo.

Agradecemos a Otmar Venjakob quien incondicionalmente apoyó este proyecto, con ánimos de atraer a más estudiantes hispanohablantes a la Teoría de Iwasawa.

Una parte esencial de los capítulos 2 y 3 está basada en un curso dictado por Jean-François Jaulent en la Universidad de Burdeos en 2014, a quien agradecemos sus detalladas explicaciones.

agradecerle a  
Cornelius

## Notación

El símbolo  $p$  sin mayor explicación siempre denota un primo, y si no decimos otra cosa asumimos que es impar (la mayoría de lo que haremos funciona también si  $p = 2$ , pero así la presentación es ligeramente más fácil).

Para evitar confusión con los números naturales, escribiremos  $\mathbb{N}_{\geq 0}$  para los números enteros  $\geq 0$  y  $\mathbb{N}_{\geq 1}$  para aquellos  $\geq 1$  y no usaremos el símbolo  $\mathbb{N}$ .

Fijemos cerraduras algebraicas  $\overline{\mathbb{Q}}$  de  $\mathbb{Q}$ ,  $\overline{\mathbb{Q}}_\ell$  de  $\mathbb{Q}_\ell$  para cada primo  $\ell$  y  $\mathbb{C}$  de  $\mathbb{R}$  y encajes de  $\overline{\mathbb{Q}}$  en  $\overline{\mathbb{Q}}_\ell$  y en  $\mathbb{C}$ .

Escribimos  $G_{\mathbb{Q}}$  para el grupo absoluto de Galois de  $\mathbb{Q}$ , es decir  $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , y similarmente para los otros campos. Entonces nuestros encajes definen inclusiones de grupos

$$G_{\mathbb{Q}_\ell} \hookrightarrow G_{\mathbb{Q}}, \quad G_{\mathbb{R}} \hookrightarrow G_{\mathbb{Q}}.$$

En particular, tiene sentido hablar de la conjugación compleja en objetos con una acción de  $G_{\mathbb{Q}}$ .

# Índice general

<b>1</b>	<b>Preámbulo</b>	<b>9</b>
1.1	Estructuras algebraicas profinitas . . . . .	9
1.2	Compendio de la teoría de números algebraica . . . . .	13
1.3	Campos ciclotómicos . . . . .	17
1.4	Teoría de Kummer y un poco de teoría de campos de clases . . . . .	18
1.5	Números $p$ -ádicos y caracteres . . . . .	20
<b>2</b>	<b>El álgebra de Iwasawa</b>	<b>25</b>
2.1	El anillo de series de potencias . . . . .	25
2.2	Medidas . . . . .	30
2.3	Idempotentes y el álgebra de Iwasawa para grupos más grandes . . . . .	35
<b>3</b>	<b>Módulos noetherianos sobre el álgebra de Iwasawa</b>	<b>39</b>
3.1	Pseudo-isomorfismos . . . . .	39
3.2	$\Lambda$ -módulos noetherianos de torsión . . . . .	42
3.3	Teorema de estructura . . . . .	44
3.4	Resultados adicionales sobre $\Lambda$ -módulos . . . . .	48
3.5	Ideales característicos . . . . .	50
3.6	Adjuntos de Iwasawa . . . . .	52
<b>4</b>	<b>Grupos de clases y el teorema de Iwasawa</b>	<b>59</b>
4.1	Grupos de Clases en Extensiones Ciclotómicas . . . . .	59
4.2	Extensiones $\mathbb{Z}_p$ . . . . .	62
4.3	Propiedades de los grupos de clases como $\Lambda$ -módulos . . . . .	64
4.4	Teorema de Iwasawa . . . . .	67
4.5	Sobre los invariantes $\mu$ y $\lambda$ . . . . .	71
<b>5</b>	<b>Funciones <math>L</math> <math>p</math>-ádicas</b>	<b>73</b>
5.1	Proemio sobre las funciones $L$ . . . . .	73
5.2	Teoría elemental $p$ -ádica de valores de la función zeta . . . . .	78
5.3	La construcción de funciones $L$ $p$ -ádicas mediante elementos de Stickelberger . . . . .	87
5.4	Suplementos y consecuencias de la existencia de las funciones $L$ $p$ -ádicas . . . . .	93
5.5	La teoría de Coleman y otras maneras de construir la función zeta $p$ -ádica . . . . .	97
<b>6</b>	<b>La Conjetura Principal de Iwasawa</b>	<b>103</b>
6.1	Las formulaciones de la Conjetura Principal . . . . .	103
6.2	La equivalencia de las formulaciones . . . . .	106
6.3	Consecuencias de la Conjetura Principal . . . . .	111
6.4	Unos comentarios sobre la demostración de la Conjetura Principal . . . . .	115
<b>7</b>	<b>Generalizaciones</b>	<b>117</b>
7.1	Teoría de Iwasawa para aritmética logarítmica . . . . .	117
7.2	Generalizaciones de la Conjetura Principal: Curvas elípticas, Motivos y la Conjetura Equivariante de los Números de Tamagawa . . . . .	117
	<b>Bibliografía</b>	<b>141</b>

*Índice general*

**Índice**

**147**

# Capítulo 1

## Preámbulo

En este capítulo coleccionamos algunos resultados de varias partes de matemáticas que necesitaremos a continuación y damos referencias para ellos. El lector es libre de saltar este capítulo y solo consultarlo por necesidad.

### 1.1. Estructuras algebraicas profinitas

Estructuras algebraicas profinitas son generalizaciones de estructuras algebraicas finitas que en muchos aspectos se comportan similares y juegan un papel importante en la teoría de Iwasawa y en la teoría de números en general. Una referencia muy útil que explica muchos aspectos del álgebra profinita es el libro [RZ10], a que remitimos para más detalles.

**Definición 1.1:** Un *grupo profinito* es un grupo topológico que, como grupo topológico, es isomorfo a un límite de grupos finitos. De la misma manera definimos *anillos profinitos*, *módulos profinitos* y *álgebras profinitas* sobre anillos profinitos.

Un grupo profinito se llama *pro- $p$*  si es (isomorfo a un) límite de grupos finitos cuyos órdenes son potencias de  $p$ , y similarmente para anillos etcétera.

Grupos profinitos aparecen naturalmente en la teoría de Galois para extensiones infinitas. Resumamos estos resultados aquí.

Fijamos una extensión de Galois de campos  $L/K$  con grupo de Galois  $G$ . Sea  $\mathcal{Z}$  el conjunto de campos intermedios entre  $K$  y  $L$  y  $\mathcal{S}$  el conjunto de subgrupos de  $G$ . Si  $L/K$  es finito entonces el teorema principal de la teoría de Galois dice que los mapeos

$$\begin{aligned} F: \mathcal{S} &\rightarrow \mathcal{Z}, & H &\mapsto L^H := \{x \in L : \forall \sigma \in H : \sigma(x) = x\} \\ U: \mathcal{Z} &\rightarrow \mathcal{S}, & M &\mapsto \text{Gal}(L/M) \end{aligned}$$

son biyecciones inversas la una a la otra. Si  $L/K$  es infinito, es fácil ver que todavía tenemos  $F \circ U = \text{id}_{\mathcal{Z}}$ . Sin embargo, la composición  $U \circ F$  en general no es la identidad, como muestra el ejemplo siguiente. Sean  $p$  y  $\ell$  primos diferentes con  $\ell \neq 2$ . Consideramos la extensión de Galois de  $K = \mathbb{F}_p$  que es dada por

$$L := \bigcup_{i=0}^{\infty} K_i$$

donde para  $i \in \mathbb{N}_{\geq 1}$ ,

$$K_i := \mathbb{F}_{p^{\ell^i}}$$

que es la única extensión de  $K$  de grado  $\ell^i$ . Sea  $G = \text{Gal}(L/K)$  y  $H$  el subgrupo generado por el Frobenius  $\text{Frob}$ . Entonces  $L^G = L^H = K$ , pero se puede construir un elemento de  $G$  que no está en  $H$ . Para esto sea  $e_i = 1 + \ell + \ell^2 + \dots + \ell^{i-1}$  para  $i \in \mathbb{N}_{\geq 1}$ . Cada  $x \in L$  está en algún  $K_i$  y definimos

$$\sigma(x) = \text{Frob}^{e_i}(x).$$

Porque  $e_{i+1} \equiv e_i \pmod{\ell^i}$  tenemos  $\text{Frob}^{e_{i+1}}|_{K_i} = \text{Frob}^{e_i}|_{K_i}$ , así que esto define un elemento  $\sigma \in G$ . Si  $\sigma \in H$  entonces existiría  $n \in \mathbb{N}_{\geq 0}$  con  $\sigma = \text{Frob}^n$ . Esto significaría

$$n \equiv e_i \pmod{\ell^i}.$$

Multiplicando ambos lados por  $(\ell - 1)$  obtenemos  $n(\ell - 1) \equiv 1 \pmod{\ell^i}$  para cada  $i \in \mathbb{N}_{\geq 1}$ , es decir  $n(\ell - 1) = 1$ , que no puede ser porque  $\ell > 2$ .

Aun así, este ejemplo nos da una idea como se podría reparar la situación. Aunque  $\sigma \notin H$ , los  $\text{Frob}^{e_i} \in H$  «aproximan»  $\sigma$  en el sentido que coinciden con  $\sigma$  en subextensiones  $K_i$  mas y mas grandes (pero siempre finitas). Eso sugere definir la siguiente topología.

**Definición 1.2:** Sea  $L/K$  una extensión de Galois con grupo  $G$ . La *topología de Krull* es definida con decir que los subgrupos

$$\text{Gal}(L/M), \quad M \text{ una subextensión finita}$$

sean una base de vecindades del elemento neutro.

Es decir, dos elementos  $\sigma, \tau \in G$  están «cerca» si y solo si existe una subextensión finita  $M$  con  $\sigma^{-1}\tau \in \text{Gal}(L/M)$  para la cual  $\text{Gal}(L/M)$  sea «pequeño», pues si y solo si coinciden en un subcampo «grande».

Se verifica facilmente que  $G$  entonces es un grupo topológico, es decir multiplicación y inversión son continuas. Además, para una extensión finita obtenemos la topología discreta. Con esta topología tenemos

$$U(F(H)) = \overline{H}$$

para cada subgrupos  $H$  de  $G$ . Esto implica la siguiente generalización del teorema principal de la teoría de Galois.

**Teorema 1.3 (Teorema principal de la teoría de Galois infinita):** Sea  $L/K$  una extensión de Galois con grupo  $G$ ,  $\mathcal{Z}$  el conjunto de campos intermedios entre  $K$  y  $L$   $\mathcal{S}$  el conjunto de los subgrupos cerrados de  $G$ .

(a) Los mapeos

$$\begin{aligned} F: \mathcal{S} &\rightarrow \mathcal{Z}, & H &\mapsto L^H \\ U: \mathcal{Z} &\rightarrow \mathcal{S}, & M &\mapsto \text{Gal}(L/M) \end{aligned}$$

son biyecciones inversos el uno al otro que inviertan inclusiones.

(b) Un campo intermedio  $M$  es normal sobre  $K$  si y solo si el subgrupo  $\text{Gal}(L/M)$  es normal en  $G$ , en que caso la restricción a  $M$  da un isomorfismo

$$\text{Gal}(L/K)/\text{Gal}(L/M) \xrightarrow{\cong} \text{Gal}(M/K).$$

(c) Un campo intermedio  $M$  es finito sobre  $K$  si y solo si el subgrupo  $\text{Gal}(L/M)$  es abierto en  $G$ .

(d) El mapeo canónico

$$G \xrightarrow{\cong} \varprojlim_{\substack{M \in \mathcal{Z} \\ \text{finito}}} \text{Gal}(M/K) = \varprojlim_{\substack{H \in \mathcal{S} \\ \text{abierto}}} G/H$$

es un isomorfismo.

*Demostración:* [RZ10, Thm. 2.11.3] □

En particular, este teorema muestra que cada grupo de Galois es un grupo profinito.<sup>1</sup> Un ejemplo de un anillo profinito son los enteros  $p$ -ádicos

$$\mathbb{Z}_p = \varprojlim_{r \in \mathbb{N}_{\geq 1}} \mathbb{Z}/p^r \mathbb{Z}$$

o más generalmente el anillo de enteros de una extensión finita de  $\mathbb{Q}_p$ .

**Definición 1.4:** Sea  $G$  un grupo profinito. Entonces un elemento  $g \in G$  se llama *generador topológico* si el subgrupo generado por  $g$  es denso en  $G$ .

Por ejemplo,  $1 \in \mathbb{Z}_p$  es un generador topológico.

**Nota 1.5:** La propiedad de un grupo topológico de ser profinito puede ser caracterizado de manera puramente topológica: Un grupo topológico es profinito si y solo si es compacto, Hausdorff y totalmente desconectado. Lo mismo es verdad para un anillo topológico; aquí, esto incluso es equivalente al anillo siendo solo compacto y Hausdorff. Véase [RZ10, Thm. 2.1.3, Prop. 5.1.2] para estos hechos. Generalizando esto, un grupo topológico se llama *localmente profinito* si es Hausdorff, totalmente desconectado y localmente compacto; análogamente se define anillos y álgebras localmente profinitos.

Muchas construcciones del álgebra abstracta tienen análogos profinitos. Por ejemplo,  $\mathbb{Z}$  tiene la propiedad de que para cualquier grupo  $G$  y cada elemento  $g \in G$  hay un único morfismo de grupos  $f: \mathbb{Z} \rightarrow G$  tal que  $f(1) = g$ . El grupo profinito  $\mathbb{Z}_p$  tiene una propiedad similar: Para cualquier grupo pro- $p$   $G$  y cada elemento  $g \in G$  hay un único morfismo de grupos topológicos  $f: \mathbb{Z}_p \rightarrow G$  tal que  $f(1) = g$ . Se dice que  $\mathbb{Z}_p$  es un *grupo abeliano pro- $p$  libre* de rango 1. Por esta razón, como cada grupo abeliano es un módulo sobre  $\mathbb{Z}$  de manera única, cada grupo abeliano pro- $p$  es de manera única un módulo sobre  $\mathbb{Z}_p$ .

Otra construcción que queremos extrapolar al mundo profinito es la del álgebra de grupos. Si  $R$  es un anillo y  $G$  es un grupo, tenemos el álgebra de grupos  $R[G]$  con la propiedad siguiente: para cada  $R$ -álgebra  $S$  y cada morfismo de grupos  $G \rightarrow S^\times$  hay una única extensión a un morfismo de  $R$ -álgebras  $R[G] \rightarrow S$ .

**Definición 1.6:** Sea  $R$  un anillo profinito y  $G$  un grupo profinito. Definimos el *anillo de grupos profinito* como

$$R[[G]] := \varprojlim_{\substack{N \triangleleft G \\ \circ}} R[G/N],$$

el límite tomado sobre todos los subgrupos normales abiertos de  $G$ .

El grupo  $G$  puede ser visto canónicamente como subconjunto de  $R[[G]]$  y el álgebra de grupos ordinaria  $R[G]$  es una  $R$ -subálgebra que es densa, véase [RZ10, Lem. 5.3.5].

**Proposición 1.7:** Sea  $R$  un anillo profinito,  $G$  un grupo profinito y  $S$  una  $R$ -álgebra profinita. Entonces cada morfismo de grupos topológicos  $G \rightarrow S^\times$  se extiende de manera única a un morfismo de  $R$ -álgebras topológicas

$$R[[G]] \rightarrow S.$$

*Demostración:* Por la propiedad universal del álgebra de grupos ordinaria  $R[G]$  y porque este anillo es denso en  $R[[G]]$ , es claro que la extensión es única si existe. Escribimos  $S = \varprojlim_i S_i$  con  $R$ -álgebras finitas  $S_i$ . Notemos que entonces  $S^\times = \varprojlim_i S_i^\times$ , en particular  $S^\times$  es un grupo topológico (¡Eso no es necesariamente cierto por un anillo topológico arbitrario

<sup>1</sup> También es verdad que cada grupo profinito es un grupo de Galois, véase [RZ10, Thm. 2.11.5].

porque la inversión no tiene que ser continua!). Para cada  $i$  consideramos la composición  $G \rightarrow S^\times \rightarrow S_i^\times$ . Por continuidad se factoriza a través del grupo finito  $G/N$  para un subgrupo normal abierto  $N$ . La propiedad del álgebra de grupos  $R[G/N]$  nos da un morfismo de  $R$ -álgebras  $R[G/N] \rightarrow S_i$  que claramente es continuo. Si componemos esto con la proyección de  $R[[G]]$  obtenemos un morfismo  $R[[G]] \rightarrow S_i$ . La familia de estos morfismos para cada  $i$  es obviamente compatible y la propiedad universal del límite luego da el morfismo  $R[[G]] \rightarrow S$  que deseamos.  $\square$

Si  $R$  es un anillo,  $G$  es un grupo y  $M$  es un  $R$ -módulo con una acción  $R$ -lineal de  $G$ , entonces  $M$  es de manera única un módulo sobre  $R[G]$ . Algo similar es verdad en el álgebra profinita, aunque hay que tener cuidado con algunos detalles topológicos.

**Proposición 1.8:** *Sea  $R$  un anillo profinito,  $G$  un grupo profinito y  $M$  un  $R$ -módulo profinito con una acción continua y  $R$ -lineal de  $G$ . Asumamos que podemos escribir  $M$  como  $M = \varprojlim_i M/U_i$ , los  $U_i$  siendo submódulos abiertos de  $M$  estables bajo la acción de  $G$ .*

*Entonces  $M$  es de manera canónica un módulo sobre  $R[[G]]$ .*

*Demostración:* Escribimos  $M_i = M/U_i$ , que es un módulo finito. Porque  $U_i$  es estable bajo la acción de  $G$  obtenemos una acción de  $G$  en  $M_i$ , es decir un morfismo  $G \rightarrow \text{Aut}_R(M_i)$ . Porque estos morfismos son compatibles si cambiamos  $i$ , obtenemos un morfismo continuo

$$G \rightarrow \varprojlim_i \text{Aut}_R(M_i)$$

de grupos profinitos. Usando que  $\varprojlim_i \text{Aut}_R(M_i) = (\varprojlim_i \text{End}_R(M_i))^\times$ , la propiedad universal del álgebra profinita de grupos induce un morfismo de  $R$ -álgebras

$$R[[G]] \rightarrow \varprojlim_i \text{End}_R(M_i) \rightarrow \text{End}_R(M)$$

que da  $M$  una estructura canónica como  $R[[G]]$ -módulo.  $\square$

La hipótesis en la proposición anterior es cierta por ejemplo si cada submódulo abierto de  $M$  es estable bajo la acción de  $G$ , o si  $M$  es dado como límite  $M = \varprojlim M_i$  con  $R[[G]]$ -módulos finitos.

**Nota 1.9:** En general, sea  $R$  un anillo conmutativo y  $G$  un grupo. Como mencionamos, un  $R[G]$ -módulo es lo mismo que un  $R$ -módulo con una acción  $R$ -lineal de  $G$  – algo así se llama *representación  $R$ -lineales de  $G$* . Si  $V$  y  $W$  son dos tal representaciones, hacemos los morfismos de  $R$ -módulos  $\text{Hom}_R(V, W)$  entre ellos un  $R[G]$ -módulo en definir la acción de  $G$  como

$$(gf)(v) = g(f(g^{-1}v)) \quad \text{para } g \in G, f \in \text{Hom}_R(V, W), v \in V.$$

Similarmente, si  $R$  es un anillo conmutativo profinito,  $G$  es un grupo profinito y  $V, W$  son  $R[[G]]$ -módulos entonces definimos una acción de  $G$  en  $\text{Hom}_R(V, W)$  con la misma fórmula. Si  $V$  y  $W$  cumplen la hipótesis de la proposición 1.8 entonces es fácil ver que  $\text{Hom}_R(V, W)$  la cumple también, así que en esta situación  $\text{Hom}_R(V, W)$  es un  $R[[G]]$ -módulo.

## Ejercicios

**Ejercicio 1.1:** Demuestre que el grupo absoluto de Galois de un campo finito es canónicamente isomorfo a  $\widehat{\mathbb{Z}}$ , que es definido por

$$\widehat{\mathbb{Z}} := \varprojlim_{n \in \mathbb{N}_{\geq 1}} \mathbb{Z}/n\mathbb{Z}$$

donde el conjunto  $\mathbb{N}_{\geq 1}$  sobre que tomamos el límite es ordenado por divisibilidad y los mapeos entre los  $\mathbb{Z}/n\mathbb{Z}$  son las proyecciones canónicas. Bajo este isomorfismo,  $1 \in \widehat{\mathbb{Z}}$  corresponde al morfismo Frobenius. Use el teorema 1.3 para esto.

**Ejercicio 1.2:** Sean  $p$  y  $\ell$  primos diferentes. Demuestre que cada morfismo de un grupo pro- $p$  a un grupo pro- $\ell$  es trivial.

**Ejercicio 1.3:** Formule la afirmación de la proposición 1.7 usando funtores adjuntos.

**Ejercicio 1.4:** Demuestre que para cada grupo pro- $p$   $G$  y cada elemento  $g \in G$  existe un único morfismo de grupos profinitos  $f: \mathbb{Z}_p \rightarrow G$  con  $f(1) = g$ . Demuestre también la afirmación análoga con grupos profinitos arbitrarios y  $\widehat{\mathbb{Z}}$  en lugar de  $\mathbb{Z}_p$ . Formule estas afirmaciones usando funtores representables o adjuntos; vea también [RZ10, §3.3].

**Ejercicio 1.5:** Demuestre que la propiedad universal del álgebra de grupos profinita de la proposición 1.7 se generaliza de la manera siguiente. Si  $R$  es un anillo profinito,  $G$  un grupo profinito y  $S$  es una  $R$ -álgebra localmente profinita (véase la nota 1.5) entonces cada morfismo continuo  $G \rightarrow S^\times$  se extiende de manera única a un morfismo de  $R$ -álgebras topológicas

$$R[[G]] \rightarrow S.$$

## 1.2. Compendio de la teoría de números algebraica

Aquí resumamos los resultados más básicos de la teoría de números algebraica que vamos usar en el resto del texto. El lector debería ser familiar con estas definiciones.

Los objetos de estudio central de la teoría de números algebraica son los siguientes.

**Definición 1.10:** (a) Un *campo de números* es una extensión finite  $K$  de  $\mathbb{Q}$ . Su *anillo de enteros* son los elementos  $\mathcal{O}_K$  que son enteros sobre  $\mathbb{Z}$ .

(b) Si  $K/\mathbb{Q}$  es cualquier extensión algebraica, no necesariamente finita, todavía podemos definir su *anillo de enteros*  $\mathcal{O}_K$  como el conjunto de los elementos enteros sobre  $\mathbb{Z}$ .

Se estudia estos campos sobre todo via los ideales de su anillo de enteros, como explicamos a continuación.

**Definición 1.11:** (a) Un *ideal fraccional* es un  $\mathcal{O}_K$ -submódulo no trivial de  $K$  finitamente generado. En particular, un ideal de  $\mathcal{O}_K$  es un ideal fraccional. Denotamos  $\text{Div}(\mathcal{O}_K)$  el conjunto de ideales fraccionales de  $\mathcal{O}_K$ .

(b) Para un ideal fraccional  $I$  sea  $I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}$ . Esto también es un ideal fraccional que se llama el *ideal inverso* de  $I$ .

(c) El producto de dos ideales fraccionales  $I, J$  es el  $\mathcal{O}$ -submódulo de  $K$  generado por todos los elementos  $ij$  con  $i \in I, j \in J$ .

(d) Un *ideal fraccional principal* es un ideal fraccional de la forma  $\alpha\mathcal{O}_K$  con  $\alpha \in K^\times$ , que denotamos también  $(\alpha)$ . Denotamos  $\text{Prin}(\mathcal{O}_K)$  el subconjunto de  $\text{Div}(\mathcal{O}_K)$  de los ideales fraccionales principales.

En general, los elementos de  $\mathcal{O}_K$  no tienen una factorización única en primos, como es el caso en el anillo  $\mathbb{Z}$ . Pero lo que es verdad es que los ideales fraccionales tienen una tal factorización.

**Teorema 1.12:** *Los ideales fraccionales  $\text{Div}(\mathcal{O}_K)$  con la multiplicación y inversión como en la definición 1.11 constituyen un grupo abeliano con elemento neutro  $\mathcal{O}_K$ . Este grupo es libre generado por los ideales primos no ceros de  $\mathcal{O}_K$ . Es decir, cada ideal fraccional  $I$  escribe de forma única (salvo al orden) como*

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

con ideales primos diferentes  $\mathfrak{p}_i$  y  $e_i \in \mathbb{Z}$ .

*Demostración:* [Neu99, Chap. I, (3.3)] □

Esto sugiere que es mejor trabajar con ideales fraccionales en lugar de elementos de  $K^\times$  – de hecho, esto es como se originó la palabra «ideal», porque son como «números idealizados» de  $K$ . La discrepancia entre los elementos de  $K^\times$  y los ideales fraccionales es medida por dos grupos:

**Definición 1.13:** El grupo de clases de  $K$  es el cociente

$$\text{Cl}(K) = \text{Div}(\mathcal{O}_K) / \text{Prin}(\mathcal{O}_K).$$

Tenemos una sucesión exacta

$$1 \rightarrow \mathcal{O}_K^\times \rightarrow K^\times \rightarrow \text{Div}(\mathcal{O}_K) \rightarrow \text{Cl}(K) \rightarrow 1.$$

Es decir, el grupo  $\mathcal{O}_K^\times$  mide qué tan lejos está la asociación  $\alpha \mapsto (\alpha)$ , de  $K^\times$  a ideales fraccionales, de ser única. Por su lado, el grupo  $\text{Cl}(K)$  mide «cuántos más ideales que ideales principales hay» o «qué tan lejos está la factorización en primos de elementos de  $\mathcal{O}_K$  de ser única». De hecho,  $\text{Cl}(K)$  es trivial si y solo si  $\mathcal{O}_K$  es un dominio de ideales principales. Por eso es muy importante estudiar los grupos  $\mathcal{O}_K^\times$  y  $\text{Cl}(K)$ . El primero es descrito por el teorema siguiente.

**Teorema 1.14 (Teorema de las unidades de Dirichlet):** Sea  $r$  la cantidad de encajes  $K \rightarrow \mathbb{R}$  y  $c$  la cantidad de parejas conjugadas de morfismos  $K \rightarrow \mathbb{C}$  con imagen no contenida en  $\mathbb{R}$ . Entonces (de manera no canónica)

$$\mathcal{O}_K^\times \simeq \mu(K) \times \mathbb{Z}^{r+c-1},$$

donde  $\mu(K)$  son las raíces de la unidad en  $K$ .

*Demostración:* [Neu99, Chap. I, (7.4)] □

Sobre el grupo de clases solo sabemos lo siguiente.

**Teorema 1.15:** El grupo  $\text{Cl}(K)$  es finito.

*Demostración:* [Neu99, Chap. I, (6.3)] □

En general es muy difícil describir su estructura. La Teoría de Iwasawa permite obtener resultados sobre el grupo de clases en algunas situaciones, como vamos a explicar en las secciones más adelante.

**Definición 1.16:** El orden del grupo de clases,  $\#\text{Cl}(K)$ , se llama el número de clases de  $K$  y se denota  $h_K$ .

**Definición 1.17:** Sea  $K$  un campo de números. Una plaza de  $K$  es

- (1) un ideal primo no nulo de  $\mathcal{O}_K$ , o
- (2) un encaje  $K \hookrightarrow \mathbb{R}$ , o
- (3) una pareja de encajes  $K \hookrightarrow \mathbb{C}$  conjugadas con imagen no contenida en  $\mathbb{R}$ .

Las plazas de tipo (1) se llaman *plazas no arquimedeanas* y las plazas de tipo (2) o (3) se llaman *plazas arquimedeanas*; más específicamente, las de tipo (2) se llaman *plazas reales* y las de tipo (3) *plazas complejas*.

Equivalentemente y más uniformemente, se puede definir una plaza de un campo de números  $K$  como una clase de equivalencia de un valor absoluto en  $K$ , es decir, de una

función  $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$  que es multiplicativa, cumple la desigualdad triangular y que toma el valor 0 sólo en 0 (dos valores absolutos son equivalentes si definen la misma topología en  $K$ ). Se puede verificar que cada valor absoluto en  $K$  viene o de la valuación en un ideal primo no nulo (en que caso cumple la desigualdad triangular ultramétrica y se llama no arquimedea) o de un encaje en  $\mathbb{R}$  o  $\mathbb{C}$  (en que caso se llama arquimedea). Véase [Neu99, §II.3] para más detalles.

Sea  $L/K$  una extensión finita de campos de números. Para cada ideal primo  $\mathfrak{p}$  de  $\mathcal{O}_K$  podemos descomponer el ideal  $\mathfrak{p}\mathcal{O}_L$  generado por  $\mathfrak{p}$  en  $\mathcal{O}_L$  como

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

con ideales primos  $\mathfrak{P}_i$  de  $\mathcal{O}_L$  y  $e_i \in \mathbb{N}_{\geq 1}$ . En esta situación decimos que cada de los  $\mathfrak{P}_i$  está *arriba* de  $\mathfrak{p}$  y  $\mathfrak{p}$  está *debajo* de cada uno de los  $\mathfrak{P}_i$ .

Para plazas arquimedeanas  $\sigma$  de  $L$  y  $\tau$  de  $K$  decimos que  $\sigma$  está *arriba* de  $\tau$  y  $\tau$  está *debajo* de  $\sigma$  si  $\sigma|_K = \tau$ .

**Definición 1.18:** (a) Los exponentes  $e_i$  se llaman *grado de ramificación*. Para cada  $i$  el grado de la extensión  $f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$  se llama *grado de inercia*. El primo  $\mathfrak{P}_i$  se llama *ramificado* si  $e_i > 1$  y se llama *totalmente ramificado* si además  $f_i = 1$ . Decimos que el primo  $\mathfrak{p}$  es *ramificado* si uno de los  $\mathfrak{P}_i$  lo es y *totalmente ramificado* si todos de los  $\mathfrak{P}_i$  lo son. La extensión  $L/K$  se llama *ramificada* si existe un ideal primo  $\mathfrak{p} \subseteq \mathcal{O}_K$  no cero que es ramificado.

(b) Una plaza arquimedea de  $K$  se llama *ramificada* si es una plaza real que está debajo de una plaza compleja de  $L$ .

**Ejemplo 1.19:** Consideramos la extensión  $\mathbb{Q}(i)/\mathbb{Q}$ . Su anillo de enteros es  $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1)$ , así que para un primo  $p$  tenemos

$$\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[X]/(X^2 + 1) \cong \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \text{si } p \equiv 1 \pmod{4}, \\ \mathbb{F}_{p^2} & \text{si } p \equiv 3 \pmod{4}, \\ \mathbb{F}_p[X]/(X + 1)^2 & \text{si } p = 2. \end{cases}$$

De ahí podemos ver que los primos tal que  $p \equiv 3 \pmod{4}$  siguen siendo primos en  $\mathbb{Z}[i]$ , los primos tal que  $p \equiv 1 \pmod{4}$  se descomponen en un producto de dos primos diferentes de  $\mathbb{Z}[i]$  y el primo 2 se escribe como  $2 = \mathfrak{p}^2$  con un primo  $\mathfrak{p}$  de  $\mathbb{Z}[i]$ , que pues está ramificado y es la única plaza no arquimedea que está ramificada. Además,  $\mathbb{Q}(i)$  obviamente tiene una única plaza arquimedea, que es compleja y pues ramificada, porque extiende la única plaza arquimedea de  $\mathbb{Q}$ , que es real.

Siempre tenemos  $\sum_{i=1}^g e_i f_i = [L : K]$  (véase [Neu99, Chap. I, (8.2)]). Si la extensión  $L/K$  es Galois, los  $e_i$  y  $f_i$  son iguales para cada  $i$  (véase [Neu99, Chap. I, (9.1) y p. 55]), y los llamamos simplemente  $e$  y  $f$ . Entonces  $[L : K] = efg$ .

**Definición 1.20:** Sea  $L/K$  una extensión Galois de campos de números y

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e$$

la descomposición de un ideal primo de  $\mathcal{O}_K$  como arriba. El grupo  $\text{Gal}(L/K)$  actúa en los  $\mathfrak{P}_i$  transitivamente [Neu99, Chap. I, (9.1)].

(a) Para cada  $i$  el estabilizador de  $\mathfrak{P}_i$  se llama *grupo de descomposición* de  $\mathfrak{P}_i$  y se denota  $G_{\mathfrak{P}_i/\mathfrak{p}}$ .

(b) El núcleo de la aplicación natural sobreyectiva [Neu99, Chap. I, (9.4)]

$$G_{\mathfrak{P}_i} \twoheadrightarrow \text{Gal}(\mathcal{O}_L/\mathfrak{P}_i/\mathcal{O}_K/\mathfrak{p})$$

se llama el *grupo de inercia* de  $\mathfrak{P}_i$  y se denota  $I_{\mathfrak{P}_i/\mathfrak{p}}$ .

**Proposición 1.21:** *En la situación de la definición 1.20 tenemos*

$$\#G_{\mathfrak{P}_i/\mathfrak{p}} = ef, \quad \#I_{\mathfrak{P}_i/\mathfrak{p}} = e.$$

*En particular,  $\mathfrak{p}$  es no ramificado si y solo si  $I_{\mathfrak{P}_i/\mathfrak{p}}$  es trivial y es totalmente ramificado si y solo si  $I_{\mathfrak{P}_i/\mathfrak{p}} = G_{\mathfrak{P}_i/\mathfrak{p}}$  (para algún, o equivalentemente todo  $i$ ).*

*Demostración:* [Neu99, Chap. I, (9.6)] □

El resultado anterior nos permite extender estas definiciones a extensiones infinitas. Aquí seguimos [Was97, Appendix, §2].

**Definición 1.22:** Sea  $L/K$  una extensión de Galois, posiblemente infinita, donde  $K$  es una extensión algebraica no necesariamente finita de  $\mathbb{Q}$ . Sea  $\mathfrak{P}$  un ideal primo de  $\mathcal{O}_L$  y  $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ , que es un ideal primo de  $\mathcal{O}_K$ . En esta situación decimos que  $\mathfrak{P}$  está *arriba* de  $\mathfrak{p}$  y  $\mathfrak{p}$  está *debajo* de  $\mathfrak{P}$ .

(a) El *grupo de descomposición* de  $\mathfrak{P}$  es

$$G_{\mathfrak{P}/\mathfrak{p}} := \{\sigma \in \text{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

(b) El *grupo de inercia* de  $\mathfrak{P}$  es

$$I_{\mathfrak{P}/\mathfrak{p}} := \{\sigma \in G_{\mathfrak{P}/\mathfrak{p}} \mid \forall x \in \mathcal{O}_K : \sigma(x) \equiv x \pmod{\mathfrak{P}}\}.$$

(c) Decimos que  $\mathfrak{P}$  es *no ramificado* si  $I_{\mathfrak{P}/\mathfrak{p}}$  es trivial y es *totalmente ramificado* si  $I_{\mathfrak{P}/\mathfrak{p}} = G_{\mathfrak{P}/\mathfrak{p}}$ .

(d) Decimos que un primo  $\mathfrak{p}$  de  $\mathcal{O}_K$  es *ramificado* o *totalmente ramificado* si existe un primo  $\mathfrak{P}$  de  $\mathcal{O}_L$  arriba de  $\mathfrak{p}$  que lo es (equivalentemente, todos los primo  $\mathfrak{P}$  de  $\mathcal{O}_L$  arriba de  $\mathfrak{p}$  lo son).

Terminamos la sección con la definición importante de norma de ideales.

**Definición 1.23:** Sea  $L/K$  una extensión finita campos de números de grado  $n$ . El morfismo de grupos abelianos

$$N: \text{Div}(\mathcal{O}_L) \rightarrow \text{Div}(\mathcal{O}_K), \quad \mathfrak{P} \mapsto \mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}}$$

donde  $\mathfrak{P}$  es un ideal primo en  $\mathcal{O}_L$  y  $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$  se llama *norma relativa de ideales*. Tiene la propiedad de que para cada  $I \in \text{Div}(\mathcal{O}_K)$  tenemos  $N(I\mathcal{O}_L) = I^n$ . Envía ideales principales a ideales principales y por eso induce un morfismo

$$N: \text{Cl}(L) \rightarrow \text{Cl}(K)$$

que también llamamos *norma relativa de ideales*.

### 1.3. Campos ciclotómicos

En esta sección introducimos los ejemplos de campos de números que serán los más importantes en este texto y alistamos algunas de sus propiedades.

**Definición 1.24:** Si  $m \in \mathbb{N}_{\geq 1}$  escribimos  $\mathbb{Q}(\mu_m)$  para el campo generado sobre  $\mathbb{Q}$  por las raíces de la unidad de orden  $m$ . Se llama *el  $m$ -ésimo campo ciclotómico*. Es un campo de números Galois cuyo grupo de Galois es isomorfo canónicamente a  $(\mathbb{Z}/m\mathbb{Z})^\times$  vía

$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\cong} \text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}), \quad a \mapsto \sigma_a \quad (1.1)$$

con  $\sigma_a$  actuando en una raíz de la unidad  $\zeta$  como  $\sigma_a(\zeta) = \zeta^a$ . Muchas veces tomamos este isomorfismo como una identificación.

En esta situación escribimos  $\mu_m$  para el subgrupo de  $\mathbb{Q}(\mu_m)^\times$  de las raíces  $m$ -ésimas de la unidad.

**Proposición 1.25:** *El anillo de enteros de  $\mathbb{Q}(\mu_m)$  es  $\mathbb{Z}[\xi]$ , donde  $\xi$  es una raíz  $m$ -ésima primitiva de la unidad.*

*Demostración:* [Neu99, Chap. 1, (10.2)] □

Notemos que para cada campo ciclotómico  $\mathbb{Q}(\mu_m)$  la conjugación compleja es un automorfismo bien definido, es decir independiente del encaje en  $\mathbb{C}$ . Bajo el isomorfismo (1.1) corresponde a  $-1 \in (\mathbb{Z}/m\mathbb{Z})^\times$ .

En todos los siguientes resultados suponemos que  $p$  es primo.

**Proposición 1.26:** *Sea  $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\mu_p)}$ . Entonces cada elemento  $u \in \mathcal{O}^\times$  se puede escribir como  $u = \xi v$  con  $\xi \in \mu_p$  y  $v \in (\mathcal{O}^\times)^+$ , donde  $(\mathcal{O}^\times)^+ \subseteq \mathcal{O}^\times$  son los elementos fijos por la conjugación compleja.*

*Demostración:* [Was97, Prop. 1.5] □

Los siguientes resultados son esenciales para entender la ramificación en las extensiones ciclotómicas.

**Lema 1.27:** *Sea  $\xi$  una  $p^r$ -raíz primitiva de la unidad y sea  $(p^r, k) = 1$ , entonces  $\frac{\xi^k - 1}{\xi - 1}$  es una unidad en  $\mathbb{Z}[\mu_{p^r}]$ .*

*Demostración:* Dejemos esto como ejercicio; véase el ejercicio 1.6, donde demostramos una afirmación más general. □

**Lema 1.28:** *Sea  $\xi$  una  $p^r$ -raíz primitiva de la unidad. Entonces  $(1 - \xi)$  es un ideal primo en  $\mathbb{Q}(\mu_{p^r})$  y  $(1 - \xi)^{(p-1)p^{r-1}} = (p)$ , es decir  $(p)$  es totalmente ramificado en  $\mathbb{Q}(\mu_{p^r})$ . En particular,  $(1 - \xi)$  es el único ideal de  $\mathbb{Q}(\mu_{p^r})$  arriba de  $(p)$ .*

*Demostración:* El conjunto de las  $p^r$ -raíces de la unidad satisfacen la ecuación  $X^{p^r} - 1 = 0$ . Si son primitivas no pueden tener orden menor a  $p^r$  por lo que tenemos

$$\frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + 1 = \prod_{(k, p^r)=1} (X - \xi^k),$$

evaluando las expresiones en 1 y tomando los ideales principales generados por los elementos, tenemos

$$(p) = \prod_{(k, p^r)=1} (1 - \xi^k).$$

Por el lema 1.27, hay una igualdad de ideales  $(1 - \xi) = (1 - \xi^k)$  para  $k$  tal que  $(k, p^r) = 1$ . Es decir  $(p) = (1 - \xi)^{(p-1)p^{r-1}}$ , como el grado de la extensión  $[\mathbb{Q}(\mu_{p^r}) : \mathbb{Q}]$  es  $(p-1)p^{r-1}$  tenemos que  $(1 - \xi)$  debe de ser primo y por lo tanto  $p$  es totalmente ramificado. □

**Proposición 1.29:** *Un primo  $\ell$  es ramificado en  $\mathbb{Q}(\mu_m)$  si y solo si  $\ell \mid m$ , salvo si  $\ell = 2$  y  $(4, m) = 2$ .*

*Demostración:* Si  $\ell \mid m$  entonces  $\mathbb{Q}(\mu_\ell) \subset \mathbb{Q}(\mu_m)$ . Como  $\ell$  ramifica en  $\mathbb{Q}(\mu_\ell)$  (lema 1.28) también lo hace en  $\mathbb{Q}(\mu_m)$ . Ahora, si  $\ell$  no divide a  $m = \prod p^{r_i}$ , entonces  $\ell$  no ramifica en cada  $\mathbb{Q}(\mu_{p^{r_i}})$  ya que el discriminante de  $\mathbb{Q}(\mu_{p^{r_i}})$  es una potencia de  $p$  [Was97, Prop. 2.1]. Por lo tanto, tampoco ramifica en el compuesto  $\mathbb{Q}(\mu_m)$ .  $\square$

También vamos a estudiar campos ciclotómicos infinitos.

**Definición 1.30:** Si  $p$  es un primo y  $N \in \mathbb{N}_{\geq 1}$  no es divisible por  $p$ , entonces escribimos  $\mathbb{Q}(\mu_{Np^\infty})$  para la extensión infinita de  $\mathbb{Q}$  generada por todas las raíces de la unidad de orden  $Np^r$  para cada  $r \in \mathbb{N}_{\geq 0}$ . Denotamos  $\mu_{Np^\infty} \subseteq \mathbb{Q}(\mu_{Np^\infty})^\times$  el subgrupo de estas raíces de la unidad.

Por la teoría de Galois infinita, su grupo de Galois es isomorfo a

$$\begin{aligned} \text{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}) &\simeq \varprojlim_{r \in \mathbb{N}_{\geq 0}} \text{Gal}(\mathbb{Q}(\mu_{Np^r})/\mathbb{Q}) \simeq \varprojlim_{r \in \mathbb{N}_{\geq 0}} (\mathbb{Z}/Np^r\mathbb{Z})^\times \\ &\simeq \varprojlim_{r \in \mathbb{N}_{\geq 0}} ((\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})^\times) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times. \end{aligned}$$

En particular, si  $N = 1$ , tenemos un isomorfismo

$$\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\simeq} \mathbb{Z}_p^\times. \quad (1.2)$$

El siguiente resultado, es sólo una reformulación de la proposición 1.29 para campos ciclotómicos infinitos.

**Proposición 1.31:** *Un primo  $\ell$  es ramificado en  $\mathbb{Q}(\mu_{Np^\infty})$  si y solo si  $\ell = p$  o  $\ell \mid N$ , salvo si  $\ell = 2$  y  $(4, Np) = 2$ .*

## Ejercicios

**Ejercicio 1.6:** Aquí demostramos una versión más general del lema 1.27 que será útil en la sección 5.5. Sea  $p \neq 2$  un primo.

Sea  $r \in \mathbb{N}_{\geq 1}$ ,  $K = \mathbb{Q}(\mu_{p^r})$  y  $\xi \in K^\times$  una raíz primitiva  $p^r$ -ésima de la unidad. Para  $a, b \in \mathbb{Z}$  coprimos y primos a  $p$  definimos

$$c_r(a, b) = \frac{\xi^{-a/2} - \xi^{a/2}}{\xi^{-b/2} - \xi^{b/2}} \in K$$

(notemos que  $2 \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ , así que  $\xi^{1/2} \in K$ ).

Demuestre que  $c_r(a, b) \in \mathcal{O}_K^\times$ . Para eso es útil escribir

$$c_r(a, b) = \xi^{a/2-b/2} \frac{\xi^a - 1}{\xi^b - 1}$$

y expresar la fracción usando un  $t \in \mathbb{Z}$  tal que  $a \equiv bt \pmod{p^r}$ .

## 1.4. Teoría de Kummer y un poco de teoría de campos de clases

La teoría de campos de clases es una teoría poderosa que permite describir las extensiones abelianas de un campo local o global en gran generalidad. Aquí solo vamos a necesitar unos casos especiales. La teoría de Kummer describe una clase particular de extensiones abelianas de cualquier campo. Aquí resumamos lo que necesitamos de esto. Empezemos con los resultados más importantes de la teoría de Kummer.

**Definición 1.32:** Sea  $d \in \mathbb{N}_{\geq 1}$  y  $F$  un campo cuya característica no divida a  $d$  y contenga las raíces  $d$ -ésimas de la unidad. Una extensión abeliana  $L/F$  tal que el grupo de Galois  $\text{Gal}(L/F)$  tiene exponente  $d$  se llama *extensión de Kummer* de exponente  $d$ .

Para cada subconjunto  $\Delta \subseteq F^\times$  la extensión  $F(\sqrt[d]{\Delta})$  siempre es una extensión de Kummer. Al revés, se cumple que también cada extensión de Kummer es de esta forma:

**Proposición 1.33 (Kummer):** Sea  $L/F$  una extensión de Kummer de exponente  $d \in \mathbb{N}_{\geq 1}$  y  $\Delta = (L^\times)^d \cap F^\times$ . Entonces:

- (a) Tenemos  $L = F(\sqrt[d]{\Delta})$ .
- (b) La asociación

$$\langle \cdot, \cdot \rangle : \text{Gal}(L/F) \times \left( \sqrt[d]{\Delta} / (\sqrt[d]{\Delta} \cap F^\times) \right) \rightarrow \mu_d \subseteq F^\times, \quad \langle \sigma, a \rangle = \frac{\sigma(a)}{a}$$

es un apareamiento perfecto de grupos abelianos que se llama el apareamiento de Kummer.

*Demostración:* Esto es demostrado en [Neu99, Chap. 4, (3.3), (3.6)]; allí el apareamiento es escrito

$$\langle \cdot, \cdot \rangle : \text{Gal}(L/F) \times \Delta / (F^\times)^d \rightarrow \mu_d \subseteq F^\times, \quad \langle \sigma, a \rangle = \frac{\sigma(\sqrt[d]{a})}{\sqrt[d]{a}}$$

pero con el lema de la serpiente es fácil ver que esto es equivalente a lo de arriba.  $\square$

**Proposición 1.34:** Sean  $K \subseteq F \subseteq L$  campos tal que todas las extensiones sean Galois y  $L/F$  es una extensión de Kummer, y como antes sea  $\Delta = (L^\times)^d \cap F^\times$ . El grupo  $\text{Gal}(L/K)$  actúa por conjugación en su subgrupo normal  $\text{Gal}(L/F)$  y actúa también en  $\sqrt[d]{\Delta} \subseteq L$  y en  $\mu_d \subseteq F$ .

Entonces el apareamiento de la proposición 1.33 (b) es equivariante en el sentido

$$\langle g\sigma g^{-1}, ga \rangle = g \langle \sigma, a \rangle \quad \text{para cada } g \in \text{Gal}(L/K), \sigma \in \text{Gal}(L/F), a \in \sqrt[d]{\Delta}.$$

*Demostración:* Esto es una consecuencia directa de la definición del apareamiento.  $\square$

**Nota 1.35:** Usamos la notación de la proposición 1.34. En esta situación el apareamiento perfecto de la proposición 1.33 (b) define isomorfismos de grupos abelianos

$$\begin{aligned} \text{Gal}(L/F) &\xrightarrow{\cong} \text{Hom}_{\mathbb{Z}} \left( \sqrt[d]{\Delta} / (\sqrt[d]{\Delta} \cap F^\times), \mu_d \right), & \sigma &\mapsto \langle \sigma, \cdot \rangle, \\ \sqrt[d]{\Delta} / (\sqrt[d]{\Delta} \cap F^\times) &\xrightarrow{\cong} \text{Hom}_{\mathbb{Z}}(\text{Gal}(L/F), \mu_d), & a &\mapsto \langle \cdot, a \rangle. \end{aligned}$$

En cada de  $\text{Gal}(L/F)$ ,  $\sqrt[d]{\Delta} / (\sqrt[d]{\Delta} \cap F^\times)$  y  $\mu_d$  tenemos acciones de  $\text{Gal}(L/K)$ . Además en la nota 1.9 definimos una acción de  $\text{Gal}(L/K)$  en los  $\text{Hom}_{\mathbb{Z}}(-, -)$  que aparecen en el lado derecho. Entonces la afirmación de la proposición 1.34 significa que los isomorfismos de arriba no solo son isomorfismos de grupos abelianos sino de  $\mathbb{Z}[\text{Gal}(L/K)]$ -módulos.

**Proposición 1.36:** Sea  $F$  un campo de números y  $L/F$  una extensión de Kummer de exponente  $d \in \mathbb{N}_{\geq 1}$ . Si  $\mathfrak{p}$  es un ideal primo de  $F$  tal que existe un  $a \in \Delta$  con  $\mathfrak{p} \mid a$ , pero  $\mathfrak{p}^d \nmid a$ , entonces  $\mathfrak{p}$  es ramificado en la extensión  $L/F$ .

*Demostración:* Véase [Koc97, Prop. 1.83 (2)]; note que el « $\mathfrak{p} \nmid a$ » allá es una errata.  $\square$

Continuamos con unos resultados de la teoría de campos de clases.

**Definición 1.37:** Sea  $K$  un campo de números. La extensión máxima abeliana no ramificada de  $K$  se llama el *campo de clases de Hilbert* de  $K$ . Esta extensión siempre existe y es finita.

La teoría de campos de clases permite describir su grupo de Galois, que va a explicar el nombre. Sea  $H$  el campo de clases de Hilbert de un campo de números  $K$ , que claramente es Galois. Si  $\mathfrak{p}$  es un ideal primo de  $K$  y  $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g$  su decomposición en  $H$  (sin exponentes porque es no ramificada), entonces para cada  $\mathfrak{P}_i$  tenemos un único elemento de Frobenius en  $\text{Gal}(H/K)$  que genera el grupo de Galois de la extensión residual  $\text{Gal}((\mathcal{O}_H/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p}))$ , y como  $\text{Gal}(H/K)$  actúa transitivamente en los  $\mathfrak{P}_i$  y es abeliano, este elemento sólo depende de  $\mathfrak{p}$ , y lo denotamos  $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(H/K)$ . Véase [Neu99, §I.9] para más detalles.

**Teorema 1.38:** *La asociación*

$$\mathfrak{p} \mapsto \text{Frob}_{\mathfrak{p}}$$

*induce un isomorfismo*

$$\left( \frac{H/K}{\cdot} \right) : \text{Cl}(K) \xrightarrow{\simeq} \text{Gal}(H/K).$$

*Demostración:* Véase [Neu99, Prop. VI.6.9 y §VI.7]; notemos que lo que nosotros llamamos el campo de clases de Hilbert se llama el «campo de clases de Hilbert pequeño» para Neukirch porque el define la ramificación de las plazas arquimedianas de una manera no tan estándar.  $\square$

## Ejercicios

**Ejercicio 1.7:** Sea  $K$  un campo de números que es Galois sobre  $\mathbb{Q}$  y  $H$  su campo de clases de Hilbert. Entonces  $\text{Gal}(K/\mathbb{Q})$  actúa en los ideales de  $K$ . Demuestre que para cada ideal primo  $\mathfrak{p}$  de  $K$  y cada  $\sigma \in \text{Gal}(K/\mathbb{Q})$  tenemos

$$\left( \frac{H/K}{\sigma(\mathfrak{p})} \right) = \tilde{\sigma} \left( \frac{H/K}{\mathfrak{p}} \right) \tilde{\sigma}^{-1}$$

donde  $\tilde{\sigma}$  es un levantamiento de  $\sigma$  a  $\text{Gal}(H/\mathbb{Q})$ .

## 1.5. Números $p$ -ádicos y caracteres

Para nosotros, un *carácter* será un morfismo de grupos de la forma  $G \rightarrow R^\times$  con  $G$  un grupo y  $R$  un anillo. Si  $G$  y  $R$  además son espacios topológicos, *siempre asumiremos que los caracteres entre ellos son continuos*. En la mayoría de los casos  $G$  será un grupo profinito y  $R$  será un anillo profinito o un campo topológico.

Hay unos caracteres de importancia especial, que tienen que ver con los números  $p$ -ádicos y los campos ciclotómicos. En esta sección introducimos y estudiamos esos caracteres.

Asumamos que el lector conozca los números  $p$ -ádicos  $\mathbb{Z}_p$  y  $\mathbb{Q}_p$ :  $\mathbb{Q}_p$  es la completación de  $\mathbb{Q}$  por el valor absoluto  $p$ -ádico y  $\mathbb{Z}_p$  es su anillo de enteros (equivalentemente, los elementos con valor absoluto  $\leq 1$ ), o alternativamente  $\mathbb{Z}_p$  es el límite inverso de los grupos finitos  $\mathbb{Z}/p^r\mathbb{Z}$  ( $r \in \mathbb{N}_{\geq 1}$ ) y  $\mathbb{Q}_p$  es su campo de cocientes. Resumamos unos hechos fundamentales sobre las extensiones de  $\mathbb{Q}_p$ .

**Proposición 1.39:** *Sea  $K/\mathbb{Q}_p$  una extensión finita. Entonces el valor absoluto  $p$ -ádico se extiende de manera única a  $K$  y  $K$  es completo por la topología definida por este valor absoluto.*

*Sea  $\mathcal{O}$  la cerradura integral de  $\mathbb{Z}_p$  en  $K$ . Entonces  $\mathcal{O} = \{x \in K : |x| \leq 1\}$ , y eso es un anillo local de valuación discreta y completo por la topología definida por las potencias de su ideal máximo (que es principal)  $\pi\mathcal{O} = \{x \in K : |x| < 1\}$ . El campo residual  $k = \mathcal{O}/\pi\mathcal{O}$  es una extensión finita de  $\mathbb{F}_p$ . En particular,  $\mathcal{O}$  es un anillo profinito.*

*Demostración:* [Neugg, Chap. II, (4.8), (3.8), (3.9), (5.2)] □

**Lema 1.40 (Lema de Representación):** *Sea  $\mathcal{O}$  un anillo local de valuación discreta completo con campo residual  $k = \mathcal{O}/\pi\mathcal{O}$  finito. Sea  $R$  un sistema de representantes de  $k$  en  $\mathcal{O}$ . Entonces todo elemento  $x \in \mathcal{O}$  se escribe de manera única como*

$$x = \sum_{i \in \mathbb{N}_{\geq 0}} a_i \pi^i,$$

con  $a_i \in R$ .

*Demostración:* Sea  $x \in \mathcal{O}$ , entonces tomando el mapeo canónico de  $\mathcal{O}$  a su campo de residuos tenemos que  $x \equiv a_0 \pmod{\pi}$  para algún  $a_0 \in R$ . Por lo tanto  $x - a_0 = x_1\pi$  con  $x_1 \in \mathcal{O}$ , aplicamos ahora el mapeo canónico a  $x_1$ , i.e.  $x_1 \equiv a_1 \pmod{\pi}$  para algún  $a_1 \in R$ . Entonces tenemos

$$\begin{aligned} x &= a_0 + x_1\pi \quad \text{con } x_1 \in \mathcal{O} \\ &= a_0 + a_1\pi + x_2\pi^2 \quad \text{con } x_2 \in \mathcal{O} \\ &\vdots \\ &= \sum_{i=0}^{\infty} a_i \pi^i. \end{aligned} \quad \square$$

**Ejemplo 1.41:** Con  $\mathcal{O} = \mathbb{Z}_p$ ,  $\pi = (p)$  y  $k = \mathbb{F}_p$  tenemos que  $R = \{0, 1, 2, \dots, p-1\}$  es un sistema de representantes de  $\mathbb{F}_p$  en  $\mathbb{Z}_p$  con el que podemos escribir cada  $x \in \mathbb{Z}_p$  como

$$x = \sum_{i \geq 0} a_i p^i \quad \text{con } a_i \in \{0, 1, \dots, p-1\}.$$

**Definición 1.42:** Sea  $K/\mathbb{Q}_p$  una extensión finita con anillo de enteros  $\mathcal{O}$  y ideal máximo  $\pi\mathcal{O}$ . Entonces

$$1 + \pi\mathcal{O} \subseteq \mathcal{O}^\times$$

es un subgrupo cuyos elementos se llaman *unidades principales*.

Estudiamos con más detalle la estructura del grupo  $\mathbb{Z}_p^\times$ .

**Lema 1.43:** *Existe un isomorfismo topológico canónico  $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$ .*

*Demostración:* Sólo demostramos esto en el caso  $p \neq 2$ , el caso  $p = 2$  siendo similar. Sea  $r \in \mathbb{N}_{\geq 1}$ , la composición

$$1 + p\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p^\times \twoheadrightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times$$

induce una sucesión exacta

$$1 \rightarrow \frac{1 + p\mathbb{Z}_p}{1 + p^r\mathbb{Z}_p} \rightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow 1.$$

Esta sucesión se escinde:

$$(\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times, \quad a \mapsto a^{p^{r-1}}$$

es una sección del mapeo de la derecha, porque  $a^p \equiv a \pmod{p}$ . Más precisamente, este mapeo toma una clase en  $(\mathbb{Z}/p\mathbb{Z})^\times$ , la levanta a un entero  $a \in \mathbb{Z}$ , envía esto a  $a^{p^{r-1}}$  y luego a

la clase módulo  $p^r$ . Por supuesto hay que asegurarse que esto no depende del levantamiento. Para esto, si reemplazamos  $a$  con  $a + bp$ , este es enviado a

$$\sum_{i=0}^r \binom{p^{r-1}}{i} a^i (bp)^{p^{r-1}-i}$$

y se puede verificar que  $\binom{p^{r-1}}{i} p^{p^{r-1}-i}$  siempre es divisible por  $p$  si  $0 \leq i < p^{r-1}$ . Omitimos los detalles aquí.

La afirmación resulta al tomar el límite.  $\square$

**Proposición 1.44:** *Sea  $p \neq 2$ . Las series de la función exponencial y del logaritmo*

$$\exp(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!}, \quad \text{resp.} \quad \log(1+y) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{y^n}{n}$$

*convergen para  $x, y \in p\mathbb{Z}_p$ , respectivamente, y dan isomorfismos de grupos topológicos*

$$p\mathbb{Z}_p \xrightleftharpoons[\log]{\exp} 1 + p\mathbb{Z}_p$$

*inversos el uno al otro.*

*Es decir, como grupo topológico  $1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p$  canónicamente. En particular, para cada  $s \in \mathbb{Z}_p$  y  $u \in 1 + p\mathbb{Z}_p$ , el elemento  $u^s \in 1 + p\mathbb{Z}_p$  es bien definido.*

*Demostración:* La primera afirmación es demostrada en [Neu99, Chap. II, (5.4) y (5.5)]. Porque  $p\mathbb{Z}_p \simeq \mathbb{Z}_p$  como grupo topológico, la segunda afirmación resulta; escribimos  $\Phi: \mathbb{Z}_p \xrightarrow{\simeq} 1 + p\mathbb{Z}_p$  para el isomorfismo. Finalmente, para  $s \in \mathbb{Z}_p$  y  $u \in 1 + p\mathbb{Z}_p$  definimos  $u^s$  como  $\Phi(s\Phi^{-1}(u))$ .  $\square$

Más generalmente, tenemos la siguiente descripción del grupo de unidades de  $\mathcal{O}$ , donde  $\mathcal{O}$  es el anillo de enteros de una extensión finita de  $\mathbb{Q}_p$ .

**Proposición 1.45:** *Con  $\mathcal{O}$  como arriba con ideal máximo  $\pi\mathcal{O}$  y campo residual  $k$ , tenemos*

$$\mathcal{O}^\times \simeq k^\times \times (1 + \pi\mathcal{O}).$$

*Además,  $1 + \pi\mathcal{O}$  es (no canónicamente) isomorfo al producto de un grupo  $p$  finito cíclico y  $\mathbb{Z}_p^d$  con  $d = [K : \mathbb{Q}_p]$ ; en particular es un grupo pro- $p$ .*

*Demostración:* [Neu99, Chap. II, (5.3), (5.7) (i)]  $\square$

Terminamos la sección con definir y estudiar unos caracteres importantes.

**Definición 1.46:** (a) Por el lema 1.43 tenemos una sección

$$\omega: \mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$$

a la proyección  $\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \rightarrow \mathbb{F}_p^\times$ . Esta sección  $\omega$  se llama *carácter de Teichmüller*.

(b) Al isomorfismo

$$\kappa: \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\simeq} \mathbb{Z}_p^\times$$

de (1.2) se le llama *carácter ciclotómico*.

- (c) Usando el isomorfismo canónico  $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$  podemos ver el carácter de Teichmüller como carácter

$$\omega: \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \rightarrow \mathbb{Z}_p^\times$$

o también como carácter de  $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ . Definimos otro carácter<sup>2</sup>

$$\kappa_0 = \omega^{-1}\kappa: \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \rightarrow \mathbb{Z}_p^\times.$$

Entonces  $\kappa_0$  es la composición del carácter ciclotómico con la proyección

$$\mathbb{Z}_p^\times \twoheadrightarrow 1 + p\mathbb{Z}_p$$

usando el isomorfismo del lema 1.43.

**Nota 1.47:** Definimos

$$\mathbb{Z}_p(1) := \varprojlim_{r \in \mathbb{N}_{\geq 1}} \mu_{p^r},$$

donde  $\mu_{p^r}$  sean aquí las raíces  $p^r$ -ésimas de la unidad en  $\overline{\mathbb{Q}}$  y las aplicaciones  $\mu_{p^{r+1}} \rightarrow \mu_{p^r}$  son  $\xi \mapsto \xi^p$ . Entonces  $\mathbb{Z}_p(1)$  es un  $\mathbb{Z}_p$ -módulo compacto que es no canónicamente isomorfo a  $\mathbb{Z}_p$  (porque  $\mu_{p^r}$  es no canónicamente isomorfo a  $\mathbb{Z}/p^r\mathbb{Z}$ ). Además  $\mathbb{Z}_p(1)$  tiene una acción de  $G_{\mathbb{Q}}$ . Si vemos el carácter ciclotómico como carácter de  $G_{\mathbb{Q}}$  vía  $G_{\mathbb{Q}} \twoheadrightarrow \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\kappa} \mathbb{Z}_p^\times$  entonces la acción de  $G_{\mathbb{Q}}$  en  $\mathbb{Z}_p(1)$  es descrita por

$$gz = \kappa(g)z \quad \text{para cada } z \in \mathbb{Z}_p(1), g \in G_{\mathbb{Q}}.$$

Sea  $z \in \mathbb{Z}_p^\times$  y lo escribimos como  $z = (f, u) \in \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$  usando el isomorfismo del lema 1.43. Entonces en  $\mathbb{Z}_p^\times$

$$\omega(f) = \lim_{j \rightarrow \infty} z^{p^j}.$$

En particular, si  $\bar{a} \in \mathbb{F}_p^\times$  y  $a \in \mathbb{Z}$  es un levantamiento, entonces

$$\omega(\bar{a}) = \lim_{j \rightarrow \infty} a^{p^j}.$$

**Lema 1.48:** Cada carácter  $\chi: \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \rightarrow \mathbb{Z}_p^\times$  es de la forma  $\chi = \omega^a \kappa_0^s$  con únicos  $a \in \{1, \dots, p-1\}$  y  $s \in \mathbb{Z}_p$ . Aquí la notación  $\kappa_0^s$  tiene sentido gracias a la proposición 1.44.

*Demostración:* Identificamos  $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$  con  $\mathbb{Z}_p^\times$  usando el carácter ciclotómico. Por la descomposición del lema 1.43 es claro que cada carácter  $\chi: \mathbb{Z}_p^\times \rightarrow \mathbb{Z}_p^\times$  se descompone en  $\chi = \psi \times \eta$  con

$$\psi: \mathbb{F}_p^\times \rightarrow \mathbb{Z}_p^\times, \quad \eta: 1 + p\mathbb{Z}_p \rightarrow \mathbb{Z}_p^\times.$$

Porque  $1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p$  no tiene torsión, la imagen de  $\psi$  está contenida en  $\mathbb{F}_p^\times$  y por eso  $\psi$  es una potencia del carácter de Teichmüller (véase ejercicio 1.9). Por otro lado, si componemos  $\eta$  con la proyección  $\mathbb{Z}_p^\times \rightarrow \mathbb{F}_p^\times$  obtenemos un morfismo de un grupo pro- $p$  a un grupo de orden primo a  $p$ , que necesariamente es trivial según el ejercicio 1.2, y vemos que la imagen de  $\eta$  está contenida en  $1 + p\mathbb{Z}_p$ . Usando la proposición 1.44, podemos estudiar los homomorfismos continuos  $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$ . Pero como explicamos en la sección 1.1, estos homomorfismos son únicamente determinados por la imagen de  $1 \in \mathbb{Z}_p$ , y esta imagen puede ser cualquier elemento de  $\mathbb{Z}_p$ .  $\square$

<sup>2</sup> En la literatura también es común escribir este carácter como  $\langle \cdot \rangle$  en lugar de  $\kappa_0$ , es decir  $\kappa_0(x) = \langle x \rangle$ .

## Ejercicios

**Ejercicio 1.8:** Demuestre que

$$\omega(f) = \lim_{j \rightarrow \infty} z^{p^j}$$

para cada  $z \in \mathbb{Z}_p^\times$  que escribimos como  $z = (f, u) \in \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$  usando el isomorfismo del lema 1.43.

**Ejercicio 1.9:** Demuestre que cada carácter  $\mathbb{F}_p^\times \rightarrow \overline{\mathbb{Q}_p}^\times$  es una potencia del carácter de Teichmüller  $\omega$ .

# Capítulo 2

## El álgebra de Iwasawa

En el caso en que  $\Gamma$  es un pro- $p$  grupo cíclico isomorfo a  $\mathbb{Z}_p$ , el *álgebra de Iwasawa*  $\Lambda = \mathbb{Z}_p[[\Gamma]]$  con coeficientes en  $\mathbb{Z}_p$  se presenta como una trinidad matemática: Por definición es una álgebra de grupos profinita, por lo tanto tiene una estructura algebraica y topológica; una vez escogido un generador  $\gamma \in \Gamma$  esta se puede identificar al álgebra de series formales sobre  $\mathbb{Z}_p$ ; además los elementos de  $\Lambda$  pueden ser vistos como medidas en  $\Gamma$  con valores en  $\mathbb{Z}_p$ .

Esta trinidad explica su enorme importancia: Es un objeto versátil y por eso aparece en varios contextos. Primero, en su talle de álgebra de grupos profinita, muchos objetos son naturalmente módulos sobre  $\Lambda$  – en cuanto tenemos acción razonable de  $\Gamma$  en un grupo pro- $p$  abeliano, ya tenemos un  $\Lambda$ -módulo (véase la proposición 1.8). En las aplicaciones,  $\Gamma$  normalmente es un grupo de Galois, que actúa naturalmente en una multitud de objetos. Si entonces identificamos  $\Lambda$  con el anillo de series de potencia formales sobre  $\mathbb{Z}_p$ , la manejabilidad de este anillo permite desarrollar una teoría útil de estructura de sus módulos que permite definir invariantes importantes (sección 2.1 y capítulo 3). Finalmente, el punto de vista de medidas facilita una conexión de dichos módulos a objetos de origen analítico, como funciones  $L$   $p$ -ádicas (sección 2.2 y capítulo 5).

### 2.1. El anillo de series de potencias

En esta sección empezaremos estudiando las propiedades de las series formales  $\mathcal{O}[[T]]$  en una variable sobre un anillo local de valuación discreta  $\mathcal{O}$ . El ejemplo más importante para nosotros es el en que  $\mathcal{O}$  es el anillo de enteros de una extensión finita de  $\mathbb{Q}_p$ , por ejemplo  $\mathcal{O} = \mathbb{Z}_p$ . No obstante, algunos de los resultados de esta sección pueden ser generalizados, por ejemplo al caso en que  $\mathcal{O}$  es un anillo local conmutativo noetheriano (ver [NSW08, Cap. V. §3]). En particular demostramos que si  $\Gamma$  es un pro- $p$  grupo libre de rango 1 y  $\mathcal{O}$  es un anillo de valuación discreta, entonces  $\mathcal{O}[[T]]$  es isomorfo de manera no canónica al anillo de grupo profinito  $\mathcal{O}[[\Gamma]]$ .

Sea  $\mathcal{O}$  un anillo local de valuación discreta, completo por la topología definida por las potencias de su ideal máximo  $\pi\mathcal{O}$  de cuerpo residual  $k = \mathcal{O}/\pi\mathcal{O}$  finito, de manera que  $\mathcal{O}$  es compacto. Denotaremos  $\Lambda$  el álgebra

$$\Lambda = \mathcal{O}[[T]]$$

de las series formales en una variable con coeficientes en  $\mathcal{O}$ .

**Proposición 2.1:**  $\Lambda$  es un anillo local de ideal máximo  $\mathfrak{M} = \pi\Lambda + T\Lambda$ .

*Demostración:* Un elemento  $f = \sum_{i=0}^{\infty} f_i T^i \in \Lambda$  diferente de cero es invertible sí y sólo si su coeficiente constante  $\lambda_0$  es invertible en  $\mathbb{Z}_p$ . De hecho si  $f \neq 0$  es invertible entonces existe  $f^{-1}$  tal que  $ff^{-1} = 1$ , en particular  $f_0 f_0^{-1} = 1 \in \mathbb{Z}_p$ . Del otro lado si  $f_0$  es invertible entonces podemos escribir  $f = f_0(1 + gT)$  para un  $g \in \Lambda$ . Entonces el elemento  $f^{-1} = f_0^{-1} \sum_{i=0}^{\infty} g^i T^i$  es un inverso de  $f$ .

Entonces tenemos  $\Lambda^\times = \Lambda \setminus \mathfrak{M}$ . □

**Observación:** El ideal  $\mathfrak{M}$  no es principal como era el caso del anillo  $\mathcal{O}$ .

Equipamos  $\Lambda$  con la topología  $\mathfrak{M}$ -ádica, tomando los  $(\mathfrak{M}^n)_{n \in \mathbb{N}_{\geq 1}}$  como sistema fundamental de vecindades alrededor del  $0$ . Esto hace de  $\Lambda$  un anillo local completo, con campo de residuos finito  $k = \Lambda/\mathfrak{M} = \mathcal{O}/\pi\mathcal{O}$ . De hecho  $\Lambda$  es un espacio topológico compacto, separable y noetheriano.

**Definición 2.2:** (a) Sea  $f = \sum_{n=0}^{\infty} a_n T^n \in \Lambda \setminus \pi\Lambda$  y  $\bar{f} \in k[[T]]$  su reducción. El *grado de Weierstraß* de  $f$  es la valuación en  $T$  de  $\bar{f}$ , es decir el mínimo  $n \in \mathbb{N}_{\geq 0}$  tal que  $a_n \notin \pi\mathcal{O}$ .

(b) Sea  $f \in \mathcal{O}[T]$ . Entonces  $f$  se llama *distinguido* si es mónico y su grado es igual a su grado de Weierstraß, es decir el coeficiente superior es 1 y todos los demás están en  $\pi\mathcal{O}$ . Algunos textos llaman estos *polinomio de Weierstraß*.

**Lema 2.3 (Lema de división):** Sea  $f$  un elemento de  $\Lambda \setminus \pi\Lambda$  y  $\nu$  su grado de Weierstraß. Entonces todo elemento de  $g \in \Lambda$  se escribe de manera única como

$$g = f\lambda + r, \quad \text{con } \lambda \in \Lambda \text{ y } r \in \mathcal{O}_{\nu-1}[T],$$

donde  $\mathcal{O}_{\nu-1}[T]$  es el  $\mathcal{O}$ -módulo de los polinomios de grado a lo más  $\nu - 1$ . Equivalentemente

$$\Lambda = f\Lambda \oplus \mathcal{O}_{\nu-1}[T].$$

*Demostración:* Sea  $\nu$  el grado de Weierstraß de  $f$ , entonces escribimos

$$f = T^\nu \mu + \pi R, \quad \text{con } R \in \mathcal{O}_{\nu-1}[T],$$

para un  $\mu \in \Lambda^\times$ .

*Existencia:* Sea  $g \in \Lambda$ , entonces podemos escribir

$$\begin{aligned} g &= \sum_{i=0}^{\nu-1} a_i T^i + T^\nu \sum_{i=\nu}^{\infty} a_i T^{i-\nu} \\ &= T^\nu g' + r_0 \quad \text{con } g' \in \Lambda \text{ y } r_0 \in \mathcal{O}_{\nu-1}[T]. \end{aligned}$$

Definimos  $a_0 = \mu^{-1}g'$ , entonces

$$\begin{aligned} g - a_0 f &= T^\nu g' + r_0 - \mu^{-1}g'(T^\nu \mu + \pi R) \\ &= T^\nu g' + r_0 - g' T^\nu - \pi R \mu^{-1}g' \\ &= r_0 - \underbrace{\pi R \mu^{-1}g'}_{\in \Lambda} \\ &= r_0 - \pi g_1. \end{aligned}$$

Sea  $g_1 = T^\nu g'_1 + r_1$  con  $g'_1 \in \Lambda$  y  $r_1 \in \mathcal{O}_{\nu-1}[T]$ , y definimos  $a_1 = \mu^{-1}g'_1$ . Tenemos

$$\begin{aligned} g_1 - a_1 f &= T^\nu g'_1 + r_1 - \mu^{-1}g'_1(T^\nu \mu + \pi R) \\ &= T^\nu g'_1 + r_1 - g'_1 T^\nu - \pi R \mu^{-1}g'_1 \\ &= r_1 - \pi R \mu^{-1}g'_1 \\ &= r_1 - \pi g_2; \end{aligned}$$

entonces para  $n \geq 2$  (siguiendo el mismo razonamiento) sea  $g_n = T^\nu g'_n + r_n$  con  $g'_n \in \Lambda$ ,  $r_n \in \mathcal{O}_{\nu-1}[T]$  y definimos  $a_n = \mu^{-1}g'_n$ . Con  $g = g_0$ , tenemos

$$g_n - a_n f = r_n - \pi g_{n+1},$$

para todo  $n \geq 0$ , por lo tanto

$$g - \left( \sum_{i=0}^n (-1)^i a_i \pi^i \right) f = \sum_{i=0}^n (-1)^i r_i \pi^i + (-1)^{n+1} \pi^{n+1} g_{n+1} \quad \text{para } n \geq 0.$$

Tomando límites tenemos que  $(-1)^{n+1} \pi^{n+1} g_{n+1} \rightarrow 0$  por lo tanto  $g - \lambda f = r$  con  $\lambda \in \Lambda$  y  $r \in \mathcal{O}_{\nu-1}[T]$ .

*Unicidad:* Sea  $\lambda f = r \in f\Lambda \cap \mathcal{O}_{\nu-1}[T]$ . Módulo  $\pi$  tenemos  $\bar{\lambda}\bar{f} = \bar{\lambda}\bar{\mu}T^\nu = \bar{r}$ , entonces  $\bar{\lambda}\bar{f} = \bar{r} = 0$ , es decir  $\pi \mid \lambda$  y  $\pi \mid r$ , entonces

$$\frac{\lambda}{\pi} f = \frac{r}{\pi},$$

volviendo a iterar el proceso vemos que  $\pi^n \mid \lambda$  y  $\pi^n \mid r$  para todo  $n \geq 0$ , por lo tanto  $\lambda = r = 0$ .  $\square$

**Teorema 2.4 (Teorema de preparación de Weierstraß):** *Todo elemento  $f \in \Lambda \setminus \pi\Lambda$  se escribe de manera única como*

$$f = \mu(T^\nu + \pi Q),$$

con  $Q \in \mathcal{O}_{\nu-1}[T]$ . Es decir, como producto de un invertible  $\mu \in \Lambda^\times$  y de un polinomio distinguido  $P = T^\nu + \pi Q$ .

*Demostración:* Sea  $f = T^\nu \mu + \pi R$  como en el lema de división. Aplicamos el lema de división a  $T^\nu$ , es decir

$$T^\nu = \lambda f + r, \quad \text{con } r \in \mathcal{O}_{\nu-1}[T].$$

Entonces módulo  $\pi$  tenemos

$$T^\nu = \bar{\lambda}\bar{\mu}T^\nu + \bar{r},$$

por lo tanto  $\bar{r} = 0$  y  $\bar{\lambda}\bar{\mu} = 1$ . En particular  $r = \pi Q$  para algún  $Q \in \mathcal{O}_{\nu-1}[T]$  y  $\lambda$  es invertible. Concluimos que  $f = \lambda^{-1}(T^\nu - r)$ .  $\square$

**Corolario 2.5:** *Los polinomios distinguidos e irreducibles  $P \in \mathcal{O}[T]$  son también irreducibles en  $\Lambda$ .*

*Demostración:* Sea  $P \in \mathcal{O}[T]$  distinguido e irreducible. Supongamos que  $P = f_1 f_2$  con  $f_i \in \Lambda$ , luego por el Teorema de preparación de Weierstraß tenemos  $P = \mu_1 P_1 \mu_2 P_2$  con  $\mu_i \in \Lambda^\times$  y  $P_i$  polinomios distinguidos en  $\mathcal{O}[T]$ , como la manera de expresar  $P$  es única esto implica que  $\mu_1 \mu_2 = 1$  y  $P = P_1 P_2$ .  $\square$

**Observación:** Los polinomios de Eisenstein son irreducibles en  $\Lambda$ .

**Corolario 2.6:** *El álgebra  $\Lambda$  es un dominio de factorización única cuyos elementos irreducibles son*

- El uniformizante  $\pi$  de  $\mathcal{O}$ .
- Los polinomios distinguidos e irreducibles en  $\mathcal{O}[T]$ .

*Demostración:* Sea  $f \in \Lambda$ , sea  $\pi^k$  la mayor potencia de  $\pi$  que divide  $f$ . Entonces  $f = \pi^k g$  donde  $g \in \Lambda \setminus \pi\Lambda$ , el resultado sigue aplicando a  $g$  el teorema de preparación de Weierstraß.  $\square$

**Lema 2.7:** Sean  $f$  y  $g$  elementos no nulos en  $\Lambda$  tal que  $d$  es su máximo común divisor. Entonces el ideal  $f\Lambda + g\Lambda$  está contenido en el ideal principal  $d\Lambda$  con índice finito.

*Demostración:* La primera aseveración es directa. Para la segunda afirmación podemos suponer que  $f$  y  $g$  son coprimos, además por el Teorema de preparación de Weierstraß (teorema 2.4) podemos suponer que  $f$  y  $g$  son polinomios y al menos uno de ellos es distinguido, digamos  $f = T^\nu + \pi Q$  para algún  $Q \in \mathcal{O}_{\nu-1}[T]$ .

Consideremos el resultante  $\text{Res}(f, g)$  de  $f$  y  $g$ , es no nulo pues  $f$  y  $g$  son coprimos, además siendo un elemento de  $\mathcal{O}$  lo podemos escribir  $\text{Res}(f, g) = \mu\pi^\alpha$  con  $\mu \in \mathcal{O}^\times$  y  $\alpha \in \mathbb{N}_{\geq 0}$ . El resultante  $\text{Res}(f, g)$  está en el ideal generado por  $f$  y  $g$ , por lo tanto, también  $\pi^\alpha \in f\Lambda + g\Lambda$  porque  $\mu$  es invertible. Entonces tenemos la siguiente congruencia

$$T^{\nu\alpha} \equiv \pi^\alpha Q^\alpha \equiv 0 \pmod{(f\Lambda + g\Lambda)}.$$

Por lo que  $f\Lambda + g\Lambda$  contiene  $T^{\nu\alpha}$  y  $\pi^\alpha$ , lo cual implica  $(\Lambda : f\Lambda + g\Lambda) \leq (\Lambda : T^{\nu\alpha}\Lambda + \pi^\alpha\Lambda)$ , siendo la expresión del lado derecho una potencia de  $p$  divisible por  $\nu\alpha$ .  $\square$

**Corolario 2.8:** Sean  $f, g \in \Lambda \setminus \{0\}$  coprimos (es decir, su máximo común divisor es 1). Entonces el ideal  $f\Lambda + g\Lambda$  tiene índice finito en  $\Lambda$ .

**Proposición 2.9:** Todo ideal (no nulo)  $\mathfrak{A}$  del álgebra  $\Lambda$  está contenido en un ideal principal mínimo  $a\Lambda$ . Entonces decimos que  $a$  es un pseudo-generator del ideal  $\mathfrak{A}$  y tenemos  $(a\Lambda : \mathfrak{A})$  finito.

*Demostración:* Sabemos que  $\Lambda$  es un anillo noetheriano, entonces un módulo noetheriano sobre sí mismo. Por lo tanto sea  $\mathfrak{A} = \sum_{i=1}^m f_i\Lambda$ . Denotemos  $D$  el máximo común divisor de los  $f_i$ . Tenemos

$$\mathfrak{A} \subset a\Lambda \quad \Leftrightarrow \quad a \mid f_i, \quad \forall i = 1, \dots, m$$

por lo que el mínimo ideal principal que contiene a  $\mathfrak{A}$  es  $D\Lambda$ . Por último,  $(D\Lambda : \mathfrak{A})$  es finito por el lema 2.7.  $\square$

**Observación:** Si  $\mathfrak{A}$  no es principal, entonces tenemos  $a \notin \mathfrak{A}$ . Por ejemplo  $\mathfrak{A} = \mathfrak{M}$ , entonces  $\mathfrak{A} \subset (1) = \Lambda$  porque  $\mathfrak{M}$  es máximo.

Sea  $p = \text{car}(\mathcal{O}/\pi\mathcal{O})$  y supongamos que  $\Gamma$  es un  $p$ -grupo profinito libre de rango 1, es decir existe un isomorfismo no canónico de  $\Gamma$  al grupo aditivo de  $\mathbb{Z}_p$ .

**Definición 2.10:** Para  $r \geq 0$  consideremos los polinomios distinguidos

$$\omega_r = (T + 1)^{p^r} - 1. \quad (2.1)$$

Definimos el  $r$ -ésimo polinomio ciclotómico como

$$\Phi_r = \frac{\omega_r}{\omega_{r-1}} \quad (2.2)$$

para  $r \geq 1$  y  $\Phi_0 = \omega_0$ .

**Teorema 2.11:** Supongamos que  $\gamma$  es un generador topológico de  $\Gamma$ . Entonces la aplicación

$$\Lambda = \mathcal{O}[[T]] \xrightarrow{\sim} \mathcal{O}[[\Gamma]], \quad T \mapsto \gamma - 1$$

es un isomorfismo de  $\mathcal{O}$ -álgebras topológicas. En particular,  $\Lambda$  es una  $\mathcal{O}$ -álgebra profinita.

*Demostración:* Para  $r \geq 0$  usaremos los polinomios  $\omega_r$  y denotamos  $\Gamma_r$  el único subgrupo de  $\Gamma$  tal que  $\Gamma/\Gamma_r \simeq \mathbb{Z}_p/p^r\mathbb{Z}_p$ . Por el lema de división (lema 2.3) tenemos

$$\Lambda/\omega_r\Lambda \simeq \mathcal{O}[T]/\omega_r\mathcal{O}[T] \quad \text{para todo } r \geq 0,$$

además tenemos los isomorfismos de  $\mathcal{O}$ -álgebras para todo  $r \geq 0$

$$\begin{aligned} \mathcal{O}[T]/\omega_r\mathcal{O}[T] &\xrightarrow{\varphi_r} \mathcal{O}[\Gamma/\Gamma_r] \\ T \text{ mód } \omega_r &\mapsto \gamma - 1 \text{ mód } \Gamma_r. \end{aligned}$$

Los inversos de estos morfismos están dados por

$$\gamma \text{ mód } \Gamma_r \mapsto T + 1 \text{ mód } \omega_r.$$

Como en la definición 2.10, tenemos  $\omega_{r+1} = \omega_r\Phi_{r+1}$  por lo tanto las proyecciones  $\Lambda/\omega_{r+1} \rightarrow \Lambda/\omega_r$  son compatibles con los isomorfismos  $\varphi_r$ , es decir el diagrama

$$\begin{array}{ccc} \Lambda/\omega_{r+1} & \xrightarrow{\varphi_{r+1}} & \mathcal{O}[\Gamma/\Gamma_{r+1}] \\ \downarrow & & \downarrow \\ \Lambda/\omega_r & \xrightarrow{\varphi_r} & \mathcal{O}[\Gamma/\Gamma_r] \end{array}$$

es conmutativo y tomando límites inversos en ambos lados tenemos

$$\varprojlim_r \Lambda/\omega_r \xrightarrow{\simeq} \varprojlim_r \mathcal{O}[\Gamma/\Gamma_r] = \mathcal{O}[[\Gamma]].$$

Falta demostrar entonces que el límite del lado izquierdo es isomorfo al álgebra de series formales  $\Lambda$ .

Sea  $\psi: \Lambda \rightarrow \varprojlim_r \Lambda/\omega_r$ , veamos que

$$\begin{aligned} \ker \psi &= \{f \in \Lambda \mid f \in \omega_r\Lambda \ \forall r \geq 0\} \\ &\subseteq \bigcap_{r \geq 0} \omega_r\Lambda \\ &= 0, \end{aligned}$$

la última igualdad se deduce del hecho que

$$\mathfrak{M}^{p^r} = (\pi, T)^{p^r} \supset (p, T)^{p^r} \supset \omega_r\Lambda, \quad (2.3)$$

y los  $(\mathfrak{M}^r)_{r \in \mathbb{N}_{\geq 1}}$  forman una base de vecindarios alrededor de 0 de  $\Lambda$  con la topología  $\mathfrak{M}$ -ádica.

Finalmente, sea  $f = (f_r)_{r \geq 0}$  un elemento de  $\varprojlim_r \Lambda/\omega_r$ , entonces

$$f_r \equiv f_t \text{ mód } \omega_{r+1}$$

para todo  $0 \leq t \leq r$ . Es decir  $f_r - f_t \in \omega_r\Lambda$ , en particular  $f_r - f_t \in \mathfrak{M}^{r+1}$  por (2.3) para todo  $r \geq t \geq 0$ . Por lo tanto  $f \in \Lambda$  ya que  $\Lambda$  es compacto por la topología  $\mathfrak{M}$ -ádica.  $\square$

Para  $G$  un grupo profinito y  $R$  un anillo profinito llamamos *álgebra de Iwasawa* de  $G$  con coeficientes en  $R$  al anillo de grupos profinito

$$\Lambda(G) := R[[G]] = \varprojlim_{U \trianglelefteq G} R[G/U]$$

(aquí normalmente  $R = \mathcal{O}$  es el anillo de enteros de una extensión finita de  $\mathbb{Q}_p$ , por ejemplo  $R = \mathbb{Z}_p$ , y debería ser claro del contexto).

En el caso en que  $\Gamma$  es un  $p$ -grupo profinito libre de rango 1 y  $\mathcal{O}$  un anillo de valuación discreta, el teorema 2.11 nos dice que el álgebra de Iwasawa  $\Lambda(\Gamma)$  de  $\Gamma$  es isomorfa a las series formales  $\mathcal{O}[[T]]$  en una variable con coeficientes en  $R$ . En este caso particular, denotamos simplemente  $\Lambda := \Lambda(\Gamma)$  si no hay confusión.

## Ejercicios

**Ejercicio 2.1:** Demuestre que los polinomios  $\Phi_r \in \Lambda$  de la definición 2.10 son elementos distinguidos e irreducibles en  $\Lambda$ .

**Ejercicio 2.2:** Cada serie de potencia  $f \in \mathcal{O}[[T]]$  define una función

$$\pi\mathcal{O} \rightarrow \mathcal{O}, \quad x \mapsto f(x)$$

(verifique que esto es bien definido). Asumamos que esta función tiene una infinitud de ceros. Usa el Teorema de preparación de Weierstraß para demostrar que entonces  $f = 0$ .

**Ejercicio 2.3:** Demuestre las inclusiones (2.3) del teorema 2.11.

**Ejercicio 2.4:** Sea  $G$  un  $p$ -grupo abeliano profinito libre de rango  $n$  y  $\mathcal{O}$  un anillo de valuación discreta, demuestre que el álgebra de Iwasawa  $\Lambda(G)$  es isomorfa al álgebra de series formales  $\mathcal{O}[[T_1, \dots, T_m]]$  en  $m$  variables con coeficientes en  $\mathcal{O}$ .

## 2.2. Medidas

En esta sección explicamos cómo los elementos del álgebra de Iwasawa  $\Lambda(G)$  pueden ser vistos como medidas en  $G$ , para cualquier grupo profinito  $G$ . Luego lo estudiamos en más detalle en el caso especial  $G = \Gamma$  con  $\Gamma \simeq \mathbb{Z}_p$ . Este punto de vista no será tan importante en este texto, pero es muy común en la literatura y no debería faltar aquí.

Fijamos un anillo  $\mathcal{O}$  como anteriormente, que sea un anillo local de valuación discreta, completo por la topología definida por las potencias de su ideal máximo. El ejemplo más importante es en el que  $\mathcal{O}$  es el anillo de enteros de una extensión finita de  $\mathbb{Q}_p$ . Esta teoría se puede desarrollar en más generalidad, pero así será suficiente para nosotros.

**Definición 2.12:** Sea  $G$  un grupo profinito. Escribimos  $C(G, \mathcal{O})$  como el  $\mathcal{O}$ -módulo de funciones continuas  $G \rightarrow \mathcal{O}$  y  $C^\infty(G, \mathcal{O})$  como el submódulo de funciones localmente constantes. Definimos una norma en  $C(G, \mathcal{O})$  como

$$|f| = \sup_{g \in G} |f(g)| \quad (f \in C(G, \mathcal{O})).$$

El submódulo  $C^\infty(G, \mathcal{O})$  puede ser caracterizado de diferentes maneras según el ejercicio 2.5.

**Proposición 2.13:**  $C(G, \mathcal{O})$  es completo con respecto a la norma introducida en la definición 2.12 y  $C^\infty(G, \mathcal{O})$  es denso.

*Demostración:* Demostramos sólo la densidad y dejamos la completitud como ejercicio, porque los argumentos son muy similares.

Para ver la densidad de  $C^\infty(G, \mathcal{O})$  sean dados  $\varepsilon > 0$  y  $f \in C(G, \mathcal{O})$ . Para cada  $w$  en la imagen de  $f$  sea  $B(w, \varepsilon) \subseteq \mathcal{O}$  la bola de radio  $\varepsilon$  alrededor de  $w$ . Porque la topología en  $\mathcal{O}$  está definida por una ultramétrica,  $B(w, \varepsilon)$  es abierta y cerrada. La preimagen  $U_w = f^{-1}(B(w, \varepsilon)) \subseteq G$  entonces también es abierta y cerrada. Los  $U_w$  (para todos los  $w$ ) obviamente cubren  $G$ , y porque  $G$  es compacto podemos elegir una cantidad finita  $w_1, \dots, w_n$  tal que los  $U_{w_i}$  para  $i = 1, \dots, n$  cubren  $G$ . Pongamos para cada tal  $i$

$$A_i = U_{w_i} \setminus \bigcup_{j=i+1}^n U_{w_j}, \quad i = 1, \dots, n$$

(que todavía es abierto y cerrado) y definimos una función

$$f' = \sum_{i=1}^n w_i \mathbb{1}_{A_i}$$

(donde  $\mathbb{1}$  denota la función indicador). Entonces

$$|f - f'| = \sup_{x \in X} |f(x) - f_0(x)| = \max_{i=1, \dots, n} \sup_{x \in A_i} |f(x) - w_i| \leq \varepsilon$$

y la densidad de  $C^\infty(G, \mathcal{O})$  resulta.  $\square$

**Definición 2.14:** Definimos  $D(G, \mathcal{O}) = \text{Hom}_{\mathcal{O}}(C(G, \mathcal{O}), \mathcal{O})$ , donde « $\text{Hom}_{\mathcal{O}}$ » son homomorfismos *continuos* de  $\mathcal{O}$ -módulos. Los elementos de  $D(G, \mathcal{O})$  se llaman *medidas* en  $G$  con valores en  $\mathcal{O}$ .

Si  $f \in C(G, \mathcal{O})$  y  $\mu \in D(G, \mathcal{O})$  a veces escribimos

$$\int_G f d\mu$$

en lugar de  $\mu(f)$ .

Una consecuencia importante de la proposición 2.13 es que de hecho  $D(G, \mathcal{O}) = \text{Hom}_{\mathcal{O}}(C^\infty(G, \mathcal{O}), \mathcal{O})$  (ejercicio 2.6).

**Proposición 2.15:** (a) *Existe un isomorfismo canónico de  $\mathcal{O}$ -módulos topológicos*

$$\Lambda(G) \simeq D(G, \mathcal{O}).$$

(b) *Sea  $\chi: G \rightarrow \mathcal{O}^\times$  un carácter y  $\mu \in D(G, \mathcal{O})$ , y escribimos  $\mu$  también para la imagen de  $\mu$  en  $\Lambda(G)$  bajo el isomorfismo de (a). Entonces la imagen de  $\mu$  bajo el morfismo canónico  $\Lambda(G) \rightarrow \mathcal{O}$  inducido por  $\chi$  es*

$$\int_G \chi d\mu.$$

(c) *El isomorfismo de (a) se convierte un isomorfismo de  $\mathcal{O}$ -álgebras si definimos la multiplicación en  $D(G, \mathcal{O})$  como la convolución*

$$\int_G f d(\mu_1 * \mu_2) = \int_G \left( \int_G f(gh) d\mu_1(g) \right) d\mu_2(h) \text{ para } f \in C(G, R), \mu_1, \mu_2 \in D(G, R).$$

*Demostración:* De los ejercicios 2.5 y 2.6 se ve fácilmente que

$$D(G, \mathcal{O}) = \varinjlim_{U \trianglelefteq G} D(G/U, \mathcal{O}).$$

Pero como  $G/U$  es un grupo finito discreto,  $C(G/U, \mathcal{O})$  es un  $\mathcal{O}$ -módulo libre de rango finito con una base canónica dada por los elementos de  $G/U$ , y pues lo mismo es cierto para su módulo dual. Esto muestra que canónicamente

$$D(G/U, \mathcal{O}) \simeq C(G/U, \mathcal{O}) \simeq \mathcal{O}[G/U]$$

como  $\mathcal{O}$ -módulos. La afirmación (a) resulta pues de la definición de  $\Lambda(G)$ .

Por la construcción del isomorfismo que acabamos de explicar es obvio que un elemento  $g \in G$  corresponde a la medida de Dirac  $\delta_g$  que envía  $f \mapsto f(g)$  para  $f \in C(G, \mathcal{O})$ . Por eso el

morfismo  $D(G, \mathcal{O}) \rightarrow \mathcal{O}$ ,  $\mu \mapsto \mu(\chi)$  coincide con  $\chi$  si lo restringimos a  $G \subseteq \Lambda(G) \simeq D(G, \mathcal{O})$ . Esto demuestra que la composición  $\Lambda(G) \rightarrow D(G, \mathcal{O}) \rightarrow \mathcal{O}$  debe ser el morfismo dado por la propiedad universal porque ese es único. De ahí que (b) resulta.

Si  $g_1, g_2 \in G$  y  $\delta_{g_1}, \delta_{g_2}$  son las medidas de Dirac correspondientes, entonces de la definición de la convolución resulta fácilmente que  $\delta_{g_1} * \delta_{g_2} = \delta_{g_1 g_2}$ . Por lo tanto

$$G \rightarrow D(G, \mathcal{O})^\times, \quad g \mapsto \delta_g$$

es un morfismo de grupos topológicos que induce un morfismo de  $\mathcal{O}$ -álgebras  $\Lambda(G) \rightarrow D(G, \mathcal{O})$ . Pero de la construcción es claro que este coincide con el isomorfismo de (a), tenemos pues (c).  $\square$

A partir de ahora identificamos  $\Lambda(G)$  con las medidas  $D(G, \mathcal{O})$  y pues vemos elementos de  $\Lambda(G)$  como funciones en  $C(G, \mathcal{O})$ .

**Definición 2.16:** Escribimos  $\mathcal{Q}(G)$  como el anillo de cocientes de  $\Lambda(G)$ , es decir la localización en que invertimos todos los elementos que no sean divisores de cero. Además sea  $I(G) \subset \Lambda(G)$  el *ideal de aumentación*, es decir el núcleo del morfismo  $\Lambda(G) \rightarrow \mathcal{O}$  que envía todos los elementos de  $G$  a 1.

Llamamos un elemento de  $\mathcal{Q}(G)$  una *pseudo-medida* si  $(g-1)\mu \in \Lambda(G)$  para cada  $g \in G$ .

Notemos que para cada pseudo-medida  $\mu$ ,  $I(G)\mu$  es un ideal en  $\Lambda(G)$ .

El morfismo  $\chi: \Lambda(G) \rightarrow \mathcal{O}$  inducido por un carácter  $\chi: G \rightarrow \mathcal{O}^\times$  se extiende a un elemento  $\frac{a}{b} \in \mathcal{Q}(G)$  si y sólo si  $b \notin \ker \chi$ . Si  $\mu = \frac{a}{b}$  es una pseudo-medida entonces  $b \notin \ker \chi$  siempre es cierto si  $\chi$  no es trivial: porque  $(g-1)\mu \in \Lambda(G)$  para cada  $g \in G$  significa que para cada  $g$  existe un  $c_g \in \Lambda(G)$  tal que  $g-1 = c_g b$ , y si escogemos un  $g \in G$  con  $\chi(g) \neq 1$  entonces  $\chi(b)\chi(c_g) = \chi(g-1) = \chi(g) - 1 \neq 0$  y pues  $\chi(b) \neq 0$ . Esto demuestra que la siguiente definición tiene sentido.

**Definición 2.17:** Si  $\mu \in \mathcal{Q}(G)$  es una pseudo-medida y  $\chi: G \rightarrow \mathcal{O}^\times$  es un carácter no trivial, entonces ponemos

$$\int_G \chi d\mu := \frac{1}{\chi(g) - 1} \int_G \chi d((g-1)\mu)$$

para  $g \in G$  tal que  $\chi(g) \neq 1$ .

Es claro que la expresión que acabamos de definir no depende de  $g$ .

A partir de entonces reemplazamos  $G$  por el grupo  $\mathbb{Z}_p$ . Si  $x \in \mathbb{Z}_p$  entonces escribimos  $[x]$  para el elemento del grupo  $\mathbb{Z}_p \subseteq \Lambda(\mathbb{Z}_p)^\times$  para distinguirlo del elemento  $x \in \mathbb{Z}_p \subseteq \Lambda(\mathbb{Z}_p)$  en el anillo de coeficientes. Tenemos entonces el generador topológico canónico [1].

En este caso describimos con más detalle los tres puntos de vista del álgebra de Iwasawa. Tenemos un diagrama conmutativo de isomorfismos continuos

$$\begin{array}{ccc} \Lambda(\mathbb{Z}_p) & \xleftrightarrow{\text{de la proposición 2.15}} & D(\mathbb{Z}_p, \mathcal{O}) \\ & \swarrow \text{del teorema 2.11} & \nearrow \Upsilon \\ & \mathcal{O}[[T]] & \nearrow \mathcal{M} \end{array} \quad (2.4)$$

Al rato vamos a describir más explícitamente los mapoes  $\mathcal{M}$  y  $\Upsilon$ . Primero deduzcamos el siguiente resultado.

**Teorema 2.18 (Mahler):** Cada función  $f \in C(\mathbb{Z}_p, \mathcal{O})$  se escribe de manera única como

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n} \quad (x \in \mathbb{Z}_p) \quad (2.5)$$

con coeficientes  $a_n \in \mathcal{O}$  tal que  $\lim_{n \rightarrow \infty} a_n = 0$ . Aquí  $\binom{x}{0} = 1$  y

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \quad (n \in \mathbb{N}_{\geq 0}, x \in \mathbb{Z}_p). \quad (2.6)$$

Por otro lado, cada serie de la forma (2.5) converge y define un elemento de  $C(\mathbb{Z}_p, \mathcal{O})$ .

*Demostración:* Es fácil ver que cada serie de la forma (2.5) converge y define un elemento de  $C(\mathbb{Z}_p, \mathcal{O})$ ; omitimos los detalles aquí. Para ver la unicidad utilizamos el mapeo

$$\Delta: C(\mathbb{Z}_p, \mathcal{O}) \rightarrow C(\mathbb{Z}_p, \mathcal{O}), \quad \Delta f(x) = f(x+1) - f(x) \quad (x \in \mathbb{Z}_p).$$

Porque para  $n \in \mathbb{N}_{\geq 0}$  y  $x \in \mathbb{Z}_p$  tenemos (usando el ejercicio 2.9)

$$\Delta \binom{x}{n} = \binom{x+1}{n} - \binom{x}{n} = \binom{x}{n-1}$$

resulta que si  $f \in C(\mathbb{Z}_p, \mathcal{O})$  es de la forma (2.5) entonces  $a_n = \Delta^n f(0)$  para cada  $n \in \mathbb{N}_{\geq 0}$ . Esto demuestra la unicidad de los coeficientes.

Para demostrar que cada  $f \in C(\mathbb{Z}_p, \mathcal{O})$  se escribe en esta forma, fijemos  $x \in \mathbb{Z}_p$ . El elemento  $[x] \in \Lambda(G)$  corresponde a la medida de Dirac  $\delta_x \in D(\mathbb{Z}_p, \mathcal{O})$ , y también a la serie de potencias

$$(1+T)^x = \sum_{n=0}^{\infty} \binom{x}{n} T^n \in \mathcal{O}[[T]].$$

Usamos la medida  $\Upsilon(T^n) \in D(\mathbb{Z}_p, \mathcal{O})$  que corresponde a  $T^n$  para cada  $n$ . Porque todos los isomorfismos en (2.4) son continuos, obtenemos

$$f(x) = \delta_x(f) = \sum_{n=0}^{\infty} \binom{x}{n} \Upsilon(T^n)(f)$$

y obtenemos la afirmación poniendo  $a_n = \Upsilon(T^n)(f)$ . □

**Corolario 2.19:** *Los mapeos  $\mathcal{M}$  y  $\Upsilon$  en el diagrama (2.4) son dados por*

$$\mathcal{M}(\mu) = \sum_{n=0}^{\infty} c_n(\mu) T^n \quad \text{con } c_n(\mu) = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) = \mu \left( \binom{\cdot}{n} \right) \quad \text{para } \mu \in D(\mathbb{Z}_p, \mathcal{O}), n \in \mathbb{N}_{\geq 0},$$

$$\Upsilon(g)(f) = \sum_{n=0}^{\infty} a_n b_n \quad \text{para } f = \sum_{n=0}^{\infty} a_n \binom{\cdot}{n} \in C(\mathbb{Z}_p, \mathcal{O}), g = \sum_{n=0}^{\infty} b_n T^n \in \mathcal{O}[[T]],$$

donde usamos el teorema 2.18 de Mahler para escribir  $f$  en esta forma.

*Demostración:* La continuidad de  $\Upsilon$  implica que

$$\Upsilon(g)(f) = \sum_{n=0}^{\infty} b_n \Upsilon(T^n)(f)$$

para  $g = \sum_{n=0}^{\infty} b_n T^n \in \mathcal{O}[[T]]$  y  $\Upsilon(T^n)(f) = a_n$  según la demostración del teorema 2.18. Esto demuestra la fórmula para  $\Upsilon$ .

La afirmación para  $\mathcal{M}$  resulta si verificamos que la fórmula de arriba define un mapeo inverso a  $\Upsilon$ . Esto es un cálculo corto que dejamos como ejercicio. □

**Ejercicios**

**Ejercicio 2.5:** Demuestre que para una función  $f \in C(G, \mathcal{O})$  los siguientes enunciados son equivalentes:

- (a)  $f \in C^\infty(G, \mathcal{O})$ ;
- (b) existe un subgrupo abierto  $H \subseteq G$  tal que  $f$  se factoriza como una función  $G/H \rightarrow \mathcal{O}$ ;
- (c) la imagen de  $f$  es finita.

**Ejercicio 2.6:** (a) Demuestre que  $C(G, \mathcal{O})$  es completo con respecto a la norma introducida en la definición 2.12 (la primera afirmación de la proposición 2.13).

- (b) Deduzca de la proposición 2.13 que  $D(G, \mathcal{O}) = \text{Hom}_{\mathcal{O}}(C^\infty(G, \mathcal{O}), \mathcal{O})$ .

**Ejercicio 2.7:** Demuestre que los morfismos  $\mathcal{M}$  y  $\Upsilon$  (si las definimos por las fórmulas en el corolario 2.19) son inversos el uno al otro.

**Ejercicio 2.8:** Demuestre que para  $g \in \mathcal{O}[[T]]$  tenemos

$$\int_{\mathbb{Z}_p} d\Upsilon(g) = g(0).$$

**Ejercicio 2.9:** Demuestre las siguientes relaciones para los binomios:

- (a) Para cada  $n \in \mathbb{N}_{\geq 0}$  y  $x \in \mathbb{Z}_p$ ,

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

- (b) Para cada  $j, k, x \in \mathbb{N}_{\geq 0}$  con  $k \leq x$

$$\binom{j+k}{k} \binom{x}{j+k} = \binom{x}{k} \binom{x-k}{j}.$$

- (c) Para  $x, k \in \mathbb{N}_{\geq 0}$  con  $k \leq x$

$$\sum_{j=0}^{x-k} (-1)^j \binom{x-k}{j} = \begin{cases} 1, & k = x, \\ 0, & 0 \leq k < x. \end{cases}$$

Use el teorema del binomio para esto.

**Ejercicio 2.10:** En este ejercicio damos una demostración directa y elemental del teorema 2.18 de Mahler (sin usar el los isomorfismos en (2.4)), siguiendo [Hid93, §3.1] (sin la parte de la unicidad, que ya demostramos de una manera elemental en el teorema 2.18).

Sea  $f \in C(\mathbb{Z}_p, \mathcal{O})$ . Para  $n \in \mathbb{N}_{\geq 0}$  definimos

$$a_n = \sum_{k=0}^n (-1)^k \binom{n}{k} f(n-k) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(k).$$

- (a) Use relaciones del ejercicio 2.9 para verificar que

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

para  $n \in \mathbb{N}_{\geq 1}$ .

- (b) Deduzca el teorema de Mahler.

## 2.3. Idempotentes y el álgebra de Iwasawa para grupos más grandes

Hasta ahora estudiamos el álgebra de Iwasawa de la forma  $\mathcal{O}[\Gamma]$  con un grupo profinito  $\Gamma$  isomorfo a  $\mathbb{Z}_p$ , pero al final queremos usar el anillo análogo para grupos más grandes de la forma  $\Delta \times \Gamma$  con  $\Delta$  un grupo finito. En esta sección estudiamos estas álgebras para que los *idempotentes ortogonales* son una herramienta útil. Resumamos sus propiedades, que son bien conocidas. En el ejercicio 2.13 damos algunas indicaciones de la demostración.

**Lema 2.20:** *Sea  $A$  un dominio entero y  $\Delta$  un grupo abeliano finito tal que  $\#\Delta \in A^\times$  y  $A$  contiene las raíces de la unidad de orden  $\#\Delta$ . Para cada carácter  $\chi: \Delta \rightarrow A^\times$  definimos*

$$e_\chi = \frac{1}{\#\Delta} \sum_{\delta \in \Delta} \chi(\delta)^{-1} \delta \in A[\Delta].$$

*Este elemento se llama idempotente asociado a  $\chi$ .*

*Entonces tenemos lo siguiente:*

- (a)  $e_\chi^2 = e_\chi$  para cada  $\chi$ ;
- (b)  $e_\chi \delta = \chi(\delta) e_\chi$  para cada  $\chi$  y  $\delta \in \Delta$ ;
- (c)  $e_\chi e_\psi = 0$  si  $\chi \neq \psi$ ;
- (d)  $\sum_\chi e_\chi = 1$ , la suma tomada sobre todos los  $\chi$  posibles.

*Ahora sea  $M$  un  $A[\Delta]$ -módulo. Para cada  $\chi: \Delta \rightarrow A^\times$  escribimos*

$$M[\chi] = \{m \in M \mid \forall \delta \in \Delta: \delta m = \chi(\delta)m\}$$

*para el espacio propio de  $\chi$  en  $M$ . Entonces*

- (e)  $M[\chi] = e_\chi M$ ;
- (f)  $M = \bigoplus_\chi M[\chi]$ , la suma tomada de nuevo sobre todos los  $\chi: \Delta \rightarrow A^\times$  posibles.

Ahora sea  $G$  un grupo profinito de la forma  $G = \Delta \times \Gamma$  con un grupo finito  $\Delta$  y un grupo profinito  $\Gamma$ . Además sea  $A$  un anillo conmutativo topológico tal que  $\#\Delta \in A^\times$  y  $A$  contenga las raíces de la unidad de orden  $\#\Delta$ . Escribimos

$$A[[G]] := \varprojlim_N A[G/N],$$

el límite tomado sobre todos los subgrupos normales abiertos de  $G$ .<sup>1</sup> Entonces  $A[[G]]$  es un  $A[\Delta]$ -módulo y podemos aplicar el lema 2.20. Se verifica fácilmente (usando lema 2.20 (b)) que para cada  $\chi$  de hecho  $e_\chi A[[G]]$  es un  $A$ -álgebra topológica con multiplicación  $(e_\chi g)(e_\chi h) = e_\chi(gh)$  para  $g, h \in G$ .

**Lema 2.21:** *Para cada  $\chi: \Delta \rightarrow A^\times$  existe un isomorfismo canónico de  $A$ -álgebras topológicas*

$$E_\chi: e_\chi A[[G]] \xrightarrow{\cong} A[[\Gamma]].$$

*Es decir,*

$$A[[G]] \simeq \bigoplus_\chi A[[\Gamma]],$$

*la suma tomada sobre todos los  $\chi: \Delta \rightarrow A^\times$ .*

<sup>1</sup> Es decir, si  $A$  es un anillo profinito, esto es el anillo de grupos profinito que definimos antes, pero ahora permitimos anillos más generales como coeficientes. En las aplicaciones el anillo  $A$  será un anillo profinito o una extensión finita de  $\mathbb{Q}$  o  $\mathbb{Q}_p$ .

*Demostración:* Primero observamos que  $A[[G]] = \varprojlim_N A[\Delta \times \Gamma/N]$ , el límite tomado esta vez sobre los subgrupos normales abiertos de  $\Gamma$ . Fijemos un tal subgrupo  $N$ . Entonces es suficiente construir un isomorfismo  $e_\chi A[\Delta \times \Gamma/N] \simeq A[\Gamma/N]$ , la afirmación resulta de esto tomando el límite.

Para cada  $g = (\delta, \gamma) \in \Delta \times \Gamma/N$  tenemos  $e_\chi g = \chi(\delta)\gamma e_\chi$  (véase lema 2.20). El mapeo

$$e_\chi g \mapsto \chi(\delta)\gamma$$

se extiende  $A$ -linealmente a un morfismo de  $A$ -módulos  $e_\chi A[\Delta \times \Gamma/N] \rightarrow A[\Gamma/N]$ . Por otra parte el mapeo

$$A[\Gamma/N] \rightarrow e_\chi A[\Delta \times \Gamma/N], \quad \gamma \mapsto e_\chi(1, \gamma) \quad (\gamma \in \Gamma/N)$$

se extiende a un morfismo en la otra dirección. Un cálculo fácil muestra que estos morfismos son inversos el uno al otro, además es obvio de sus definiciones que los mapeos son multiplicativos.  $\square$

La aplicación más importante de esto será la situación en que  $A = \mathcal{O}$  es el anillo de enteros en una extensión finita de  $\mathbb{Q}_p$  y  $G$  es isomorfo a  $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$ , con  $\Delta$  correspondiendo a  $\mathbb{F}_p^\times$  y  $G$  a  $1 + p\mathbb{Z}_p$ , que es entonces isomorfo a  $\mathbb{Z}_p$  y que por eso denotamos  $\Gamma$ . Entonces  $\mathcal{O}$  contiene las raíces  $(p-1)$ -ésimas de la unidad y  $p-1 \in \mathcal{O}^\times$ . Fijemos un isomorfismo  $G \simeq \mathbb{Z}_p^\times$ . Entonces los caracteres de  $\Delta$  son las potencias del carácter de Teichmüller  $\omega$ .

**Corolario 2.22:** *Para cada  $i \in \{1, \dots, p-1\}$  existe un isomorfismo canónico de  $\mathcal{O}$ -álgebras profinitas*

$$E_{\omega^i} : e_{\omega^i} \mathcal{O}[[G]] \xrightarrow{\simeq} \mathcal{O}[[\Gamma]].$$

Es decir,  $\mathcal{O}[[\mathcal{G}]] \simeq \bigoplus_{i=1}^{p-1} \mathcal{O}[[\Gamma]]$ .

En particular, todos los  $e_{\omega^i} \mathcal{O}[[G]]$  son isomorfos a  $\mathcal{O}[[T]]$  (no canónicamente, después de elegir un generador topológico de  $\Gamma$ , véase teorema 2.11) y podemos aplicar los resultados de nuestro estudio de este anillo.

## Ejercicios

**Ejercicio 2.11:** Sea  $\Delta$  un grupo abeliano finito y  $A$  un anillo conmutativo que contiene las raíces  $\#\Delta$ -ésimas de la unidad. Denotamos  $\widehat{\Delta}$  el grupo de caracteres  $\Delta \rightarrow A^\times$  (con multiplicación puntual). Demuestre que  $\widehat{\Delta} \simeq \Delta$  no canónicamente; en particular, existen  $\#\Delta$  caracteres  $\Delta \rightarrow A^\times$ . Use el teorema de estructura de grupos abelianos finitos para esto.

**Ejercicio 2.12:** Sea  $\Delta$  un grupo abeliano finito y  $A$  un dominio entero que contiene las raíces  $\#\Delta$ -ésimas de la unidad.

(a) Sea  $\delta \in \Delta$  fijado. Demuestre que

$$\sum_{\chi} \chi(\delta) = \begin{cases} \#\Delta & \text{si } \delta = 1, \\ 0 & \text{si } \delta \neq 1 \end{cases}$$

(la suma corriendo por todos los caracteres  $\chi: \Delta \rightarrow A^\times$ ).

(b) Sea  $\chi: \Delta \rightarrow A^\times$  fijado. Demuestre que

$$\sum_{\delta} \chi(\delta) = \begin{cases} \#\Delta & \text{si } \chi = 1, \\ 0 & \text{si } \chi \neq 1 \end{cases}$$

(la suma corriendo por todos los  $\delta \in \Delta$ ).

### 2.3 Idempotentes y el álgebra de Iwasawa para grupos más grandes

Puede ser útil usar el ejercicio 2.11 para esto.

**Ejercicio 2.13:** Sea  $\Delta$  un grupo abeliano finito y  $A$  un dominio entero que contiene las raíces  $\#\Delta$ -ésimas de la unidad. Demuestre las propiedades de los idempotentes del lema 2.20.

Las propiedades (a) y (b) se puede verificar con cálculos directos usando que la multiplicación con un elemento permuta los elementos del grupo  $\Delta$ , que permite transformar las sumas. La relación (c) resulta de (b) considerando el elemento  $e_\chi e_\psi$ . La relación (d) resulta del ejercicio 2.12. Las afirmaciones (e) y (f) son consecuencias directas de las propiedades anteriores.

**Ejercicio 2.14:** Consideramos la situación del lema 2.21. El morfismo

$$\Gamma \rightarrow G = \Delta \times \Gamma, \quad \gamma \mapsto (1, \gamma)$$

induce un morfismo de  $A$ -álgebras  $A[[\Gamma]] \rightarrow A[[G]]$ . Componiendo este con el isomorfismo del lema 2.21 obtenemos un morfismo de  $A$ -álgebras

$$A[[\Gamma]] \rightarrow \bigoplus_x A[[\Gamma]].$$

Demuestre que este morfismo es la aplicación diagonal  $x \mapsto (x, \dots, x)$ .



## Capítulo 3

# Módulos noetherianos sobre el álgebra de Iwasawa

Después de haber conocido el álgebra de Iwasawa vamos a estudiar módulos sobre ella. Esto es interesante porque aparecen de manera natural en muchas situaciones (véase por ejemplo la proposición 1.8) y porque admiten una teoría de estructura muy similar a la de módulos sobre anillos de ideales principales.

Recordemos que un  $R$ -módulo  $M$  es llamado *noetheriano* si todos sus submódulos son finitamente generados. Equivalentemente, si satisface la condición de la cadena ascendente en el orden parcial formado por sus submódulos e inclusiones. Equivalentemente, que para un conjunto  $S$  no vacío de submódulos de  $M$  existe un submódulo máximo, es decir un submódulo  $M_0$  de  $M$  tal que para cualquier elemento  $N$  de  $S$  que contenga  $M_0$  tenemos  $N = M_0$ .

Un anillo conmutativo se llama *noetheriano* si es noetheriano como módulo sobre sí mismo. Observemos que un módulo sobre un anillo noetheriano es noetheriano si y solo si es finitamente generado. Como vamos a estudiar sobre todo módulos sobre el álgebra de Iwasawa (¡que es un anillo noetheriano!) podemos usar las expresiones «noetheriano» y «finitamente generado» sinónimamente en este caso.

Además los módulos noetherianos se comportan bien en sucesiones exactas cortas, ya que si tenemos una sucesión exacta de  $R$ -módulos

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0,$$

entonces  $M$  es noetheriano si y solamente si  $M'$  y  $M''$  son noetherianos. Es decir, la categoría de los  $R$ -módulos noetherianos es una subcategoría de Serre de la categoría de los  $R$ -módulos.

Para un elemento  $x$  en un  $R$ -módulo  $M$  definimos el *anulador* de  $x$  como

$$\text{ann}(x) = \{r \in \Lambda \mid r \cdot x = 0\}.$$

Un elemento  $x \neq 0$  es dicho de *torsión* si su anulador no es trivial. Un módulo  $M$  se llama de *torsión* si todos sus elementos son elementos de torsión y se llama *libre de torsión* si ninguno de sus elementos es elemento de torsión.

Observemos que si  $M$  es un  $R$ -módulo noetheriano, entonces existen  $x_1, \dots, x_d \in M$  tales que  $M = \sum_{i=1}^d Rx_i$ , por lo tanto tenemos que

$$\text{ann}(M) := \bigcap_{x \in M} \text{ann}(x) = \bigcap_{i=1}^d \text{ann}(x_i).$$

### 3.1. Pseudo-isomorfismos

**Definición 3.1:** Decimos que  $M$  es un  $\Lambda$ -módulo, si es un grupo topológico abeliano y Hausdorff, además de un  $\Lambda$ -módulo tal que la acción de  $\Lambda$  es continua.

**Proposición 3.2:** Decimos que un  $\Lambda$ -módulo  $M$  noetheriano es pseudo-nulo si satisface las siguientes condiciones equivalentes

- (a) Para todo ideal primo  $\mathfrak{p}$  de altura  $\leq 1$ , el localizado  $M_{\mathfrak{p}}$  es trivial.
- (b) El único ideal primo que contiene al anulador  $\text{ann}(M)$  es  $\mathfrak{p} = \mathfrak{M}$ .
- (c)  $M$  es finito.

*Demostración:* (a)  $\Rightarrow$  (b): Si  $x \in M$  y denotamos  $x_{\mathfrak{p}}$  su imagen en  $M_{\mathfrak{p}}$ , entonces  $x_{\mathfrak{p}} = 0$  si existe un  $s \in \Lambda \setminus \mathfrak{p}$  tal que  $sx = 0$ , es decir  $s \in \text{ann}(M) \not\subseteq \mathfrak{p}$ . Por lo que claramente el único ideal que contiene a  $\text{ann}(M)$  tiene que ser el ideal máximo.

(b)  $\Rightarrow$  (a): Si  $\text{ann}(M) \not\subseteq \mathfrak{p}$  entonces existe  $s \notin \mathfrak{p}$  tal que  $sM = 0$ , es decir  $M_{\mathfrak{p}} = 0$ .

(b)  $\Rightarrow$  (c): Si el único ideal que contiene  $\text{ann}(M)$  es  $\mathfrak{M}$  tenemos que el radical  $\text{Rad}(\text{ann}(M)) = \mathfrak{M}$ . Luego como  $\Lambda$  es noetheriano  $\text{ann}(M) \supset \mathfrak{M}^k$ , para algún  $k$  suficientemente grande (ver el ejercicio 3.6). Finalmente, si escribimos  $M = x_1\Lambda + \dots + x_d\Lambda$  y tomamos en cuenta que  $\text{ann}(M) \subset \text{ann}(x)$  para todo  $x \in M$ , obtenemos que  $|M| \leq (\Lambda : \mathfrak{M}^k)^d$ .

(c)  $\Rightarrow$  (b): Si  $M$  es finito, entonces

$$\mathfrak{M}M \supset \mathfrak{M}^2M \supset \mathfrak{M}^3M \supset \dots$$

es una filtración estricta de módulos finitos que eventualmente es 0. Es decir  $\text{ann}(M) \supset \mathfrak{M}^k$  par algún  $k$ , por lo que ningún ideal de altura 1 contiene al anulador.

**Observación:**

- (a) Un  $\Lambda$ -módulo pseudo-nulo es de torsión ya que  $M \otimes_{\Lambda} K = M_{(0)} = 0$ .
- (b) El orden de un  $\Lambda$ -módulo pseudo-nulo siempre es una potencia de  $p$  (porque es un  $\mathbb{Z}_p$ -módulo).

**Definición 3.3:** (a) Un morfismo  $\phi$  de  $\Lambda$ -módulos sera llamado *pseudo-inyectivo* (respectivamente *pseudo-sobreyectivo*) luego de que el núcleo  $\ker(\phi)$  (respectivamente su co-núcleo  $\text{coker}(\phi)$ ) es pseudo-nulo.

(b) Un morfismo que es pseudo-inyectivo y pseudo-sobreyectivo, decimos que es un *pseudo-isomorfismo*.

(c) Si  $\varphi : M \rightarrow N$  es un pseudo-isomorfismo escribimos  $M \sim N$ .

**Observación:** Tenemos que  $\varphi : M \rightarrow N$  es un pseudo-isomorfismo si equivalentemente  $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$  es un isomorfismo para todos los ideales  $\mathfrak{p}$  de altura menor o igual que 1.

**Ejercicios**

**Ejercicio 3.1:** La relación de pseudo-isomorfismo generalmente no es simétrica, demuestre que  $\mathfrak{M} \sim \Lambda$  pero  $\Lambda \not\sim \mathfrak{M}$  (no obstante, tenga en cuenta el ejercicio 3.11).

**Ejercicio 3.2:** La relación de pseudo-isomorfismo es transitiva: demuestre que la composición de dos pseudo-isomorfismos es un pseudo-isomorfismo.

**Ejercicio 3.3:** Sea  $M$  un  $\Lambda$ -módulo noetheriano. Demuestre que  $M$  es pseudo-nulo si y solamente si existen  $f$  y  $g$  elementos coprimos de  $\Lambda$  tal que  $fM = gM = 0$ .

**Ejercicio 3.4:** Sea  $\varphi: M \rightarrow N$  un pseudo-isomorfismo de  $\Lambda$ -módulos y  $a = \max\{|\ker(\varphi)|, |\operatorname{coker}(\varphi)|\}$ . Sean  $\alpha: M \rightarrow M$  y  $\beta: N \rightarrow N$  morfismos de  $\Lambda$ -módulos tales que el siguiente diagrama conmuta

$$\begin{array}{ccc} M & \xrightarrow{\alpha} & M \\ \downarrow \varphi & & \downarrow \varphi \\ N & \xrightarrow{\beta} & N. \end{array}$$

Tenemos un diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \alpha(M) & \longrightarrow & M & \longrightarrow & M/\alpha(M) & \longrightarrow & 0 \\ & & \downarrow \varphi' & & \downarrow \varphi & & \downarrow \varphi'' & & \\ 0 & \longrightarrow & \beta(N) & \longrightarrow & N & \longrightarrow & N/\beta(N) & \longrightarrow & 0 \end{array}$$

con líneas exactas.

(a) Demuestre que

$$|\ker(\varphi')|, |\operatorname{coker}(\varphi')|, |\operatorname{coker}(\varphi'')| \leq a \text{ and } |\ker(\varphi'')| \leq a^2.$$

(b) Deduzca que si  $\varphi: M \rightarrow N$  es un pseudo-isomorfismo y  $\nu \in \Lambda$  entonces  $\varphi_\nu: M/\nu M \rightarrow N/\nu N$  también es un pseudo-isomorfismo y  $|\ker \varphi_\nu| \leq a^2, |\operatorname{coker} \varphi_\nu| \leq a$ .

(c) En la misma situación, deduzca que

$$M/\nu M \text{ es finito} \iff N/\nu N \text{ es finito.}$$

**Ejercicio 3.5:** Recordemos que el *soporte de un módulo*  $M$  está definido como el conjunto de los ideales primos tales que la localización es no trivial, es decir

$$\operatorname{sop}(M) = \{\mathfrak{p} \subset R \text{ primo} \mid M_{\mathfrak{p}} \neq 0\}.$$

Sea  $M$  un  $\Lambda$ -módulo noetheriano y sea  $\alpha \in \Lambda$  un elemento diferente de cero tal que  $\operatorname{sop}(\Lambda/\alpha\Lambda)$  y  $\{\mathfrak{p} \in \operatorname{sop}(M) \mid \mathfrak{p} \text{ es de altura } 1\}$  son disjuntos. Entonces la multiplicación por  $\alpha$  en  $M$  es un pseudo-isomorfismo.

**Ejercicio 3.6:** Recordemos que el *radical de un ideal*  $I$  en un anillo conmutativo  $R$  está definido como el conjunto de los elementos  $r \in R$  que al elevarlos a alguna potencia pertenecen a  $I$ , es decir

$$\operatorname{Rad}(I) = \{r \in R \mid r^n \in I\}.$$

(a) Demuestre que

$$\operatorname{Rad}(I) = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ I \subset \mathfrak{p}}} \mathfrak{p}.$$

(b) En particular, si  $M$  es un módulo finitamente generado sobre un anillo noetheriano  $R$ . Entonces

$$\operatorname{Rad}(\operatorname{ann}(M)) = \bigcap_{\mathfrak{p} \in \operatorname{sop}(M)} \mathfrak{p}.$$

(c) Con las hipótesis anteriores, si  $\operatorname{Rad}(\operatorname{ann}(M)) = \mathfrak{M}$  entonces  $\operatorname{ann}(M) \supset \mathfrak{M}^k$ , para algún  $k$  suficientemente grande.

### 3.2. $\Lambda$ -módulos noetherianos de torsión

Recordemos que si  $F$  es un submódulo finito de un  $\Lambda$ -módulo  $M$ , entonces  $F$  es de torsión. Si usted no recuerda esto, lo invitamos a hacer el ejercicio al final de la sección.

**Proposición 3.4:** *Sea  $M$  un  $R$ -módulo noetheriano.  $M$  contiene un submódulo máximo finito  $F$ , y  $M/F$  no contiene submódulos finitos no triviales.*

*Demostración:* El conjunto de los submódulos finitos de  $M$  contiene un elemento máximo  $F$  por la propiedad noetheriana, de lo contrario si  $G$  es otro módulo que no está contenido en  $F$ , entonces  $F + G$  es finito y contiene  $F$ .  $\square$

El anulador de  $M$  es un ideal. En el caso especial  $R = \Lambda$ , la siguiente proposición revela su naturaleza.

**Proposición 3.5:** *Si  $M$  es un  $\Lambda$ -módulo sin submódulos finitos no triviales, su anulador  $\text{ann}(M)$  es principal.*

*Demostración:* Sea  $M = \Lambda x_1 + \cdots + \Lambda x_d$ . Escribamos  $m \in M$  como  $m = \sum_{i=1}^d \lambda_i x_i$ . Supongamos que  $\text{ann}(M)$  no es principal, entonces por la proposición 2.9,  $\text{ann}(M)$  está contenido en un ideal principal  $a\Lambda$  con índice finito y  $aM$  es no trivial. Existe un morfismo sobreyectivo  $(a\Lambda / \text{ann}(M))^d \twoheadrightarrow aM$ , por lo tanto

$$|aM| = (aM : \text{ann}(M)M) \leq (a\Lambda : \text{ann}(M))^d,$$

lo cual contradice nuestra hipótesis en la carencia de submódulos finitos no triviales.  $\square$

**Lema 3.6:** *Sea  $M$  un  $\Lambda$ -módulo noetheriano y de torsión, sin submódulos finitos no triviales. Sea  $f = f_1 f_2$  una factorización de su anulador con  $f_1$  y  $f_2$  coprimos. Entonces tenemos*

$$M \sim f_1 M \oplus f_2 M \quad \text{y} \quad f_1 M \oplus f_2 M \sim M$$

con  $\text{ann}(f_1 M) = f_2 \Lambda$  y  $\text{ann}(f_2 M) = f_1 \Lambda$ .

*Demostración:* Es claro que la suma  $f_1 M + f_2 M$  es directa, ya que si  $x \in f_1 M \cap f_2 M$ , por la proposición 2.9 tenemos que  $\Lambda / \text{ann}(x) \simeq \Lambda x$  es finito. Como  $M$  no contiene submódulos finitos no triviales concluimos que  $x = 0$ . Por lo tanto tenemos la siguiente sucesión exacta

$$0 \rightarrow f_1 M \oplus f_2 M \rightarrow M \rightarrow M / f_1 M \oplus f_2 M.$$

Veamos que el mapeo  $x \mapsto f_1 x + f_2 x$  es inyectivo. El núcleo de la aplicación es  $\{x \in M \mid f_1 x = -f_2 x\}$ , por lo que el núcleo es anulado por  $(f_1 + f_2)$  y  $f$ . Entonces si  $x$  es un elemento del núcleo tenemos

$$(f_1 + f_2)\Lambda + f\Lambda \subset \text{ann}(x) \subset \Lambda$$

pero  $\Lambda / \text{ann}(x) \simeq x\Lambda$  es finito por la proposición 2.9 ya que  $(f_1 + f_2)$  y  $f$  son coprimos. Por lo tanto  $x = 0$  y tenemos la siguiente sucesión exacta

$$0 \rightarrow M \rightarrow f_1 M \oplus f_2 M \rightarrow (f_1 M \oplus f_2 M) / (f_1 + f_2)M.$$

Por último, demostramos que los conúcleos son finitos. Observemos que  $M / f_1 M \oplus f_2 M$  es anulado por  $f_1$  y por  $f_2$ . Es decir, al localizar en  $\mathfrak{p}$ , existe siempre un elemento  $f_i$  tal que  $f_i M \in f_1 M \oplus f_2 M$ . Por lo que el localizado es nulo para todo  $\mathfrak{p}$  de altura  $\geq 1$ .

Por último, tenemos que

$$(f_1 + f_2)(f_1 M \oplus f_2 M) \subset (f_1 + f_2)M \subset f_1 M \oplus f_2 M,$$

además es fácil ver que

$$f_1M \oplus f_2M / (f_1 + f_2)(f_1M \oplus f_2M)$$

es anulado por  $f_1$  y  $f_2$ . Por lo tanto pseudo-nulo.  $\square$

**Lema 3.7:** Sean  $M$  y  $N$   $\Lambda$ -módulos noetherianos y de torsión, ambos sin submódulos finitos no triviales. Entonces  $M \sim N$  si y solamente si  $N \sim M$ .

*Demostración:* Sea  $M \xrightarrow{\varphi} N$  un pseudo-isomorfismo. Sea  $c \in \Lambda$  un elemento coprimo a  $f$ , el generador de  $\text{ann}(M)$ , tal que  $c$  anula  $\ker(\varphi)$  (ejercicio 3.3). La restricción de  $\varphi$  a  $cM$  es inyectiva, y  $cM$  es de índice finito en  $M$ .

La imagen  $\varphi(cM)$  es de índice finito en  $N$  (ejercicio 3.4). Es decir, podemos elegir  $d$  coprimo con  $g$ , el generador de  $\text{ann}(N)$ , tal que  $dN \subset \varphi(cM)$ . La multiplicación por  $d$  en  $N$  es pseudo-inyectiva. Como la composición de pseudo-isomorfismos es un pseudo-isomorfismo (ejercicio 3.2), tenemos un pseudo isomorfismo

$$N \rightarrow dN \xrightarrow{\varphi^{-1}} cM \hookrightarrow M,$$

donde  $\varphi^{-1}(dN) \subset cM$  y como  $\varphi(dM) \subseteq dN$ , tenemos que  $dM \subseteq \varphi^{-1}(dN)$  y deducimos que  $\text{coker}(\varphi^{-1})$  es pseudo-nulo.  $\square$

El lema precedente es de hecho cierto con más generalidad y es una consecuencia del teorema de estructura. La relación de pseudo-isomorfismo es una relación de equivalencia entre los  $\Lambda$ -módulos noetherianos de torsión (ver el ejercicio 3.11).

**Proposición 3.8:** Sea  $M$  un  $\Lambda$ -módulo noetheriano y de torsión sin submódulo finito y con anulador de la forma  $\mathfrak{p}^e$  con  $\mathfrak{p}$  un ideal primo principal de  $\Lambda$ . Entonces  $M$  es pseudo-isomorfo a una suma directa

$$M \sim \bigoplus_{i=1}^k \Lambda/\mathfrak{p}^{e_i}.$$

*Demostración:* Primero supongamos que  $\mathfrak{p} = P$  con  $P$  un polinomio distinguido e irreducible. El cociente  $\Lambda/P^e$  es un  $\mathcal{O}$ -módulo libre de dimensión  $e \deg(P)$ . Por lo tanto, como  $M$  es finitamente generado como  $\Lambda/P^e$ -módulo, también lo es como  $\mathcal{O}$ -módulo. El submódulo de  $\mathcal{O}$ -torsión  $T_{\mathcal{O}}(M)$  de  $M$ , por el teorema de estructura de módulos finitamente generados sobre anillos principales, es anulado por una potencia  $\pi^m$  del uniformizante de  $\mathcal{O}$ . Por lo que  $T_{\mathcal{O}}(M)$  es un  $\Lambda$ -módulo anulado por  $\pi^m$  y por  $P^e$ , entonces pseudo-nulo. Por hipótesis,  $M$  no contiene submódulos finitos no triviales, de donde concluimos que  $M$  es libre de  $\mathcal{O}$ -torsión y por lo tanto libre. Sea  $d = \text{rg}_{\mathcal{O}} M$ , vamos a proceder por inducción para demostrar el resultado.

Si  $d = 0$  no hay nada que demostrar. Supongamos que la hipótesis es cierta para  $M$  de rango menor que  $d$ .

Sea  $x \in M$  de anulador mínimo  $P^e$  y consideremos la sucesión exacta corta

$$0 \longrightarrow \Lambda x \longrightarrow M \longrightarrow M/\Lambda x \longrightarrow 0.$$

Por hipótesis de inducción  $M/\Lambda x$  es pseudo-isomorfo a una suma directa  $M' = \bigoplus_{i=1}^m \Lambda/\mathfrak{p}^{e_i}$ . Tomemos un  $c \notin \mathfrak{p}$ , tal que la imagen de  $M/\Lambda x$  contiene  $cM'$ . Escribimos

$$cM' = \bigoplus_{i=1}^m \Lambda cx_i$$

con  $x_i \in M'$ . Tomamos levantamientos  $y_i$  en  $M$  de los  $cx_i$ . Dado que  $P \nmid x$ , podemos escribir

$$P^{e_i} y_i = f P^{e'_i} x \in \Lambda x$$

con  $P \nmid f$  y  $e'_i \geq e_i$ . Sea  $z_i = y_i - f P^{e'_i - e_i} x$  en  $M$ . Claramente las imágenes  $\bar{z}_i$  y  $\bar{y}_i$  de  $z_i$  y de  $y_i$  en  $M/\Lambda x$  coinciden, además  $P^{e_i} z_i = 0$  en  $M$ , por lo tanto  $\Lambda z_i \simeq \Lambda/\mathfrak{p}^{e_i}$ . La suma  $\sum_{i=1}^m \Lambda z_i$  es directa, isomorfa a

$$\bigoplus_{i=1}^m \Lambda/\mathfrak{p}^{e_i}.$$

Definamos por último

$$M'' = \left( \bigoplus_{i=1}^m \Lambda z_i \right) + \Lambda x,$$

la suma es directa y es un submódulo de  $M$ . El cociente  $M''/\Lambda x = \bigoplus_{i=1}^m \Lambda \bar{z}_i$  es isomorfo a  $M'$ . Como  $M/\Lambda x$  y  $M'$  son pseudo-isomorfos, tenemos que el morfismo inducido

$$(M/\Lambda x)/(M''/\Lambda x) \longrightarrow M'/(M''/\Lambda x) = 0$$

tiene núcleo y conúcleo finitos (ver el ejercicio 3.4). De donde tenemos que  $M/M''$  es finito y por el lema 3.7 tenemos que  $M \sim M''$ .

Ahora supongamos que  $\mathfrak{p} = \pi$ . El cociente  $M/\pi M$  es un  $k[[T]]$  módulo noetheriano, por lo tanto es una suma directa de un módulo finito y un módulo libre de dimensión  $d$ . Vamos a demostrar el enunciado por inducción sobre la dimensión del módulo libre.

Supongamos que  $d = 0$ , entonces  $M/\pi M$  es finito, anulado por una potencia de  $T$  digamos  $T^m$ . Tenemos  $T^m M \subset \pi M$ , es decir  $T^{em} M = 0$ , ya que  $\pi^e M = 0$ . Es decir,  $M$  es anulado por  $T^{em}$  y  $\pi^e$ , por lo tanto pseudo-nulo.

Supongamos que la hipótesis se verifica para dimensiones menores que  $d$  y sea entonces  $M/\pi M$  una suma directa de un módulo finito y un  $k[[T]]$ -módulo libre de dimensión  $d$ . Luego procedemos con la inducción exactamente como en el caso anterior, tomando un elemento  $x \in M$  de anulador mínimo  $\pi^e$ . □

## Ejercicios

**Ejercicio 3.7:** Demuestre que todo  $\Lambda$ -módulo  $M$  noetheriano es pseudo-isomorfo a  $M/F$  donde  $F$  es su submódulo máximo finito.

**Ejercicio 3.8:** Sea  $M$  un módulo noetheriano. Demuestre que todo submódulo finito de  $M$  es de torsión.

## 3.3. Teorema de estructura

Para un  $\Lambda$ -módulo noetheriano  $M$  escribimos

- (a)  $T(M)$  como su submódulo de torsión.
- (b)  $F(M) = M/T(M)$  su cociente maximal libre de torsión.

**Proposición 3.9:** Sea  $M$  un  $\Lambda$ -módulo noetheriano libre de torsión. Entonces  $M$  es pseudo-isomorfo a  $\Lambda^d$  para un único  $d \geq 0$ .



Sea  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$  el conjunto de ideales primos de altura 1 de  $\Lambda$  para los cuales  $T(M)_{\mathfrak{p}_i} \neq 0$ , es decir  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\} \subset \text{sop}(T(M))$ . Si el conjunto es vacío, i.e.  $h = 0$ , entonces  $T(M)$  es pseudo-nulo. Tenemos la composición de pseudo-isomorfismos

$$M \rightarrow F(M) \hookrightarrow T(M) \oplus F(M),$$

de donde obtenemos el resultado.

Ahora supongamos que  $h \geq 1$ . Entonces  $S^{-1}\Lambda$  es un dominio de ideales principales (ver ejercicio 3.9). Además  $T(S^{-1}M) = S^{-1}T(M)$ , lo cual junto con el teorema de estructura de módulos sobre dominios de ideales principales que  $S^{-1}M = S^{-1}T(M) \oplus F(S^{-1}M)$ . Es decir, la proyección de  $S^{-1}M$  en  $S^{-1}T(M)$  admite una sección.

El anillo  $\Lambda$  es noetheriano, por lo tanto  $M$  es un  $\Lambda$ -módulo finitamente presentable. Tenemos la siguiente identidad [Eis95, Prop. 2.10]

$$\text{Hom}_{S^{-1}\Lambda}(S^{-1}M, S^{-1}T(M)) = S^{-1} \text{Hom}_{\Lambda}(M, T(M)).$$

La proyección  $\pi : S^{-1}M \rightarrow S^{-1}T(M)$  la podemos escribir como  $\pi = \frac{f_0}{s_0}$  para un  $s_0$  en  $S$  y

$f_0 : M \rightarrow T(M)$ . Entonces  $\frac{f_0}{s_0}|_{S^{-1}T(M)} = \text{id}_{S^{-1}T(M)}$ .

Ahora sea  $x \in T$ , entonces  $\frac{f_0(x)}{s_0} = \frac{x}{1}$ . Por la definición de localización en  $S$  tenemos que existe  $s_1 \in S$  tal que  $s_1(f_0(x) - s_0x) = 0$ , equivalentemente  $s_1f_0(x) = s_0s_1x$ . Haciendo  $f_1 = s_1f_0$  tenemos que

$$f_1|_{T(M)} = s_0s_1 \text{id}_{T(M)}.$$

Definiendo

$$f = (f_1, g) : M \longrightarrow T(M) \oplus F(M)$$

donde  $g$  es el mapeo canónico de  $M$  a  $F(M)$ , tenemos el diagrama conmutativo

$$\begin{array}{ccccccc} 0 & \longrightarrow & T(M) & \longrightarrow & M & \longrightarrow & F(M) \longrightarrow 0 \\ & & \downarrow f_1|_{T(M)} & & \downarrow f & & \parallel \\ 0 & \longrightarrow & T(M) & \longrightarrow & M & \longrightarrow & F(M) \longrightarrow 0 \end{array}$$

De donde obtenemos que  $\ker(f_1|_{T(M)}) = \ker(f)$  y  $\text{coker}(f_1|_{T(M)}) = \text{coker}(f)$ . Finalmente, es fácil ver que la multiplicación por  $s_0s_1$  en  $T(M)$  es un pseudo-isomorfismo.  $\square$

**Definición 3.11:** Decimos que un  $\Lambda$ -módulo  $E$  es *elemental* si es de la forma

$$E = \Lambda^r \oplus \left( \bigoplus_{i=1}^k \Lambda/\mathfrak{p}_i^{e_i} \Lambda \right),$$

donde los  $\mathfrak{p}_i$  ideales primos (posiblemente repetidos) de  $\Lambda$  de altura 1 y  $r, e_i \geq 0$  son enteros.

El siguiente teorema es uno de los pilares en teoría de Iwasawa. A pesar de que  $\Lambda$  no sea un anillo principal, es muy interesante que tengamos un teorema de estructura salvo pseudo-isomorfismos. Como veremos más adelante, este resultado y unas técnicas de descenso nos permitirán demostrar el teorema de Iwasawa (teorema 4.22) sobre grupos de clases.

**Teorema 3.12 (Teorema de Estructura):** *Todo  $\Lambda$ -módulo noetheriano es pseudo-isomorfo a un único  $\Lambda$ -módulo elemental  $E$*

$$M \sim E = \Lambda^{\rho} \oplus \left( \bigoplus_{i=1}^m \Lambda / \pi^{\mu_i} \Lambda \right) \oplus \left( \bigoplus_{j=1}^l \Lambda / P_j \Lambda \right)$$

donde los  $P_j$  son polinomios distinguidos ordenados por divisibilidad.

*Demostración:* Sea  $M$  un  $\Lambda$ -módulo noetheriano.  $M$  es pseudo-isomorfo a la suma directa de un módulo de torsión  $T(M)$  sin submódulo finito y de un  $\Lambda$ -módulo libre  $L$  de rango finito (proposición 3.10 y ejercicio 3.7). Teniendo anulador principal (proposición 3.5), el submódulo  $T(M)$  es pseudo-isomorfo a una suma directa de submódulos  $T_{\mathfrak{p}_i}(M)$  con anuladores primarios  $\mathfrak{p}_i^{e_i}$  (lema 3.6). A su vez, los submódulos  $T_{\mathfrak{p}_i}(M)$  son pseudo-isomorfos a una suma directa de la forma  $\bigoplus_{j=1}^{k_i} \Lambda / \mathfrak{p}_i^{e_{i,j}}$  con  $e_{i,1} \geq e_{i,2} \geq \dots \geq e_{i,k_i} > 0$  (proposición 3.8).

Finalmente, sea  $P_j = \prod_{\mathfrak{p}_i \neq \pi} \mathfrak{p}_i^{e_{i,j}}$ , con la convención  $e_{i,j} = 0$  si  $j > k_i$ . Definiendo  $l$  como el máximo de los  $k_i$ , obtenemos que  $P_l | P_{l-1} | \dots | P_1$ . El resultado sigue aplicando el lema 3.7.  $\square$

A continuación definimos los *invariantes*  $\mu$  y  $\lambda$  asociados al polinomio característico del  $\Lambda$ -submódulo de torsión de un módulo noetheriano  $M$ .

**Definición 3.13:** Usamos la situación y la notación del teorema 3.12.

- (a) Escribimos  $\mu = \sum_{i=1}^m \mu_i$  y  $P = \prod_{j=1}^l P_j$  y definimos el *polinomio característico* del submódulo de  $\Lambda$ -torsión de  $M$  como  $P$ .
- (b) Definimos  $\lambda = \deg P = \sum_{j=1}^l \deg P_j$ .

El nombre «polinomio característico» es justificado por el ejercicio 3.10.

### Ejercicios

**Ejercicio 3.9:** Sea  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\} \neq \emptyset$  un conjunto de ideales primos de altura 1 de  $\Lambda$ . Demuestre que:

- (a)  $S_i = \Lambda \setminus \mathfrak{p}_i$  es un conjunto multiplicativo. Esto es,  $1 \in S_i$  y para todo  $x, y \in S_i$ , entonces  $xy \in S_i$ .
- (b) la intersección  $S = \bigcap S_i$  también es un conjunto multiplicativo igual a  $\Lambda \setminus \bigcup \mathfrak{p}_i$ .
- (c)  $S^{-1}\Lambda$  es un anillo semi-local, es decir tiene un número finito de ideales maximales (*Consejo:* utilice el lema de evitación de ideales primos).
- (d)  $S^{-1}\Lambda$  es un anillo de Dedekind, es decir es integralmente cerrado, noetheriano y sus ideales primos son maximales.
- (e)  $S^{-1}\Lambda$  es un dominio de ideales principales.

**Ejercicio 3.10:** Escribimos  $K$  como el campo de fracciones de  $\mathcal{O}$ . Sea  $M$  un  $\Lambda$ -módulo de torsión. Definimos  $V = K \otimes_{\mathcal{O}} M$ , que es un espacio vectorial de dimensión finita sobre  $K$ . La aplicación  $V \rightarrow V$  definida como multiplicación por  $T$  es  $K$ -lineal. Demuestre que el polinomio característico de esta aplicación es justamente el polinomio característico de  $M$ .

**Ejercicio 3.11:** Demuestre que la relación de pseudo-isomorfismo es simétrica en los módulos de torsión (así que es una relación de equivalencia). Es decir, demuestre que si  $M$  y  $N$  son  $\Lambda$ -módulos noetherianos de torsión entonces

$$M \sim N \iff N \sim M.$$

Use el teorema de estructura y el lema 3.6 para esto.

### 3.4. Resultados adicionales sobre $\Lambda$ -módulos

Recordemos que  $\mathfrak{M} = (\pi, T)$  denota el ideal máximo de  $\Lambda$ , donde  $\pi \in \mathcal{O}$  es un uniformizante.

**Lema 3.14:** *Sea  $X$  un  $\Lambda$ -módulo compacto. Entonces*

$$\bigcap_{r \in \mathbb{N}_{\geq 1}} \mathfrak{M}^r X = 0.$$

*Demostración:* Sea  $U$  un vecindario de 0 en  $X$ , recordemos que un  $\Lambda$ -módulo compacto tiene un sistema fundamental de vecindarios de cero formado de submódulos abiertos [NSWo8, Cor. 5.2.5]. Sea  $z \in X$ , como  $\Lambda$  es completo las sucesiones  $(\pi^r)_{r \in \mathbb{N}_{\geq 1}}$  y  $(T^r)_{r \in \mathbb{N}_{\geq 1}}$  convergen a 0 en  $\Lambda$ . Por lo tanto existe  $s_0$  tal que  $\pi^s z, T^s z$  son elementos de  $U$  para  $s \geq s_0$ .

Sea  $r \geq 2s_0$ , entonces para  $i + j = r$

$$\pi^i T^j = \begin{cases} (\pi^{i-s_0} T^j) \pi^{s_0}, & \text{si } i \geq s_0; \\ (\pi^i T^{j-s_0}) T^{s_0}, & \text{si } j \geq s_0. \end{cases}$$

Es decir  $\pi^i T^j z \in U$  para todo  $i + j = r$ .

Las aplicaciones  $x \mapsto \pi^{s_0} x$  y  $x \mapsto T^{s_0} x$  son continuas, las preimágenes  $V$  y  $W$  de  $U$ , respectivamente, son abiertas. La intersección  $U_z := V \cap W$  es un conjunto abierto no vacío. Tenemos entonces que  $\pi^i T^j U_z \subset U$  para  $i + j = r$ , además como  $U$  es un  $\Lambda$ -submódulo para cualquier combinación lineal  $\alpha = \sum_{i+j=r} \lambda_{i,j} \pi^i T^j$  con  $\lambda_{i,j} \in \Lambda$  y  $u \in U_z$  tenemos  $\alpha u \in U$ .

Hemos demostrado que para todo  $z \in X$  existe un vecindario  $U_z$  y un  $r$  suficientemente grande tal que  $\mathfrak{M}^r U_z \subseteq U$ . Como  $X$  es compacto, existe un número finito  $U_{z_1}, \dots, U_{z_k}$  que cubren  $X$ . Sea  $r = \max\{r_1, \dots, r_k\}$  tal que  $\mathfrak{M}^{r_i} U_{z_i} \subseteq U$ , entonces

$$\mathfrak{M}^r X \subset U,$$

lo que demuestra el resultado al tomar la intersección de todos los vecindarios  $U$  de 0.  $\square$

**Lema 3.15 (Lema de Nakayama Topológico):** *Sea  $X$  un  $\Lambda$ -módulo compacto.  $X$  es noetheriano si y solamente si  $X/\mathfrak{M}X$  es finito.*

*Demostración:* Si  $X$  es noetheriano la implicación es clara. Supongamos entonces que  $X/\mathfrak{M}X$  es finito. En particular, existen  $x_1, x_2, \dots, x_d \in X$  que generan  $X/\mathfrak{M}X$  como grupo abeliano. Sea

$$Y = x_1 \Lambda + \dots + x_d \Lambda \subseteq X.$$

El  $\Lambda$ -módulo  $Y$  es cerrado por ser la imagen de  $\Lambda^d \rightarrow Y$ . La proyección  $X \rightarrow X/Y$  es continua, por lo tanto  $X/Y$  es compacto con la topología  $\mathfrak{M}$ -ádica inducida. Tenemos  $Y + \mathfrak{M}X = X$ , es decir  $\mathfrak{M}^r(X/Y) = X/Y$  para todo  $r \geq 0$ . Por el lema 3.14 tenemos  $X/Y = 0$ , es decir  $Y = X$  y por lo tanto  $x_1, \dots, x_d$  generan  $X$ .  $\square$

El siguiente corolario se deduce inmediatamente del lema anterior.

**Corolario 3.16:** *Sea  $X$  un  $\Lambda$ -módulo compacto, entonces*

$$X/\mathfrak{M}X = 0 \iff X = 0.$$

En el siguiente resultado aparecen de nuevo los polinomios  $\omega_r$  de la definición 2.10.

**Proposición 3.17:** *Sea  $X$  un  $\Lambda$ -módulo noetheriano. Entonces*

$$\begin{aligned} X \text{ es de torsión} &\iff \text{rg}_{\mathcal{O}} X < \infty \\ &\iff \text{rg}_{\mathcal{O}} X/\omega_r X \text{ está acotado para todo } r \geq 0. \end{aligned}$$

*Demostración:* Primero notemos que el enunciado es invariante bajo pseudo-isomorfismos. Sea  $f: X \rightarrow E$  un pseudo-isomorfismo de  $X$  a un módulo elemental  $E$  (ver la definición 3.11 y el teorema 3.12). Tenemos que  $X \otimes_{\Lambda} \text{Frac}(\Lambda) \simeq E \otimes_{\Lambda} \text{Frac}(\Lambda)$ . Es decir  $X$  es de torsión si y solamente si  $E$  es de torsión. Igualmente del ejercicio 3.4 deducimos que  $\text{rg}_{\mathcal{O}} X < \infty \Leftrightarrow \text{rg}_{\mathcal{O}} E < \infty$ . Igualmente,  $\text{rg}_{\mathcal{O}} X/\omega_r X$  está acotado para todo  $r \geq 0$  si y solamente si  $\text{rg}_{\mathcal{O}} E/\omega_r E$  está acotado para todo  $r \geq 0$ . Por lo tanto podemos remplazar  $X$  por  $E$  y bastará analizar el enunciado para los tipos de factores de un módulo elemental, es decir  $\Lambda$ ,  $\Lambda/\pi^e$  o  $\Lambda/P^e$  donde  $P$  es un polinomio distinguido.

Veamos que  $\Lambda \otimes_{\mathcal{O}} L$  es un  $L$ -espacio vectorial de dimensión infinita (donde  $L$  es el campo de cocientes de  $\mathcal{O}$ ). Además  $\Lambda/\pi^e$  es isomorfo a  $\mathcal{O}/\pi^e[[T]]$  y  $\Lambda/P^e$  es isomorfo a  $\mathcal{O}[T]/P^e$ . Cuando tensamos con  $L$  los diferentes tipos de factores obtenemos  $L$ -espacios vectoriales. El primero infinito, el segundo trivial y el tercero finito. Es decir,  $E$  es de torsión si y solamente si  $\text{rg}_{\mathcal{O}} E < \infty$ .

Aplicando el funtor exacto  $- \otimes_{\mathcal{O}} L$  a

$$0 \longrightarrow \omega_r E \longrightarrow E \longrightarrow E/\omega_r E \longrightarrow 0,$$

deducimos que  $\text{rg}_{\mathcal{O}} E < \infty$  implica que  $\text{rg}_{\mathcal{O}} E/\omega_r E$  está acotado para todo  $r$ .

Por otro lado, tomemos  $E$  no de torsión, entonces  $\rho \geq 1$  como en el teorema 3.12. Si  $\Lambda$  es un factor de  $E$  entonces por el lema de división (lema 2.3, usando la notación de allá)

$$\Lambda/\omega_r \simeq \mathcal{O}_{p^r-1}[T],$$

es decir  $\Lambda/\omega_r$  es isomorfo al  $\mathcal{O}$ -módulo de los polinomios de grado a lo más  $p^r - 1$ . Es claro que el rango de  $\mathcal{O}_{p^r-1}[T]$  sobre  $\mathcal{O}$  es proporcional a  $r$ , y por lo tanto no acotado.  $\square$

Terminamos la sección con algunos resultados auxiliares que serán útiles más tarde.

**Lema 3.18:** *Sea  $M$  un  $\Lambda$ -módulo noetheriano de torsión y sea  $(F) = \text{car}_{\Lambda}(M)$  su ideal característico. Además sea  $\nu \in \Lambda$ . Entonces  $M/\nu M$  es finito si y solo si  $\nu$  y  $F$  son coprimos.*

*Demostración:* Fijemos un pseudo-isomorfo

$$M \rightarrow E := \left( \bigoplus_{i=1}^m \Lambda/(\pi^{\mu_i}) \right) \oplus \left( \bigoplus_{j=1}^l \Lambda/(P_j) \right)$$

a un  $\Lambda$ -módulo elemental  $E$ . Entonces  $F = \pi^{\mu} \prod_j P_j$  con  $\mu = \sum_i \mu_i$ .

Primero asumamos que  $\nu$  y  $F$  son coprimos. Entonces  $\nu$  es coprimo a  $\pi$  y a todos los  $P_j$ . Usando el ejercicio 3.4 obtenemos un pseudo-isomorfo

$$M/\nu M \rightarrow \left( \bigoplus_{i=1}^m \Lambda/(\pi^{\mu_i}, \nu) \right) \oplus \left( \bigoplus_{j=1}^l \Lambda/(P_j, \nu) \right)$$

y cada de los sumandos a la derecha es finito según el corolario 2.8. Por eso  $M/\nu M$  también tiene que ser finito.

Por otro lado asumamos que  $\nu$  y  $F$  no son coprimos, es decir existe  $d \in \Lambda$  que no es una unidad y divide a  $\nu$  y a  $F$ . Sabemos que  $\Lambda$  es un dominio de factorización única, que  $\pi$  es coprimo a cada uno de los  $P_j$  y además que los  $P_j$  son ordenados por divisibilidad. Por eso podemos asumir que  $d$  divide a  $\pi$  o a  $P_1$  (y a  $\nu$ , por supuesto). En el primer caso podemos asumir que  $d = \pi$  y en el segundo que  $d = P$  es un polinomio distinguido no trivial. Entonces tenemos sobrecciones canónicas

$$E/\nu E \rightarrow E/dE \rightarrow \Lambda/\pi\Lambda \quad \text{o} \quad E/\nu E \rightarrow E/dE \rightarrow \Lambda/P\Lambda.$$

Porque  $\Lambda/\pi\Lambda$  y  $\Lambda/P\Lambda$  son infinitos,  $E/\nu E$  y pues  $M/\nu M$  también tienen que ser infinitos.  $\square$

**Lema 3.19:** Sea  $E$  un  $\Lambda$ -módulo elemental y  $\nu \in \Lambda$  tal que  $\text{rg}_{\mathcal{O}} E[\nu] = 0$  y  $E/\nu E$  es finito. Escribimos  $E[\nu]$  como el núcleo de la multiplicación con  $\nu$  en  $E$ . Entonces  $E[\nu] = 0$ .

*Demostración:* Sin pérdida de generalidad podemos asumir que  $E$  es de la forma  $\Lambda$  o  $\Lambda/\pi^\mu \Lambda$  con  $\mu \in \mathbb{N}_{\geq 1}$  o  $\Lambda/P\Lambda$  con  $P$  un polinomio distinguido.

En el primer caso  $E = \Lambda$  tenemos  $E[\nu] = 0$  porque  $\Lambda$  no tiene divisores de cero. En el caso  $E = \Lambda/\pi^\mu \Lambda$ , si  $E[\nu] \neq 0$  entonces la clase de  $\nu$  tiene que ser un divisor de cero en  $\Lambda/\pi^\mu \Lambda$ , es decir es un divisor de  $\pi^\mu$  en  $\Lambda$ . Pero en este caso  $E/\nu E$  es infinito.

Sea entonces  $E = \Lambda/P\Lambda$ . Si  $E[\nu] \neq 0$  entonces existe un  $h \in \Lambda$  con  $\nu h = P$ , y sin pérdida de generalidad  $h, \nu \in \mathcal{O}[T]$  y  $\deg \nu, \deg h > 0$ . Pero entonces  $h\mathcal{O}[T]/P\mathcal{O}[T]$  es un submódulo de  $E[\nu]$  cuyo rango es mayor que 0, contradiciendo a  $\text{rg}_{\mathcal{O}} E[\nu] = 0$ .  $\square$

**Corolario 3.20:** Si  $M$  es un  $\Lambda$ -módulo noetheriano de torsión y  $\nu \in \Lambda$  es coprimo a  $\text{car}_\Lambda M$  entonces  $M[\nu]$  es finito.

*Demostración:* Usando el teorema de estructura es suficiente demostrar esto para  $\Lambda$ -módulos elementales, por eso remplacemos  $M$  con un módulo elemental  $E$  como en la demostración de la proposición 3.17. Según el lema 3.18  $E/\nu E$  es finito, pues por el lema 3.19 es suficiente demostrar que  $\text{rg}_{\mathcal{O}} E[\nu] = 0$ . Eso resulta de la sucesión exacta

$$0 \rightarrow E[\nu] \rightarrow E \xrightarrow{\nu} E \rightarrow E/\nu E \rightarrow 0,$$

usando que el  $\mathcal{O}$ -rango de  $E$  es finito porque  $E$  es de torsión (corolario 4.14).  $\square$

### 3.5. Ideales característicos

La teoría de estructura que desarrollamos anteriormente permite definir una invariante importante de  $\Lambda$ -módulos noetherianos: el ideal característico. Esta invariante va a aparecer en la Conjetura Principal de Iwasawa.

Sea  $\mathcal{O}$  el anillo de enteros en una extensión finita de  $\mathbb{Q}_p$ ,  $\Gamma$  un grupo profinito isomorfo a  $\mathbb{Z}_p$  y escribimos  $\Lambda = \mathcal{O}[[\Gamma]]$  para su álgebra de Iwasawa. Después de fijar un generador topológico  $\gamma$  de  $\Gamma$ , el teorema 2.11 nos permite identificar  $\Lambda$  con el anillo de series de potencias  $\mathcal{O}[[T]]$ .

Si  $M$  es un  $\Lambda$ -módulo noetheriano, el teorema de estructura 3.12 dice que  $M$  es pseudo-isomorfo a un único  $\Lambda$ -módulo elemental de la forma

$$M \sim E = \Lambda^\rho \oplus \left( \bigoplus_{i=1}^m \Lambda/\pi^{\mu_i} \Lambda \right) \oplus \left( \bigoplus_{j=1}^l \Lambda/P_j \Lambda \right)$$

y en la definición 3.13 definimos el invariante  $\mu \in \mathbb{N}_{\geq 0}$  y el polinomio característico  $P = \prod_{j=1}^l P_j$  de  $M$ . El elemento  $\pi^\mu P \in \Lambda$  no es bien definido porque  $\pi$  solo es determinado salvo a una unidad. Pero esto significa que la siguiente definición tiene sentido (aunque hay que verificar que no depende del  $\gamma$  que eligimos).

**Definición 3.21:** Para cada  $\Lambda$ -módulo noetheriano  $M$  definimos su *ideal característico* como

$$\text{car}_\Lambda(M) := (\pi^\mu P)$$

con  $\mu$  y  $P$  como arriba.

Recordemos otra vez que el teorema de estructura puede ser visto como un análogo del teorema de estructura para grupos abelianos finitamente generados. En esta situación análoga, el «ideal característico» de un grupo abeliano finitamente generado sería el ideal

en  $\mathbb{Z}$  generado por el orden de la parte finita del grupo. Por eso, heurísticamente podemos imaginar el ideal característico como análogo del «orden de un grupo» y de hecho resultará un invariante muy importante de un módulo.

Porque en las aplicaciones usaremos álgebras de Iwasawa para grupos más grandes como en la sección 2.3, generalicemos la definición del ideal característico a esa situación. Esto es puramente formal y nada profundo, aunque un poco técnico.

Sea  $\Delta$  un grupo finito cuyo orden  $\#\Delta$  es inversible en  $\mathcal{O}$  y tal que  $\mathcal{O}$  contiene las raíces  $\#\Delta$ -ésimas de la unidad. El ejemplo más importante será el en que  $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \simeq \mathbb{F}_p^\times$ . Sea  $G = \Delta \times \Gamma$  con  $\Gamma$  como antes. El álgebra de Iwasawa  $\Lambda(G) = \mathcal{O}[[G]]$  para el grupo  $G$  entonces se descompone como

$$\Lambda(G) = \bigoplus_{\chi} e_{\chi} \Lambda(G)$$

según el lema 2.21, con cada  $e_{\chi} \Lambda(G)$  isomorfo a  $\Lambda = \Lambda(\Gamma)$ , donde  $\chi$  corre por los caracteres  $\Delta \rightarrow \mathcal{O}^\times$ .

Fijemos un subconjunto  $I \subseteq \text{Hom}(\Delta, \mathcal{O}^\times)$  y escribimos

$$\Lambda^I(G) := \bigoplus_{\chi \in I} e_{\chi} \Lambda(G).$$

Para cada  $\Lambda^I(G)$ -módulo  $M$  y  $\chi \in I$ ,  $e_{\chi} M$  es un  $e_{\chi} \Lambda(G)$ -módulo, y  $M$  tiene las propiedades «noetheriano» o «de torsion» como  $\Lambda^I(G)$ -módulo si y solo si cada  $e_{\chi} M$  para  $\chi \in I$  las tiene como  $e_{\chi} \Lambda(G)$ -módulo.

Desde ahora asumamos que  $M$  es un  $\Lambda^I(G)$ -módulo noetheriano y de torsion. Entonces para cada  $i \in I$  el teorema de estructura nos da una sucesión exacta

$$0 \rightarrow K_i \rightarrow \bigoplus_{j=1}^s \Lambda(\Gamma)/f_{ij} \rightarrow e_i M \rightarrow C_i \rightarrow 0$$

con  $K_i$  y  $C_i$  finitos, los  $f_{ij}$  siendo de la forma  $\pi^{\mu_j}$  o un polinomio distinguido, y donde  $s$  sin pérdida de generalidad *no* depende de  $i$  (eso lo podemos lograr para definir los  $f_{ij}$  superfluos como 1). Si definimos para  $j = 1, \dots, s$

$$g_j = (f_{ij})_{i \in I} \in \Lambda^I(G)$$

entonces obtenemos una sucesión exacta

$$0 \rightarrow K \rightarrow \bigoplus_{j=1}^s \Lambda^I(G)/g_j \rightarrow M \rightarrow C \rightarrow 0$$

con  $K$  y  $C$  finitos.

**Definición 3.22:** (a) Para cada  $\Lambda^I(G)$ -módulo noetheriano y de torsion  $M$ , su *ideal característico* es

$$\text{car}_{\Lambda^I(G)}(M) := (g_1 \cdots g_s) \subseteq \Lambda^I(G).$$

(b) Llamamos un  $\Lambda^I(G)$ -módulo  $E$  *elemental* si  $e_i E$  es elemental para cada  $i \in I$ , así que el módulo  $\bigoplus_j \Lambda^I(G)/g_j$  de arriba es un tal módulo.

### Ejercicios

**Ejercicio 3.12:** Verifique que el ideal característico de un  $\Lambda(\Gamma)$ -módulo noetheriano no depende del isomorfismo  $\Lambda(\Gamma) \simeq \mathcal{O}[[T]]$  inducido por la elección del generador topológico  $\gamma$  de  $\Gamma$ .

**Ejercicio 3.13:** Sea  $M$  un  $\Lambda^I(G)$ -módulo. Demuestre que  $M$  es

(a) noetheriano;

(b) de torsión

como  $\Lambda^I(G)$ -módulo si y solo si cada  $e_\chi M$  para  $\chi \in I$  lo es como  $e_\chi \Lambda(G)$ -módulo.

**Ejercicio 3.14:** Demuestre que el ideal característico es multiplicativo en sucesiones exactas, es decir para cada sucesión exacta

$$0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$$

de  $\Lambda^I(G)$ -módulos tenemos

$$\text{car}_{\Lambda^I(G)}(M) = \text{car}_{\Lambda^I(G)}(N) \text{car}_{\Lambda^I(G)}(Q).$$

## 3.6. Adjuntos de Iwasawa

Como en las secciones anteriores sea  $\Lambda = \mathcal{O}[[T]]$  con  $\mathcal{O}$  el anillo de enteros en una extensión finita  $L$  de  $\mathbb{Q}_p$ .

En esta sección seguimos [Sha, §3.5] para explicar los *adjuntos de Iwasawa*, que es una manera de asociar un módulo «adjunto»  $\alpha(M)$  a un  $\Lambda$ -módulo  $M$  noetheriano de torsión que de hecho es pseudo-isomorfo a  $M$ , introducidos por Iwasawa en [Iwa73]. En este texto vamos a usar esta teoría exclusivamente para demostrar la equivalencia de dos versiones de la Conjetura Principal de Iwasawa en la sección 6.2. El lector a gusto puede saltarse esta sección y volver a consultarla si se interesa en la demostración de dicha equivalencia.

Como preparación citamos una versión de la teoría de dualidad de Pontryagin, que vamos a necesitar a continuación.

**Definición 3.23:** Sea  $\mathcal{A}$  la categoría de  $\mathcal{O}$ -módulos topológicos Hausdorff localmente compactos cuya topología es definida por una base de vecindades de 0 que consiste en  $\mathcal{O}$ -submódulos. Además sea  $\mathcal{A}_{\text{comp}}$  la subcategoría llena de  $\mathcal{A}$  de módulos compactos y  $\mathcal{A}_{\text{disc}}$  la de módulos discretos.

Para cada módulo  $M \in \mathcal{A}$  sea

$$M^\vee := \text{Hom}_{\mathcal{O}}(M, L/\mathcal{O})$$

con la topología compacto-abierta (y donde « $\text{Hom}_{\mathcal{O}}$ » significa homomorfismos de  $\mathcal{O}$ -módulos topológicos). Este  $M^\vee$  se llama el *dual de Pontryagin* de  $M$ .

En las aplicaciones usaremos  $\Lambda$ -módulos noetherianos, que son elementos de la categoría  $\mathcal{A}$ .

**Teorema 3.24 (Pontryagin):** Para  $M \in \mathcal{A}$ ,  $M^\vee$  es nuevamente un elemento de  $\mathcal{A}$ . La asociación

$$(\cdot)^\vee : \mathcal{A} \rightarrow \mathcal{A}, \quad M \mapsto M^\vee$$

es un funtor contravariante aditivo que es una antiequivalencia de  $\mathcal{A}$  a sí mismo, y es un cuasi-inverso a sí mismo. Es decir, para cada módulo  $M \in \mathcal{A}$  hay un isomorfismo  $M \rightarrow M^{\vee\vee}$  natural en  $M$ . Este isomorfismo es dado por el mapeo canónico

$$M \rightarrow M^{\vee\vee}, \quad m \mapsto (f \mapsto f(m)).$$

Además,  $M^\vee$  es discreto si y solo si  $M$  es compacto, y viceversa. Es decir, el funtor  $(\cdot)^\vee$  induce antiequivalencias entre  $\mathcal{A}_{\text{comp}}$  y  $\mathcal{A}_{\text{disc}}$ .

*Demostración:* [SV16, Prop. 5.4] □

**Nota 3.25:** ¡El funtor  $(\cdot)^\vee: \mathcal{A} \rightarrow \mathcal{A}$  en general *no* conserva sucesiones exactas, aunque es una equivalencia de categorías! Recuerde que un funtor en general se llama *exacto* si conserva límites y colímites finitos (entre categorías que los admiten). Para funtores entre categorías abelianas esto es equivalente a pedir que conserve sucesiones exactas. Obviamente cada equivalencia de categorías (como  $(\cdot)^\vee$ ) es un funtor exacto, pero la categoría  $\mathcal{A}$  no es abeliana.

Sin embargo, si en una sucesion exacta

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

todos los módulos  $A, B, C$  son compactos o todos son discretos, entonces la sucesion dual

$$0 \rightarrow C^\vee \rightarrow B^\vee \rightarrow A^\vee \rightarrow 0$$

es también exacta. Esto es cierto porque las categorías  $\mathcal{A}_{\text{comp}}$  y  $\mathcal{A}_{\text{disc}}$  son abelianas; también puede ser visto como consecuencia de [SV16, Rem. 5.5].<sup>1</sup>

**Definición 3.26:** Usamos los polinomios

$$\omega_r = (T + 1)^{p^r} - 1 \in \Lambda$$

y  $\Phi_r \in \Lambda$  como en la definición 2.10, para cada  $r \in \mathbb{N}_{\geq 1}$ . Recuerde que  $\omega_r = \Phi_r \omega_{r-1}$  y los polinomios  $\Phi_r$  son irreducibles (ejercicio 2.1). Ponemos para cada  $r \geq m$

$$\nu_{r,m} := \frac{\omega_r}{\omega_m} = \Phi_r \cdots \Phi_{m+1}. \quad (3.1)$$

Los polinomios  $\nu_{r,m}$  y sus parientes serán importantes en las siguientes definiciones y afirmaciones. Como preparación demostramos algunas propiedades importantes de ellos. Fijamos un uniformizante  $\pi$  de  $\mathcal{O}$ .

**Lema 3.27:** *Sea  $M$  un  $\Lambda$ -módulo finito. Entonces existe  $s \gg 0$  y  $t \geq s$  tal que  $\Phi_s \cdots \Phi_t$  anula a  $M$ .*

*Demostración:* Sea  $I \subseteq \Lambda$  el anulador de  $M$ . Entonces  $I$  es el núcleo de la aplicación continua  $\Lambda \rightarrow \text{End}_\Lambda(M)$ , que demuestra que  $I$  es un ideal abierto (porque  $\text{End}_\Lambda(M)$  es finito). Por eso una potencia de  $T$  debe estar en  $I$ . Hacemos  $s \in \mathbb{N}_{\geq 1}$  tan grande tal que  $T^{p^s} \in I$ . Entonces

$$(1 + T)^{p^s} = 1 + \sum_{i=1}^{p^s-1} \binom{p^s}{i} T^{p^s-i} + T^{p^s} \equiv 1 + pg \pmod{I}$$

con  $g \in \Lambda$ . Esto implica que

$$\begin{aligned} \Phi_s &= \frac{(1 + T)^{p^s} - 1}{(1 + T)^{p^{s-1}} - 1} \\ &= (1 + T)^{(p-1)p^{s-1}} + (1 + T)^{(p-2)p^{s-1}} + \cdots + (1 + T)^{p^{s-1}} + 1 \\ &\equiv (1 + pg)^{p-1} + (1 + pg)^{p-2} + \cdots + (1 + pg) + 1 \\ &= ph \pmod{I} \end{aligned}$$

con algún  $h \in \Lambda$ . Esto tambien es cierto para los  $\Phi_{s'}$  con  $s' \geq s$ . Por la misma razón que con  $T$ , una potencia de  $p$  debe estar en  $I$ . Concluimos que existe  $t \geq s$  tal que  $\Phi_s \cdots \Phi_t \in I$ . □

<sup>1</sup> El teorema de categorías de Baire implica que morfismos entre módulos compactos siempre son estrictos (con una demostración similar a la del teorema de la función abierta).

**Lema 3.28:** Sea  $f \in \Lambda$  un polinomio distinguido. Entonces para  $s \gg 0$  suficientemente grande  $\Phi_s$  es divisible por  $\pi$  módulo  $f$ , es decir existe  $g \in \Lambda$  tal que

$$\Phi_s \equiv \pi g \pmod{f}.$$

*Demostración:* Sea  $d \in \mathbb{N}_{\geq 0}$  el grado de  $f$ . Entonces si  $s$  es tan grande tal que  $p^{s-1} \geq d$  tenemos  $(1+T)^{p^{s-1}} \equiv 1 + \pi h$  módulo  $f$ , con  $h \in \mathcal{O}[T]$ , porque  $f$  es distinguido. La afirmación resulta de un cálculo análogo a aquel que hicimos en la demostración del lema 3.27.  $\square$

**Lema 3.29:** Para cada  $\Lambda$ -módulo noetheriano  $M$  existe un  $m \in \mathbb{N}_{\geq 1}$  tal que para cada  $r \geq m$  los  $\nu_{r,m}$  son coprimos a  $\text{car}_\Lambda(M)$ .

*Demostración:* Esto es una consecuencia del teorema de estructura y (3.1), porque  $\Lambda$  es un dominio de factorización única y los  $\Phi_r$  son irreducibles.  $\square$

**Lema 3.30:** Sea  $M$  un  $\Lambda$ -módulo  $M$  noetheriano de torsión y sea  $m \in \mathbb{N}_{\geq 1}$  suficientemente grande tal que para  $r \geq m$  los  $\nu_{r,m}$  son coprimos a  $\text{car}_\Lambda(M)$ . Consideramos el módulo

$$A_m := \varinjlim_{r \geq m} M/\nu_{r,m}M$$

donde el mapeo  $M/\nu_{r,m}M \rightarrow M/\nu_{r+1,m}M$  con respecto a cual tomamos el límite es  $x \mapsto \frac{\omega_{r+1}}{\omega_r}x$ . Entonces  $A_m$  no depende de  $m$ .

*Demostración:* Estudiamos el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_r & \longrightarrow & \frac{M}{\Phi_{m+1} \cdots \Phi_r M} & \xrightarrow{\Phi_m} & \frac{M}{\Phi_m \cdots \Phi_r M} & \longrightarrow & \frac{M}{\Phi_m M} & \longrightarrow & 0 \\ & & \downarrow \Phi_{r+1} & & \downarrow \Phi_{r+1} & & \downarrow \Phi_{r+1} & & \downarrow \Phi_{r+1} & & \\ 0 & \longrightarrow & N_{r+1} & \longrightarrow & \frac{M}{\Phi_{m+1} \cdots \Phi_{r+1} M} & \xrightarrow{\Phi_m} & \frac{M}{\Phi_m \cdots \Phi_{r+1} M} & \longrightarrow & \frac{M}{\Phi_m M} & \longrightarrow & 0 \\ & & \downarrow \Phi_{r+2} & & \downarrow \Phi_{r+2} & & \downarrow \Phi_{r+2} & & \downarrow \Phi_{r+2} & & \\ 0 & \longrightarrow & N_{r+2} & \longrightarrow & \frac{M}{\Phi_{m+1} \cdots \Phi_{r+2} M} & \xrightarrow{\Phi_m} & \frac{M}{\Phi_m \cdots \Phi_{r+2} M} & \longrightarrow & \frac{M}{\Phi_m M} & \longrightarrow & 0 \\ & & \downarrow \Phi_{r+3} & & \downarrow \Phi_{r+3} & & \downarrow \Phi_{r+3} & & \downarrow \Phi_{r+3} & & \\ & & \vdots & & \vdots & & \vdots & & \vdots & & \end{array}$$

Aquí los mapeos con flechas etiquetadas son multiplicación por este elemento y los mapeos con flechas no etiquetadas son inclusiones o proyecciones canónicas. Los  $N_r, N_{r+1}, \dots$  en la primera columna sean definidos como los núcleos de la multiplicación por  $\Phi_m$ , así que las sucesiones horizontales son exactas.

El colímite de la segunda columna es  $A_m$  y el colímite de la tercera columna es  $A_{m-1}$  (supongamos que ya para  $r \geq m-1$  los  $\nu_{r,m}$  son coprimos a  $\text{car}_\Lambda(M)$ ). Tomar colímites de sistemas de módulos es un funtor exacto, por eso es suficiente demostrar que los colímites de las columnas exteriores son cero.

Estudiamos la primera columna. Sea  $i \in \mathbb{N}_{\geq 0}$  y  $x \in M$  un representante de un elemento de  $N_{r+i}$ . Entonces existe  $d \in M$  tal que  $\Phi_m x = \Phi_m \cdots \Phi_{r+i} d$ , es decir  $x - \Phi_{m+1} \cdots \Phi_{r+i} d \in M[\Phi_m]$  (donde  $M[\Phi_m]$  denota el núcleo de la multiplicación por  $\Phi_m$  en  $M$ ). Esto demuestra que la aplicación canónica

$$M[\Phi_m] \rightarrow N_{r+i} \subseteq M/\Phi_{m+1} \cdots \Phi_{r+i}M$$

es sobreyectiva para cada  $i$ .

Por el corolario 3.20  $M[\Phi_m]$  es finito. Notemos que también todos los módulos que aparecen en el diagrama son finitos (esto sigue del lema 3.18), en particular  $M/\Phi_m M$ . Entonces para que los colímites de las columnas exteriores sean ceros, es suficiente ver que cada elemento de un  $\Lambda$ -módulo finito está anulado si lo multiplicamos con  $\Phi_s \Phi_{s+1} \dots \Phi_t$  para  $t \geq s \gg r$  suficientemente grande. Esto lo hemos demostrado en el lema 3.27.  $\square$

**Definición 3.31:** Sea  $M$  un  $\Lambda$ -módulo  $M$  noetheriano de torsión.

(a) Hacemos  $M^\vee = \text{Hom}_{\mathcal{O}}(M, L/\mathcal{O})$  un  $\Lambda$ -módulo con la acción

$$\lambda f(m) = f(\lambda m) \quad \text{para } \lambda \in \Lambda, f \in M^\vee, m \in M.$$

(b) Definimos

$$\alpha(M) = \varprojlim_{r \geq m} (M/\nu_{r,m} M)^\vee = (\varinjlim_{r \geq m} M/\nu_{r,m} M)^\vee$$

con  $m$  como en el lema 3.30. Esto es un  $\Lambda$ -módulo que se llama el *adjunto de Iwasawa* de  $M$ .

En la definición 3.31 (b) la igualdad entre el límite y el colímite (que más bien es un isomorfismo canónico) es cierta porque el funtor  $(\cdot)^\vee$  es exacto (nota 3.25).

Más abstractamente se puede definir el adjunto de Iwasawa de un  $\Lambda$ -módulo noetheriano de torsión como  $\alpha(M) := \text{Ext}_\Lambda^1(M, \Lambda)$ , que puede ser útil porque se extiende directamente a situaciones más generales. Véase [NSWo8, Def. (5.5.5), Prop. (5.5.6)] para una demostración por que esto da lo mismo que la definición 3.31 (b).

Estudiamos algunas propiedades del funtor  $\alpha$ .

**Proposición 3.32:** *La asociación  $\alpha$  define un funtor contravariante aditivo de la categoría de  $\Lambda$ -módulos noetherianos de torsión a si misma, enviando sucesiones exactas a la derecha a sucesiones exactas a la izquierda.*

*Demostración:* Si  $M \rightarrow N$  es un morfismo de  $\Lambda$ -módulos noetherianos de torsión entonces podemos escoger  $m$  en la definición de  $\alpha$  suficientemente grande para ambos, así que obtenemos morfismos

$$M/\nu_{r,m} M \rightarrow N/\nu_{r,m} N \quad \text{para cada } r \geq m$$

y pues, aplicando  $(\cdot)^\vee$  y tomando el límite, un morfismo  $\alpha(N) \rightarrow \alpha(M)$ . Así  $\alpha$  define un funtor contravariante. Porque

$$M/\nu_{r,m} M = M \otimes_{\Lambda} \Lambda/\nu_{r,m} \Lambda$$

y el producto tensorial y la dualidad  $(\cdot)^\vee$  son aditivos,  $\alpha$  también es aditivo. Además,  $\alpha$  envía sucesiones exactas a la derecha a sucesiones exactas a la izquierda porque el producto tensorial es exacto a la derecha, la dualidad  $(\cdot)^\vee$  en este caso envía sucesiones exactas a sucesiones exactas (nota 3.25) y el funtor tomando el límite también es exacto porque tomamos límites de módulos finitos, para cuales la condición de Mittag-Leffler siempre es cierta. Falta ver que  $\alpha(M)$  nuevamente es noetheriano y de torsión. Esto va a resultar del teorema 3.34 abajo.  $\square$

**Proposición 3.33:** *El funtor  $\alpha$  envía pseudo-isomorfismos a pseudo-isomorfismos.*

*Demostración:* Sea  $M \rightarrow N$  un pseudo-isomorfismo. Como mencionamos en la demostración de la proposición 3.32, tomar el límite inverso y duales es exacto en módulos finitos. Por eso,  $\alpha(N) \rightarrow \alpha(M)$  es un pseudo-isomorfismo si y solo si las órdenes de los núcleos y conúcleos de

$$M/\nu_{r,m} M \rightarrow N/\nu_{r,m} N$$

son acotadas para  $r \rightarrow \infty$  (donde fijamos  $m$  suficientemente grande). Pero esto resulta del ejercicio 3.4 (b).  $\square$

La siguiente propiedad del funtor  $\alpha$  es la razón por qué es importante para nosotros.

**Teorema 3.34:** *Sea  $M$  un  $\Lambda$ -módulo noetheriano de torsión. Entonces existe un pseudo-isomorfo*

$$\alpha(M) \sim M.$$

*Demostración:* Sea  $E$  un  $\Lambda$ -módulo elemental y  $E \rightarrow M$  un pseudo-isomorfo. Aplicando  $\alpha$  a este pseudo-isomorfismo y usando la proposición 3.33 obtenemos un pseudo-isomorfismo de  $\Lambda$ -módulos  $\alpha(M) \rightarrow \alpha(E)$ . Por eso es suficiente demostrar la afirmación en el caso de un módulo elemental. Porque además  $\alpha$  es aditivo, es suficiente demostrar esto en los casos en que  $M = \Lambda/\pi^\mu$  con  $\mu \in \mathbb{N}_{\geq 1}$  y  $M = \Lambda/f$  con un polinomio distinguido  $f \in \Lambda$ .

Empezamos con el caso  $M = \Lambda/\pi^\mu$ . Ponemos  $\gamma = 1 + T$  y  $m = 0$ , entonces para cada  $r \geq 0$  tenemos  $\omega_r = \gamma^{p^r} - 1$  y  $1, \gamma, \gamma^2, \dots, \gamma^{p^r-1}$  es un  $\mathcal{O}$ -base de  $M/\nu_{r,0}M$ . Para cada  $f \in M/\nu_{r,0}M$  lo escribimos

$$f = \sum_{i=0}^{p^r-1} a_i \gamma^i, \quad a_i \in \mathcal{O}$$

y definimos

$$\psi_r: M/\nu_{r,0}M \rightarrow (M/\nu_{r,0}M)^\vee, \quad \psi_r(f)(\gamma^i) = \frac{a_i}{\pi^\mu}.$$

Entonces se puede verificar directamente que  $\psi_r$  es biyectivo,  $\Lambda$ -lineal y que el diagrama

$$\begin{array}{ccc} M/\nu_{r+1,0}M & \xrightarrow{\psi_{r+1}} & (M/\nu_{r+1,0}M)^\vee \\ \downarrow & & \downarrow \\ M/\nu_{r,0}M & \xrightarrow{\psi_r} & (M/\nu_{r,0}M)^\vee \end{array}$$

es conmutativo (aquí el mapeo a la izquierda es la proyección canónica y el mapeo a la derecha es dual a la multiplicación con  $\Phi_{r+1}$  en  $M/\nu_{r,0}M \rightarrow M/\nu_{r+1,0}M$ . Tomando el límite obtenemos  $\alpha(M) \simeq \varprojlim_r M/\nu_{r,0}M$ . La afirmación pues resulta porque  $M = \Lambda/\pi^\mu$  y  $\bigcap_{r \geq 0} \omega_r \Lambda = 0$  (véase la demostración del teorema 2.11).

Ahora sea  $M = \Lambda/(f)$  y sea  $d \in \mathbb{N}_{\geq 1}$  el grado de  $f$ . Entonces el lema 3.28 dice que  $\Phi_r$  para  $r \gg 0$  actúa en  $M$  como multiplicación con una potencia de  $\pi$ . Esto implica que

$$\begin{aligned} \alpha(M) &\simeq \varprojlim_{s \in \mathbb{N}_{\geq 1}} (M/\pi^s M)^\vee = \varprojlim_{s \in \mathbb{N}_{\geq 1}} \text{Hom}_{\mathcal{O}}(M/\pi^s M, L/\mathcal{O}) \\ &\simeq \varprojlim_{s \in \mathbb{N}_{\geq 1}} \text{Hom}_{\mathcal{O}}(M/\pi^s M, \mathcal{O}/\pi^s) \simeq \text{Hom}_{\mathcal{O}}(M, \mathcal{O}) \end{aligned}$$

como  $\Lambda$ -módulos, donde  $\Lambda$  actúa en  $\text{Hom}_{\mathcal{O}}(M, \mathcal{O})$  como  $(\lambda\phi)(m) = \phi(\lambda m)$  para  $\lambda \in \Lambda$ ,  $\phi \in \text{Hom}_{\mathcal{O}}(M, \mathcal{O})$  y  $m \in M$ . El lema de división (lema 2.3) nos permite escribir cada  $g \in \Lambda$  como  $g = qf + r$  con únicos  $q, r \in \Lambda$  y  $r$  un polinomio de grado  $< d$ . Definimos un mapeo

$$\varepsilon: \Lambda \rightarrow \mathcal{O}$$

que envía  $g$  al coeficiente de  $T^{d-1}$  en este  $r$ . Usando esto definimos

$$\theta: M = \Lambda/(f) \rightarrow M^\vee = \text{Hom}_{\mathcal{O}}(M, \mathcal{O}), \quad g \mapsto [h \mapsto \varepsilon(gh)]$$

Se verifica que esto es un morfismo de  $\Lambda$ -módulos bien definido. Si  $r \in \mathcal{O}[T]$  es un polinomio de grado  $k < d$  no nulo, que es representante de un elemento no nulo de  $M$ , entonces  $\theta(r)(T^{d-1-k}) = \varepsilon(T^{d-1-k}r) \neq 0$ , por eso  $\theta$  es inyectivo. Porque los  $\mathcal{O}$ -rangos de  $M$  y  $\text{Hom}_{\mathcal{O}}(M, \mathcal{O})$  son iguales, el conúcleo de  $\theta$  tiene que ser finito, así que  $\theta$  es un pseudo-isomorfismo.<sup>2</sup>  $\square$

<sup>2</sup> De hecho,  $\theta$  es incluso sobreyectivo, es decir un isomorfismo, pero lo no necesitaremos y omitimos la demostración.

Concluimos esta sección con generalizar los resultados al caso de módulos sobre el álgebra de Iwasawa para grupos más grandes, como en la sección 2.3. Sólo discutimos esto en el caso que vamos a necesitar en la aplicación, que es el en que  $G = \Delta \times \Gamma$  con  $\Delta \simeq \mathbb{F}_p^\times$  y  $\Gamma \simeq \mathbb{Z}_p$ . Fijemos estos isomorfismos, así que obtenemos un isomorfismo  $\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]]$ . En el resultados siguientes, sólo nos interesamos en la existencia de un pseudo-isomorfismo y no nos importa si sea canónico o no – de hecho, el pseudo-isomorfismo depende de los elecciones que hicimos, pero esto nos da igual.

Gracias al corolario 2.22, podemos identificar  $\mathcal{O}[[G]]$  con  $(\mathcal{O}[[T]])^{p-1}$ , así que un módulo sobre  $\mathcal{O}[[G]]$  es lo mismo que  $p-1$  módulos sobre  $\mathcal{O}[[T]]$ .

**Definición 3.35:** Sea  $M$  un  $\mathcal{O}[[G]]$ -módulo noetheriano de torsión. Para  $r \in \mathbb{N}_{\geq 1}$  sea  $w_r \in \mathcal{O}[[G]]$  el elemento que corresponde a  $(\omega_r, \dots, \omega_r) \in (\mathcal{O}[[T]])^{p-1}$ . Entonces definimos

$$\alpha(M) = \varprojlim_{r \geq m} (M / \frac{w_r}{w_m} M)^\vee = (\varinjlim_{r \geq m} M / \frac{w_r}{w_m} M)^\vee$$

con  $m$  suficientemente grande, de manera análoga a la definición 3.31 (b). Equivalentemente, obtenemos  $\alpha(M)$  via aplicar  $\alpha$  a cada uno de los  $p-1$  módulos sobre  $\mathcal{O}[[T]]$ , es decir

$$\alpha(M) = \bigoplus_{i=1}^{p-1} \alpha(e_{\omega^i} M).$$

**Corolario 3.36:** Sea  $M$  un  $\mathcal{O}[[G]]$ -módulo noetheriano de torsión. Entonces existe un pseudo-isomorfo

$$\alpha(M) \sim M.$$

*Demostración:* Esto resulta directamente del teorema 3.34, aplicandolo en cada componente separadamente.  $\square$

### Ejercicios

**Ejercicio 3.15:** Demuestre que las diferentes descripciones de  $\alpha(M)$  en la definición 3.35 son equivalentes. Use el ejercicio 2.14 para esto.

**Ejercicio 3.16:** Demuestre que si  $M$  es un  $\Lambda$ -módulo finito entonces  $\alpha(M) = 0$ . Use el lema 3.28 para esto.



# Capítulo 4

## Grupos de clases y el teorema de Iwasawa

La teoría que desarrollamos en los capítulos 2 y 3 todavía no tiene nada que ver con aritmética. En este capítulo empezamos a conectarla con objetos aritméticos, más precisamente con grupos de clases de campos de números. Que uno puede estudiar los grupos de clases con estos métodos fue una de las ideas más importantes de Iwasawa, y a continuación vamos a ilustrar que tan prolífico es este enfoque. Vamos a obtener resultados sobre grupos de clases como el famoso teorema I de Iwasawa y muchos más. Aparte de ser interesantes para sí mismo, algunos resultados también preparan el lado algebraico de la Conjetura Principal, que estudiaremos en el capítulo 6.

### 4.1. Grupos de Clases en Extensiones Ciclotómicas

Comenzamos esta sección con algunos teoremas sobre grupos de clases que luego nos serán útiles. Sea  $K$  un campo de números y  $\mathcal{O}_K$  su anillo de enteros.

**Teorema 4.1:** *Supongamos que  $L/K$  es una extensión de campos de números que no contiene ninguna extensión no trivial  $F$  no ramificada de  $K$ . Entonces el número de clases  $h_K$  divide a  $h_L$ . Además, la aplicación norma (definición 1.23) de  $\text{Cl}_L$  a  $\text{Cl}_K$  es sobreyectiva.*

*Demostración:* Sea  $H$  la máxima extensión no ramificada de  $K$ . Por la teoría de campos de clases  $\text{Gal}(H/K) \simeq \text{Cl}_K$  (teorema 1.38). Además por hipótesis  $H \cap L = K$ . Entonces  $LH/L$  es una extensión abeliana no ramificada de índice  $[LH : L] = [H : K]$ , que además está contenida en la máxima extensión no ramificada  $M$  de  $L$ . El resultado sigue del siguiente diagrama

$$\begin{array}{ccc} \text{Cl}_L & \xrightarrow{\sim} & \text{Gal}(M/L) \\ \downarrow \text{Norm} & & \downarrow \text{Res} \\ \text{Cl}_K & \xrightarrow{\sim} & \text{Gal}(H/K). \end{array} \quad \square$$

**Lema 4.2:** *Sean  $G$  un  $p$ -grupo e  $I$  un subgrupo propio de  $G$ . Existe un subgrupo normal  $G_1$  de  $G$  de índice  $p$  que contiene a  $I$ .*

*Demostración:* Vamos a proceder por inducción sobre  $G$ . Supongamos que para todo  $p$ -grupo  $H$  con  $|H| < |G|$  y un subgrupo propio  $I' < H$ , existe un subgrupo normal  $G'_1 < H$  de índice  $p$  con  $I' \subseteq G'_1$ .

Para  $a$  un elemento en el centro  $Z(G)$  de orden  $p$  sean

$$H = G/\langle a \rangle \quad \text{e} \quad I' = I/\langle a \rangle \cap I.$$

Por la hipótesis de inducción existe un subgrupo  $G'_1$  de  $H$  de índice  $p$  tal que  $I' \subseteq G'_1$ .

Sea  $\pi$  la proyección de  $G$  en  $H$ . Sea  $G_1 = \langle \pi^{-1}(G'_1), a \rangle$ .  $G_1$  es un subgrupo normal de  $G$  y además contiene a  $I$ . Por último, es fácil ver que

$$G/G_1 \rightarrow H/G'_1$$

es un isomorfismo de grupos de orden  $p$ .  $\square$

**Teorema 4.3:** *Sea  $L/K$  una extensión de Galois finita de campos de números y  $\text{Gal}(L/K)$  es un  $p$ -grupo. Supongamos que existe a lo más un primo ramificado en  $L$ , además si  $p \mid h_L$  entonces  $p \mid h_K$ .*

*Demostración:* Supongamos que  $p \mid h_L$ . Sean  $M$  y  $H$  las máximas  $p$ -extensiones no ramificadas de  $L$  y  $K$  respectivamente. Por la teoría de campos de clases tenemos  $\text{Cl}_L(p) = \text{Gal}(M/L)$  y  $\text{Cl}_K(p) = \text{Gal}(H/K)$ . La extensión  $M/K$  es de Galois pues  $M/L$  es máxima, denotamos  $G = \text{Gal}(M/K)$ .

Supongamos que  $L/K$  no es ramificada. Vamos a proceder por inducción. Como  $G$  es un  $p$ -grupo admite una secuencia de subgrupos

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_n = G$$

tal que  $G_i$  es normal en  $G$  y  $G_{i+1}/G_i$  es cíclico de orden  $p$  [Lan02, Cor. 6.6 I.§6]. Entonces basta probar que  $p \mid h_{L_1}$  para  $L/L_1$ , donde  $L_1$  es la subextensión de  $L$  fijada por  $G_1$ . El resultado sigue del hecho que  $L/L_1$  es abeliana no ramificada de índice  $p$ . Por lo tanto  $p \mid h_K$ .

Ahora supongamos que  $\mathfrak{p}$  en  $K$  ramifica. Sea  $\mathfrak{P}$  el primo de  $L$  arriba de  $\mathfrak{p}$ . Sea  $I_{\mathfrak{P}}$  el subgrupo de inercia de  $\mathfrak{P}$  en  $G$ . Como  $M/L$  no es ramificada, entonces  $L \cap H = K$ , además

$$|I_{\mathfrak{P}}| \leq [L : K] < |G|.$$

Por el lema 4.2 tenemos que existe un subgrupo normal  $G_1$  de  $G$  de índice  $p$ , tal que  $I \leq G_1$ . Los grupos de inercia de otros primos de  $M$  son conjugados de  $I_{\mathfrak{P}}$  y por lo tanto están contenidos en  $G_1$ . Pero  $G_1$  fija una extensión de Galois de  $K$  de índice  $p$ , por lo tanto abeliana, es decir  $p \mid h_K$ .  $\square$

El teorema precedente y el teorema 4.1 aplicados a extensiones ciclotómicas nos dan el siguiente resultado.

**Corolario 4.4:** *Sea  $r \in \mathbb{N}_{\geq 1}$ , entonces*

$$p \mid h_{\mathbb{Q}(\mu_p)} \iff p \mid h_{\mathbb{Q}(\mu_{p^r})}.$$

*Demostración:* Recordemos que el único primo que ramifica en  $\mathbb{Q}(\mu_{p^r})$  es  $p$ , además es totalmente ramificado (proposición 1.29). Entonces  $(\Leftarrow)$  es claro por el teorema 4.3 y  $(\Rightarrow)$  se sigue del teorema 4.1.  $\square$

Terminamos esta sección con un resultado clásico de Kummer, que será utilizado en la demostración de que la Conjetura Principal de Iwasawa implica al criterio de Kummer del teorema II.

**Teorema 4.5 (Kummer):** *Sea  $K = \mathbb{Q}(\mu_p)$  y  $C$  la  $p$ -parte del grupo de clases de  $K$ . Escribimos  $C^{\pm}$  para los subgrupos donde la conjugación compleja actúa por  $\pm 1$ , respectivamente. Entonces*

$$C^- = 0 \iff C = 0.$$

*En otras palabras,  $p \mid h_p \iff p \mid h_p^-$ , donde  $h_p = h_{\mathbb{Q}(\mu_p)}$ ,  $h_p^+ = h_{\mathbb{Q}(\mu_p)^+}$  y  $h_p^- = h_p/h_p^+$ , con  $\mathbb{Q}(\mu_p)^+$  siendo el subcampo de  $\mathbb{Q}(\mu_p)$  fijo por la conjugación compleja.*

*Demostración:* Seguimos [Lang0, Thm. 13.2.1] o [Was97, §10.2, esp. Thm. 10.11]. Sea  $L/K$  la extensión máxima abeliana no ramificada de exponente  $p$ , que es una extensión de Kummer, y sea  $G := \text{Gal}(L/K)$ . Entonces  $G \simeq C(p)$  por la teoría de campos de clases (teorema 1.38), donde  $C(p)$  es la  $p$ -torsión de  $C$ , que es un espacio vectorial sobre  $\mathbb{F}_p$ . Según el ejercicio 1.7,

este isomorfismo es equivariante para la acción de la conjugación compleja  $\mathbf{c} \in \text{Gal}(K/\mathbb{Q})$ , donde esta actúa en  $G$  por conjugación con un levantamiento  $\tilde{\mathbf{c}} \in \text{Gal}(L/\mathbb{Q})$  de  $\mathbf{c}$  que fijamos por el resto de la demostración. Vamos a demostrar

$$\dim_{\mathbb{F}_p} C(p)^+ \leq \dim_{\mathbb{F}_p} C(p)^-,$$

que implica la afirmación.

Usamos la teoría de Kummer descrito en la proposición 1.33. Sea  $\Delta := (L^\times)^p \cap K^\times$  y  $V = \sqrt[p]{\Delta}/(\sqrt[p]{\Delta} \cap K^\times)$ , así que  $L = K(\sqrt[p]{\Delta})$  y tenemos un apareamiento perfecto

$$G \times V \rightarrow \mu_p$$

de espacios vectoriales sobre  $\mathbb{F}_p$ . El grupo  $\text{Gal}(L/\mathbb{Q})$  actúa naturalmente en  $V$ , y esto nos da una acción de  $\tilde{\mathbf{c}} \in \text{Gal}(L/\mathbb{Q})$  en  $V$ ; escribimos  $V^\pm$  para las partes donde  $\tilde{\mathbf{c}}$  actúa por  $\pm 1$ . Según la proposición 1.34 el apareamiento tiene la propiedad

$$\langle \tilde{\mathbf{c}}\sigma\tilde{\mathbf{c}}^{-1}, \tilde{\mathbf{c}}v \rangle = \mathbf{c} \langle \sigma, v \rangle \quad \text{para cada } \sigma \in G, v \in V.$$

Porque  $p \neq 2$ , los únicos elementos en  $\mu_p$  fijos por  $\mathbf{c}$  son  $\pm 1$ , y porque  $G$  y  $V$  son espacios vectoriales sobre  $\mathbb{F}_p$ , la propiedad anterior implica que la restricción del apareamiento a  $G^+ \times V^+$  es trivial (aquí usamos el ejercicio 1.2). Ya que  $V = V^+ \oplus V^-$ , el apareamiento pues se restringe a un apareamiento perfecto

$$G^+ \times V^- \rightarrow \mu_p$$

y por eso  $\dim_{\mathbb{F}_p} C(p)^+ = \dim_{\mathbb{F}_p} G^+ = \dim_{\mathbb{F}_p} V^-$ .

Sea  $b \in \sqrt[p]{\Delta} \subseteq L^\times$ . Entonces  $K(b)/K$  no es ramificado, y según la proposición 1.36 el ideal fraccional generado por  $b^p \in K^\times$  entonces tiene que ser de la forma  $(b^p) = \mathfrak{b}^p$  con un ideal fraccional  $\mathfrak{b}$  de  $K$ . Esto nos permite definir un homomorfismo

$$\varphi: V \rightarrow C(p), \quad b \mapsto \mathfrak{b}$$

que es obviamente equivariante para la conjugación compleja y pues induce

$$\varphi^-: V^- \rightarrow C(p)^-.$$

Vamos a demostrar que  $\varphi^-$  es inyectivo, que termina la demostración.

Fijamos  $b \in \sqrt[p]{\Delta}$  tal que su clase en  $V$  está en el núcleo de  $\varphi^-$ . Entonces podemos escribir  $b^p = a^p u$  con  $a \in K^\times$  y  $u \in \mathcal{O}_K^\times$ . El elemento  $u$  no es únicamente determinado, pero su clase en  $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p$  sí lo es, y está en  $(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p)^-$ . Según la proposición 1.26 podemos escribir  $u \in \mathcal{O}_K$  como  $u = \zeta v$  con  $\zeta \in \mu_p$  y  $v \in (\mathcal{O}_K^\times)^+$ . Entonces  $\bar{u} = \zeta^{-1}v$  y también  $\bar{u} = u^{-1}c^p = \zeta^{-1}v^{-1}c^p$  con algún  $c \in (\mathcal{O}_K^\times)^+$ , y obtenemos  $v^2 = c^p$ . Pero según el teorema de las unidades de Dirichlet,  $(\mathcal{O}_K^\times)^+$  es  $\{\pm 1\}$  por un grupo abeliano libre, que implica que  $v \in (\mathcal{O}_K^\times)^p$ , digamos  $v = w^p$ . Concluimos que  $b^p = (aw)^p \zeta$ . El campo  $L$  contiene  $K(b) = K(\sqrt[p]{\zeta})$ , pero porque  $L$  no es ramificado,  $\zeta = 1$ . Por eso  $b = aw\xi$  con algún  $\xi \in \mu_p$ , es decir  $b \in K^\times$ , así que su clase en  $V$  es trivial.  $\square$

## Ejercicios

**Ejercicio 4.1:** Para  $r \in \mathbb{N}_{\geq 1}$  sea  $h_{p^r} = h_{\mathbb{Q}(\mu_{p^r})}$ . Además sea  $\mathbb{Q}(\mu_{p^r})^+$  el subcampo de  $\mathbb{Q}(\mu_{p^r})$  fijo por la conjugación compleja,  $h_{p^r}^+$  su número de clases y  $h_{p^r}^- = h_{p^r}/h_{p^r}^+$ .

Demuestre que

$$p \mid h_p^- \iff p \mid h_{p^r}^-,$$

usando el corolario 4.4 y el teorema 4.5.

## 4.2. Extensiones $\mathbb{Z}_p$

Sea  $K$  un campo de números y  $p$  un número primo.<sup>1</sup> Sea  $K_\infty$  una extensión de Galois infinita de  $K$ , decimos que  $K_\infty$  es una  $\mathbb{Z}_p$ -extensión (igualmente llamada extensión  $\mathbb{Z}_p$ ) si  $\text{Gal}(K_\infty/K)$  es isomorfo al grupo aditivo del anillo  $\mathbb{Z}_p$  de los enteros  $p$ -ádicos.

**Proposición 4.6:** *Todo campo de números  $K$  tiene una  $\mathbb{Z}_p$ -extensión.*

*Demostración:* La extensión ciclotómica  $\mathbb{Q}(\mu_{p^r})/\mathbb{Q}$  obtenida al agregar una raíz primitiva  $p^r$ -ésima de la unidad es abeliana, de grado  $\varphi(p^r) = (p-1)p^{r-1}$  y de grupo de Galois  $\text{Gal}(\mathbb{Q}(\mu_{p^r})/\mathbb{Q})$  isomorfo a  $(\mathbb{Z}/p^r\mathbb{Z})^\times$  para todo  $r \geq 0$ . Consideremos la extensión infinita

$$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{r \geq 0} \mathbb{Q}(\mu_{p^r}),$$

su grupo de Galois  $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$  es isomorfo a  $\varprojlim_n (\mathbb{Z}/p^r\mathbb{Z})^\times \simeq \mathbb{Z}_p^\times$ . Por el lema de representación (lema 1.40) tenemos  $\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$ . Sea  $\mathbb{Q}^c$  la subextensión de  $\mathbb{Q}(\mu_{p^\infty})$  fijada por  $(\mathbb{Z}/p\mathbb{Z})^\times$ , entonces  $\text{Gal}(\mathbb{Q}^c/\mathbb{Q}) \simeq \mathbb{Z}_p$ .

Sea  $K^c = K\mathbb{Q}^c$  y sea  $F = \mathbb{Q}^c \cap K$ , entonces

$$\text{Gal}(\mathbb{Q}^c/F) \simeq \text{Gal}(K^c/K)$$

son isomorfos. Tenemos  $\text{Gal}(\mathbb{Q}^c/F) \simeq p^k\mathbb{Z}_p$  para algún  $k \in \mathbb{N}_{\geq 1}$ , pero  $p^k\mathbb{Z}_p \simeq \mathbb{Z}_p$ , entonces  $\text{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$ .  $\square$

La  $\mathbb{Z}_p$ -extensión construida en la proposición 4.6 se llama la  $\mathbb{Z}_p$ -extensión ciclotómica de  $K$  y en ocasiones la denotamos  $K^c$ .

Sea  $K_\infty/K$  una  $\mathbb{Z}_p$ -extensión. Por la teoría de Galois infinita los subgrupos cerrados de  $\mathbb{Z}_p$  corresponden a subextensiones de  $K_\infty$ . Es fácil de ver que bajo la topología  $p$ -ádica los subgrupos cerrados (abiertos) de  $\mathbb{Z}_p$  son de la forma  $p^r\mathbb{Z}_p$ . Por lo que los subgrupos cerrados de  $\mathbb{Z}_p$  fijan extensiones finitas  $K_r$  de  $K$  tales que  $\text{Gal}(K_r/K) \simeq \mathbb{Z}/p^r\mathbb{Z}$ . Es decir, una  $\mathbb{Z}_p$ -extensión  $K_\infty$  es una torre infinita de campos de números

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty = \bigcup_{r \geq 0} K_r, \quad (4.1)$$

tal que  $\text{Gal}(K_r/K) \simeq \mathbb{Z}/p^r\mathbb{Z}$ .

A continuación mencionamos algunas propiedades sobre ramificación en las  $\mathbb{Z}_p$ -extensiones. Comenzamos con un teorema que nos será útil más adelante para explicar la conjetura de Leopoldt.

**Proposición 4.7:** *Sea  $L$  una extensión abeliana de un campo de números  $K$  tal que  $\text{Gal}(L/K) \simeq \mathbb{Z}_p^d$  para algún entero  $d \geq 0$ . Entonces  $L/K$  es no ramificado fuera de  $p$ .*

*Demostración:* Sea  $\mathfrak{p}$  una plaza de  $K$  que no divide a  $p$ . Sea  $I_{\mathfrak{p}}$  el subgrupo de inercia de  $\mathfrak{p}$  en  $\text{Gal}(K^{\text{ab}}/K)$ . Por la teoría de campos de clases la imagen de  $I_{\mathfrak{p}}$  en  $\text{Gal}(L/K)$  es finita. Sin embargo, el grupo  $\mathbb{Z}_p^d$  es libre de torsión, por lo tanto el subgrupo de inercia de  $\mathfrak{p}$  en  $\text{Gal}(L/K)$  es nulo.  $\square$

**Proposición 4.8:** *Sea  $K_\infty$  una  $\mathbb{Z}_p$ -extensión de un campo de números  $K$ . Entonces al menos una plaza  $\mathfrak{p}$  arriba de  $p$  ramifica en  $K_\infty/K$ .*

<sup>1</sup> Como siempre, suponemos que  $p$  es impar para facilitar la exposición, pero los resultados tienen análogos en el caso  $p = 2$ .

*Demostración:* Supongamos que ninguna plaza  $\mathfrak{p} \mid p$  ramifica. En particular por la proposición 4.7 esto implicaría que  $K_\infty/K$  es no ramificada, pero la máxima extensión no ramificada de un campo de números es una extensión finita.  $\square$

Para un campo de números  $K$  denotamos  $[K : \mathbb{Q}]$  su dimensión como espacio vectorial sobre  $\mathbb{Q}$ . Además denotamos  $r$  el número de encajes reales  $K \hookrightarrow \mathbb{R}$  y  $c$  el número de pares de encajes complejos conjugados  $K \hookrightarrow \mathbb{C}$ .

Si  $X$  es un  $\mathbb{Z}_p$ -módulo compacto, entonces  $X/pX$  (resp.  $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ ) es un espacio vectorial sobre  $\mathbb{F}_p$  (resp. sobre  $\mathbb{Q}_p$ ).

**Definición 4.9:** Llamamos *rango de  $X$  sobre  $\mathbb{F}_p$*  (resp. *sobre  $\mathbb{Z}_p$* ) a la dimensión de  $X/pX$  (resp. a la dimensión de  $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ ) y lo denotamos  $\text{rg}_{\mathbb{F}_p}(X)$  (resp.  $\text{rg}_{\mathbb{Z}_p}(X)$ ).

**Teorema 4.10:** Sea  $M$  la máxima extensión pro- $p$  abeliana no ramificada fuera de  $p$  de un campo de números  $K$ . Entonces  $\text{rg}_{\mathbb{F}_p}(\text{Gal}(M/K))$  es finito y

$$c + 1 \leq \text{rg}_{\mathbb{Z}_p} \text{Gal}(M/K) \leq [K : \mathbb{Q}].$$

*Demostración:* Para una plaza  $\mathfrak{p}$  de  $K$  sobre  $p$ , sea  $U_{\mathfrak{p}}^{(1)}$  el grupo de unidades principales del campo local  $K_{\mathfrak{p}}$ . Consideremos el producto

$$U = \prod_{\mathfrak{p} \mid p} U_{\mathfrak{p}}^{(1)}$$

y sea  $E = \{\varepsilon \in K \mid \varepsilon \in U_{\mathfrak{p}}^{(1)} \text{ para todo } \mathfrak{p} \mid p\}$ . Denotamos  $\overline{E}$  la cerradura de  $E$  en  $U$ , y denotamos  $H'$  la extensión máxima no ramificada de  $K$  en  $K_\infty$ , que por la teoría de campos de clases debe ser finita y además

$$\text{Gal}(M/H') \simeq U/\overline{E}$$

De aquí deducimos que  $\text{rg}_{\mathbb{F}_p}(\text{Gal}(M/K))$  es finito, ya que  $\text{rg}_{\mathbb{F}_p}(\text{Gal}(M/H'))$  es finito y  $\text{rg}_{\mathbb{F}_p}(U)$  es finito, pues el grupo de unidades principales  $U_{\mathfrak{p}}^{(1)}$  de un campo local  $K_{\mathfrak{p}}$  es el producto de un grupo cíclico finito y de un  $\mathbb{Z}_p$ -módulo de rango  $[K_{\mathfrak{p}} : \mathbb{Q}_p]$  según la proposición 1.45. Por esta última observación también tenemos que

$$\begin{aligned} \text{rg}_{\mathbb{Z}_p}(U) &= \sum_{\mathfrak{p} \mid p} \text{rg}_{\mathbb{Z}_p} U_{\mathfrak{p}} \\ &= \sum_{\mathfrak{p} \mid p} [K_{\mathfrak{p}} : \mathbb{Q}_p] \\ &= [K : \mathbb{Q}]. \end{aligned}$$

Recordemos que por el teorema de Dirichlet, el anillo de enteros  $O_K$  de  $K$  es un producto de un grupo finito y de un  $\mathbb{Z}$ -módulo libre de dimensión  $r + c - 1$  generado por las unidades fundamentales. La imagen de las unidades fundamentales bajo los encajes  $K^\times \hookrightarrow K_{\mathfrak{p}}^\times$  está en  $U_{\mathfrak{p}}^{(1)}$  para toda plaza  $\mathfrak{p} \mid p$ . Por lo tanto,  $\text{rg}_{\mathbb{Z}_p} \overline{E} \leq r + c - 1$ . Finalmente como

$$\text{rg}_{\mathbb{Z}_p} \text{Gal}(M/K) = \text{rg}_{\mathbb{Z}_p} \text{Gal}(M/H') = \text{rg}_{\mathbb{Z}_p}(U) - \text{rg}_{\mathbb{Z}_p}(\overline{E}),$$

tenemos  $c + 1 \leq \text{rg}_{\mathbb{Z}_p}(\text{Gal}(M/K)) \leq [K : \mathbb{Q}]$ .  $\square$

**Teorema 4.11:** Sea  $\widehat{K}$  el compuesto de todas las  $\mathbb{Z}_p$ -extensiones de un campo de números. Entonces  $\widehat{K}/K$  es una extensión abeliana y  $\text{Gal}(\widehat{K}/K) \simeq \mathbb{Z}_p^d$ , donde  $d = \text{rg}_{\mathbb{Z}_p} \text{Gal}(M/K)$ .

*Demostración:* Por la proposición 4.7 la extensión  $\widehat{K}$  está contenida en  $M$ . Por la teoría de Galois, el rango con respecto a  $\mathbb{Z}_p$  del grupo de Galois  $\text{Gal}(M/\widehat{K})$  es nulo.  $\square$

**Conjetura 4.12 (Conjetura de Leopoldt):** *Sea  $d$  el rango sobre  $\mathbb{Z}_p$  de  $\text{Gal}(\widehat{K}/K)$ , entonces  $d = c + 1$ , es decir, existen  $c + 1$   $\mathbb{Z}_\ell$ -extensiones independientes sobre  $K$ .*

Existen muchas versiones equivalentes de esta conjetura a través de cuales es relacionada con varios objetos, una lista se encuentra en [NSWo8, (10.3.6)]. Esto enfatiza en la importancia de la conjetura – por ejemplo tiene que ver con las funciones  $L$   $p$ -ádicas que vamos a estudiar en el capítulo 5; véase [Was97, §5.5] para más sobre esta conexión. La conjetura de Leopoldt es conocida en el caso especial en que  $K$  es una extensión abeliana de los números racionales  $\mathbb{Q}$  o de un campo cuadrático imaginario.

### Ejercicios

**Ejercicio 4.2:** Sea  $K^c$  la  $\mathbb{Z}_p$ -extensión ciclotómica de un campo de números  $K$ . Demuestre que  $K^c$  es ramificada en todo primo  $\mathfrak{p}$  sobre  $p$ . Además demuestre que si  $K = \mathbb{Q}$ , entonces  $K^c$  es totalmente ramificada en  $p$ .

**Ejercicio 4.3:** Demuestre que si  $K = \mathbb{Q}$  entonces sólo hay una  $\mathbb{Z}_p$ -extensión de  $\mathbb{Q}$ , i. e. la  $\mathbb{Z}_p$ -extensión ciclotómica.

## 4.3. Propiedades de los grupos de clases como $\Lambda$ -módulos

Sea  $\Lambda = \mathbb{Z}_p[[T]]$  el álgebra de Iwasawa con coeficientes en  $\mathbb{Z}_p$ . Recordemos que en este caso  $\mathfrak{M} = (p, T)$ . En la sección 3.4 demostramos algunas propiedades de los  $\Lambda$ -módulos compactos. Estas nos serán útiles aquí pues los  $\Lambda$ -módulos con que trabajaremos son finitamente generados, y estos son compactos por ser la imagen continua de  $\Lambda^d$  para algún  $d$ .

Sea  $K_\infty/K$  una  $\mathbb{Z}_p$ -extensión de grupo de Galois  $\Gamma = \text{Gal}(K_\infty/K)$  y sea  $L_\infty$  una extensión abeliana de  $K_\infty$  tal que  $L_\infty/K$  es una extensión de Galois de grupo  $G = \text{Gal}(L_\infty/K)$ . Si denotamos  $X = \text{Gal}(L_\infty/K_\infty)$  tenemos que  $\Gamma$  actúa continuamente por conjugación en  $X$

$$x^\gamma = \tilde{\gamma}x\tilde{\gamma}^{-1} \quad \text{para todo } x \in X \text{ y } \gamma \in \Gamma, \quad (4.2)$$

donde  $\tilde{\gamma}$  es un levantamiento de  $\gamma$  a  $G$ . Esta construcción de hecho es un patrón general, véase el ejercicio 4.4. En nuestra situación  $X$  es un subgrupo cerrado normal de  $G$  tal que

$$\Gamma \simeq G/X.$$

Fijando un generador  $\gamma \in \Gamma$  podemos extender la acción de  $\Gamma$  sobre  $X$  al álgebra de Iwasawa  $\Lambda$  (teorema 2.11), i. e. hacemos de  $X$  un  $\Lambda$ -módulo compacto. Además, como  $\Gamma$  es un  $\mathbb{Z}_p$ -módulo libre, existe una sección de  $\mathbb{Z}_p$ -módulos que describe el producto semi-directo

$$G = \Gamma \ltimes X. \quad (4.3)$$

Como de costumbre denotamos  $\Gamma_r$  el único subgrupo cerrado de  $\Gamma$  tal que  $\Gamma/\Gamma_r \simeq \mathbb{Z}/p^r\mathbb{Z}$ . Topológicamente  $\Gamma_r$  es generado por  $\gamma^{p^r}$ . Sea  $\omega_r := \omega_r(\gamma)$  (cf. definición 2.10), el submódulo  $\omega_r X$  es el mínimo  $\Gamma$ -submódulo tal que  $\Gamma_r$  actúa trivialmente en  $X/\omega_r X$ . Por lo tanto  $\omega_r X$  no depende de la  $\Lambda$ -estructura en  $X$ .

**Lema 4.13:** *Sea  $G_r$  el grupo de Galois  $\text{Gal}(L_\infty/K_r)$ . Denotamos  $\overline{H}$  la cerradura topológica de  $H$ . Entonces*

$$\overline{[G_r, G_r]} = \omega_r X.$$

### 4.3 Propiedades de los grupos de clases como $\Lambda$ -módulos

*Demostración:* Podemos escribir  $G_r = \Gamma_r \rtimes X$ . Sean  $a = \alpha x$  y  $b = \beta y$  elementos de  $G_r$  con  $\alpha, \beta \in \Gamma_r$  y  $x, y \in X$ . Es un ejercicio fácil (cf. ejercicio 4.5) ver que

$$[a, b] = aba^{-1}b^{-1} = (x^\alpha)^{1-\beta}(y^\beta)^{\alpha-1}.$$

Se cumple que  $1 - \beta$  y  $\alpha - 1$  son divisibles por  $\omega_r$ , por eso  $[a, b] \in \omega_r X$ .

Por el otro lado, haciendo  $\beta = 1$  y  $\alpha = \gamma^{p^r}$  vemos que  $y^{\gamma^{p^r}-1} \in \overline{[G_r, G_r]}$ . Es decir,  $\omega_r X \subseteq \overline{[G_r, G_r]}$ .  $\square$

Denotamos  $L_r$  la máxima subextensión de  $L_\infty$  abeliana sobre  $K_r$  (cf. (4.1)). Entonces  $L_\infty$  es la unión de los  $L_r$ . Del lema precedente deducimos inmediatamente que

$$\omega_r X = \text{Gal}(L_\infty/L_r) \quad \text{y} \quad X/\omega_r X = \text{Gal}(L_r/K_\infty). \quad (4.4)$$

Con la notación de la definición 4.9, obtenemos los siguientes resultados. En particular, una consecuencia del corolario 3.16 es el siguiente resultado que nos será útil próximamente.

**Corolario 4.14:**  $X$  es noetheriano si y solamente si  $\text{rg}_{\mathbb{F}_p}(\text{Gal}(L_0/K))$  es finito.

*Demostración:* Sea  $Y = X/\omega_0 X$ . Entonces  $X/\mathfrak{M}X = Y/pY$ , por lo que  $X/\mathfrak{M}X$  es finito si y solamente si  $\text{rg}_{\mathbb{F}_p} Y$  es finito. Pero  $\text{rg}_{\mathbb{F}_p} Y + \text{rg}_{\mathbb{F}_p} \Gamma = \text{rg}_{\mathbb{F}_p} \text{Gal}(L_0/K)$ .  $\square$

Vamos a aplicar los resultados de la sección 3.4 a  $\Lambda$ -módulos asociados a las siguientes extensiones y grupos de Galois.

**Definición 4.15:** Sea  $K_\infty/K$  una  $\mathbb{Z}_p$ -extensión. Para  $r \in \mathbb{N}_{\geq 0}$  denotamos

- $K_r$  = el único subcampo de la  $\mathbb{Z}_p$ -extensión  $K_\infty/K$  tal que  $\text{Gal}(K_r/K) \simeq \mathbb{Z}/p^r \mathbb{Z}$ ,
- $H_r$  = la máxima extensión abeliana pro- $p$  de  $K_r$  no ramificada,
- $M_r$  = la máxima extensión abeliana pro- $p$  de  $K_r$  ramificada sólo en  $p$ ,
- $C_r$  = la  $p$ -parte del grupo de clases  $\text{Cl}(K_r)$ ,
- $X_r = \text{Gal}(H_r/K_r)$ ,
- $Y_r = \text{Gal}(M_r/K_r)$ .

Escribimos  $H_\infty$  para el compuesto de todos los campos  $H_r$  para  $r \in \mathbb{N}_{\geq 0}$ , y análogamente definimos  $M_\infty$ . Estudiamos los módulos

- $X_\infty := \text{Gal}(H_\infty/K_\infty) = \varprojlim_{r \in \mathbb{N}_{\geq 0}} X_r$ ,
- $Y_\infty := \text{Gal}(M_\infty/K_\infty) = \varprojlim_{r \in \mathbb{N}_{\geq 0}} Y_r$ .

Aquí los límites son tomados con respecto a los mapeos de restricción entre los grupos de Galois.

El campo  $H_r$  es el  $p$ -campo de clases de Hilbert de  $K_r$ , es decir la máxima extensión abeliana pro- $p$  no ramificada, y el teorema 1.38 describe su grupo de Galois: existe un isomorfismo canónico  $X_r \simeq C_r$  grupos abelianos para cada  $r \in \mathbb{N}_{\geq 0}$ . El grupo de Galois  $\text{Gal}(K_r/K)$  actúa naturalmente en  $C_r$ , y de hecho el isomorfismo  $X_r \simeq C_r$  es compatible

con esta acción (esto sigue del ejercicio 1.7). Si  $N_r: C_{r+1} \rightarrow C_r$  denota la norma relativa de ideales (definición 1.23) entonces se puede comprobar que el diagrama

$$\begin{array}{ccc} X_{r+1} & \xrightarrow{\sim} & C_{r+1} \\ \downarrow & & \downarrow N_r \\ X_r & \xrightarrow{\sim} & C_r \end{array} \quad (4.5)$$

es conmutativo para  $r$  suficientemente grande (para esto hay que usar que  $H_r \cap K_{r+1} = K_r$ , que es cierto para  $r$  suficientemente grande; véase [Was97, p. 277 y lem. 13.3]). Esto muestra que  $X_\infty \simeq \varprojlim_{r \in \mathbb{N}_{\geq 0}} C_r$  como  $\Lambda$ -módulo, el límite de los  $C_r$  tomado con respecto a la norma.

**Teorema 4.16:** *El módulo  $Y_\infty$  es noetheriano.*

*Demostración:* Tenemos que  $M_0$  es la máxima extensión abeliana pro- $p$  de  $K$ , por el teorema 4.10 tenemos que  $\text{rg}_{\mathbb{F}_p} \text{Gal}(M_0/K)$  es finito, de donde deducimos la afirmación del corolario 4.14.  $\square$

**Corolario 4.17:**  *$X_\infty$  es un  $\Lambda$ -módulo noetheriano y de torsión.*

*Demostración:*  $X_\infty$  es isomorfo a un cociente de  $Y_\infty$ , ya que la máxima extensión abeliana pro- $p$  no ramificada  $H_\infty$  de  $K_\infty$  está contenida en  $M_\infty$ . Por lo tanto,  $X_\infty$  es noetheriano.

Ahora veamos que es de torsión. Sea  $S_0$  el conjunto de plazas de  $K$  que ramifican en  $K_\infty$ . El conjunto  $S_0$  es no vacío y finito (proposición 4.7 y proposición 4.8). Sea  $I_{\mathfrak{p}} \subseteq \Gamma$  el subgrupo de inercia de la plaza  $\mathfrak{p} \in S_0$ . Sabemos que  $I_{\mathfrak{p}}$  es un subgrupo cerrado de  $\Gamma$  entonces isomorfo a  $\Gamma_{r_{\mathfrak{p}}}$  para algún  $r_{\mathfrak{p}} \geq 0$ .

Sea

$$r_0 = \max_{\mathfrak{p} \in S_0} \{r_{\mathfrak{p}}\},$$

entonces la extensión  $K_\infty/K_{r_0}$  es totalmente ramificada en las plazas de  $K_r$  arriba de  $S_0$ . En particular, el número de plazas  $s$  de  $K_r$  que ramifican en  $K_\infty$  es el mismo para todo  $r \geq r_0$ .

Ahora usaremos la construcción al inicio de la sección, en el caso

$$L_\infty = H_\infty \quad \text{y} \quad X = X_\infty = \text{Gal}(H_\infty/K_\infty).$$

Recordemos que  $L_r$  es la máxima extensión abeliana de  $K_r$  contenida en  $H_\infty$ .

Sean  $\mathfrak{p}_1, \dots, \mathfrak{p}_s$  las plazas en  $K_r$ , con  $r \geq r_0$ , que ramifican en  $K_\infty$ . Sea  $I_i$  el subgrupo de inercia de  $\text{Gal}(L_r/K_r)$  para  $i = 1, \dots, s$ . Como  $L_n/K_\infty$  es no ramificada y los  $\mathfrak{p}_i$  ramifican totalmente en  $K_\infty$  obtenemos

$$I_i \simeq \Gamma_r \simeq \mathbb{Z}_p, \quad \text{para } i = 1, \dots, s.$$

La extensión  $H_r$  está contenida en  $L_r$ , ya que  $H_r K_\infty$  es abeliana sobre  $K_r$  y no ramificada sobre  $K_\infty$ . Además, las únicas plazas de  $K_r$  que ramifican en  $L_r$  son precisamente  $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ , entonces

$$\text{Gal}(L_r/H_r) = I_1 \cdots I_s.$$

Para todo  $r \geq r_0$  tenemos

$$\begin{aligned} \text{rg}_{\mathbb{Z}_p} X/\omega_r X &= \text{rg}_{\mathbb{Z}_p} \text{Gal}(L_r/K_\infty) \\ &= \text{rg}_{\mathbb{Z}_p} \text{Gal}(L_r/K) - 1 \\ &= \text{rg}_{\mathbb{Z}_p} \text{Gal}(L_r/H_r) - 1 \\ &\leq s - 1. \end{aligned}$$

El resultado sigue observando que  $\text{rg}_{\mathbb{Z}_p} X/\omega_r X \leq \text{rg}_{\mathbb{Z}_p} X/w_{r+1} X$  y de la proposición 3.17.  $\square$

## Ejercicios

**Ejercicio 4.4:** Sea

$$1 \rightarrow A \rightarrow D \rightarrow G \rightarrow 1$$

una sucesión exacta de grupos donde  $A$  es abeliano. Para  $\sigma \in G$  sea  $\tilde{\sigma} \in D$  un levantamiento y definimos

$$\sigma \bullet a = \tilde{\sigma} a \tilde{\sigma}^{-1} \text{ para } a \in A.$$

Demuestre que esto está bien definido y define una acción de  $\mathbb{Z}$ -lineal de  $G$  en  $A$ . Verifique que esta acción es continua si todos son grupos topológicos, los morfismos en la sucesión son continuos y si el mapeo  $D \rightarrow G$  admite una sección continua (no necesariamente un morfismo de grupos).

**Ejercicio 4.5:** Sea  $G = H \times N$ , con  $H$  y  $N$  abelianos. Entonces para todo  $g_1 = h_1 n_1$  y  $g_2 = h_2 n_2$  elementos de  $G$  tenemos

$$[g_1, g_2] = (n_1^{h_1})^{1-h_2} (n_2^{h_2})^{h_1-1}.$$

## 4.4. Teorema de Iwasawa

Continuamos usando la notación de la definición 4.15, en particular sea  $K_\infty/K$  una  $\mathbb{Z}_p$ -extensión. Además, usaremos continuamente la construcción de la sección pasada en el caso especial

$$L_\infty = H_\infty \quad \text{y} \quad X = X_\infty = \text{Gal}(H_\infty/K_\infty).$$

Al inicio de esta sección (en la proposición 4.18 y sus corolarios) hacemos la siguiente hipótesis que es verificada en los casos que trataremos en la exposición de las funciones  $L$   $p$ -ádicas, es decir en las  $\mathbb{Z}_p$ -extensiones ciclotómicas  $\mathbb{Q}^c$  y  $\mathbb{Q}(\mu_p)^c$ .

**Hipótesis:** Los primos  $\mathfrak{p}_1, \dots, \mathfrak{p}_s$  de  $K$  que ramifican en la  $\mathbb{Z}_p$ -extensión  $K_\infty$  son totalmente ramificados.

Sea  $I_i$  el subgrupo de inercia de  $G = \text{Gal}(H_\infty/K)$  correspondiente a la plaza  $\mathfrak{p}_i$ , con  $i = 1, \dots, s$ . Por la hipótesis anterior, tenemos que  $I_i \simeq \Gamma$  ya que  $X_\infty$  es no ramificado. Escogiendo un generador topológico  $\gamma$  de  $\Gamma$ , llamamos  $\sigma_i$  la imagen de  $\gamma$  en  $I_i$ . El isomorfismo  $G = I_i X_\infty = X_\infty I_i$  (ver (4.3)) nos permite escribir  $\sigma_i = a_i \sigma_1$ , para  $a_i$  elementos de  $X_\infty$ , claramente  $a_1 = 1$ .

**Proposición 4.18:** Sea  $T_0$  el  $\mathbb{Z}_p$ -submódulo generado por  $\{a_i \mid 2 \leq i \leq s\}$  y  $\omega_0 X_\infty$ . Sea  $T_r = \frac{\omega_r}{\omega_0} T_0$ , entonces

$$C_r \simeq X_\infty / T_r \quad \text{para } r \geq 0.$$

*Demostración:* Claramente  $H_0$  es la máxima extensión abeliana no ramificada de  $K = K_0$  contenida en  $H_\infty$ . El grupo de Galois  $X_0 = \text{Gal}(H_0/K_0)$  es igual a  $X_0 = G / \text{Gal}(H_\infty/H_0)$  donde  $\text{Gal}(H_\infty/H_0)$  corresponde al subgrupo mínimo de  $G$  que contiene  $[G, G] = \omega_0 X$  (4.13) al igual que los subgrupos de inercia  $I_1, \dots, I_s$ . Escribiendo  $G$  como el producto semi-directo (4.3) de  $I_1$  y  $X_\infty$  obtenemos

$$C_0 \simeq X_\infty / T_0.$$

Ahora, como  $K_\infty/K_r$  es una  $\mathbb{Z}_p$ -extensión, su grupo de Galois es cíclico generado por  $\gamma^{p^r}$  y los subgrupos de inercia  $I_i$  por  $\sigma_i^{p^r}$ . Además veamos que

$$\begin{aligned} \sigma_i^{p^r} &= (a_i \sigma_1)^{p^r} \\ &= a_i \sigma_1 a_i \sigma_1^{-1} \sigma_1^2 a_i \sigma_1^{-2} \cdots \sigma_1^{p^r-1} a_i \sigma_1^{1-p^r} \sigma_1^{p^r} \\ &= a_i^{\omega_r/\omega_0} \sigma_1^{p^r}. \end{aligned}$$

Procediendo como anteriormente tenemos el resultado.  $\square$

**Corolario 4.19:** Para la  $\mathbb{Z}_p$ -extensión ciclotómica de  $\mathbb{Q}(\mu_p)$  tenemos para  $r \in \mathbb{N}_{\geq 0}$

$$C_r \simeq X_\infty / \omega_r X_\infty = X_\infty / (\gamma^{p^r} - 1) X_\infty$$

donde  $\gamma$  es un generador topológico de  $\Gamma$ .

*Demostración:* Esto sigue de la proposición anterior porque en este caso  $s = 1$  según el lema 1.28, así que  $Y_0 = \omega_0 X_\infty = T X_\infty = (\gamma - 1) X_\infty$ .  $\square$

**Corolario 4.20:** Tenemos  $X_\infty = 0 \iff X_\infty^- = 0$ , donde  $X_\infty^-$  es la parte donde la conjugación compleja actúa por  $-1$ .

*Demostración:* Sea  $X_\infty^- = 0$ . Se ve fácilmente que el isomorfismo del corolario 4.19 es compatible con la acción de la conjugación compleja, así que  $\text{Cl}(\mathbb{Q}(\mu_p))^- = C_0^- \simeq X_\infty^- / \omega_0 X_\infty^- = 0$ . Entonces el teorema 4.5 implica que  $C_0 = 0$ , es decir  $p \nmid h_{\mathbb{Q}(\mu_p)}$ . El corolario 4.4 implica que  $p \nmid h_{\mathbb{Q}(\mu_{p^r})}$  para cada  $r \geq 0$ , es decir  $X_\infty = 0$ .  $\square$

**Proposición 4.21:** Sea  $E$  el  $\Lambda$ -módulo elemental de  $\Lambda$ -torsión tal que  $\left| E / \left( \frac{\omega_r}{\omega_e} E \right) \right|$  es finito para todo  $r \geq e$ . Entonces existe  $c$  tal que

$$\left| E / \left( \frac{\omega_r}{\omega_e} E \right) \right| = p^{\mu p^r + \lambda r + c}, \quad \text{para } r \gg 0,$$

donde  $\mu$  y  $\lambda$  son los invariantes de la definición 3.13.

*Demostración:* Basta con analizar los distintos factores que aparecen en  $E$ . Como  $X_\infty$  es de  $\Lambda$ -torsión, entonces hay solamente dos tipos de factores por analizar.

Sea  $X = \Lambda / (p^m)$ , entonces

$$X / \frac{\omega_r}{\omega_e} X \simeq \Lambda / (p^m, \frac{\omega_r}{\omega_e})$$

Como  $\frac{\omega_r}{\omega_0}$  es un polinomio distinguido  $P$  de grado  $p^r - p^e$ . Por el lema de división 2.3 tenemos

$$\Lambda / (p^m, \frac{\omega_r}{\omega_e}) \simeq (\mathbb{Z}/p^m \mathbb{Z})_{p^r - p^e - 1}[T],$$

es decir cada elemento de la izquierda es representado por un polinomio de grado menor a  $p^r - p^e$  con coeficientes en  $\mathbb{Z}/p^m \mathbb{Z}$ . Es decir

$$\left| X / \frac{\omega_r}{\omega_e} X \right| = p^{m(p^r - p^e)} = p^{mp^r + c}$$

para  $r \gg 0$  y  $c$  constante.

Ahora sea  $X = \Lambda / (P)$ , donde  $P$  es un polinomio distinguido de grado  $d$ . Para todo  $r$  tal que  $p^r \geq d$  tenemos que  $\frac{\omega_{r+2}}{\omega_{r+1}}$  actúa en  $X$  por multiplicación por  $p$  y una unidad (ver el ejercicio 4.6). Por lo tanto para  $r_0 \geq e$  tal que  $p^{r_0} \geq d$  tenemos

$$\frac{\omega_{r_0+2}}{\omega_e} X = \frac{\omega_{r_0+2}}{\omega_{r_0+1}} \left( \frac{\omega_{r_0+1}}{\omega_e} X \right) = p \frac{\omega_{r_0+1}}{\omega_e} X,$$

y por inducción obtenemos

$$\frac{\omega_r}{\omega_e} X = p^{r-r_0-1} \frac{\omega_{r_0+1}}{\omega_e} X \quad \text{para } r > r_0.$$

Al pasar al cociente obtenemos

$$\begin{aligned}
 \left| X / \frac{\omega_r}{\omega_e} X \right| &= \left| X / p^{r-r_0-1} \frac{\omega_{r_0+1}}{\omega_e} X \right| \\
 &= \left| X / p^{r-r_0-1} X \right| \left| p^{r-r_0-1} X / p^{r-r_0-1} \frac{\omega_{r_0+1}}{\omega_e} X \right| \\
 &= \left| X / p^{r-r_0-1} X \right| \left| X / \frac{\omega_{r_0+1}}{\omega_e} X \right| \\
 &= p^{d(r-r_0-1)} \left| X / \frac{\omega_{r_0+1}}{\omega_e} X \right|
 \end{aligned}$$

Finalmente como  $\left| X / \frac{\omega_r}{\omega_e} X \right|$  es finito para todo  $r \geq 0$ , tenemos que existe una constante  $c$  tal que

$$\left| X / \frac{\omega_r}{\omega_e} X \right| = p^{dr+c},$$

para  $r$  suficientemente grande.  $\square$

**Teorema 4.22 (Iwasawa):** Sea  $K$  un campo de números y  $p$  un primo. Para cada  $r \in \mathbb{N}_{\geq 0}$  sea  $K_r/K$  una extensión tal que  $\text{Gal}(K_r/K) \simeq \mathbb{Z}/p^r\mathbb{Z}$ , y sea  $p^{e_r}$  la máxima potencia de  $p$  que divide el orden del grupo de clases de  $K_r$ . Entonces existen constantes  $\mu, \lambda \in \mathbb{N}_{\geq 0}$  y  $\nu \in \mathbb{Z}$  tal que

$$e_r = \mu p^r + \lambda r + \nu \quad \text{para } r \gg 0.$$

*Demostración:* Sea  $K_\infty/K$  una  $\mathbb{Z}_p$ -extensión. Existe  $r_0 \geq 0$  tal que todos los primos que ramifican en la extensión  $K_\infty/K_{r_0}$  son totalmente ramificados. Aplicando la proposición 4.18 a la extensión  $K_\infty/K_{r_0}$  vemos que

$$C_r \simeq X_\infty / \frac{\omega_r}{\omega_{r_0}} T_{r_0} \quad \text{para todo } r \geq r_0,$$

donde  $T_{r_0}$  es el módulo generado por  $\omega_{r_0}$  y los respectivos  $a_i$ , que dependen de los subgrupos de inercia de  $\text{Gal}(H_\infty/K_{r_0})$ .

Ahora, como  $C_{r_0} \simeq X_\infty/T_{r_0}$  es finito, tenemos que

$$\begin{aligned}
 |C_r| &= |X_\infty/T_{r_0}| \left| T_{r_0} / \frac{\omega_r}{\omega_{r_0}} T_{r_0} \right| \\
 &= p^c \left| T_{r_0} / \frac{\omega_r}{\omega_{r_0}} T_{r_0} \right|
 \end{aligned}$$

para alguna constante  $c \geq 0$ , además tenemos que

$$T_{r_0} \sim X_\infty \sim E = \left( \bigoplus_{i=1}^m \Lambda / \pi^{\mu_i} \Lambda \right) \oplus \left( \bigoplus_{j=1}^l \Lambda / P_j \Lambda \right)$$

con  $E$  elemental como en el teorema 3.12 y sin factor libre por el corolario 4.17. Por lo tanto basta determinar el factor  $\left| T_{r_0} / \frac{\omega_r}{\omega_{r_0}} T_{r_0} \right|$ . Consideremos el siguiente diagrama para  $r \geq r_0$

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \frac{\omega_r}{\omega_{r_0}} T_{r_0} & \longrightarrow & T_{r_0} & \longrightarrow & T_{r_0} / \frac{\omega_r}{\omega_{r_0}} T_{r_0} \longrightarrow 0 \\
 & & \downarrow \varphi'_r & & \downarrow \varphi & & \downarrow \varphi''_r \\
 0 & \longrightarrow & \frac{\omega_r}{\omega_{r_0}} E & \longrightarrow & E & \longrightarrow & E / \frac{\omega_r}{\omega_{r_0}} E \longrightarrow 0
 \end{array}$$

Por el ejercicio 3.4 tenemos que  $|\ker \varphi'_r|$ ,  $|\operatorname{coker} \varphi'_r|$ ,  $|\ker \varphi''_r|$ ,  $|\operatorname{coker} \varphi''_r|$  son finitos, además son constantes para  $r$  suficientemente grande ya que:

- Las sucesiones  $(|\ker \varphi'_r|)_{r \geq r_0}$ ,  $(|\operatorname{coker} \varphi'_r|)_{r \geq r_0}$  y  $(|\operatorname{coker} \varphi''_r|)_{r \geq r_0}$  son monótonas y acotadas (ver el ejercicio 4.7).
- Por el lema de la serpiente tenemos que

$$|\ker \varphi''_r| = |\ker \varphi'_r|^{-1} |\ker \varphi| |\operatorname{coker} \varphi'_r| |\operatorname{coker} \varphi|^{-1} |\operatorname{coker} \varphi''_r|,$$

y para  $r \gg 0$  los términos de la derecha son constantes por el inciso anterior.

Es decir existe una constante  $c'$  tal que

$$\left| T_{r_0} / \frac{\omega_r}{\omega_{r_0}} T_{r_0} \right| = p^{c'} \left| E / \frac{\omega_r}{\omega_{r_0}} E \right|$$

para  $r$  suficientemente grande. El teorema sigue directamente aplicando la proposición 4.21.  $\square$

## Ejercicios

**Ejercicio 4.6:** Sea  $X = \Lambda/(P)$  con  $P$  distinguido de grado  $d$ . Recuerde que  $\omega_r(X) = X^{p^r} - 1$  (definición 2.10).

- (a) Demuestre que si  $p^r \geq d$  entonces

$$\omega_r(1 + T) \equiv p \cdot Q \pmod{P},$$

para algún polinomio  $Q$ .

- (b) Luego demuestre que

$$\omega_{r+1}(1 + T) \equiv p^2 \cdot Q' \pmod{P},$$

para algún polinomio  $Q'$ .

- (c) Finalmente demuestre que

$$\omega_{r+2}(1 + T) \equiv p(1 + p \cdot Q'') \omega_{r+1}(1 + T) \pmod{P},$$

para algún polinomio  $Q''$ .

- (d) Concluya que  $\frac{\omega_{r+2}}{\omega_{r+1}}$  actúa en  $X$  como multiplicación por  $p$  módulo una unidad en  $\Lambda$ . (Use el isomorfismo del teorema 2.11 que hace corresponder  $\omega_r(1 + T)$  con  $\omega_r := \omega_r(\gamma)$ .)

**Ejercicio 4.7:** Sea  $T$  un  $\Lambda$ -módulo de torsión y  $\varphi : T \rightarrow E$  un pseudo-isomorfismo donde  $E$  es un módulo elemental. Con la notación del ejercicio 3.4 sea  $\alpha = \beta = \frac{\omega_r}{\omega_e}$  y supongamos que  $\frac{\omega_r}{\omega_e} T$  es finito para todo  $r \geq e$ . Suponga que  $s \geq r$ .

- (a) Demuestre que  $\frac{\omega_s}{\omega_e} T \subset \frac{\omega_r}{\omega_e} T$  y  $\frac{\omega_s}{\omega_e} E \subset \frac{\omega_r}{\omega_e} E$ .

- (b) Concluya que  $|\ker \varphi'_s| \leq |\ker \varphi'_r|$  y  $|\operatorname{coker} \varphi''_r| \leq |\operatorname{coker} \varphi''_s|$ .

- (c) Demuestre que si  $x$  es un levantamiento de un elemento en  $\operatorname{coker} \varphi'_r$  entonces  $\frac{\omega_s}{\omega_r} x$  es un levantamiento de un elemento en  $\operatorname{coker} \varphi'_s$ .

- (d) Concluya que  $|\operatorname{coker} \varphi'_s| \leq |\operatorname{coker} \varphi'_r|$ .

## 4.5. Sobre los invariantes $\mu$ y $\lambda$

El teorema 4.22 describe el crecimiento de la parte  $p$  de los grupos de clases asociados a los subcampos finitos (suficientemente grandes) de una  $\mathbb{Z}_p$ -extensión. El exponente de estos grupos, depende de un término exponencial  $\mu \cdot p^r$  y de un término lineal  $\lambda \cdot r + \nu$ . En esta sección haremos un compendio de algunos resultados conocidos sobre los invariantes de Iwasawa.

**Proposición 4.23:** *Sea  $X$  un  $\Lambda$ -módulo noetheriano de torsión. Entonces*

$$\begin{aligned} \mu(X) = 0 &\iff \operatorname{rg}_{\mathbb{F}_p} X < \infty \\ &\iff \operatorname{rg}_{\mathbb{F}_p} X/\omega_r X \text{ está acotado para todo } r \geq 0. \end{aligned}$$

La proposición anterior es análoga a la proposición 3.17. Esta nos provee criterios para determinar cuándo el término exponencial no aparece en el exponente.

**Teorema 4.24 (Ferrero-Washington):** *Sea  $K/\mathbb{Q}$  una extensión abeliana de  $\mathbb{Q}$  y  $p$  un número primo, sea  $K_\infty/K$  la  $\mathbb{Z}_p$ -extensión ciclotómica de  $K$ . Entonces  $\mu = 0$ .*

*Demostración:* Referencia a annals y a iwasawa.

**Observación:** Iwasawa demostró que  $\mu \neq 0$  para.. en \*\*Ref.



# Capítulo 5

## Funciones $L$ $p$ -ádicas

En la teoría de las funciones  $L$ , como la función zeta de Riemann, hay dos fenómenos importantes que implican la existencia de análogos  $p$ -ádicos de esas funciones. Primero, algunos valores especiales de esas funciones, que a priori son números complejos, de hecho son números algebraicos o incluso racionales (en general después de dividir por un factor transcendental normalizante). Y segundo, esos valores son en un sentido  $p$ -ádicamente continuos, que significa que hay congruencias entre ellos. De la definición no es inmediato que las funciones  $L$  tienen estas propiedades: Algunos valores especiales siquiera están bien definidos después de considerar la continuación analítica de la función. Sin duda estos fenómenos son inmensamente sorprendentes, ocasionando que la existencia de las funciones  $L$   $p$ -ádicas en general no sea nada trivial.

Aquí explicamos la teoría de las funciones  $L$   $p$ -ádicas en el caso más básico: la función zeta de Riemann, y ligeramente más general, las funciones  $L$  de Dirichlet. La idea de construir un tal análogo  $p$ -ádico de funciones  $L$  era de Kubota y Leopoldt [KL64] y era más tarde reinterpretada por Iwasawa, como explicaremos en la sección 5.3.

### 5.1. Proemio sobre las funciones $L$

Aquí colectamos unos hechos analíticos sobre las funciones  $L$  que nos interesan. Como este texto pone su énfasis más en la teoría algebraica omitimos la mayoría de las demostraciones en esta sección.

**Definición 5.1:** Una *serie de Dirichlet* es una serie de la forma

$$\sum_{n=1}^{\infty} a_n n^{-s}$$

con coeficientes  $a_n \in \mathbb{C}$ .

**Proposición 5.2:** Para cada serie de Dirichlet

$$\sum_{n=1}^{\infty} a_n n^{-s}$$

existe un  $\sigma_0 \in [-\infty, \infty]$  tal que la serie converge localmente uniformemente para los  $s \in \mathbb{C}$  con  $\operatorname{Re} s > \sigma_0$  y diverge para  $\operatorname{Re} s < \sigma_0$ . Este  $\sigma_0$  se llama abscisa de convergencia.

La función definida por una serie de Dirichlet en el semiplano de convergencia es holomorfa.

Si los coeficientes son multiplicativos en el sentido

$$a_{nm} = a_n a_m \text{ para todo } m, n \in \mathbb{N}_{\geq 1}$$

entonces la serie tiene un producto de Euler

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_{\ell \text{ primo}} (1 - a_{\ell} \ell^{-s})^{-1}$$

para los  $s \in \mathbb{C}$  con  $\operatorname{Re} s > \sigma_0$ .

*Demostración:* [Zag81, §1, Satz 1, §2, Satz 1] □

El ejemplo más importante es la serie de Dirichlet con  $a_n = 1$  para cada  $n$ .

**Definición 5.3:** La función zeta de Riemann es la función

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{\ell \text{ primo}} (1 - \ell^{-s})^{-1}$$

para  $s \in \mathbb{C}$ . Su abscisa de convergencia es  $\sigma_0 = 1$ .

Muchas veces las series de Dirichlet tienen una continuación analítica, como muestra el resultado siguiente. Porque este resultado es de fondo para nuestro análisis de las funciones  $L$  vamos a esbozar su demostración.

**Proposición 5.4:** Sea

$$L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

una serie de Dirichlet cuya abscisa de convergencia  $\sigma_0$  no es  $+\infty$  (es decir, hay al menos un  $s \in \mathbb{C}$  para el cual la serie converge). Definimos para los números reales  $t < 0$

$$f(t) = - \sum_{n=1}^{\infty} t a_n e^{nt}$$

(¡esto converge!) y asumimos que esta función se extiende a  $t = 0$  y se escribe como

$$f(t) = \sum_{n=0}^{\infty} b_n \frac{t^n}{n!}, \quad t \leq 0$$

con coeficientes  $b_n \in \mathbb{C}$  y donde la serie converge absolutamente.<sup>1</sup>

Entonces la función  $L$  tiene una continuación meromorfa a todo  $\mathbb{C}$  con un solo polo de orden 1 en  $s = 1$  si  $b_0 \neq 0$  y holomorfa si  $b_0 = 0$ . Además,

$$L(1 - n) = -\frac{b_n}{n}$$

para  $n \in \mathbb{N}_{\geq 1}$ .

*Demostración:* Seguimos [Zag81, §7, Satz 1]; véase allá para más detalles. Primero observemos que los coeficientes  $a_n$  pueden crecer a lo más polinomialmente, por lo demás la serie de Dirichlet  $L(s)$  sería divergente para todo  $s \in \mathbb{C}$ . Por eso la serie que define  $f(t)$  converge absolutamente para  $t < 0$ .

Para la demostración conviene más usar la función

$$F(t) := \frac{f(-t)}{t} = \sum_{n=1}^{\infty} a_n e^{-nt} \quad (t \geq 0)$$

en lugar de  $f$ , que se escribe como serie absolutamente convergente

$$F(t) = \sum_{n=-1}^{\infty} c_n t^n \quad \text{con} \quad c_n = (-1)^{n+1} \frac{b_{n+1}}{(n+1)!} \quad (t \geq 0). \quad (5.1)$$

---

<sup>1</sup> Esta hipótesis se puede relajar, pero en nuestras aplicaciones siempre será cierta. La hipótesis menos fuerte que es suficiente es un poco complicada de describir, véase [Zag81, p. 48] para ella.

La afirmación sobre los valores de  $L(1-n)$  entonces es equivalente a

$$L(1-n) = (-1)^n n! c_n \quad \text{para } n \in \mathbb{N}_{\geq 1}. \quad (5.2)$$

Necesitamos la *fórmula de transformación de Mellin*, que involucra la función  $\Gamma$

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt \quad (s \in \mathbb{C}, \operatorname{Re}(s) > 0).$$

Es fácil ver que

$$\int_0^1 t^{s-1} dt \text{ converge} \iff \operatorname{Re}(s) > 0 \quad \text{para } s \in \mathbb{C} \quad (*)$$

y que  $\int_1^\infty g(t)t^{s-1} dt$  converge para cada  $s \in \mathbb{C}$  si  $g$  es una función que decrece exponencialmente para  $t \rightarrow \infty$ , por eso el integral de arriba constituyendo la función  $\Gamma$  converge para los  $s \in \mathbb{C}$  con parte real positiva. La función  $\Gamma$  se extiende a una función meromorfa en todo de  $\mathbb{C}$  con polos en los enteros negativos y sin ceros (es decir  $1/\Gamma$  es una función holomorfa en  $\mathbb{C}$  y tiene ceros en los enteros negativos). De la fórmula arriba se obtiene fácilmente

$$\int_0^\infty t^{s-1} e^{-nt} dt = \Gamma(s)n^{-s} \quad (n \in \mathbb{N}_{\geq 1})$$

(con una sustitución  $r = nt$ ) y pues, por la convergencia absoluta de  $L(s)$ ,

$$\Gamma(s)L(s) = \int_0^\infty F(t)t^{s-1} dt$$

para  $s \in \mathbb{C}$  con  $\operatorname{Re}(s) > \sigma_0$  – esto es la anunciada fórmula de transformación. Queremos ver que el integral al lado derecho de hecho converge para más que estos  $s$ .

Descomponemos el integral como  $\Gamma(s)L(s) = I_1(s) + I_2(s)$  con

$$I_1(s) = \int_0^1 F(t)t^{s-1} dt, \quad I_2(s) = \int_1^\infty F(t)t^{s-1} dt.$$

El integral  $I_2(s)$  de hecho converge para cada  $s \in \mathbb{C}$  porque  $F(t)$  decrece exponencialmente para  $t \rightarrow \infty$  y pues da una función holomorfa en  $\mathbb{C}$ , y solo tenemos que estudiar el integral  $I_1(s)$ . Para eso usamos (5.1), que nos da para  $s \in \mathbb{C}$  con  $\operatorname{Re}(s) > \sigma_0$  y cada  $N \in \mathbb{N}_{\geq 1}$

$$I_1(s) = \int_0^1 \sum_{n=-1}^{N-1} c_n t^{n+s-1} dt + \int_0^1 \sum_{n=N}^\infty c_n t^{n+s-1} dt.$$

El primero sumando es igual a

$$\sum_{n=-1}^N \frac{c_n}{n+s}$$

y pues es meromorfo en  $\mathbb{C}$  con polos para  $s \in \{-N, \dots, 1\}$ . El integral en el segundo sumando se puede estimar con

$$\int_0^1 \left( \sum_{n=N}^\infty |c_n| \right) t^{N+s-1} dt,$$

que converge para cada  $s \in \mathbb{C}$  con  $\operatorname{Re}(s) > -N$  según (\*).

Porque  $N$  arriba era arbitrario, en total esto demuestra que la función  $\Gamma(s)L(s)$  tiene una continuación meromorfa a todo de  $\mathbb{C}$  con (posiblemente) polos simples en  $\{n \in \mathbb{Z} : n \geq -1\}$ .

Por eso  $L(s)$  tiene una continuación meromorfa a todo de  $\mathbb{C}$  con posiblemente un polo simple en  $s = 1$ . Se sabe que los residuos de la función  $\Gamma$  son dados por

$$\operatorname{Res}_{s=-n} \Gamma(s) = \frac{(-1)^n}{n!} \quad \text{para } n \in \mathbb{N}_{\geq 1}.$$

De esto obtenemos a fórmula (5.2). □

En el caso de la función zeta, tenemos

$$f(t) = -t \sum_{n=1}^{\infty} (e^t)^n = \frac{t}{1 - e^{-t}} \quad (t \leq 0).$$

Esta función es holomorfa en todo de  $\mathbb{C}$ , por eso es analítica y tiene una representación

$$\frac{t}{1 - e^{-t}} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \quad (t \in \mathbb{C})$$

con coeficientes  $B_n$ . Son racionales por que la serie de arriba es la serie de Taylor, así que

$$B_n = f^{(n)}(0) \in \mathbb{Q} \quad \text{para } n \in \mathbb{N}_{\geq 0}.$$

**Definición 5.5:** Los coeficientes  $B_n \in \mathbb{Q}$  definidos arriba se llaman *números de Bernoulli*.<sup>2</sup> Notemos que  $B_n = 0$  si  $n > 1$  es impar, porque  $f(t) = f(-t) + t$ .

Esto demuestra:

**Proposición 5.6:** La función zeta tiene una continuación meromorfa a todo  $\mathbb{C}$  con un único polo en  $s = 1$  de orden 1, y

$$\zeta(1 - n) = -\frac{B_n}{n} \in \mathbb{Q}$$

para  $n \geq 1$ , los  $B_n$  siendo los números de Bernoulli.

**Ejemplo 5.7:** Los primeros números de Bernoulli no nulos son

$$B_0 = 1, B_1 = \frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, \\ B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, B_{14} = \frac{7}{6}, B_{16} = -\frac{3617}{510}, \dots$$

Es útil estudiar también series de Dirichlet ligeramente más generales. Para esto fijamos un encaje  $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ .

**Definición 5.8:** Sea  $N \in \mathbb{N}_{\geq 1}$ . Un *carácter de Dirichlet* es un homomorfismo de grupos

$$\chi: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \overline{\mathbb{Q}}^\times.$$

Se llama *primitivo* si no se factoriza a través de  $(\mathbb{Z}/M\mathbb{Z})^\times$  para algún  $M \mid N$ ,  $M \neq N$ , y en este caso  $N$  se llama el *conductor* de  $\chi$ . Los valores de  $\chi$  son raíces de la unidad y generan un subcampo de  $\overline{\mathbb{Q}}$  que llamamos  $\mathbb{Q}(\chi)$ .

<sup>2</sup> En algunos textos se encuentra la definición con  $f(t) = \frac{t}{e^t - 1}$  en lugar del  $f$  de arriba. Esto da los mismos números de Bernoulli salvo para  $B_1$ , en cual caso da  $B_1 = -\frac{1}{2}$  en lugar de  $B_1 = \frac{1}{2}$ .

Si  $\chi$  es un carácter de Dirichlet, definimos una función que también llamamos  $\chi$  así

$$\chi: \mathbb{N}_{\geq 1} \rightarrow \overline{\mathbb{Q}}^\times, \quad n \mapsto \begin{cases} \chi(n \bmod N), & (N, n) = 1, \\ 0, & (N, n) > 1. \end{cases}$$

La función  $L$  de Dirichlet de  $\chi$  es la serie de Dirichlet

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n)n^{-s}.$$

Aunque esta función depende del encaje escogido, no lo incluimos en la notación porque siempre será claro del contexto.

La función  $\chi$  es claramente multiplicativa, así que la función  $L(\chi, -)$  tiene un producto de Euler

$$L(\chi, s) = \prod_{\ell \text{ primo}} (1 - \chi(\ell)\ell^{-1})^{-1}.$$

En este caso la abscisa de convergencia es  $\sigma_0 = 0$  (salvo si  $\chi$  es trivial; véase [Zag81, p. 42]). Otra vez podemos aplicar la proposición 5.4 para obtener una continuación analítica y formulas para los valores en los enteros negativos, similarmente a la proposición 5.6. Omitimos los detalles y simplemente enunciamos el resultado.

**Proposición 5.9:** Sea  $\chi$  un carácter de Dirichlet de conductor  $N > 1$ . Ponemos

$$f_\chi(t) := \sum_{a=1}^N \frac{\chi(a)te^{at}}{e^{Nt} - 1} \quad (t \in \mathbb{C}).$$

Esta función se escribe como una serie

$$f_\chi(t) = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!} \quad (t \in \mathbb{C})$$

con coeficientes  $B_{n,\chi} \in \mathbb{Q}(\chi)$  que se llaman números de Bernoulli generalizados por  $\chi$ . La función  $L(\chi, -)$  tiene una continuación holomorfa a todo  $\mathbb{C}$  y

$$L(\chi, 1 - n) = -\frac{B_{n,\chi}}{n} \in \mathbb{Q}(\chi) \quad \text{para cada } n \geq 1.$$

Terminamos esta sección con introducir los polinomios de Bernoulli, que serán usados en unas demostraciones siguientes.

**Definición 5.10:** Para cada  $n \in \mathbb{N}_{\geq 1}$  definimos un polinomio

$$B_n(X) = \sum_{i=0}^n \binom{n}{i} B_i X^{n-i} \in \mathbb{Q}[X]$$

que se llama el *polinomio de Bernoulli*  $n$ -ésimo.

**Lema 5.11:** Definimos una función

$$F(t, x) = \frac{te^{t(1+x)}}{e^t - 1} \quad (t, x \in \mathbb{C}).$$

Entonces para cada  $x, t \in \mathbb{C}$  tenemos

$$F(t, x) = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}.$$

*Demostración:* Porque  $F(t, x) = f(t)e^{tx}$  para  $t, x \in \mathbb{C}$ , esto resulta directamente de la fórmula del producto de Cauchy:

$$F(t, x) = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \sum_{n=0}^{\infty} x^n \frac{t^n}{n!} = \sum_{n=0}^{\infty} \sum_{i=0}^n \binom{n}{i} B_i x^{n-i} \frac{t^n}{n!} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}. \quad \square$$

## Ejercicios

**Ejercicio 5.1:** Demuestre que la función zeta de Riemann tiene abscisa de convergencia  $\sigma_0 = 1$  y las funciones  $L$  de Dirichlet para caracteres de Dirichlet no triviales tienen abscisa de convergencia  $\sigma_0 = 0$ .

**Ejercicio 5.2:** Demuestre que una serie de Dirichlet cuyas coeficientes son multiplicativos tiene un producto de Euler.

**Ejercicio 5.3:** Sea  $f(t) = \frac{t}{1 - e^{-t}}$  para  $t \in \mathbb{R}$  como en la definición 5.5.

(a) Verifique que  $f(t) = -t \sum_{n=1}^{\infty} (e^t)^n$  para  $t \leq 0$ .

(b) Verifique la relación  $f(t) = f(-t) + t$  para  $(t \in \mathbb{R})$ .

**Ejercicio 5.4:** Calcule unos de los primeros números de Bernoulli.

**Ejercicio 5.5:** Sea  $\chi$  un carácter de Dirichlet de conductor  $N$ . Verifique la relación

$$f_{\chi}(t) = \frac{1}{N} \sum_{a=1}^N \chi(a) F\left(Nt, \frac{a}{N} - 1\right) \quad \text{para } t \in \mathbb{C},$$

donde  $f_{\chi}$  es la función de la proposición 5.9 y  $F$  es la función del lema 5.11. Use esto para derivar la siguiente fórmula para los números de Bernoulli generalizados:

$$B_{n,\chi} = N^{n-1} \sum_{a=1}^N \chi(a) B_n\left(\frac{a}{N} - 1\right) \quad \text{para } n \in \mathbb{N}_{\geq 1}.$$

Concluya que si  $\chi$  es no trivial entonces

$$B_{1,\chi} = \frac{1}{N} \sum_{a=1}^N \chi(a)a.$$

## 5.2. Teoría elemental $p$ -ádica de valores de la función zeta

La Conjetura Principal de la Teoría de Iwasawa establece una conexión entre ciertos módulos sobre el álgebra de Iwasawa  $\Lambda$  y funciones  $L$  como las de la sección anterior, usando los análogos  $p$ -ádicos de dichas funciones que mencionamos anteriormente. Para formular esta conexión precisamente es necesario ver las funciones  $L$   $p$ -ádicas como elementos del álgebra de Iwasawa  $\Lambda$ . No obstante, la idea detrás de la construcción de dichas funciones se puede entender desde un punto de vista más elemental, como explicaremos a continuación. Cabe notar que la mayoría de los resultados en esta sección no son necesarios para el resto del texto, incluso en la Teoría de Iwasawa moderna este enfoque ha sido rebasado por construcciones más generales como las que veremos en la siguiente sección. Así pues, dedicamos esta sección al estudio de estas proposiciones elementales con el fin de fomentar la intuición del lector.

Empecemos estudiando en mas detalle los números de Bernoulli. El objetivo original de Bernoulli era calcular expresiones como

$$1^n + 2^n + 3^n + \dots + k^n$$

para  $k, n \in \mathbb{N}_{\geq 1}$  y expresarlas como un polinomio en  $k$ . Su resultado es la siguiente *fórmula de Bernoulli*.

**Lema 5.12 (Bernoulli):** *Si definimos*

$$S_n(k) = \sum_{a=1}^k a^n$$

para  $n, k \in \mathbb{N}_{\geq 1}$ , entonces

$$S_n(k) = \frac{1}{n+1} \sum_{i=1}^n \binom{n+1}{i} B_i k^{n-i+1}.$$

*Demostración:* Usamos los polinomios de Bernoulli y la función  $F$  del lema 5.11. Porque  $F(t, x) - F(t, x-1) = te^{tx}$  tenemos

$$B_{n+1}(x) - B_{n+1}(x-1) = (n+1)x^n$$

para cada  $n \in \mathbb{N}_{\geq 0}$  y  $x \in \mathbb{C}$ . Pongamos aquí  $x = 1, \dots, k$  y sumemos todas las ecuaciones, que nos da

$$S_n(k) = \frac{1}{n+1} (B_{n+1}(k) - B_{n+1}(0)).$$

La fórmula entonces resulta de la definición de los polinomios de Bernoulli. □

En el siguiente resultado vemos los números de Bernoulli como números  $p$ -ádicos y obtenemos por ejemplo la propiedad importante de que son  $p$ -ádicamente acotados.

**Proposición 5.13 (Clausen-von Staudt):** *Sea  $n \in \mathbb{N}_{\geq 1}$  par y  $p \neq 2$  un primo.*

- (a) *Si  $p-1 \nmid n$  entonces  $B_n \in \mathbb{Z}_p$ .*
- (b) *Si  $p-1 \mid n$  entonces  $B_n + \frac{1}{p} \in \mathbb{Z}_p$ .*

*En particular,  $pB_n \in \mathbb{Z}_p$ , es decir  $|B_n|_p \leq p$ . Además, si  $p-1 \mid n$  entonces  $pB_n \equiv -1 \pmod{p}$ .*

*Demostración:* Esta demostración es combinada de [Lang0, §2.2, B3, p. 35] y [Was97, Thm. 5.10]. Usamos otra vez los polinomios de Bernoulli de la definición 5.10 y también la función

$$F(t, x) = \frac{te^{t(1+x)}}{e^t - 1} \quad (t, x \in \mathbb{C})$$

del lema 5.11.

Empezamos con derivar una relación para los polinomios de Bernoulli. Para cada  $m \in \mathbb{N}_{\geq 1}$  tenemos

$$\sum_{a=0}^{m-1} (e^t)^a = \frac{e^{mt} - 1}{e^t - 1}.$$

Usando esto, obtenemos para cada  $x, t \in \mathbb{C}$

$$\begin{aligned} F(t, x) &= \frac{te^{(1+x)t}}{e^{mt} - 1} \sum_{a=0}^{m-1} e^{at} = \sum_{a=0}^{m-1} \frac{te^{(x+1+a)t}}{e^{mt} - 1} \\ &= \frac{1}{m} \sum_{a=0}^{m-1} \frac{mte^{\frac{x+1+a}{m}mt}}{e^{mt} - 1} = \frac{1}{m} \sum_{a=0}^{m-1} F\left(mt, \frac{x+1+a}{m}\right) \\ &= \frac{1}{m} \sum_{a=0}^{m-1} \sum_{n=0}^{\infty} B_n\left(\frac{x+1+a}{m}\right) \frac{(mt)^n}{n!} \\ &= \sum_{n=0}^{\infty} \left( m^{n-1} \sum_{a=0}^{m-1} B_n\left(\frac{x+1+a}{m}\right) \right) \frac{t^n}{n!} \end{aligned}$$

y pues

$$B_n(X) = m^{n-1} \sum_{a=1}^m B_n\left(\frac{X+a}{m}\right)$$

para cada  $n \in \mathbb{N}_{\geq 1}$ .

Ahora continuamos con inducción en  $n$ , es decir sea  $n \geq 2$  par y asumamos que la afirmación es cierta para cada  $i < n$ . Pongamos  $m = p$  y  $X = 0$  en la relación de arriba, que nos da

$$B_n = B_n(0) = p^{n-1} \sum_{a=1}^p B_n\left(\frac{a}{p}\right) = p^{n-1} \sum_{a=1}^p \sum_{i=0}^n \binom{n}{i} B_i\left(\frac{a}{p}\right)^{n-i} = \sum_{i=0}^n \sum_{a=1}^p \binom{n}{i} (pB_i) a^{n-i} p^{i-2}.$$

Por inducción sabemos que  $pB_i \in \mathbb{Z}_p$  para  $i < n$ , así que en la suma sobre  $i$  todos los sumandos para  $i = 2, \dots, n-1$  están en  $\mathbb{Z}_p$ . Porque  $B_1 = \frac{1}{2}$  y  $p \neq 2$ , el sumando para  $i = 1$  también está en  $\mathbb{Z}_p$ . Por eso (nota que  $B_0 = 1$ )

$$B_n \equiv \sum_{a=1}^p (a^n p^{-1} + B_n p^{n-1}) \pmod{\mathbb{Z}_p}$$

o equivalentemente

$$(1 - p^n)B_n - \frac{1}{p} \sum_{a=1}^{p-1} a^n \in \mathbb{Z}_p.$$

Porque  $1 - p^n \in \mathbb{Z}_p^\times$  es suficiente mostrar que

$$\sum_{a=1}^{p-1} a^n \equiv \begin{cases} 0 & \text{si } p-1 \nmid n, \\ -1 & \text{si } p-1 \mid n \end{cases} \pmod{p}.$$

El caso en que  $p-1 \mid n$  es claro gracias al pequeño teorema de Fermat. Sea  $u \in \mathbb{Z}$  tal que su clase módulo  $p$  genera  $\mathbb{F}_p^\times$ . Entonces multiplicación con  $u$  induce un automorfismo de  $\mathbb{F}_p^\times$ , así que

$$(u^n - 1) \sum_{a=1}^{p-1} a^n = \sum_{a=1}^{p-1} (ua)^n - \sum_{a=1}^{p-1} a^n \equiv 0 \pmod{p}.$$

Si  $p-1 \nmid n$  entonces  $u^n \not\equiv 1 \pmod{p}$ , y la afirmación resulta.  $\square$

Estos dos resultados se pueden usar para encontrar una representación  $p$ -ádica de los números de Bernoulli:

**Corolario 5.14:** Para cada  $n \in \mathbb{N}_{\geq 1}$  tenemos en  $\mathbb{Q}_p$

$$B_n = \lim_{j \rightarrow \infty} \frac{1}{p^j} S_n(p^j).$$

*Demostración:* Con el lema 5.12 tenemos

$$\frac{1}{p^j} S_n(p^j) = \frac{1}{n+1} \sum_{i=1}^n \binom{n+1}{i} B_i p^{j(n-1)} = B_n + p^j \cdot C_j$$

con  $C_j \in \mathbb{Z}$  que, si bien es cierto que depende de  $j$ , su valor absoluto  $p$ -ádico es acotado independientemente de  $j$ , como se ve fácilmente con la proposición 5.13.  $\square$

Gracias a esto, podemos demostrar las *congruencias de Kummer*, que son el primer paso en la dirección para obtener una función zeta  $p$ -ádica.

**Proposición 5.15 (Kummer):** Sea  $p \neq 2$  primo y  $k, m, n \in \mathbb{N}_{\geq 1}$ , y sea  $c \in \mathbb{Z}$  no divisible por  $p$ . Asumamos que  $m \equiv n \pmod{p^k(p-1)}$ . Entonces

$$(1 - c^m)(1 - p^{m-1}) \frac{B_m}{m} \equiv (1 - c^n)(1 - p^{n-1}) \frac{B_n}{n} \pmod{p^{k+1}}.$$

Si  $m, n$  no son divisibles por  $p-1$  entonces incluso

$$(1 - p^{m-1}) \frac{B_m}{m} \equiv (1 - p^{n-1}) \frac{B_n}{n} \pmod{p^{k+1}}.$$

*Demostración (según [Pang7]):* Primero notamos que para cada  $x \in \mathbb{Z}$  con  $(x, p) = 1$  tenemos

$$x^m \equiv x^n \pmod{p^{k+1}} \quad (*)$$

porque  $p^k(p-1) = \#(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times$ . En particular,  $1 - c^m \equiv 1 - c^n \pmod{p^{k+1}}$ . Si  $m \not\equiv 0 \pmod{p-1}$ , entonces siempre existe un  $c \in \mathbb{Z}$  no divisible por  $p$  tal que  $c^m \not\equiv 1 \pmod{p}$ . Por eso la segunda congruencia resulta de la primera.

Del corolario 5.14 vemos fácilmente que en  $\mathbb{Q}_p$

$$(1 - p^{m-1}) B_m = \lim_{j \rightarrow \infty} \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^m$$

y por eso, si  $j \in \mathbb{N}_{\geq 1}$  es suficientemente grande, tenemos

$$\left| (1 - p^{m-1}) B_m - \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^m \right|_p \leq p^{-(k+1)}.$$

Para este  $j$  resulta que

$$(1 - c^m)(1 - p^{m-1}) \frac{B_m}{m} \equiv (1 - c^m) \frac{1}{mp^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^m \pmod{p^{k+1}}.$$

Llamamos  $A \in \mathbb{Q}$  el número racional del lado derecho. Notemos que la congruencia de arriba no es una igualdad en  $\mathbb{Z}/p^{k+1}\mathbb{Z}$ , porque ambos lados pueden contener potencias no triviales de  $p$  en su denominador. Pero su diferencia no contiene potencias de  $p$  en el denominador y el numerador es divisible por  $p^{k+1}$ .

Por lo tanto

$$A = \frac{1}{m} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} \frac{a^m - (ca)^m}{p^j}.$$

Para cada  $a$  ocurriendo en esta suma sea  $b_a \in \{1, \dots, p^j\}$  el único elemento con  $b_a \equiv ca \pmod{p^j}$ . Como  $(c, p) = 1$ , es decir  $c \in (\mathbb{Z}/p^j\mathbb{Z})^\times$ , el mapeo  $a \mapsto b_a$  es una permutación del conjunto

$$\{a \in \{1, \dots, p^j\} : p \nmid a\},$$

y esto nos da

$$A = \frac{1}{m} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} \frac{b_a^m - (ca)^m}{p^j}.$$

Ahora pongamos  $t_a = \frac{b_a - ca}{p^j} \in \mathbb{Z}$ . Entonces

$$b_a^m - (ca)^m = (ca + p^j t)^m - (ca)^m = \sum_{i=1}^m \binom{m}{i} (ca)^{m-i} (p^j t)^i = mp^j t (ca)^{m-1} + K \cdot p^{2j}$$

para un  $K \in \mathbb{Z}$ . Sustituyendo esto en el cálculo anterior obtenemos

$$A = \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} t_a (ca)^{m-1} + p^j \frac{K(p-1)p^{j-1}}{m}.$$

Si hacemos  $j$  tan grande que la fracción de la derecha no contenga una potencia de  $p$  en el denominador y el numerador sea divisible por  $p^{k+1}$ , entonces usando la ecuación (\*) obtenemos la primera congruencia módulo  $p^{k+1}$ :

$$(1 - c^m)(1 - p^{m-1}) \frac{B_m}{m} \equiv A \equiv \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} t_a (ca)^{m-1} \stackrel{(*)}{\equiv} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} t_a (ca)^{n-1} \equiv (1 - c^n)(1 - p^{n-1}) \frac{B_n}{n}. \quad \square$$

La observación importante de Kubota y Leopoldt era que las congruencias que acabamos de demostrar pueden ser reinterpretados en la forma siguiente.

**Proposición 5.16:** *Existe una única función continua*

$$\zeta_{p,0}: \mathbb{Z}_p \setminus \{1\} \rightarrow \mathbb{Q}_p$$

tal que

$$\zeta_{p,0}(1 - n) = (1 - p^{n-1})\zeta(1 - n)$$

para todo  $n \in \mathbb{N}_{\geq 1}$  con  $n \equiv 0 \pmod{p-1}$ .

*Demostración:* Fijemos un  $c \in \mathbb{Z}$  que no es divisible por  $p$ .

Primero observemos que las congruencias de Kummer significan que la función

$$f: D := \{n \in \mathbb{N}_{\geq 1} : p-1 \mid n\} \rightarrow \mathbb{Q}_p, \quad n \mapsto (1 - c^n)(1 - p^{n-1}) \frac{B_n}{n}$$

es uniformemente continua para la métrica  $p$ -ádica: En efecto, esta continuidad significa que

$$\forall \varepsilon > 0 \exists \delta > 0 \forall m, n \in D: |m - n|_p < \delta \implies |f(m) - f(n)|_p < \varepsilon.$$

Si  $m, n \in D$ , la congruencia  $m \equiv n \pmod{p-1}$  es cierta automáticamente. Si asumimos sin pérdida de generalidad que  $\varepsilon$  es de la forma  $\varepsilon = p^{-(k+1)}$  con  $k \in \mathbb{N}_{\geq 1}$ , podemos poner  $\delta = p^{-k}$  y la afirmación es equivalente a las congruencias de Kummer.

Segundo, observemos que el conjunto  $D$  es denso en  $\mathbb{Z}_p$ : necesitamos ver que para cada  $z \in \mathbb{Z}$  y  $k \in \mathbb{N}_{\geq 1}$  existe un  $l \in \mathbb{Z}$  con  $p^k l - z \in D$  (porque entonces  $z$  está en la cerradura de  $D$ ). Por eso simplemente tomamos  $l$  como un entero que satisface

$$l \equiv \frac{a-z}{p^k} \pmod{p-1}$$

y suficientemente grande tal que  $p^k l - z \in \mathbb{N}_{\geq 1}$ .

El conjunto  $D$  es denso también en  $\mathbb{Z}_p \setminus \{1\}$ , y esto demuestra que la función que buscamos es única si existe. Por la densidad de  $D$  en  $\mathbb{Z}_p$  y la continuidad uniforme, la función  $f$  de arriba se extiende a una función continua  $f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ . Entonces escogimos  $c \in 1 + p\mathbb{Z}$  y definimos  $\zeta_p$  como

$$\zeta_{p,0}: \mathbb{Z}_p \setminus \{1\} \rightarrow \mathbb{Q}_p, \quad 1-s \mapsto -\frac{f(s)}{1-c^s},$$

donde  $c^s$  con  $s \in \mathbb{Z}_p$  es bien definido gracias a la proposición 1.44. Es claro que esta función tiene la propiedad deseada, y por la unicidad es independiente de  $c$ .  $\square$

La función que acabamos de construir se podría llamar de buena fe «función zeta  $p$ -ádica de Riemann». Sin embargo, todavía no es la función que se puede usar en la Teoría de Iwasawa – la «verdadera» construcción la haremos en la siguiente sección. Para motivar el resultado que demostraremos, continuamos estudiando la función que hemos construido. Por ejemplo, ¿cómo se comporta para los  $n$  con  $n \not\equiv 0 \pmod{p-1}$ ?

Antes de discutir esto, necesitamos un análogo del corolario 5.14 para los números de Bernoulli generalizados para un carácter de Dirichlet  $\chi$ . Para esto fijamos encajes  $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$  y  $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ , que nos permiten ver números algebraicos como números complejos o números  $p$ -ádicos a conveniencia.

**Proposición 5.17:** *Sea  $\chi$  un carácter de Dirichlet de conductor  $N$ . Pongamos*

$$S_{n,\chi}(k) = \sum_{a=1}^k \chi(a) a^n.$$

Entonces en  $\overline{\mathbb{Q}_p}$

$$B_{n,\chi} = \lim_{j \rightarrow \infty} \frac{1}{Np^j} S_{n,\chi}(Np^j).$$

*Demostración:* La demostración es la misma que la del corolario 5.14, usando la fórmula

$$S_{n,\chi}(kN) = \frac{1}{n+1} \sum_{i=1}^n \binom{n+1}{i} B_{i,\chi}(kN)^{n+1-i}$$

que generaliza el lema 5.12. Esta última fórmula se puede obtener similarmente que la del lema 5.12, véase [Iwa72, p. 11].  $\square$

Nuestros encajes fijados nos permiten en particular considerar el carácter de Teichmüller  $\omega$  como carácter de Dirichlet y definir su serie  $L$  y números de Bernoulli.

**Proposición 5.18:** *Tenemos*

$$\zeta_{p,0}(1-n) = -(1-\omega^{-n}(p)p^{n-1}) \frac{B_{n,\omega^{-n}}}{n}$$

para todo  $n \in \mathbb{N}_{\geq 1}$ , donde  $\omega$  es el carácter de Teichmüller.

*Demostración:* Fijemos  $n \in \mathbb{N}_{\geq 1}$ , y sin pérdida de generalidad supongamos que  $n \not\equiv 0 \pmod{p-1}$ , porque en el caso  $p-1 \mid n$  ya sabemos el resultado. Notemos que el conductor de  $\omega^{-n}$  es  $p$  si  $p-1 \nmid n$ , así que la afirmación en este caso simplemente es  $\zeta_{p,0}(1-n) = -B_{n,\omega^{-n}}/n$ .

Necesitamos una sucesión  $(n_k)_{k \in \mathbb{N}_{\geq 1}}$  de enteros positivos, todos divisibles por  $p-1$ , que converja a  $n$  en  $\mathbb{Z}_p$ : podemos usar

$$n_k = n(p^k(p-2) + 1) = n((p^k - 1)^2 - p^{k+1}(p^{k-1} - 1)).$$

Por el corolario 5.14,

$$-(1 - p^{n_k-1})B_{n_k} = -\lim_{j \rightarrow \infty} \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^{n_k}.$$

Ahora queremos hacer  $k \rightarrow \infty$  e intercambiar este con el límite  $j \rightarrow \infty$ . Para que esto sea permitido, tenemos que ver que la convergencia para  $j \rightarrow \infty$  es uniforme con respecto a  $k$ . Para la claridad de la demostración probaremos esto en el lema siguiente.

Ahora intercambiamos los límites con respecto a  $k$  y  $j$  y obtenemos

$$\lim_{k \rightarrow \infty} (1 - p^{n_k-1})B_{n_k} = \lim_{j \rightarrow \infty} \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} \lim_{k \rightarrow \infty} a^{n_k}.$$

Como  $n_k = n - np^k + n(p-1)p^k$ , tenemos en  $\mathbb{Z}_p$  según el ejercicio 1.8

$$\lim_{k \rightarrow \infty} a^{n_k} = \lim_{k \rightarrow \infty} a^n (a^{p^k})^{-n} (a^{p^k})^{(p-1)n} = a^n \omega(a)^{-n} \omega(a)^{(p-1)n} = \omega^{-n}(a) a^n,$$

porque  $\omega(a)$  es una raíz de la unidad  $(p-1)$ -ésima. Usando la proposición 5.17, esto nos da

$$\lim_{k \rightarrow \infty} (1 - p^{n_k-1})B_{n_k} = \lim_{j \rightarrow \infty} \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} \omega^{-n}(a) a^n = B_{n,\omega^{-n}}$$

y por eso

$$\lim_{k \rightarrow \infty} \zeta_{p,0}(1 - n_k) = -\frac{B_{n,\omega^{-n}}}{n}$$

como deseamos. □

Falta ver la convergencia uniforme que nos permitió en la demostración arriba intercambiar los límites. Esto no depende de la forma concreta de la sucesión  $(n_k)$ .

**Lema 5.19:** *Tenemos*

$$\forall \varepsilon > 0 \exists J_\varepsilon \in \mathbb{N}_{\geq 1} \forall j \geq J_\varepsilon \forall n \in \mathbb{N}_{\geq 1} : \left| \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^n - (1 - p^{n-1})B_n \right|_p \leq \varepsilon.$$

*Demostración:* Sean  $n, j \in \mathbb{N}_{\geq 1}$ . Si sustituimos en la relación (véase también el ejercicio 5.12)

$$\sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^n = S_n(p^j) - p^n S_n(p^{j-1})$$

la fórmula de Bernoulli (lema 5.12), después de un poco de cálculos obtenemos

$$\frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^n = \frac{1}{n+1} \sum_{i=1}^n \binom{n+1}{i} B_i p^{j(n-i)} (1-p^{i-1}).$$

Si  $i = n$  en la suma de la derecha, el sumando correspondiente es  $(n+1)(1-p^{n-1})B_n$ , pues

$$\begin{aligned} \left( \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^n - (1-p^{n-1})B_n \right) &= \frac{1}{n+1} \sum_{i=1}^{n-1} \binom{n+1}{i} B_i p^{j(n-i)} (1-p^{i-1}) \\ &= p^j \sum_{i=1}^{n-1} \frac{p^{n-i}}{n+1-i} \binom{n}{i} B_i (1-p^{i-1}). \end{aligned}$$

Tenemos que acotar esta expresión. Claramente  $\left| \binom{n}{i} \right|_p \leq 1$  y  $|1-p^{i-1}|_p = 1$ . Además, por el teorema de Clausen-von Staudt (proposición 5.13) tenemos

$$|B_n|_p \leq p.$$

Demostremos que para cada  $i = 1, \dots, n-1$  tenemos

$$\left| \frac{p^{n-i}}{n+1-i} \right|_p \leq 1,$$

lo cual es equivalente a  $v_p(n+1-i) \leq n-i$ . Para cada  $k \in \mathbb{N}_{\geq 1}$ ,  $p^k$  es el menor número natural para cual  $v_p$  toma el valor  $k$ . Porque siempre que  $p^k \geq k+1$ , se tiene  $v_p(k+1) \leq k$ . Haciendo  $k = n-i$  nos da la desigualdad deseada.

Ahora sea  $\varepsilon > 0$ , que sin pérdida de generalidad es de la forma  $\varepsilon = p^{-J}$  con un  $J \in \mathbb{N}_{\geq 1}$ . Entonces ponemos  $J_\varepsilon = J+1$  y pues tenemos para  $j \geq J_\varepsilon$  y cada  $n \in \mathbb{N}_{\geq 1}$ :

$$\left| \frac{1}{p^j} \sum_{\substack{a=1 \\ p \nmid a}}^{p^j} a^n - (1-p^{n-1})B_n \right|_p \leq p^{-j+1} \leq p^{-J_\varepsilon+1} = \varepsilon. \quad \square$$

Ahora casi estamos listos para formular el resultado que demuestra cómo la función zeta  $p$ -ádica es vista en la Teoría de Iwasawa.

En la construcción de la función  $\zeta_{p,0}$  en la proposición 5.16 usamos la primera de las congruencias de Kummer de la proposición 5.15. Si usamos la segunda en lugar de la primera, podemos construir de la misma manera funciones continuas

$$\zeta_{p,a} : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$$

para cada  $a \in \{1, \dots, p-2\}$  con la propiedad de que

$$\zeta_{p,a}(1-n) = (1-p^{n-1})\zeta(1-n)$$

para todo  $n \in \mathbb{N}_{\geq 1}$  con  $n \equiv a \pmod{p-1}$ . El mismo razonamiento que hicimos en la proposición 5.18 (véase el ejercicio 5.6) muestra que

$$\zeta_{p,a}(1-n) = -(1-\omega^{-(n+a)}(p)p^{n-1}) \frac{B_{n,\omega^{-(n+a)}}}{n} \quad (5.3)$$

para todo  $n \in \mathbb{N}_{\geq 1}$ . Estas  $p-1$  funciones se llaman ramas de la función zeta  $p$ -ádica, pero esta terminología no es muy importante porque se puede juntar las ramas en una sola función.

Sea  $G = \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ , la cual es isomorfo a  $\mathbb{Z}_p^\times$  via el carácter ciclotómico  $\kappa$ . Definimos una función en el grupo de caracteres de  $G$ .<sup>3</sup> Del lema 1.48 sabemos que cada carácter  $\chi: G \rightarrow \mathbb{Z}_p^\times$  es de la forma

$$\chi = \omega^a \kappa_0^s$$

con únicos  $a \in \{1, \dots, p-1\}$  y  $s \in \mathbb{Z}_p$ . Usando esto definimos la función zeta  $p$ -ádica de Riemann como

$$\zeta_p: \text{Hom}(G, \mathbb{Z}_p^\times) \setminus \{\kappa\} \rightarrow \mathbb{Q}_p, \quad \chi = \omega^a \kappa_0^s \mapsto \zeta_{p,a-1}(s).$$

Resumamos los resultados de esta sección en el teorema siguiente.

**Teorema 5.20:** *La función continua<sup>4</sup>*

$$\zeta_p: \text{Hom}(G, \mathbb{Z}_p^\times) \setminus \{\kappa\} \rightarrow \mathbb{Q}_p$$

tiene la propiedad de que

$$\zeta_p(\psi^{-1} \kappa^{1-n}) = (1 - \psi(p)p^{n-1})L(\psi, 1-n)$$

para cada  $n \in \mathbb{N}_{\geq 1}$  y cada carácter de Dirichlet  $\psi$  de  $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ , y esta propiedad la caracteriza únicamente.

*Demostración:* Cada carácter  $\psi$  como arriba tiene la forma  $\psi = \omega^i$  con un  $i \in \{1, \dots, p-1\}$  si identificamos  $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$  con  $(\mathbb{Z}/p\mathbb{Z})^\times$ , y entonces

$$\zeta_p(\psi^{-1} \kappa^{1-n}) = \zeta_p(\omega^{-i} \kappa^{1-n}) = \zeta_p(\omega^{-i+1-n} \kappa_0^{1-n}).$$

La propiedad anunciada pues resulta de (5.3). La unicidad la tenemos porque los caracteres  $\psi^{-1} \kappa^{1-n}$  como arriba son densos en  $\text{Hom}(G, \mathbb{Z}_p^\times) \setminus \{\kappa\}$ , pero omitimos los detalles de verificar esto.  $\square$

Aquí ya podemos reconocer el fenómeno que es típico de las funciones  $L$   $p$ -ádicas: en general, son funciones en caracteres de grupos de Galois tal que si las evaluamos en un producto de un carácter de orden finito  $\psi$  y una potencia entera del carácter ciclotómico obtenemos una modificación de un valor de una función  $L$  compleja chanfleada por  $\psi$ . Observe que la multiplicación por  $1 - \psi(p)p^{n-1}$  quita el factor de Euler para el primo  $p$  de la función  $L(\psi, -)$ . La fórmula en el teorema que describe estos valores se llama la *fórmula de interpolación*. ¡El lector debería volver a considerar cuán sorprendente es que tal cosa exista!

## Ejercicios

**Ejercicio 5.6:** Demuestre la formula (5.3). Para esto es útil usar la sucesión  $(n_k)_{k \in \mathbb{N}_{\geq 1}}$  con  $n_k = n - (n+a)p^k + n(p-1)p^k$ .

**Ejercicio 5.7:** Demuestre la unicidad de la función  $\zeta_p$  en el teorema 5.20.

<sup>3</sup> Del punto de vista moderno, en general las funciones  $L$   $p$ -ádicas son funciones en grupos de caracteres de grupos de Galois. El lector que conozca la tesis de Tate es invitado a comparar esto con el punto de vista de ahí, que considera las funciones  $L$  complejas como funciones en grupos de caracteres de grupos de idèles, que según la teoría de campos de clases son relacionados a los grupos de Galois.

<sup>4</sup> Equipamos  $\text{Hom}(G, \mathbb{Z}_p^\times)$  con la topología compactoabierta.

### 5.3. La construcción de funciones $L$ $p$ -ádicas mediante elementos de Stickelberger

Como hemos dicho anteriormente, queremos ver las funciones  $L$   $p$ -ádicas como elementos en el álgebra de Iwasawa. Explicaremos con más detalle que quiere decir esto.

En esta sección usamos la notación siguiente: Para  $m \in \mathbb{N}_{\geq 1}$  sea  $G_m$  el grupo  $\text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ , que identificamos con  $(\mathbb{Z}/m\mathbb{Z})^\times$  de la manera usual (véase definición 1.24). Si escribimos  $m = Np^r$  con  $N$  no divisible por  $p$  entonces  $G_m \simeq G_N \times G_{p^r}$  canónicamente. Escribimos  $G_{Np^\infty} = \text{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}) = \varprojlim_{r \in \mathbb{N}_{\geq 1}} G_{Np^r}$ . El grupo  $G_{p^\infty}$  será el más importante de todos y lo llamamos simplemente  $G$ . Notemos que entonces  $G_{Np^\infty} \simeq G_N \times G$ . Además, por el carácter ciclotómico tenemos un isomorfismo  $G \simeq \mathbb{Z}_p^\times$ , que se descompone como  $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$  según lema 1.43, y denotemos  $\Delta$  y  $\Gamma$  los subgrupos de  $G$  correspondiendo a  $\mathbb{F}_p^\times$  y  $1 + p\mathbb{Z}_p$ , respectivamente. Es decir,  $\Delta = G_p = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$  y  $\Gamma = \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p))$ .

Sea  $\Lambda(G)$  el álgebra de Iwasawa de  $G$ . Si  $\mu \in \Lambda(G)$  es un elemento, la propiedad universal (proposición 1.7) nos da para cada carácter  $\psi: G \rightarrow \overline{\mathbb{Q}}_p^\times$  un morfismo, que llamamos igualmente,  $\psi: \Lambda(G) \rightarrow \overline{\mathbb{Q}}_p$ .<sup>5</sup> Abusando de la notación, escribimos  $\mu(\psi) := \psi(\mu)$  como la imagen de  $\mu$  por este morfismo. De esta manera, cada elemento del álgebra de Iwasawa define una función

$$\mu: \text{Hom}(G, \overline{\mathbb{Q}}_p^\times) \rightarrow \overline{\mathbb{Q}}_p.$$

Esta función es la misma que la que obtenemos si consideramos  $\mu$  como medida en  $G$  como en la sección 2.2.

Lo que vamos a demostrar aquí es que la función  $\zeta_p$  del teorema 5.20 esencialmente viene de un tal elemento. Esto lo lograremos con una construcción completamente nueva mediante elementos de Stickelberger, la cual es independiente de los resultados de la sección anterior. En resumen, en esta sección damos otra construcción de la función  $\zeta_p$  más apegada a los métodos modernos en la Teoría de Iwasawa.

En esta sección continuamos fijando encajes  $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$  y  $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ . Aquí seguimos esencialmente [Iwa72, §6], aunque nuestro punto de vista es un poco más moderno.

**Definición 5.21:** Sea  $m \in \mathbb{N}_{\geq 1}$ , el *elemento de Stickelberger de nivel  $m$*  es

$$\Sigma_m = -\frac{1}{m} \sum_{\substack{a=1 \\ (a,m)=1}}^m a\sigma_a^{-1} \in \mathbb{Q}[G_m].$$

El interés en este elemento originalmente proviene del *teorema de Stickelberger* (véase [Was97, Thm. 6.10] y el corolario 6.21 más tarde), que dice que el ideal  $\mathbb{Z}[G_m] \cap \Sigma_m \mathbb{Z}[G_m]$  de  $\mathbb{Z}[G_m]$  anula el grupo de clases de  $\mathbb{Q}(\mu_m)$ , pero aquí nos interesamos en ese elemento por razones diferentes.

Ahora fijemos  $N$  tal que  $p$  no divide a  $N$ . Para cada  $r$  entonces tenemos el elemento de Stickelberger  $\Sigma_{Np^r} \in \mathbb{Q}[G_{Np^r}]$ . Un cálculo fácil que omitimos aquí demuestra que estos elementos son compatibles con respecto a los mapeos  $\mathbb{Q}[G_{Np^r}] \rightarrow \mathbb{Q}[G_{Np^s}]$  para  $r \geq s \geq 1$ . Así obtenemos un elemento

$$\Sigma_{Np^\infty} = (\Sigma_{Np^r})_{r \in \mathbb{N}_{\geq 1}} \in \mathbb{Q}[[G_{Np^\infty}]]$$

que llamamos el elemento de Stickelberger de nivel  $Np^\infty$ . Aquí, por supuesto,  $\mathbb{Q}[[G_{Np^\infty}]]$  denota el límite de anillos de grupos  $\mathbb{Q}[G_{Np^r}]$  aunque  $\mathbb{Q}$  no sea un anillo profinito.

<sup>5</sup> Para ser más exactos, la propiedad universal nos da esto para caracteres con valores en anillos profinitos. Pero cada carácter  $\psi: G \rightarrow \overline{\mathbb{Q}}_p^\times$  tiene valores en un subanillo de  $\overline{\mathbb{Q}}_p$  compacto, y cada anillo topológico que es Hausdorff y compacto automáticamente es profinito. Véase la nota 1.5 y el ejercicio 1.5.

Ahora sea  $K$  una extensión finita de  $\mathbb{Q}_p$  que contiene las raíces de la unidad de orden  $\varphi(N) = \#G_N$ , sea  $\mathcal{O}$  su anillo de enteros  $K$  y  $\Lambda(G) = \mathcal{O}[[G]]$ . Entonces  $K[[G_{Np^\infty}]]$  es un  $K[[G_N]]$ -módulo. Para cada carácter  $\chi: G_N \rightarrow K^\times$  tenemos el idempotente

$$e_\chi = \frac{1}{\varphi(N)} \sum_{g \in G_N} \chi(g)^{-1} g \in K[[G_N]]$$

y podemos descomponer

$$K[[G_{Np^\infty}]] = \bigoplus_{\chi} e_\chi K[[G_{Np^\infty}]]$$

(véase lema 2.20). Entonces, según el lema 2.21, para cada  $\chi$  existe un isomorfismo canónico de  $K$ -álgebras

$$E_\chi: e_\chi K[[G_{Np^\infty}]] \xrightarrow{\cong} K[[G]].$$

Veamos  $\Sigma_{Np^\infty}$  como elemento de  $K[[G_N]]$ . Además fijemos un encaje  $K \hookrightarrow \overline{\mathbb{Q}}_p$  y un carácter de Dirichlet  $\chi$  de conductor  $N$ , que podemos ver como carácter de  $G_N$  con valores en  $K$ .

**Definición 5.22:** Definimos  $\mu_\chi := E_{\chi^{-1}}(e_{\chi^{-1}} \Sigma_{Np^\infty}) \in K[[G]]$ . Este elemento se llama la *función  $L$   $p$ -ádica* de  $\chi$ .

En los siguientes teoremas vamos a justificar este nombre. El ejercicio 5.11 da una representación más explícita de este elemento que usamos a continuación.

Por simplicidad, por ahora asumimos que  $\chi$  sea no trivial, es decir  $N > 1$ . El caso del carácter trivial es similar, pero ligeramente más complicado, y lo explicaremos más tarde.

**Lema 5.23:** *De hecho  $\mu_\chi \in \Lambda(G)$  si  $\chi$  es un carácter no trivial.*

*Demostración:* Usamos la representación del ejercicio 5.11. Tenemos

$$\begin{aligned} \sum_{\substack{a=1 \\ (a, Np)=1}}^{Np^r} a \chi(a) \pi_r(\sigma_a)^{-1} &= \sum_{\substack{b=1 \\ (b, p)=1}}^{p^r} \sum_{\substack{c=1 \\ (c, Np)=1 \\ c \equiv b \pmod{p^r}}}^{Np^r} c \chi(c) \pi_r(\sigma_b)^{-1} \\ &\equiv \sum_b \left( \sum_c \chi(c) \right) b \pi_r(\sigma_b)^{-1} \pmod{p^r} \end{aligned}$$

(las últimas sumas yendo sobre los mismos  $b$  y  $c$  como en la línea anterior). Pero si  $c$  pasa por estos elementos, la clase de  $c$  módulo  $N$  pasa por todos elementos de  $G_N$ . Por eso  $\sum_c \chi(c) = 0$  porque  $\chi$  es un carácter no trivial (como demostramos en el ejercicio 2.12). Esto demuestra que la suma con que empezamos arriba es divisible por  $p^r$ , así  $\mu_{\chi, r} \in \mathcal{O}[G_{p^r}]$ .  $\square$

El elemento  $\mu_\chi \in \Lambda(G)$  que acabamos de construir se comporta como anunciamos al principio de la sección: Define una función en  $\text{Hom}(G, \overline{\mathbb{Q}}_p^\times)$  que es descrita por una fórmula de interpolación similar a la del teorema 5.20.

**Teorema 5.24:** *Sea  $\psi: G \rightarrow \overline{\mathbb{Q}}_p^\times$  un carácter de orden finito y  $n \in \mathbb{N}_{\geq 1}$ . Entonces*

$$\mu_\chi(\psi^{-1} \kappa^{1-n}) = (1 - \chi\psi(p)p^{n-1})L(\chi\psi, 1 - n).$$

La demostración de este teorema la haremos más tarde. Primero expliquemos como podemos extender la construcción al caso en que el carácter  $\chi$  sea trivial, es decir  $N = 1$ , puesto que este caso (que corresponde a la función zeta de Riemann) es el que nos interesa más.

5.3 La construcción de funciones  $L$   $p$ -ádicas mediante elementos de Stickelberger

Si  $\chi = \mathbf{1}$  es trivial, el elemento  $\mu_1$  (que en este caso simplemente es igual al elemento de Stickelberger  $\Sigma_{p^\infty} \in \mathbb{Q}_p[[G]]$  de nivel  $p^\infty$ ) se comporta similarmente. Lo que ya no funciona es la demostración del lema 5.23, que es la única ocasión en la que usamos que  $\chi$  era no trivial, y de hecho la afirmación  $\mu_1 \in \Lambda(G)$  ya no es verdad. Sin embargo  $\mu_1$  está en el anillo de cocientes de  $\Lambda(G)$ , y podemos calcular explícitamente su denominador.

**Definición 5.25:** Para cada  $N \in \mathbb{N}_{\geq 1}$  definimos un elemento

$$h_N = 1 - (1 + Np)\sigma_{1+Np}^{-1} \in \Lambda(G).$$

donde  $\sigma_{1+Np} \in G$  es el único elemento con  $\kappa(\sigma_{1+Np}) = 1 + Np$ . Además definimos para cada  $i \in \{1, \dots, p-1\}$

$$h_N^{(i)} = 1 - (1 + Np)e_{\omega^i}\sigma_{1+Np}^{-1} \in \Lambda(G)$$

donde  $e_{\omega^i}$  es el idempotente del lema 2.20.

**Lema 5.26:** Tenemos  $h_1^{(1)}\mu_1 \in \Lambda(G)$ .

*Demostración:* Aunque la afirmación de este lema es importantísima, no damos la demostración en detalle porque usa argumentos muy similares a los que explicamos en otras demostraciones de esta sección (por ejemplo en la del teorema 5.28). Sin embargo, describimos los pasos más importantes en el ejercicio 5.13.  $\square$

**Lema 5.27:** Sea  $N \in \mathbb{N}_{\geq 1}$  coprimo a  $p$ ,  $i \in \{1, \dots, p-1\}$  y  $\phi: G \rightarrow \overline{\mathbb{Q}}_p^\times$  un carácter. Escribimos  $\phi = \omega^j\phi_0$  usando la decomposición  $G \simeq \mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$  del lema 1.43, con  $j \in \{1, \dots, p-1\}$ . Entonces tenemos

$$\phi(h_N^{(i)}) = \begin{cases} 1 - (1 + Np)\phi_0(1 + Np)^{-1}, & j = i, \\ 1, & j \neq i. \end{cases}$$

En particular

$$\phi(h_N^{(i)}) = 0 \iff \phi = \omega^i\kappa_0.$$

*Demostración:* De la definición de  $e_{\omega^i}$  obtenemos fácilmente

$$\phi(e_{\omega^i}\sigma_{1+Np}^{-1}) = \frac{1}{p-1} \left( \sum_{a=1}^{p-1} \omega^{j-i}(a) \right) \phi_0(1 + Np)^{-1}.$$

La suma en los paréntesis es igual a  $p-1$  si  $j = i$  y es cero si  $j \neq i$ . Obtenemos la fórmula para  $\phi(h_N)$ .

La última afirmación entonces es cierta porque  $1 + Np$  es un generador topológico de  $1 + p\mathbb{Z}_p$ .  $\square$

Ahora podemos enunciar el teorema para el carácter trivial. Los lemas 5.26 y 5.27 muestran que, aunque  $\mu_1$  no define una función en todo  $\text{Hom}(G, \overline{\mathbb{Q}}_p^\times)$ , todavía define una función en  $\text{Hom}(G, \overline{\mathbb{Q}}_p^\times) \setminus \{\kappa\}$ .

**Teorema 5.28:** Sea  $\psi: G \rightarrow \overline{\mathbb{Q}}_p^\times$  un carácter de orden finito y  $n \in \mathbb{N}_{\geq 1}$ . Entonces

$$\mu_1(\psi^{-1}\kappa^{1-n}) = (1 - \psi(p)p^{n-1})L(\psi, 1 - n).$$

*Demostración (junta de los teoremas 5.24 y 5.28):* Asumamos sin pérdida de generalidad que  $\mathcal{O}$  sea suficientemente grande tal que el carácter  $\psi$  tenga valores en  $\mathcal{O}$ . Vamos a demostrar que, para cualquier  $N$  y  $\chi$ , tenemos

$$h_N \mu_\chi(\psi^{-1} \kappa^{1-n}) = h_N(\psi^{-1} \kappa^{1-n})(1 - \chi\psi(p)p^{n-1})L(\chi\psi, 1 - n).$$

Del ejercicio 5.8 sabemos que  $h_N(\psi^{-1} \kappa^{1-n}) \neq 0$ , por eso esto es suficiente.

Sea  $r \in \mathbb{N}_{\geq 1}$ . Usamos la notación siguiente: para cada  $a \in \{1, \dots, Np^r\}$  escribimos  $a(1 + Np) = a_1 + a_2 Np^r$  con  $0 \leq a_1 < Np^r$ . Entonces para estos  $a$  tenemos  $\chi(a(1 + Np)) = \chi(a_1)$  y  $\pi_r(\sigma_{a(1+Np)}) = \pi_r(\sigma_{a_1})$ . Sea  $h_{N,r} \in \mathcal{O}[G_{p^r}]$  la imagen de  $h_N$ . Con esto vemos (escribiendo  $\sum_a$  para la suma sobre los  $a \in \{1, \dots, Np^r\}$  coprimos a  $Np$ ):

$$\begin{aligned} h_{N,r} \mu_{\chi,r} &= \mu_{\chi,r} + \frac{1}{Np^r} \sum_a (a_1 + a_2 Np^r) \chi(a_1) \pi_r(\sigma_{a_1})^{-1} \\ &= -\frac{1}{Np^r} \sum_a a \chi(a) \pi_r(\sigma_a)^{-1} + \frac{1}{Np^r} \sum_a a_1 \chi(a_1) \pi_r(\sigma_{a_1})^{-1} + \sum_a a_2 \chi(a_1) \pi_r(\sigma_{a_1})^{-1} \\ &= \sum_a a_2 \chi(a_1) \pi_r(\sigma_{a_1})^{-1} \in \mathcal{O}[G_{p^r}] \end{aligned} \quad (5.4)$$

por que si  $a$  pasa por los  $a \in \{1, \dots, Np^r\}$  coprimos a  $Np$ ,  $a_1$  pasa por los mismos elementos.

Ahora fijamos  $r$  tal que el conductor de  $\psi$  divida a  $p^r$ , que significa que podemos ver  $\psi$  como carácter de  $G_r$ . Sea  $\kappa_r$  el isomorfismo  $G_r \xrightarrow{\sim} (\mathbb{Z}/p^r\mathbb{Z})^\times$  y  $\psi_r$  la composición de  $\psi: G_r \rightarrow \mathcal{O}^\times$  con la proyección  $\mathcal{O}^\times \rightarrow (\mathcal{O}/p^r\mathcal{O})^\times$ . Entonces tenemos diagramas conmutativos

$$\begin{array}{ccc} G & \xrightarrow{\kappa} & \mathbb{Z}_p^\times \\ \downarrow & & \downarrow \\ G_r & \xrightarrow{\kappa_r} & (\mathbb{Z}/p^r\mathbb{Z})^\times \end{array} \quad \begin{array}{ccc} G & \xrightarrow{\psi} & \mathcal{O}^\times \\ \downarrow & & \downarrow \\ G_r & \xrightarrow{\psi_r} & (\mathcal{O}/p^r\mathcal{O})^\times \end{array}$$

y como  $(\mathbb{Z}/p^r\mathbb{Z})^\times \subseteq (\mathcal{O}/p^r\mathcal{O})^\times$ , el carácter  $\psi_r^{-1} \kappa_r^{1-n}$  induce un homomorfismo  $\psi_r^{-1} \kappa_r^{1-n}: \mathcal{O}[G_r] \rightarrow \mathcal{O}/p^r$ .

Ahora consideramos  $\psi_r^{-1} \kappa_r^{1-n}(h_{N,r} \mu_{\chi,r}) \in \mathcal{O}/p^r$ . Por la definición de  $\kappa_r$  y  $\pi_r$  tenemos

$$\kappa_r^{1-n}(\pi_r(\sigma_a)^{-1}) = \kappa_r^{n-1}(\pi_r(\sigma_a)) = \kappa_r^{n-1}(\pi_r(\sigma_{a_1})) \equiv a_1^{n-1} \pmod{p^r}$$

para  $a \in \{1, \dots, Np^r\}$  coprimo a  $Np$ . Además tenemos  $\psi^{-1}(\pi_r(\sigma_a)^{-1}) = \psi(\pi_r(\sigma_a)) = \psi(a) = \psi(a_1)$  para los mismos  $a$ . Esto demuestra que

$$\psi_r^{-1} \kappa_r^{1-n}(h_{N,r} \mu_{\chi,r}) \equiv \sum_a \chi\psi(a_1) a_1^{n-1} a_2 \pmod{p^r}.$$

Ahora usamos un truco con el teorema del binomio. Este nos dice que

$$((1 + Np)a)^n = (a_1 + a_2 Np^r)^n \equiv a_1^n + n a_1^{n-1} a_2 Np^r \pmod{p^{2r}}$$

y pues

$$\begin{aligned} \chi\psi(1 + Np)(1 + Np)^n \sum_a \chi\psi(a) a^n &= \sum_a \chi\psi(a_1) ((1 + Np)a)^n \\ &\equiv \sum_a \chi\psi(a_1) a_1^n + n Np^r \sum_a \chi\psi(a_1) a_1^{n-1} a_2 \pmod{p^{2r}}. \end{aligned}$$

Pero si dos expresiones en  $\mathcal{O}$  son congruentes módulo  $p^{2r}$  y una de ellas es divisible por  $p^r$ , entonces la otra también es divisible por  $p^r$ , y si dividimos las dos por  $p^r$  entonces los resultados serán congruentes módulo  $p^r$ . Aplicamos esta observación aquí y obtenemos

$$\begin{aligned} \psi_r^{-1} \kappa_r^{1-n}(h_{N,r} \mu_{\chi,r}) &\equiv -(1 - \chi\psi(1 + Np)(1 + Np)^n) \frac{1}{nNp^j} \sum_a \chi\psi(a) a^n \\ &= -\frac{1}{n} h_N(\psi^{-1} \kappa^{1-n}) \frac{1}{Np^r} (S_{n,\chi\psi}(Np^r) - \chi\psi(p) p^n S_{n,\chi\psi}(Np^{r-1})) \text{ mód } p^r \end{aligned}$$

con  $S_{n,\chi\psi}(Np^r)$  como en la proposición 5.17 (aquí usamos una fórmula del ejercicio 5.12).

Por la conmutatividad de los diagramas de arriba, esto significa que

$$\begin{aligned} h_N \mu_\chi(\psi^{-1} \kappa^{1-n}) &\equiv \\ &= -\frac{1}{n} h_N(\psi^{-1} \kappa^{1-n}) \left( \frac{1}{Np^r} S_{n,\chi\psi}(Np^r) - \chi\psi(p) p^{n-1} \frac{1}{Np^{r-1}} S_{n,\chi\psi}(Np^{r-1}) \right) \text{ mód } p^r \end{aligned}$$

para cada  $r \in \mathbb{N}_{\geq 1}$  suficientemente grande y la afirmación pues resulta de la proposición 5.17.  $\square$

**Proposición 5.29:** *Las fórmulas de interpolación de los teoremas 5.24 y 5.28 caracterizan el elemento  $\mu_\chi$  de manera única.*

*Demostración:* Si tenemos dos elementos con esta propiedad de interpolación entonces su diferencia está en el núcleo del morfismo  $\psi^{-1} \kappa^{1-n}: \Lambda(G) \rightarrow \mathcal{O}$  para cada  $n \in \mathbb{N}_{\geq 1}$  y  $\psi$  de orden finito. Para  $i \in \{1, \dots, p-1\}$  y  $n \in \mathbb{N}_{\geq 1}$  sea  $K_{i,n} \subseteq \Lambda(G)$  el núcleo del morfismo  $\Lambda(G) = \mathcal{O}[[G]] \rightarrow \mathcal{O}$  inducido por  $\omega^i \kappa_0^{1-n}: \Delta \times \Gamma \rightarrow \mathcal{O}^\times$ . Vamos a demostrar que

$$\bigcap_{\substack{1 \leq i \leq p-1 \\ n \in \mathbb{N}_{\geq 1}}} K_{i,n} = 0.$$

Para eso usamos el morfismo  $\mathcal{O}[[G]] \rightarrow \mathcal{O}[[\Gamma]]$  inducido por

$$G \simeq \Delta \times \Gamma \rightarrow \Lambda(\Gamma)^\times, \quad g = (\delta, \gamma) \mapsto \omega^i(\delta)\gamma$$

que llamamos  $\omega^i \text{id}_\Gamma$ . Es fácil ver que entonces el diagrama

$$\begin{array}{ccc} & \xrightarrow{\omega^i \kappa_0^{1-n}} & \\ \mathcal{O}[[G]] & \xrightarrow{\omega^i \text{id}_\Gamma} \mathcal{O}[[\Gamma]] & \xrightarrow{\kappa_0^{1-n}} \mathcal{O} \end{array}$$

es conmutativo. Llamamos  $\tilde{K}_n$  el núcleo del morfismo  $\mathcal{O}[[\Gamma]] \rightarrow \mathcal{O}$  inducido por  $\kappa_0^{1-n}$ . Entonces, para cada elemento de la intersección de los  $K_{i,n}$  de arriba, su imagen bajo  $\omega^i \text{id}_\Gamma$  está en  $\tilde{K}_n$  para cada  $n \in \mathbb{N}_{\geq 1}$ . Por eso es suficiente demostrar que

$$\bigcap_{n \in \mathbb{N}_{\geq 1}} \tilde{K}_n = 0.$$

Ahora usamos el isomorfismo

$$\mathcal{O}[[T]] \xrightarrow{\simeq} \mathcal{O}[[\Gamma]], \quad T \mapsto \gamma - 1$$

del teorema 2.11 (donde usamos  $\gamma = \sigma_{1+p} \in \Gamma$  como generador topológico). Un elemento de  $\bigcap_n \tilde{K}_n$  corresponde a una serie de potencia  $f \in \mathcal{O}[[T]]$  tal que

$$f((1+p)^{1-n} - 1) = 0 \quad \text{para cada } n \in \mathbb{N}_{\geq 1}.$$

Pero el teorema de preparación de Weierstraß (teorema 2.4 y ejercicio 2.2) muestra que una serie de potencia con una infinitud de ceros es cero.  $\square$

Esto termina la construcción de las funciones  $L$   $p$ -ádicas mediante elementos de Stickelberger. Comparemos los resultados con el resultado preliminar del teorema 5.20. Ahí construimos una función continua

$$\text{Hom}(G, \overline{\mathbb{Q}}_p^\times) \setminus \{\kappa\} \rightarrow \overline{\mathbb{Q}}_p^\times$$

que es caracterizada de manera única por una fórmula de interpolación que relaciona los valores de la función con valores de funciones  $L$  complejas. Aquí construimos un elemento  $\mu_1$  en el anillo de cocientes de  $\Lambda(G)$  que define la misma función en  $\text{Hom}(G, \overline{\mathbb{Q}}_p^\times) \setminus \{\kappa\}$  y por eso la hace «más algebraica»; aunado a esto, el elemento otra vez es únicamente caracterizado por esta propiedad. Además, logramos construir un elemento análogo  $\mu_\chi$  también para las funciones  $L$  de cualquier carácter de Dirichlet  $\chi$  cuyo conductor no sea divisible por  $p$ .

### Ejercicios

**Ejercicio 5.8:** (a) Use las relaciones del lema 2.20 para demostrar que

$$h_N - 1 = \sum_{i=1}^{p-1} (h_N^{(i)} - 1)$$

(donde usamos la notación introducida en la definición 5.25).

(b) Sea  $\phi: G \rightarrow \overline{\mathbb{Q}}_p^\times$  que escribimos como  $\phi = \omega^j \phi_0$  como en el lema 5.27. Deduzca de (a) y este lema que  $\phi(h_N) = 1 - (1 + Np)\phi_0(1 + Np)^{-1}$ , independientemente de  $j$ .

(c) Concluye que  $\phi(h_N) = 0 \iff \phi_0 = \kappa_0$ .

**Ejercicio 5.9:** Demuestre que  $h_1 \in \Lambda(G)$  es un generador del núcleo de  $\kappa: \Lambda(G) \rightarrow \mathbb{Z}_p$ , así que tenemos un isomorfismo

$$\Lambda(G)/h_1 \simeq \mathbb{Z}_p.$$

Verifique que este isomorfismo es compatible con la acción de  $G$  si dejamos actuar  $g \in G$  en  $\Lambda(G)$  por multiplicación con  $g$  y en  $\mathbb{Z}_p$  por multiplicación con  $\kappa(g)$ .

**Ejercicio 5.10:** Demuestre que los elementos de Stickelberger  $\Sigma_{Np^r} \in \mathbb{Q}[G_{Np^r}]$  son compatibles con respecto a los mapeos  $\mathbb{Q}[G_{Np^r}] \rightarrow \mathbb{Q}[G_{Np^s}]$  para  $r \geq s \geq 1$ .

**Ejercicio 5.11:** Demuestre que  $\mu_\chi = (\mu_{\chi,r}) \in \varprojlim_r K[G_{p^r}]$  con

$$\mu_{\chi,r} = -\frac{1}{Np^r} \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} a\chi(a)\pi_r(\sigma_a)^{-1}$$

donde  $\pi_r: G_{Np^r} \rightarrow G_{p^r}$  es la proyección canónica.

**Ejercicio 5.12:** Sea  $S_{n,\chi\psi}(Np^r)$  como en la proposición 5.17 (para  $n, N, r \in \mathbb{N}_{\geq 1}$  y caracteres  $\chi$  y  $\psi$  como antes). Demuestra que entonces

$$\sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} \chi\psi(a)a^n = S_{n,\chi\psi}(Np^r) - \chi\psi(p)p^n S_{n,\chi\psi}(Np^{r-1}).$$

**Ejercicio 5.13:** En este ejercicio explicamos como demostrar el importante lema 5.26, lo cual dice que  $h_1^{(1)}\mu_1 \in \Lambda(G)$ .

Fijemos  $r \in \mathbb{N}_{\geq 1}$ . A continuación, cuando escribimos  $\sum_a$  esto siempre significa una suma sobre los  $a \in \{1, \dots, p^r\}$  coprimos a  $p$ .

(a) Haga un cálculo similar a (5.4) para ver que

$$h_{1,r}^{(1)} \mu_{1,r} = -\frac{1}{p^r} \sum_a a \pi_r(\sigma_a)^{-1} + \frac{1}{p^r} \sum_a a_1 e_\omega \pi_r(\sigma_{a_1})^{-1} + \text{algo en } \mathcal{O}[G_{p^r}],$$

donde escribimos otra vez  $a(1+p) = a_1 + a_2 p^r$  con  $0 \leq a_1 < p^r$  para  $a \in \{1, \dots, p^r\}$ .

Ahora consideramos la expresión  $A := \sum_a a (e_\omega - 1) \pi_r(\sigma_a)^{-1} \in \mathcal{O}[G_{p^r}]$ . Si podemos demostrar que  $A$  es divisible por  $p^r$  entonces la afirmación resulta de (a).

(b) Use la relación (d) del lema 2.20 para obtener

$$A = \sum_a a \left( \sum_{i=2}^{p-1} e_{\omega^i} \right) \pi_r(\sigma_a)^{-1}.$$

Tenemos una descomposición

$$\mathcal{O}[G_{p^r}] \simeq \bigoplus_{i=1}^{p-1} e_{\omega^i} \mathcal{O}[G_{p^r}],$$

y en el corolario 2.22 vimos que cada uno de los factores  $e_{\omega^i} \mathcal{O}[G_{p^r}]$  es isomorfo a  $\mathcal{O}[\Gamma_r]$  con  $\Gamma_r$  siendo tal que  $G_{p^r} = \Delta \times \Gamma_r$ . Escribimos  $\pi_r^0(\sigma_a)$  para el imagen de  $\pi_r(\sigma_a)$  bajo la proyección  $G_{p^r} \rightarrow \Gamma_r$ .

(c) Verifique que el imagen de  $A$  en la componente  $e_{\omega^i} \mathcal{O}[G_{p^r}] \simeq \mathcal{O}[\Gamma_r]$  corresponde bajo este isomorfismo al elemento

$$A_i := \sum_a \frac{a}{\omega(a)} \omega^{1-i}(a) \pi_r^0(\sigma_a)^{-1} \in \mathcal{O}[\Gamma_r]$$

si  $i \neq 1$  y a 0 si  $i = 1$ .

Esto demuestra que es suficiente demostrar que  $A_i$  es divisible por  $p^r$  para  $i \in \{2, \dots, p-1\}$ . Note que estos  $i$  son justamente aquellos para los cuales el carácter  $\omega^{1-i}$  es no trivial.

(d) Sea  $i \in \{2, \dots, p-1\}$ . Para  $b \in \mathbb{Z}$  con  $p \nmid b$  consideramos la suma parcial

$$\sum_{\substack{a=1 \\ (a,p)=1 \\ \pi_r^0(\sigma_a) = \pi_r^0(\sigma_b)}}^{p^r} \frac{a}{\omega(a)} \omega^{1-i}(a) \pi_r^0(\sigma_a)^{-1} \in \mathcal{O}[\Gamma_r].$$

Verifique que

$$\frac{a}{\omega(a)} \equiv \frac{b}{\omega(b)} \pmod{p^r}$$

para cada  $a$  como en la suma de arriba. Use esto para demostrar que  $A_i$  es divisible por  $p^r$  mediante el argumento que usamos para demostrar el lema 5.23.

## 5.4. Suplementos y consecuencias de la existencia de las funciones $L$ $p$ -ádicas

En la proposición 5.15 demostramos las congruencias de Kummer, que son congruencias módulo potencias de  $p$  entre (esencialmente) valores especiales de la función zeta de Riemann, y luego explicamos que estas congruencias implican la existencia de una función continua  $p$ -ádica que interpola estos valores (teorema 5.20). En la otra dirección, la existencia de los elementos del álgebra de Iwasawa que construimos en la sección anterior implica congruencias en este estilo. Este fenómeno pasa en general para cualquier elemento del álgebra de Iwasawa y pues aplica también a funciones  $L$   $p$ -ádicas más generales (vamos a mencionar unos ejemplos en el capítulo 7). Por eso explicamos la derivación de estas congruencias en una situación general y luego lo aplicamos a los elementos de la sección anterior.

Fijamos  $\mathcal{O}$ , el anillo de enteros de una extensión finita de  $\mathbb{Q}_p$ , y  $G = \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \Delta \times \Gamma$  con  $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$  y  $\Gamma \simeq \mathbb{Z}_p$ . Escribimos  $\Lambda(G) = \mathcal{O}[[G]]$  y  $\Lambda(\Gamma) = \mathcal{O}[[\Gamma]]$ .

En lo siguiente vamos a estudiar caracteres  $\psi: G \rightarrow \mathcal{O}^\times$  y los morfismos  $\Lambda(G) \rightarrow \mathcal{O}$  inducidos por ellos. Se puede ver fácilmente que cada tal carácter es de la forma  $\psi = \omega^i \psi_0$  con  $i \in \{1, \dots, p-1\}$  y  $\psi_0: \Gamma \rightarrow \mathcal{O}^\times$  un carácter (donde  $\omega$  denota el carácter de Teichmüller).

Fijamos  $\mu \in \Lambda(G)$ . Por el isomorfismo del lema 2.21,  $\mu$  corresponde a una colección

$$(\mu_1, \dots, \mu_{p-1}) \in \Lambda(\Gamma)^{p-1} \simeq \bigoplus_{i=1}^{p-1} e_i \Lambda(G) = \Lambda(G).$$

Para cada  $i \in \{1, \dots, p-1\}$  el elemento  $\mu_i \in \Lambda(\Gamma)$  puede ser definido también como la imagen de  $\mu$  bajo el morfismo  $\omega^i \text{id}_\Gamma: \Lambda(G) \rightarrow \Lambda(\Gamma)$  que ya usamos en la demostración de la proposición 5.29, inducido por

$$G \simeq \Delta \times \Gamma \rightarrow \Lambda(\Gamma)^\times, \quad g = (\delta, \gamma) \mapsto \omega^i(\delta)\gamma.$$

En otras palabras, el diagrama

$$\begin{array}{ccc} \Lambda(G) & \xrightarrow{\omega^i \text{id}_\Gamma} & \Lambda(\Gamma) \\ \downarrow \sim & & \uparrow \sim \\ \bigoplus_{i=1}^{p-1} e_{\omega^i} \Lambda(G) & \longrightarrow & e_{\omega^i} \Lambda(G) \end{array} \quad (5.5)$$

es conmutativo. Eso implica que para cada carácter  $\psi: G \rightarrow \mathcal{O}^\times$  que podemos escribir de la forma  $\psi = \omega^i \psi_0$  con  $i \in \{1, \dots, p-1\}$  y  $\psi_0: \Gamma \rightarrow \mathcal{O}^\times$  tenemos

$$\mu(\psi) = \mu_i(\psi_0). \quad (5.6)$$

Con estas preparaciones ahora podemos formular y probar dos resultados generales sobre propiedades de valores especiales de  $\mu$ .

**Proposición 5.30:** *Sea  $\mu \in \Lambda(G)$  y  $\psi: G \rightarrow \mathcal{O}^\times$  un carácter. Entonces tenemos las siguientes congruencias entre los valores de  $\mu$ : Para cada  $k \in \mathbb{N}_{\geq 1}$  existe  $l \in \mathbb{N}_{\geq 1}$  tal que para cada  $m, n \in \mathbb{Z}$  tenemos*

$$m \equiv n \pmod{(p-1)p^l} \implies \mu(\psi \kappa^m) \equiv \mu(\psi \kappa^n) \pmod{p^k}.$$

*Demostración:* Escribimos  $\psi = \omega^j \psi_0$  con  $\psi_0: \Gamma \rightarrow \mathcal{O}^\times$ . Sea  $i \in \{1, \dots, p-1\}$  fijo. La función

$$\mathbb{Z}_p \rightarrow \mathcal{O}, \quad s \mapsto \mu_i(\psi_0 \kappa^s)$$

es continua, y pues uniformemente continua porque  $\mathbb{Z}_p$  es compacto. Como ya explicamos en la demostración de la proposición 5.16, esta continuidad uniforme significa

$$\forall k \in \mathbb{N}_{\geq 1} \exists l \in \mathbb{N}_{\geq 1} \forall m, n \in \mathbb{Z}: \quad m \equiv n \pmod{p^l} \implies \mu_i(\psi_0 \kappa^m) \equiv \mu_i(\psi_0 \kappa^n) \pmod{p^k}.$$

La afirmación entonces resulta de (5.6). □

**Proposición 5.31:** *Sea  $\mu \in \Lambda(G)$  y  $\psi: G \rightarrow \mathcal{O}^\times$  un carácter que escribimos como  $\psi = \omega^i \psi_0$  con  $i \in \{1, \dots, p-1\}$  y  $\psi_0: \Gamma \rightarrow \mathcal{O}^\times$ . Entonces*

$$\mu(\psi) \in \mathcal{O}^\times \iff \mu_i \in \Lambda(\Gamma)^\times.$$

*En particular, si  $m, n \in \mathbb{Z}$  con  $m \equiv n \pmod{p-1}$  entonces*

$$\mu(\kappa^m) \in \mathcal{O}^\times \iff \mu(\kappa^n) \in \mathcal{O}^\times.$$

*Demostración:* Observemos que el morfismo  $\Lambda(\Gamma) \rightarrow \mathcal{O}$  inducido por  $\psi_0$  es local, es decir  $\psi_0(\mathfrak{M}) \subseteq \mathfrak{m}$ , donde  $\mathfrak{M}$  y  $\mathfrak{m}$  son los ideales máximos de  $\Lambda(\Gamma)$  y  $\mathcal{O}$  respectivamente. En efecto, si identificamos  $\Lambda(\Gamma) \simeq \mathcal{O}[[T]]$  mediante el isomorfismo del teorema 2.11 usando un generador topológico  $\gamma$  de  $\Gamma$ , entonces  $\mathfrak{M} = (\pi, T)$ , y solo hay que ver que  $\psi(T) \in \mathfrak{m} = \pi\mathcal{O}$  (porque por linealidad claramente  $\psi(\pi) \in \mathfrak{m}$ ). El elemento  $T$  corresponde a  $\gamma - 1$ , por eso es suficiente demostrar que la imagen de  $\Gamma \subseteq \Lambda(\Gamma)^\times$  está contenido en  $1 + \pi\mathcal{O} \subseteq \mathcal{O}^\times$  (que también demuestra que el argumento no depende del generador topológico  $\gamma$  que eligimos). Para ver esto consideremos la composición

$$\Gamma \xrightarrow{\psi_0} \mathcal{O}^\times \rightarrow (\mathcal{O}/\pi\mathcal{O})^\times$$

donde el segundo mapeo es la proyección canónica. El grupo a la derecha es finito con orden primo a  $p$  mientras el grupo a la izquierda es un grupo pro- $p$ . Por eso la composición debe ser el morfismo trivial (usamos el ejercicio 1.2), así que  $\psi_0(\Gamma) \subseteq 1 + \pi\mathcal{O}$ .

Eso y (5.6) implican que  $\mu(\omega^i \kappa_0^s) = \mu_i(\kappa_0^s) = \kappa_0^s(\mu_i) \in \mathcal{O}^\times$  si y solo si  $\mu_i \in \Lambda(\Gamma)^\times$ .  $\square$

Ahora apliquemos estos resultados a los elementos especiales que construimos en la sección anterior. El primer resultado es una reminiscencia de las congruencias de Kummer (proposición 5.15).

**Corolario 5.32:** *Sea  $\xi$  un carácter de Dirichlet cualquier. Entonces para cada  $k \in \mathbb{N}_{\geq 1}$  existe  $l \in \mathbb{N}_{\geq 1}$  tal que para cada  $m, n \in \mathbb{N}_{\geq 1}$  tenemos*

$$m \equiv n \pmod{(p-1)p^l} \implies (1 - \xi(p)p^{n-1})L(\xi, 1 - n) \equiv (1 - \xi(p)p^{m-1})L(\xi, 1 - m) \pmod{p^k}.$$

*Demostración:* Descomponemos  $\xi = \chi\psi$  con  $\chi$  de conductor no divisible por  $p$  y  $\psi$  de conductor una potencia de  $p$ . Si  $\chi$  no es trivial, la afirmación resulta de aplicar la proposición 5.30 al elemento  $\mu = \mu_\chi$  de la sección anterior, reemplazando  $\psi$  por  $\psi^{-1}$  y  $\kappa^n$  por  $\kappa^{1-n}$  y usando la fórmula de interpolación del teorema 5.24. Si  $\chi$  es trivial, tenemos que usar  $\mu_1$  y la fórmula de interpolación del teorema 5.28, que estrictamente no resulta de la proposición 5.30 porque  $\mu_1 \notin \Lambda(G)$ , pero se puede ver fácilmente que todavía funciona en esta situación (omitimos los detalles).  $\square$

**Corolario 5.33:** *Sea  $\chi$  un carácter de Dirichlet con valores en  $\mathcal{O}$  cuyo conductor no es divisible por  $p$  (permitimos el carácter trivial). Para cada  $m, n \in \mathbb{N}_{\geq 1}$ , si  $m \equiv n \pmod{p-1}$  entonces*

$$L(\chi, 1 - n) \in \mathcal{O}^\times \iff L(\chi, 1 - m) \in \mathcal{O}^\times.$$

*Demostración:* Esto resulta de la proposición 5.31 y las fórmulas de interpolación con las mismas calibraciones como en la demostración anterior (usamos que los factores de Euler  $1 - \chi(p)p^{n-1}$  siempre están en  $\mathcal{O}^\times$ ).<sup>6</sup>  $\square$

Ahora calculamos unos valores especiales más de la función zeta  $p$ -ádica que serán interesantes más tarde. Como vimos en el lema 5.26 de la sección anterior, la función zeta  $p$ -ádica es un elemento  $\mu_1$  del anillo de cocientes de  $\Lambda(G)$  tal que  $h_1^{(1)}\mu_1 \in \Lambda(G)$ . El elemento  $h_1^{(1)} \in \Lambda(G)$  tiene su único zero en el carácter  $\kappa$  (lema 5.27), por eso podemos interpretar esto como la función  $\mu_1$  tiene un único «polo» simple en  $\kappa$ , como la función zeta de Riemann compleja tiene un único polo simple en  $s = 1$ . El valor de  $h_1^{(1)}\mu_1$  es como el «residuo» de  $\mu_1$  en  $\kappa$ . En una aplicación más tarde será importante saber que este «residuo» nunca es divisible por  $p$ , y lo demostramos aquí.

<sup>6</sup> En el caso del carácter trivial tenemos que aplicar la proposición 5.31 a  $\mu = h_1^{(1)}\mu_1$ , que nos da la equivalencia afirmada solo en el caso  $m, n \not\equiv 1 \pmod{p-1}$  porque por lo demás los valores de  $h_1^{(1)}$  son divisible por  $p$  (lema 5.27). Pero aún así la afirmación es cierta también si  $m, n \equiv 1 \pmod{p-1}$ , que podemos ver de las congruencias de Kummer clásicas (proposición 5.15).

**Lema 5.34:** Para cada  $i \in \mathbb{Z}$  tenemos  $\mu_1(\omega^i) = -B_{1,\omega^{-i}} \in \mathbb{Z}_p$ .

*Demostración:* Del ejercicio 5.11 sabemos que  $\mu_1 = (\mu_{1,r})_r$  con

$$\mu_{1,r} = -\frac{1}{p^r} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^r} a\pi_r(\sigma_a)^{-1} \in \mathbb{Q}_p[G_{p^r}].$$

El morfismo  $\Lambda(G)[1/h_1^{(1)}] \rightarrow \mathbb{Q}_p$  inducido por  $\omega^i$  se factoriza a través de  $\Lambda(G)[1/h_1^{(1)}] \rightarrow \mathbb{Q}_p[G_p]$ , así que  $\mu_1(\omega^i)$  es la imagen de

$$\mu_{1,1} = -\frac{1}{p} \sum_{a=1}^{p-1} a\pi_1(\sigma_a)^{-1}$$

bajo el morfismo  $\mathbb{Q}_p[G_p] \rightarrow \mathbb{Q}_p$  inducido por  $\omega^i$ . La afirmación entonces resulta del ejercicio 5.5.  $\square$

**Nota 5.35:** Remarcamos que el elemento  $\mu_{1,1}$  simplemente es el elemento de Stickelberger  $\Sigma_p$ . Es decir, la demostración anterior muestra que  $\mu_1(\omega^i)$  es la imagen del elemento de Stickelberger  $\Sigma_p \in \mathbb{Q}[G_p] \subseteq \mathbb{Q}_p[G_p]$  bajo el morfismo  $\mathbb{Q}_p[G_p] \rightarrow \mathbb{Q}_p$  inducido por  $\omega^i$  (que es igual a  $B_{1,\omega^{-i}}$ ).

**Corolario 5.36:** Tenemos  $h_1^{(1)}\mu_1(\kappa) \in \mathbb{Z}_p^\times$ .

*Demostración:* Según la proposición 5.31, la afirmación es equivalente a  $h_1^{(1)}\mu_1(\omega\kappa_0^s) \in \mathbb{Z}_p^\times$ , para cualquier  $s \in \mathbb{Z}_p$ . Lo probemos para  $s = 0$ . Del lema 5.27 vemos que  $h_1^{(1)}(\omega) = -p$ , así que gracias al lema 5.34 sabemos que

$$h_1^{(1)}\mu_1(\omega) = pB_{1,\omega^{-1}}$$

Según el ejercicio 5.5 tenemos

$$pB_{1,\omega^{-1}} = \sum_{a=1}^{p-1} a\omega^{-1}(a)$$

y falta que ver que esto es invertible en  $\mathbb{Z}_p$ . Esto resulta porque para cada  $a \in \{1, \dots, p-1\}$  tenemos  $a\omega^{-1}(a) \in 1 + p\mathbb{Z}_p$ , así que

$$\sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv -1 \pmod{p}. \quad \square$$

Terminamos esta sección con interpretar las funciones  $L$   $p$ -ádicas geoméricamente, asumiendo que el lector conozca los conceptos básicos de la geometría algebraica. Esto no será importante a continuación, así que omitimos algunos detalles.

En lo esencial, todas las funciones  $L$   $p$ -ádicas son dadas por un elemento  $\mu$  del anillo  $\Lambda(G)$  y por eso define una sección global en el esquema  $X = \text{Spec } \Lambda(G)$ ; en el caso de la función zeta  $p$ -ádica de Riemann son un elemento del anillo de fracciones de  $\Lambda(G)$  que define un elemento de  $\mathcal{O}_X(D(h_1))$ . La fórmula de interpolación del teorema 5.24 describe los valores de esta sección en los ideales primos que son los núcleos de los morfismos  $\Lambda(G) \rightarrow \mathcal{O}$  inducidos por los caracteres de la forma  $\psi^{-1}\kappa^{1-n}$  como en el teorema. La razón detrás de la unicidad que demostramos en la proposición 5.29 es que estos ideales primos son Zariski densos en  $X$

(en el fondo esto es lo que demostramos allá). Es decir, las funciones  $L$   $p$ -ádicas son elementos de  $\mathcal{O}_X(X)$  (o  $\mathcal{O}_X(D(h_1))$ ) cuyos valores en un conjunto denso de puntos son dados por una fórmula de interpolación.

El anillo  $\Lambda(G)$  tiene una propiedad universal bonita en la categoría de  $\mathcal{O}$ -álgebras profinitas (proposición 1.7), pero el esquema  $X$  no tiene la propiedad análoga en la categoría de  $\mathcal{O}$ -esquemas porque los morfismos entre esquemas vienen de *todos* los morfismos entre anillos y no solo de los que son continuos. Es posible rescatar la propiedad universal en el mundo geométrico en usar *esquemas formales* en lugar de esquemas. Más precisamente, el espectro formal  $\mathrm{Spf} \Lambda(G)$  sí tiene una propiedad universal: representa el funtor que a cada  $\mathcal{O}$ -esquema formal (localmente noetheriano)  $Y$  asocia los caracteres (continuos!)  $G \rightarrow \mathcal{O}_Y(Y)^\times$ . De este punto de vista, la función  $L$   $p$ -ádica es una sección global en  $\mathrm{Spf} \Lambda(G)$ , es decir una función en un «espacio de módulos de caracteres». Pero ahora la imagen geométrica ya no es tan bonita: como espacio topológico  $\mathrm{Spf} \Lambda(G)$  es finito y discreto, así que la intuición de que los valores en un conjunto denso de puntos son dados por una fórmula de interpolación ya no funciona.

Se puede combinar las dos intuiciones usando la teoría de *espacios ádicos* introducida por Huber en [Hub94]. El espectro ádico  $\mathrm{Spa}(\Lambda(G), \Lambda(G))$  tiene ambas propiedades deseadas: tiene una propiedad universal análoga en la categoría de espacios ádicos sobre  $\mathcal{O}$  topológicamente de tipo finito y contiene un conjunto denso de puntos que corresponden a los caracteres  $\Lambda(G) \rightarrow \mathcal{O}$ . Por eso, la interpretación geométrica más elegante de las funciones  $L$   $p$ -ádicas es como funciones en el espacio ádico  $\mathrm{Spa}(\Lambda(G), \Lambda(G))$ .

### Ejercicios

**Ejercicio 5.14:** En la demostración del lema 5.34 el cálculo era mucho menos trabajo que en la situación similar en la demostración del teorema 5.28. ¿Por qué es esto y por qué no funciona un argumento similar para simplificar la demostración del teorema 5.28?

## 5.5. La teoría de Coleman y otras maneras de construir la función zeta $p$ -ádica

En la sección 5.3 construimos la función zeta  $p$ -ádica usando los elementos de Stickelberger. Mientras esto fue un poco laborioso, nos dio comprensión de la naturaleza de estos elementos y nos permitió demostrar los suplementos de la sección anterior. Sin embargo, también hay otros métodos para construir la función zeta  $p$ -ádica, y para la completitud queremos mencionar algunos aquí. Los resultados de esta sección no serán usados en el resto del texto, así que el lector es libre de omitir esta sección.

La manera alternativa más importante usa la teoría de las series de potencia de Coleman y unidades ciclotómicas, que son unidades de forma especial en campos ciclotómicos. Su importancia proviene de que esta construcción da aún más información sobre la función zeta  $p$ -ádica que se puede aprovechar para elaborar una demostración de la Conjetura Principal (véase sección 6.4). No vamos a explicar esta teoría aquí en completo, pero queremos esbozar unas ideas de la construcción.

Antes de empezar con esto, queremos mencionar que se puede usar los polinomios de Bernoulli que introducimos en la definición 5.10 el lugar de los elementos de Stickelberger para definir medidas en  $\mathbb{Z}_p^\times$  más directamente cuyos integrales entonces son relacionados con números de Bernoulli y pues la función zeta. Esta construcción es relacionada con la usando los elementos de Stickelberger y es explicada en [Was97, §12.1–2] o [Lang0, §2.2]. Por otra parte, en su libro [Hid93, Chap. 4], Hida desarrolla una manera para construir las funciones  $L$  de Dirichlet  $p$ -ádicas usando métodos de grupos de (co)homología que paralela la construcción de funciones  $L$   $p$ -ádicas para formas modulares, de tal manera facilitando una perspectiva completamente diferente a estas funciones.

En el resto de la sección esbozamos la construcción de la función zeta  $p$ -ádica mediante unidades ciclotómicas y la teoría de Coleman, siguiendo [CS06].

**Definición 5.37:** Para cada  $r \in \mathbb{N}_{\geq 1}$  sea  $U_r = \mathcal{O}_r^\times$  con  $\mathcal{O}_r$  siendo el anillo de enteros del campo  $\mathbb{Q}_p(\mu_{p^r})$ . Entonces la norma envía  $U_s$  a  $U_r$  para cada  $s \geq r \geq 1$  de manera compatible. Definimos

$$U_\infty = \varprojlim_{r \in \mathbb{N}_{\geq 1}} U_r,$$

el límite tomado con respecto a la norma.

El resultado de Coleman, que es demostrado en [Col79], dice lo siguiente. Fijamos para cada  $r \geq 1$  una raíz  $p^r$ -ésima primitiva de la unidad  $\xi_r$  tal que  $\xi_{r+1}^p = \xi_r$  para cada  $r \geq 1$ , y ponemos  $\pi_r = \xi_r - 1$ , que es un uniformizante de  $\mathcal{O}_r$ .

**Teorema 5.38 (Coleman):** Para cada  $u = (u_r)_{r \in \mathbb{N}_{\geq 1}} \in U_\infty$  existe un único  $f_u \in \mathbb{Z}_p[[X]]^\times$  tal que  $f_u(\pi_r) = u_r$  para cada  $r \in \mathbb{N}_{\geq 1}$ .

La demostración de este teorema es un poco laboriosa y remitimos a [Col79] o [CS06, Thm. 2.1.2 y §2.3] para ella. Las series de potencia que aparecen aquí juegan un papel diferente que las que aparecieron en el capítulo 2, por eso llamamos la variable  $X$  en lugar de  $T$ .

Vamos a aplicar el teorema de Coleman sólo a elementos de  $U_\infty$  de una forma especial.

**Definición 5.39:** Para  $a, b \in \mathbb{Z}$  coprimos a  $p$  y cada  $r \in \mathbb{N}_{\geq 1}$  usamos los elementos

$$c_r(a, b) = \frac{\xi_r^{-a/2} - \xi_r^{a/2}}{\xi_r^{-b/2} - \xi_r^{b/2}} \in U_r$$

que estudiamos en el ejercicio 1.6. Estos elementos se llaman *unidades ciclotómicas*. Por el ejercicio 5.15 tenemos  $c_r(a, b) \in U_r$  y los elementos son compatibles con respecto a la norma y pues definen un elemento

$$c(a, b) = (c_r(a, b))_{r \in \mathbb{N}_{\geq 1}} \in U_\infty.$$

Por el teorema de Coleman entonces existe una única serie de potencia  $f_{c(a,b)} \in \mathbb{Z}_p[[X]]^\times$  tal que  $f_u(\pi_r) = c_r(a, b)$  para cada  $r \in \mathbb{N}_{\geq 1}$ . No obstante, en este caso particular no es necesario usar toda la fuerza del teorema: es posible dar la serie  $f_{c(a,b)}$  de forma explícita.

**Lema 5.40:** Sea  $k \in \mathbb{Z}$  coprimo a  $p$  y

$$w_k = \frac{(1+X)^{-k/2} - (1+X)^{k/2}}{X}.$$

Entonces  $w_k \in \mathbb{Z}_p[[X]]^\times$  y  $f_{c(a,b)} = \frac{w_a}{w_b}$  para  $a, b \in \mathbb{Z}$  coprimos a  $p$ . Además, la serie de potencia  $f_{c(a,b)}$  tiene coeficientes en  $\mathbb{Q} \cap \mathbb{Z}_p$ .

*Demostración:* En  $\mathbb{Z}_p[[X]]$  vale<sup>7</sup>

$$(1+X)^s = \sum_{n=0}^{\infty} \binom{s}{n} X^n$$

<sup>7</sup> La expresión  $(1+X)^s$  es bien definida porque  $\mathbb{Z}_p[[X]] \simeq \mathbb{Z}_p[[\Gamma]]$  para cada grupo profinito  $\Gamma$  isomorfo a  $\mathbb{Z}_p$  con  $1+X$  correspondiendo a un generador topológico de  $\Gamma$ .

5.5 La teoría de Coleman y otras maneras de construir la función zeta  $p$ -ádica

para cada  $s \in \mathbb{Z}_p$ . Esto se puede ver del teorema del binomio y un argumento de continuidad. Con esto tenemos

$$\begin{aligned} w_k &= \frac{(1+X)^{-k/2} - (1+X)^{k/2}}{X} = \frac{1}{X} \left( \sum_{n=0}^{\infty} \left( \binom{-k/2}{n} - \binom{k/2}{n} \right) X^n \right) \\ &= \sum_{n=1}^{\infty} \left( \binom{-k/2}{n} - \binom{k/2}{n} \right) X^{n-1}. \end{aligned}$$

De esto vemos que  $w_k(0) = -k \in \mathbb{Z}_p^\times$ , así que  $w_k \in \mathbb{Z}_p[[X]]^\times \cap \mathbb{Q}[[X]]^\times$  (recuerde la definición de  $\binom{\cdot}{n}$  en (2.6)). El resto es claro.  $\square$

A partir de aquí sólo indicamos los próximos pasos para obtener la función zeta  $p$ -ádica a partir del elemento  $f_u$  encontrado arriba. En la sección anterior vimos  $\mathbb{Z}_p^\times$  como « $p-1$  copias de  $\mathbb{Z}_p$ ». Aquí lo consideramos mas bien como subconjunto de  $\mathbb{Z}_p$ . Como  $\mathbb{Z}_p^\times$  es abierto y cerrado de  $\mathbb{Z}_p$ , la función característica  $\mathbb{1}_{\mathbb{Z}_p^\times}$  es continua. Por eso podemos restringir medidas de  $\mathbb{Z}_p$  a  $\mathbb{Z}_p^\times$  de la manera siguiente.

**Definición 5.41:** Para  $\mu \in D(\mathbb{Z}_p, \mathbb{Z}_p)$  definimos una medida  $\mu_! \in D(\mathbb{Z}_p, \mathbb{Z}_p)$  como

$$\mu_!(f) = \mu(\mathbb{1}_{\mathbb{Z}_p^\times} f) \quad (f \in C(\mathbb{Z}_p, \mathbb{Z}_p)).$$

Además definimos una inclusión

$$i: D(\mathbb{Z}_p^\times, \mathbb{Z}_p) \rightarrow D(\mathbb{Z}_p, \mathbb{Z}_p), \quad \int_{\mathbb{Z}_p} f \, di(\eta) = \int_{\mathbb{Z}_p^\times} f|_{\mathbb{Z}_p^\times} \, d\eta \quad (\eta \in D(\mathbb{Z}_p^\times, \mathbb{Z}_p), f \in C(\mathbb{Z}_p, \mathbb{Z}_p)).$$

Se puede verificar entonces que el diagrama

$$\begin{array}{ccc} D(\mathbb{Z}_p, \mathbb{Z}_p) & \xrightarrow{\mu \mapsto \mu_!} & D(\mathbb{Z}_p, \mathbb{Z}_p) \\ \downarrow \sim & & \downarrow \sim \\ \mathbb{Z}_p[[\mathbb{Z}_p]] & \longrightarrow & \mathbb{Z}_p[[T]] \end{array}$$

es conmutativo, donde el mapeo abajo es dado por

$$g \mapsto g - \frac{1}{p} \sum_{\xi \in \mu_p} g(\xi(1+T) - 1) \quad (g \in \mathbb{Z}_p[[\mathbb{Z}_p]]).$$

Eso describe la restricción de medidas en términos de series de potencias. También se puede caracterizar las medidas en  $\mathbb{Z}_p$  que se puede obtener de esta manera: Tenemos

$$i(D(\mathbb{Z}_p^\times, \mathbb{Z}_p)) = \{\mu \in D(\mathbb{Z}_p, \mathbb{Z}_p) \mid \mu = \mu_!\}.$$

Para estos hechos véase [CS06, Lem. 3.4.1, 3.4.2].

Usando estos técnicos y una operación  $\mathcal{L}$  en series de potencias se puede obtener una medida en  $\mathbb{Z}_p^\times$  para cada elemento de  $U_\infty$ . Solo citamos el resultado aquí.

**Proposición 5.42:** Para  $f \in \mathbb{Z}_p[[X]]^\times$  ponemos

$$\mathcal{L}(f) = \frac{1}{p} \log \left( \frac{f^p(T)}{f((1+T)^p - 1)} \right).$$

Entonces esto define un morfismo  $\mathcal{L}: \mathbb{Z}_p[[X]]^\times \rightarrow \mathbb{Z}_p[[T]]$ .<sup>8</sup> Si lo componemos con el morfismo  $\Upsilon$  del corolario 2.19, entonces la composición

$$\Upsilon \circ \mathcal{L}: \mathbb{Z}_p[[X]]^\times \rightarrow D(\mathbb{Z}_p, \mathbb{Z}_p)$$

envía los elementos de la forma  $f_u$  para  $u \in U_\infty$  a  $i(D(\mathbb{Z}_p^\times, \mathbb{Z}_p))$ . De esta manera obtenemos para cada  $u \in U_\infty$  una medida  $\lambda_u \in D(\mathbb{Z}_p^\times, \mathbb{Z}_p)$ .

*Demostración:* [CS06, Lem. 2.5.1] □

Por supuesto los integrales de las medidas obtenidas de esta manera deberían tener algo que ver con las unidades en  $U_\infty$  con cuales empezamos. Para explicar esta relación usamos los mapeos

$$D: \mathbb{Z}_p[[X]] \rightarrow \mathbb{Z}_p[[X]], \quad f \mapsto (1+X)f'$$

y para cada  $n \in \mathbb{N}_{\geq 1}$

$$\delta_n: U_\infty \rightarrow \mathbb{Z}_p, \quad u \mapsto \left( D^{n-1} \left( \frac{(1+X)f'_u}{f_u} \right) \right) (0)$$

(donde «(0)» significa evaluación de la serie de potencia en  $X=0$ ).

**Lema 5.43:** (a) Para cada  $u \in U_\infty$  y  $n \in \mathbb{N}_{\geq 1}$  tenemos

$$\int_{\mathbb{Z}_p^\times} x^n d\lambda_u(x) = (1-p^{n-1})\delta_n(u).$$

(b) Para  $a, b \in \mathbb{Z}$  coprimos a  $p$  y cada  $n \in \mathbb{N}_{\geq 1}$  tenemos

$$\delta_n(c(a, b)) = (b^n - a^n)\zeta(1-n).$$

*Demostración:* Seguimos [CS06, Lem. 3.3.5, Prop. 3.5.2, Prop. 2.6.3], a donde remitimos para más detalles.

Primero vamos a describir que hace el mapeo  $D$  con medidas. Esto hacemos por el diagrama

$$\begin{array}{ccc} \mathbb{Z}_p[[T]] & \xrightarrow{D} & \mathbb{Z}_p[[T]] \\ \mathcal{M} \uparrow \downarrow \Upsilon & & \mathcal{M} \uparrow \downarrow \Upsilon \\ D(\mathbb{Z}_p, \mathbb{Z}_p) & \longrightarrow & D(\mathbb{Z}_p, \mathbb{Z}_p) \end{array}$$

que conmuta si definimos el mapeo abajo por

$$\mu \mapsto \left[ f \mapsto \int_{\mathbb{Z}_p} xf(x) d\mu(x) \right];$$

eso es fácil de verificar y omitimos aquí el cálculo que lo muestra. Inductivamente, esto nos da

$$\int_{\mathbb{Z}_p} x^n d\Upsilon(g)(x) = (D^n g(T))(0) \quad \text{para cada } g \in \mathbb{Z}_p[[T]], \quad n \in \mathbb{N}_{\geq 0}$$

(el caso  $n=0$  es el ejercicio 2.8).

Ahora ponemos  $g = \mathcal{L}(f_u)$  aquí. Un cálculo usando la definición del mapeo  $\mathcal{L}$  y de  $D$  muestra que

$$D(\mathcal{L}(f_u)) = h_u - h_u((1+T)^p - 1)$$

<sup>8</sup> Notemos que después del mapeo  $\mathcal{L}$  ya llamamos la variable  $T$ , porque estas series de potencia las identificaremos con medidas, es decir sí juegan el mismo papel que las de el capítulo 2.

5.5 La teoría de Coleman y otras maneras de construir la función zeta  $p$ -ádica

con  $h_u = (1+T)\frac{f'_u}{f_u}$ , así que inductivamente obtenemos

$$\int_{\mathbb{Z}_p} x^n d\Upsilon(\mathcal{L}(f_u))(x) = D^{n-1}(h_u - h_u((1+T)^p - 1))(0).$$

Además se puede verificar la relación

$$D^{n-1}(h_u((1+T)^p - 1)) = p^{n-1}D^{n-1}(h_u)((1+T)^p - 1).$$

Usando esto, la linealidad de  $D$  y la definición de  $\delta_n$  obtenemos (a).

Para (b) usamos que conocemos la forma de la serie de potencia involucrada: sea

$$f = \frac{(1+T)^{-a/2} - (1+T)^{a/2}}{(1+T)^{-b/2} - (1+T)^{b/2}}.$$

Sabemos del lema 5.40 que  $f_{c(a,b)} = f$  y que además esta serie de potencia tiene coeficientes en  $\mathbb{Q}$ . Esto nos permite poner números reales o complejos en  $f$ . Vamos a poner  $T = e^z - 1$  con  $z \in \mathbb{C}$  porque esto troca el mapeo  $D$  en algo simple:  $Df(e^z - 1) = \frac{d}{dz}f(e^z - 1)$ . Es decir

$$\delta_n(c(a,b)) = \left( \left( \frac{d}{dz} \right)^{n-1} g(z) \right)_{z=0}$$

con

$$g(z) = \frac{d}{dz} \log f(e^z - 1).$$

Calculando explícitamente que es  $g$  obtenemos

$$g(z) = \frac{1}{2}b \left( \frac{1}{e^{-bz} - 1} - \frac{1}{e^{bz} - 1} \right) - \frac{1}{2}a \left( \frac{1}{e^{-az} - 1} - \frac{1}{e^{az} - 1} \right)$$

Si escribimos

$$\tilde{f}(t) = \frac{t}{1 - e^{-t}} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \quad (t \in \mathbb{C})$$

para la función definiendo los números de Bernoulli (para distinguirla de la serie de potencia  $f$ ), esto es igual a

$$\begin{aligned} g(z) &= -\frac{1}{2z}(\tilde{f}(-bz) + \tilde{f}(bz)) + \frac{1}{2z}(\tilde{f}(-az) + \tilde{f}(az)) \\ &= \sum_{n=1}^{\infty} B_n \frac{z^{n-1}}{n!} (a^n - b^n) \end{aligned}$$

porque  $B_n = 0$  para  $n > 1$  impar. De esto obtenemos el resultado.  $\square$

Estamos listos para definir la función zeta  $p$ -ádica.

**Definición 5.44:** Sean  $a, b \in \mathbb{Z}$  coprimos a  $p$ . Definimos

$$\lambda_{\mathbf{1}} = \frac{\lambda_{c(a,b)}}{\sigma_b - \sigma_a}.$$

**Teorema 5.45:** El elemento  $\lambda_{\mathbf{1}}$  es una pseudo-medida, independiente de  $a$  y  $b$ , y para cada  $n \in \mathbb{N}_{\geq 1}$  tenemos

$$\int_{\mathbb{Z}_p^\times} x^n d\lambda_{\mathbf{1}}(x) = (1 - p^{n-1})\zeta(1 - n).$$

Esta propiedad lo caracteriza únicamente.

*Demostración:* Seguimos [CS06, Prop. 4.2.4]. El hecho de que la propiedad de interpolación determina únicamente al elemento  $\lambda_1$  se demuestra de manera igual como lo hicimos para el elemento  $\mu_1$  en la proposición 5.29. En particular,  $\lambda_1$  no depende de  $a$  y  $b$  una vez que sabemos la propiedad de interpolación (si es una pseudo-medida). Para ver esta fórmula solo hay que observar que

$$\int_{\mathbb{Z}_p^\times} x^n d(\sigma_b - \sigma_a) = b^n - a^n \quad \text{para cada } n \in \mathbb{N}_{\geq 1},$$

así que la fórmula sigue del lema 5.43 (b). Lo único que entonces falta que ver es que  $\lambda_1$  es una pseudo-medida. Para eso ponemos  $b = 1$  y  $a = e$  con  $e$  un generador de  $\mathbb{F}_p^\times$  tal que  $e^{p-1} \not\equiv 1 \pmod{p^2}$ . Entonces  $\sigma_e$  es un generador topológico de  $\mathbb{Z}_p^\times$ , que muestra que  $\sigma_e - 1$  es un generador del ideal de aumentación y pues  $(g-1)/(\sigma_e - 1) \in \Lambda(G)$  para cada  $g \in \mathbb{Z}_p^\times$ , así que  $\lambda_1$  es una pseudo-medida.  $\square$

El teorema anterior muestra que el elemento  $\lambda_1$  tiene una propiedad muy similar a la del elemento  $\mu_1$  del teorema 5.28, aunque no es exactamente la misma: una vez se evalúa en  $\kappa^n$  y otra vez en  $\kappa^{1-n}$ . Vamos a discutir esta discrepancia en la sección 6.1 (véase el ejercicio 6.5).

### Ejercicios

**Ejercicio 5.15:** Para  $r \in \mathbb{N}_{\geq 1}$  denotemos  $F_r = \mathbb{Q}_p(\mu_{p^r})$ . Para  $a, b \in \mathbb{Z}$  coprimos a  $p$  definimos  $c_r(a, b) \in F_r$ . Por el ejercicio 1.6 sabemos que  $c_r(a, b) \in U_r$ .

(a) Demuestre que para cada polinomio  $f \in \mathbb{Z}[X]$  tenemos

$$N_{F_r/F_{r-1}}(f(\xi_r - 1)) = \prod_{\xi \in \mu_p} f(\xi \xi_r - 1)$$

usando la sucesión exacta de grupos de Galois

$$1 \rightarrow \text{Gal}(F_r/F_{r-1}) \rightarrow \text{Gal}(F_r/\mathbb{Q}_p) \rightarrow \text{Gal}(F_{r-1}/\mathbb{Q}_p) \rightarrow 1.$$

(b) Aplique esto a  $f = X^a - 1$  y concluya que los elementos  $c_r(a, b)$  son compatibles con respecto a la norma para  $r \in \mathbb{N}_{\geq 1}$ .

## Capítulo 6

# La Conjetura Principal de Iwasawa

La Conjetura Principal de Iwasawa es una de las maneras más profundas de expresar y precisar el fenómeno de que valores especiales de funciones  $L$  complejas tengan algo que ver con aritmética. Ella utiliza las funciones  $L$   $p$ -ádicas y las conecta con objetos de origen aritmético, como grupos de clases o ciertos grupos de Galois. Más precisamente, estos objetos son de manera canónica módulos noetherianos sobre el álgebra de Iwasawa, así que tienen un ideal característico. La Conjetura Principal entonces dice que este ideal es generado por una función  $L$   $p$ -ádica. De esta manera establece la conexión de la izquierda en

$$\begin{array}{ccccc} \text{objetos de origen} & \longleftrightarrow & \text{funciones } L & \longleftrightarrow & \text{funciones } L \\ \text{aritmético} & & p\text{-ádicas} & & \text{complejas} \end{array}$$

mientras la conexión de la derecha es establecida por las fórmulas de interpolación como en los teoremas 5.28, 5.24 o 5.45. De esta manera la Conjetura Principal completa la descripción del vínculo maravilloso entre valores especiales de las funciones  $L$  y la aritmética.

La Conjetura Principal fue formulada por Iwasawa en 1969 en su artículo [Iwa69a]. En este texto Iwasawa busca analogías entre campos de funciones, es decir extensiones finitas de  $\mathbb{F}(t)$ , donde  $\mathbb{F}$  es un campo finito (equivalentemente, campos de funciones de una curva algebraica sobre un campo finito), y campos de números. Entre estos dos tipos de campos hay una multitud de similitudes, por la cual estos campos juntos son llamadas «campos globales». La Conjetura Principal de Iwasawa es un intento de formular un análogo para campos de números de los resultados de Weil acerca de curvas sobre campos finitos (que son generalizadas en las famosas Conjeturas de Weil, véase por ejemplo [FK88]). Ambos resultados – el de Weil y la Conjetura Principal de Iwasawa – conectan polinomios característicos con algún tipo de función zeta, de ahí la analogía, pero véase [Iwa69a] o [NSW08, §XI.6] para una explicación precisa.

Remarcamos que, aunque la llamamos «conjetura», de hecho es un teorema, demostrado por primera vez por Mazur y Wiles en 1984 y otra vez con métodos diferentes por Rubin alrededor de 1990. Sin embargo, esta conjetura tiene una multitud de generalizaciones a otras situaciones (unas de las cuales indicaremos en la sección 7.2), y la mayoría de estas carecen de una demostración todavía. Por eso, y por razones de historia, el teorema todavía se llama «Conjetura Principal».

### 6.1. Las formulaciones de la Conjetura Principal

Los módulos que aparecen en las formulaciones de la conjetura principal fueron introducidos en la definición 4.15. Recordemos las definiciones, que aquí solo necesitamos en un caso especial.

Para cada  $r \in \mathbb{N}_{\geq 0}$  sea

- $K_r = \mathbb{Q}(\mu_{p^r})$ ,
- $H_r$  = la extensión máxima abeliana pro- $p$  de  $K_r$  no ramificada,

- $M_r =$  la extensión máxima abeliana pro- $p$  de  $K_r$  ramificada sólo en  $p$ ,
- $C_r =$  la  $p$ -parte del grupo de clases de  $K_r$ ,
- $X_r = \text{Gal}(H_r/K_r)$ ,
- $Y_r = \text{Gal}(M_r/K_r)$ .

Escribimos  $K_\infty$  para el compósito de todos los campos  $K_r$  para  $r \in \mathbb{N}_{\geq 0}$ , y análogamente definimos  $H_\infty$  y  $M_\infty$ .<sup>1</sup> Además escribimos

- $X_\infty = \text{Gal}(H_\infty/K_\infty) = \varprojlim_{r \in \mathbb{N}_{\geq 0}} X_r$ ,
- $Y_\infty = \text{Gal}(M_\infty/K_\infty) = \varprojlim_{r \in \mathbb{N}_{\geq 0}} Y_r$ .

Usamos también la notación de la sección 5.3, es decir escribimos  $G_{p^r} = \text{Gal}(K_r/\mathbb{Q})$  para  $r \in \mathbb{N}_{\geq 0}$  y  $G = \text{Gal}(K_\infty/\mathbb{Q}) \simeq \Delta \times \Gamma$ , y  $\Lambda(G)$  para el álgebra de Iwasawa de  $G$  con coeficientes en  $\mathbb{Z}_p$ .

Tenemos sucesiones exactas de grupos de Galois

$$\begin{aligned} 1 \rightarrow X_r \rightarrow \text{Gal}(H_r/\mathbb{Q}) \rightarrow G_{p^r} \rightarrow 1, \\ 1 \rightarrow Y_r \rightarrow \text{Gal}(M_r/\mathbb{Q}) \rightarrow G_{p^r} \rightarrow 1 \end{aligned}$$

y por la construcción general descrita en el ejercicio 4.4 tenemos acciones continuas de  $G_{p^r}$  en  $X_r$  y  $Y_r$ . Estas acciones se extienden a una acción de  $G$  en  $X_\infty$  y  $Y_\infty$ , y esto hace  $X_\infty$  y  $Y_\infty$  módulos profinitos sobre  $\Lambda(G)$ .

Queremos usar algunos resultados del capítulo 4. Notemos que  $K_\infty/K_1$  es una  $\mathbb{Z}_p$ -extensión y que  $X_\infty$  y  $Y_\infty$  son los módulos de la definición 4.15 para esta  $\mathbb{Z}_p$ -extensión (pero tenga en cuenta que el  $r$  de aquí y el  $r$  de la sección 4.3 se diferencian por 1, véase el pie de página 1 en la página 104). En la sección 4.3 consideramos  $X_\infty$  como módulo sobre  $\Lambda(\Gamma)$  con  $\Gamma = \text{Gal}(K_\infty/K_1)$  mientras aquí lo consideramos como módulo sobre  $\Lambda(G)$  con  $G = \text{Gal}(K_\infty/\mathbb{Q})$ . El ejercicio 2.14 dice que bajo la identificación  $\Lambda(G) \simeq \Lambda(\Gamma)^{p-1}$  del corolario 2.22 el morfismo  $\Lambda(\Gamma) \rightarrow \Lambda(G)$  inducido por la inclusión del subgrupo  $\Gamma \subseteq G$  corresponde al mapeo diagonal  $\Lambda(\Gamma) \rightarrow \Lambda(\Gamma)^{p-1}$ . Por eso propiedades como «noetheriano» o «de torsión» son verdad para  $X_\infty$  como  $\Lambda(G)$ -módulo si lo son como  $\Lambda(\Gamma)$ -módulo. Además, estas observaciones implican también la siguiente reformulación del corolario 4.19.

**Corolario 6.1:** *Tenemos  $X_\infty/w_r X_\infty = C_{r+1}$ , donde  $w_r \in \Lambda(G)$  es el elemento que corresponde a  $(\omega_r, \dots, \omega_r) \in \Lambda(\Gamma)^{p-1}$  bajo la identificación  $\Lambda(G) \simeq \Lambda(\Gamma)^{p-1}$  del corolario 2.22.*

Del teorema 4.16 y el corolario 4.17 entonces sabemos que  $X_\infty$  y  $Y_\infty$  son noetherianos y que  $X_\infty$  incluso es de torsión como  $\Lambda(G)$ -módulos. De hecho  $Y_\infty^+$  también es de torsión (aunque  $Y_\infty$  no lo es), esto vamos a demostrar más tarde en el corolario 6.15. Además sabemos que  $X_\infty$  es isomorfo al límite inverso de los  $p$ -partes de los grupos de clases de  $K_r$  con respecto a la norma relativa de ideales (definición 1.23).

Necesitamos también la función zeta  $p$ -ádica de Riemann. Escribimos  $\mathcal{Q}$  como el anillo de cocientes de  $\Lambda(G)$  y  $I \subseteq \Lambda(G)$  como el ideal de aumentación. Sea  $\mu_1 \in \mathcal{Q}$  el elemento de definición 5.22,  $h_1 \in \Lambda(G)$  como en la definición 5.25 y  $\lambda_1 \in \mathcal{Q}$  el elemento de la definición 5.44. Entonces  $(h_1\mu_1)$  y  $I\lambda_1$  son ideales en  $\Lambda(G)$ . De hecho tenemos  $(h_1\mu_1) \subseteq$

<sup>1</sup> Estrictamente, aquí la notación es incompatible con la definición 4.15. La extensión  $K_\infty/K_1$  es una  $\mathbb{Z}_p$ -extensión ( $K_\infty/K_0$  no lo es) y si apliquemos la definición 4.15 a ella obtendríamos  $K_r = \mathbb{Q}(\mu_{p^{r+1}})$ . Esto causaría otras molestias en la notación, por eso preferimos definir  $K_r = \mathbb{Q}(\mu_{p^r})$  – comoquiera que este detalle no será importante.

$\Lambda(G)^-$  y  $I\lambda_1 \subseteq \Lambda(G)^+$ . Esto es una consecuencia del hecho de que la función zeta de Riemann es cero en los enteros negativos pares (véase el ejercicio 6.1 o [CS06, Cor. 4.2.3]).

La Conjetura Principal finalmente conecta la función de Riemann  $p$ -ádica con nuestros módulos:

**Teorema 6.2 (Conjetura Principal):** *Tenemos las igualdades de ideales en  $\Lambda(G)^-$  resp.  $\Lambda(G)^+$ :*

$$(a) \text{ car}_{\Lambda(G)^-}(X_\infty^-) = (h_1\mu_1).$$

$$(b) \text{ car}_{\Lambda(G)^+}(Y_\infty^+) = I\lambda_1.$$

(Estas dos afirmaciones son equivalentes.)

La equivalencia de las dos igualdades la demostraremos en la siguiente sección. Mencionamos que por supuesto hay muchas más posibilidades equivalentes de formular la Conjetura Principal y solo damos las dos más usuales. Para más formulaciones equivalentes véase [Lango, Appendix, §8].

Recordemos que podemos imaginar el ideal característico como un análogo del orden de algún grupo. Por eso, heurísticamente la conjetura principal dice que «ordenes de grupos de clases tienen algo que ver con valores especiales de la función zeta». En la sección 6.3 vamos a demostrar que esto de hecho es verdad en un sentido preciso (véase la proposición 6.20).

**Nota 6.3:** Mencionamos una otra manera de interpretar la Conjetura Principal (en la versión (a)). Sea  $\mathbb{Z}_p(1) = \varprojlim_r \mu_{p^r}$  como en la nota 1.47. Entonces  $\mathbb{Z}_p(1)$  es un  $\mathbb{Z}_p$ -módulo compacto con una acción continua de  $G$ , así que es un  $\Lambda(G)$ -módulo. El ejercicio 5.9 dice que su ideal característico es generado por  $h_1$ . Es decir, la Conjetura Principal dice que<sup>2</sup>

$$\text{car}_{\Lambda(G)^-}(X_\infty^-) = \text{car}_{\Lambda(G)}(\mathbb{Z}_p(1))(\mu_1),$$

que nos podemos imaginar como

$$\llbracket \mu_1 = \frac{\text{car}_{\Lambda(G)^-}(X_\infty^-)}{\text{car}_{\Lambda(G)}(\mathbb{Z}_p(1))} \rrbracket,$$

es decir la función zeta  $p$ -ádica de Riemann es el cociente de los generadores de dos ideales característicos (salvo a unidades en  $\Lambda(G)^-$ ).

En esta forma la Conjetura Principal conmemora la fórmula de números de clases [Neu99, Chap. VII, (5.11)]: está dice (en un caso especial) que

$$\text{Res}_{s=1} \zeta(s) = -\frac{2h}{w}$$

donde  $h$  es el número de clases de  $\mathbb{Q}$  (es decir  $h = 1$ ) y  $w$  es el número de raíces de la unidad en  $\mathbb{Q}$  (es decir  $w = 2$ ).

En la Conjetura Principal no aparecen los módulos enteros  $X_\infty$  o  $Y_\infty$  sino solo sus partes donde la conjugación compleja actúa por  $-1$  o  $1$ , y las afirmaciones son igualdades de ideales en  $\Lambda(G)^-$  o  $\Lambda(G)^+$ , respectivamente. Sabemos que  $(h_1\mu_1) \subseteq \Lambda(G)^-$ , es decir  $(h_1\mu_1) \cap \Lambda(G)^+ = 0$ . Por eso si una afirmación análoga a la Conjetura Principal sería verdad para todo  $\Lambda(G)$ , esto significaría que  $X_\infty^+$  debería ser finito. De hecho existe una conjetura que afirma incluso más:

<sup>2</sup> Note que aquí no hace diferencia si consideramos  $\mathbb{Z}_p(1)$  como  $\Lambda(G)$ -módulo o  $\Lambda(G)^-$ -módulo – aunque sus ideales característicos son diferentes, si multiplicamos con el de  $X_\infty^-$  son iguales porque la parte en  $\Lambda(G)^+$  entonces es 0.

komisch ... was hat Cornelius hier genau gemeint?

**Conjetura 6.4 (Kummer/Vandiver):** *Tenemos  $X_\infty^+ = 0$ . Equivalentemente y más concretamente,  $p$  no divide al número de clases del subcampo  $\mathbb{Q}(\mu_p)^+$  de  $\mathbb{Q}(\mu_p)$  fijo por la conjugación compleja.*

La conjetura de Kummer y Vandiver es controvertida entre los expertos: Hay indicaciones y heurísticas a su favor y también a su perjuicio, así que no es claro si se debería creer en su veracidad. Hasta hoy parece poco claro como se podría abordar una demostración, aunque numéricamente la conjetura ha sido confirmada para todos los primos menores que  $1,63 \cdot 10^8$ .

Si supieramos que esta conjetura sea verdad entonces la Conjetura Principal sería una igualdad de ideales  $\text{car}_{\Lambda(G)}(X_\infty) = (h_1\mu_1)$  en  $\Lambda(G)$ . Pero de hecho la conjetura de Kummer y Vandiver es más fuerte que la Conjetura Principal porque incluso la implica. Esto sigue de un teorema de Iwasawa que también es un paso importante en una de las demostraciones de la Conjetura Principal. Véase [CS06, Thm. 4.4.1] para el teorema de Iwasawa y [CS06, §4.5, Cor. 4.5.4] para una demostración que la conjetura de Kummer y Vandiver implica la Conjetura Principal.

### Ejercicios

**Ejercicio 6.1:** Demuestre que  $(h_1\mu_1) \subseteq \Lambda(G)^-$  y  $I\lambda_1 \subseteq \Lambda(G)^+$ , usando las fórmulas de interpolación de los teoremas 5.28 y 5.45 y el hecho de que  $B_n = 0$  para  $n > 1$  impar.

**Ejercicio 6.2:** Demuestre que la conjetura principal como la formulamos en esta sección es equivalente a la versión de la introducción (teorema IV). Use el lema 3.6 para esto.

**Ejercicio 6.3:** Demuestre que la versión « $X_\infty^+ = 0$ » de la conjetura de Kummer y Vandiver (conjetura 6.4) es equivalente a la versión « $p$  no divide al número de clases de  $\mathbb{Q}(\mu_p)^+$ ». Use el corolario 4.4 para esto.

## 6.2. La equivalencia de las formulaciones

Las dos afirmaciones en la Conjetura Principal (teorema 6.2) de hecho son equivalentes. Decidimos poner las dos porque ambas tienen su importancia: La versión (a) contiene el módulo  $X_\infty^-$  y por eso directamente implica resultados sobre los grupos de clases, que son objetos de gran interés (como explicaremos en la sección 6.3), mientras la versión (b) es la que se integra naturalmente en una fila de generalizaciones (como explicaremos en la sección 7.2) y por eso aparece en esta forma muchas veces en la literatura, por ejemplo en [FK06, (2.5)].

En esta sección vamos a demostrar la equivalencia de las dos versiones de la Conjetura Principal. Los resultados de esta sección no serán usados en las secciones subsecuentes, así que el lector podría considerar saltar esta sección. No obstante, vamos a ganar más conocimiento de los módulos que aparecen en la Conjetura Principal.

Nuestra demostración de la equivalencia es esencialmente elemental, usando sólo la teoría de Kummer y los adjuntos de Iwasawa que explicamos en la sección 3.6. Sin embargo, de un punto de vista más abstracto esta equivalencia puede ser demostrada con resultados de dualidad en la cohomología de Galois, usando que los adjuntos de Iwasawa son grupos Ext, como mencionamos en esta sección. Una demostración con estos métodos se encuentra en [NSW08, Thm. 11.1.8], que afirma lo mismo que la proposición 6.13 y el teorema 6.14 abajo.

Para ver la equivalencia de (a) y (b) en el teorema 6.2 necesitamos una involución en el álgebra de Iwasawa.

**Definición 6.5:** Sea  $\nu: \Lambda(G) \rightarrow \Lambda(G)$  el morfismo inducido por

$$G \rightarrow \Lambda(G)^\times, \quad g \mapsto \kappa(g)g^{-1}.$$

Si  $M$  es un  $\Lambda(G)$ -módulo, sea  $\Lambda(G)^\nu$  el  $\Lambda(G)$ -módulo  $M$  con la acción de  $\Lambda(G)$  chanfleada por  $\nu$ , es decir

$$M^\nu = \Lambda(G) \otimes_{\Lambda(G), \nu} M.$$

**Ejemplo 6.6:** Si  $f \in \Lambda(G)$  entonces canónicamente

$$(\Lambda(G)/(f))^\nu \simeq (\Lambda(G)/(\nu(f)))$$

como  $\Lambda(G)$ -módulos.

El morfismo  $\nu$  es una involución, así que  $(M^\nu)^\nu = M$  para cada  $\Lambda(G)$ -módulo  $M$ . De la definición de  $\nu$  y las propiedades de los elementos  $\mu_1$  y  $\lambda_1$  de los teoremas 5.28, 5.45 y 5.29 se deduce fácilmente que  $\nu(I\lambda_1) = (h_1\mu_1)$  (véase el ejercicio 6.5). Esto ya explica una parte de la equivalencia anunciada. Por la otra parte, en el teorema 6.14 abajo vamos a demostrar que existe un pseudo-isomorfismo  $(Y_\infty^+)^\nu \sim X_\infty^-$ .

Para preparar la demostración del teorema 6.14 estudiamos algunos objetos en más detalle con métodos de la teoría de Kummer, siguiendo [Lang, Chap. 6, §2]. Primero damos una descripción más explícita del campo  $M_\infty$ . Usamos la notación siguiente: para  $r \in \mathbb{N}_{\geq 0}$  sea  $\mathfrak{p}_r$  el único ideal sobre  $p$  de  $K_r$  (que también es el único ideal en que la extensión  $K_r/\mathbb{Q}$  es ramificada, véase el lema 1.28 y la proposición 1.29). Este ideal es principal y escribimos  $\pi_r$  como un generador (por ejemplo  $\pi_r = \xi_r - 1$  con  $\xi_r \in K_r$  una raíz primitiva  $p^r$ -ésima de la unidad).

**Proposición 6.7:** Para  $r \in \mathbb{N}_{\geq 1}$  sea

$$D_r = \{\alpha \in K_r^\times : (\alpha) = \mathfrak{a}^{p^r} \text{ para un ideal fraccional } \mathfrak{a} \text{ primo a } \mathfrak{p}_r\}.$$

Entonces

$$M_\infty = \bigcup_{r \in \mathbb{N}_{\geq 1}} K_\infty(\sqrt[p^r]{D_r}).$$

*Demostración:* Escribimos  $L := \bigcup_r K_\infty(\sqrt[p^r]{D_r})$ . Claramente,  $M_\infty$  es un compuesto de extensiones cíclicas de Kummer de  $K_\infty$  cuyos exponentes son potencias de  $p$ . Según la proposición 1.33 (a) estas extensiones son de la forma  $K_\infty(\sqrt[p^m]{\alpha})$  con  $\alpha \in K_\infty^\times$  y  $m \in \mathbb{N}_{\geq 1}$ . Es suficiente demostrar que  $K_\infty(\sqrt[p^m]{\alpha}) \subseteq L$  para cualquier tal  $\alpha$  y  $m$ .

Fijemos  $\alpha$  y  $m$  como arriba. Entonces  $\alpha \in K_r$  para algún  $r \in \mathbb{N}_{\geq 1}$ , y sin pérdida de generalidad asumamos que  $r \geq m > 1$  y  $K_r(\sqrt[p^m]{\alpha}) \subseteq M_r$ . De la proposición 1.36 sabemos que el ideal principal generado por  $\alpha$  en el anillo de enteros de  $K_r$  debe ser de la forma

$$(\alpha) = \mathfrak{a}^{p^r} \mathfrak{p}_r^t$$

con  $t \in \mathbb{Z}$  y  $\mathfrak{p}_r \nmid \mathfrak{a}$  (primero con  $\mathfrak{a}^{p^m}$  en lugar de  $\mathfrak{a}^{p^r}$ , pero lo podemos cambiar por  $\mathfrak{a}^{p^r}$  porque  $r \geq m$ ). Por eso, si definimos  $\beta := \alpha \pi_r^{-t}$  entonces  $\beta \in D_r$  y pues  $K_\infty(\sqrt[p^m]{\beta}) \subseteq K_\infty(\sqrt[p^r]{\beta}) \subseteq L$  por definición de  $L$ . Esto implica que  $K_\infty(\sqrt[p^m]{\alpha}) \subseteq L(\sqrt[p^r]{\pi_r})$ .

Para terminar la demostración probemos que de hecho  $L(\sqrt[p^r]{\pi_r}) = L$ . Si  $s > r$  entonces la extensión  $K_s/K_r$  es de grado  $p^{s-r}$  y puramente ramificada, es decir  $\mathfrak{p}_r = \mathfrak{p}_s^{s-r}$  en  $\mathcal{O}_{K_s}$ , pues  $\pi_r = \pi_s^{s-r} u$  con  $u \in \mathcal{O}_{K_s}^\times$ . Por eso, si queremos adjungar una raíz  $p^{s-r}$ -ésima de  $\pi_r$ , solo necesitamos adjungar una raíz de  $u$ , porque  $\pi_s$  ya está en  $K_\infty \subseteq L$ . Pero claramente  $\mathcal{O}_{K_s}^\times \subseteq D_s$ , por eso estas raíces ya están en  $L$ .  $\square$

Introducimos otro campo

$$E_\infty = \bigcup_{r \in \mathbb{N}_{\geq 1}} E_r, \quad \text{con } E_r = K_\infty \left( \sqrt[p^r]{\bigcup_{s \in \mathbb{N}_{\geq 1}} \mathcal{O}_{K_s}^\times} \right) \text{ para } r \in \mathbb{N}_{\geq 1}.$$

Entonces tenemos extensiones y grupos de Galois

$$\begin{array}{c}
 M_\infty \\
 \left. \begin{array}{c} | \\ E_\infty \\ | \\ K_\infty \end{array} \right\} Y_\infty \\
 G \\
 \mathbb{Q}
 \end{array}$$

Vamos a estudiar también el grupo  $\text{Gal}(M_\infty/E_\infty)$  porque tiene que ver con el grupo de clases y nos permitirá relacionar los módulos  $X_\infty$  y  $Y_\infty$ . Notemos que este grupo es un  $\Lambda(G)$ -submódulo compacto de  $Y_\infty$ .

**Definición 6.8:** Definimos

$$C^\infty = \varinjlim_{r \in \mathbb{N}_{\geq 0}} C_r,$$

el colímite tomado con respecto a los mapeos naturales entre los grupos de clases, inducidos por las inclusiones de campos  $K_r \hookrightarrow K_{r+1}$ . Esto es un  $\Lambda(G)$ -módulo discreto.

**Proposición 6.9:** *El apareamiento de Kummer induce un apareamiento perfecto*

$$\text{Gal}(M_\infty/E_\infty) \times C^\infty \rightarrow \mu_{p^\infty} \subseteq K_\infty^\times$$

de  $\mathbb{Z}_p$ -módulos topológicos, equivariante en el sentido

$$\langle g\sigma g^{-1}, ga \rangle = g \langle \sigma, a \rangle \quad \text{para cada } g \in G, \sigma \in \text{Gal}(M_\infty/E_\infty), a \in C^\infty.$$

Se restringe a un apareamiento perfecto

$$\text{Gal}(M_\infty/E_\infty)^+ \times (C^\infty)^- \rightarrow \mu_{p^\infty}.$$

*Demostración:* Para  $r \in \mathbb{N}_{\geq 1}$  definimos  $D_r$  como en la proposición 6.7. Usamos el morfismo de grupos

$${}^{p^r}\sqrt{D_r} \rightarrow C_r, \quad {}^{p^r}\sqrt{\alpha} \mapsto \mathfrak{a} \text{ para } (\alpha) = \mathfrak{a}^{p^r}$$

cuyo núcleo es  ${}^{p^r}\sqrt{\mathcal{O}_{K_r}^\times}$ , que es claramente equivariante para la acción de  $G_{p^r}$ . Escribimos  $B_r$  para su imagen, así que tenemos un isomorfismo

$${}^{p^r}\sqrt{D_r} / {}^{p^r}\sqrt{\mathcal{O}_{K_r}^\times} \simeq B_r.$$

Se verifica fácilmente que  ${}^{p^r}\sqrt{\mathcal{O}_{K_r}^\times} = {}^{p^r}\sqrt{D_r} \cap E_\infty^\times$ , por eso si combinamos el apareamiento de Kummer de la proposición 1.33 (b) con el isomorfismo anterior obtenemos un apareamiento perfecto de grupos finitos

$$\text{Gal}(E_\infty({}^{p^r}\sqrt{D_r})/E_\infty) \times B_r \rightarrow \mu_{p^r},$$

que es equivariante en el sentido que queremos (para  $G_{p^r}$ ) gracias a la proposición 1.34. Para  $s \geq r$  el diagrama

$$\begin{array}{ccccc}
 \text{Gal}(E_\infty({}^{p^r}\sqrt{D_r})/E_\infty) & \times & B_r & \longrightarrow & \mu_{p^r} \\
 \uparrow & & \downarrow & & \downarrow \\
 \text{Gal}(E_\infty({}^{p^s}\sqrt{D_s})/E_\infty) & \times & B_s & \longrightarrow & \mu_{p^s}
 \end{array}$$

es conmutativo, así que podemos tomar el límite y colímite, respectivamente. Esto junto a la proposición 6.7 nos da un apareamiento perfecto de grupos topológicos

$$\text{Gal}(M_\infty/E_\infty) \times B^\infty \rightarrow \mu_{p^\infty}$$

con  $B^\infty = \varinjlim_r B_r \subseteq C^\infty$  que es equivariante, y falta que ver que  $B^\infty = C^\infty$ .

Por la definición de  $D_r$ , los elementos de  $B_r$  son estas clases de ideales fraccionales de  $K_r$  que tienen un representante  $\mathfrak{a}$  primo a  $\mathfrak{p}_r$  tal que  $\mathfrak{a}^{p^r}$  es principal. Porque  $\mathfrak{p}_r$  ya es principal, podemos omitir «primo a  $\mathfrak{p}_r$ » aquí. El grupo  $C_r$  es la  $p$ -parte del grupo de clases, es decir sus elementos son estas clases de ideales fraccionales de  $K_r$  que tienen un representante  $\mathfrak{a}$  tal que  $\mathfrak{a}^{p^t}$  es principal para algún  $t \in \mathbb{N}_{\geq 0}$ . De estas descripciones vemos que los colímites de los  $C_r$  y  $B_r$  coinciden.

Falta demostrar que el apareamiento se restringe como anunciado. El grupo  $\text{Gal}(M_\infty/\mathbb{Q})$  actúa por conjugación en su subgrupo normal  $\text{Gal}(M_\infty/E_\infty)$ , y esto nos da una acción de la conjugación compleja  $\mathbf{c}$  en  $\text{Gal}(M_\infty/E_\infty)$ . Según la proposición 1.34 el apareamiento tiene la propiedad

$$\langle \mathbf{c}\sigma, \mathbf{c}a \rangle = \mathbf{c} \langle \sigma, a \rangle \quad \text{para cada } \sigma \in \text{Gal}(M_\infty/E_\infty), a \in C^\infty. \quad (6.1)$$

La afirmación entonces resulta del mismo argumento que usamos en la demostración del teorema 4.5.  $\square$

**Corolario 6.10:** *Tenemos isomorfismos canónicos de  $\Lambda(G)$ -módulos compactos*

$$\begin{aligned} \text{Gal}(M_\infty/E_\infty) &\xrightarrow{\cong} \text{Hom}_{\mathbb{Z}_p}(C^\infty, \mu_{p^\infty}), \\ \text{Gal}(M_\infty/E_\infty)^+ &\xrightarrow{\cong} \text{Hom}_{\mathbb{Z}_p}((C^\infty)^-, \mu_{p^\infty}) \end{aligned}$$

donde la acción de  $\Lambda(G)$  al lado derecho es la de la nota 1.9, es decir inducida por

$$(gf)(c) = g(f(g^{-1}c)) \quad \text{para } g \in G, f \in \text{Hom}_{\mathbb{Z}_p}(C^\infty, \mu_{p^\infty}), c \in C^\infty.$$

*Demostración:* Esto resulta de la proposición 6.9 y la nota 1.35.  $\square$

Como  $\mathbb{Z}_p$ -módulo,  $\mu_{p^\infty}$  es isomorfo a  $\mathbb{Q}_p/\mathbb{Z}_p$  (aunque no canónicamente). Es decir, en el corolario 6.10 podríamos replazar  $\mu_{p^\infty}$  por  $\mathbb{Q}_p/\mathbb{Z}_p$ , que es útil porque los morfismos a  $\mathbb{Q}_p/\mathbb{Z}_p$  son el dual de Pontryagin de la definición 3.23. Sin embargo, si hacemos eso tenemos que tener cuidado con la acción de  $G$  porque en el dual de Pontryagin introducimos una acción un poco diferente en la definición 3.31 (a). En el lema siguiente nos cuidamos de esta diferencia.

**Lema 6.11:** *Sea  $M$  un  $\Lambda(G)$ -módulo tal que  $\text{Hom}_{\mathbb{Z}_p}(M, \mu_{p^\infty})$  nuevamente es un  $\Lambda(G)$ -módulo como en la nota 1.9. De la definición 6.5 tenemos entonces el  $\Lambda(G)$ -módulo  $\text{Hom}_{\mathbb{Z}_p}(M, \mu_{p^\infty})^\nu$ , que como conjunto es lo mismo que  $\text{Hom}_{\mathbb{Z}_p}(M, \mu_{p^\infty})$ . Por otro lado, en  $\text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$  tenemos la estructura como  $\Lambda(G)$ -módulo introducida en la definición 3.31 (a).*

*Fijamos un isomorfismo de  $\mathbb{Z}_p$ -módulos  $\psi: \mu_{p^\infty} \xrightarrow{\cong} \mathbb{Q}_p/\mathbb{Z}_p$ . Entonces la asociación*

$$\text{Hom}_{\mathbb{Z}_p}(M, \mu_{p^\infty})^\nu \rightarrow \text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p), \quad f \mapsto \psi \circ f$$

*es un isomorfismo de  $\Lambda(G)$ -módulos.*

*Demostración:* Es claro que la asociación es biyectiva,  $\mathbb{Z}_p$ -lineal y continua. Hay que verificar que es compatible con las acciones de  $G$  en ambos lados. Esto es un cálculo fácil, aunque un poco espinoso, que dejamos como ejercicio.  $\square$

Aplicando este lema a nuestra situación obtenemos lo siguiente.

**Corolario 6.12:** *Existen isomorfismos (no canónicos) de  $\Lambda(G)$ -módulos compactos*

$$\begin{aligned}\mathrm{Gal}(M_\infty/E_\infty)^\nu &\simeq (C^\infty)^\vee, \\ (\mathrm{Gal}(M_\infty/E_\infty)^+)^\nu &\simeq ((C^\infty)^-)^\vee.\end{aligned}$$

Ahora usamos la teoría de los adjuntos de Iwasawa explicada en la sección 3.6 (que involucra duales de Pontryagin). Aplicándola a la situación de nuestro interés obtenemos el resultado siguiente.

**Proposición 6.13:** *Existe un isomorfismo canónico de  $\Lambda(G)$ -módulos*

$$\alpha(X_\infty) \simeq (C^\infty)^\vee.$$

*En particular, existe un pseudo-isomorfismo*

$$X_\infty \sim (C^\infty)^\vee.$$

*Demostración:* Por definición 3.35,  $\alpha(X_\infty) = (\varinjlim_{r \geq m} X_\infty / w_r X_\infty)^\vee$  con  $m \in \mathbb{N}_{\geq 0}$  suficientemente grande y  $w_r \in \Lambda(G)$  siendo el elemento que corresponde a  $(\omega_r, \dots, \omega_r) \in \Lambda(\Gamma)^{p-1}$  bajo la identificación  $\Lambda(G) \simeq \Lambda(\Gamma)^{p-1}$  del corolario 2.22. Aquí, « $m$  suficientemente grande» significa que para  $r \geq m$  el polinomio  $\omega_r$  es coprimo al polinomio característico de  $e_i X_\infty$  para  $i = 1, \dots, p-1$ , donde  $e_i$  es el idempotente para el carácter  $\omega^i$  (lema 2.20). El lema 3.18 dice que esto es equivalente a  $e_i X_\infty / \omega_r e_i X_\infty$  siendo finito para cada  $i$ , es decir a  $X_\infty / w_r X_\infty$  siendo finito. Pero el corolario 6.1 dice que  $X_\infty / w_r X_\infty = C_{r+1}$ , que es finito para cada  $r \in \mathbb{N}_{\geq 0}$ . Por eso podemos usar  $m = 0$  y obtenemos  $\alpha(X_\infty) = (\varinjlim_r C_r)^\vee$ , que es la primera afirmación. La segunda resulta de la primera y el corolario 3.36, que dice que un módulo es pseudo-isomorfismo a su adjunto.  $\square$

Ahora estamos listos para demostrar la equivalencia de las formulaciones.

**Teorema 6.14:** *Existe un pseudo-isomorfismo  $(Y_\infty^+)^\nu \sim X_\infty^-$ . En particular, las dos afirmaciones del teorema 6.2 son equivalentes.*

*Demostración:* El pseudo-isomorfismo de la proposición 6.13 es  $\Lambda(G)$ -lineal, pues compatible con la acción de la conjugación compleja. Además es fácil ver que  $((C^\infty)^\vee)^- = ((C^\infty)^-)^\vee$ . Combinando esto con la proposición 6.13 obtenemos un pseudo-isomorfismo  $X_\infty^- \sim (\mathrm{Gal}(M_\infty/E_\infty)^+)^\nu$ .

Para lo que falta usamos la sucesión exacta

$$1 \rightarrow \mathrm{Gal}(M_\infty/E_\infty) \rightarrow Y_\infty \rightarrow \mathrm{Gal}(E_\infty/K_\infty) \rightarrow 1.$$

Vamos a demostrar que  $\mathrm{Gal}(E_\infty/K_\infty)^+ = 0$ , que por la sucesión exacta implica  $\mathrm{Gal}(M_\infty/E_\infty)^+ = Y_\infty^+$ , con que la demostración será completa.

Para esto usamos otra vez la teoría de Kummer. De manera similar a anteriormente, tomando el (co)límite de los apareamientos de Kummer resulta un apareamiento perfecto de grupos topológicos

$$\mathrm{Gal}(E_\infty/K_\infty) \times \mathcal{O}_{K_\infty}^\times \rightarrow \mu_{p^\infty}$$

que también tiene la propiedad análoga a (6.1) (omitimos los detalles aquí). Con el mismo argumento que arriba, usando que  $\mathrm{Gal}(E_\infty/K_\infty)$  es un grupo pro- $p$ , vemos que la restricción a  $\mathrm{Gal}(E_\infty/K_\infty)^+ \times (\mathcal{O}_{K_\infty}^\times)^+$  es trivial. La restricción a  $\mathrm{Gal}(E_\infty/K_\infty) \times (\mathcal{O}_{K_\infty}^\times)^-$  también es trivial porque  $(\mathcal{O}_{K_\infty}^\times)^- = \mu_{p^\infty} \subseteq K_\infty$ , en que  $\mathrm{Gal}(E_\infty/K_\infty)$  actúa trivialmente. Es decir, la restricción del apareamiento a

$$\mathrm{Gal}(E_\infty/K_\infty)^+ \times ((\mathcal{O}_{K_\infty}^\times)^+ \oplus (\mathcal{O}_{K_\infty}^\times)^-)$$

es trivial. Pero  $(\mathcal{O}_{K_\infty}^\times)^+ \oplus (\mathcal{O}_{K_\infty}^\times)^- \subseteq \mathcal{O}_{K_\infty}^\times$  es un subgrupo de índice 2, y porque  $\text{Gal}(E_\infty/K_\infty)$  es pro- $p$  eso implica que el apareamiento es trivial en todo  $\text{Gal}(E_\infty/K_\infty)^+ \times \mathcal{O}_{K_\infty}^\times$ . Porque es perfecto en  $\text{Gal}(E_\infty/K_\infty) \times \mathcal{O}_{K_\infty}^\times$  obtenemos que  $\text{Gal}(E_\infty/K_\infty)^+ = 0$ , que termina la demostración.  $\square$

**Corolario 6.15:** *El  $\Lambda(G)$ -módulo  $Y_\infty^+$  es de torsión.*

*Demostración:* Esto resulta del teorema 6.14 porque ya sabemos que  $X_\infty^-$  es de torsión, y del hecho de que la propiedad de ser de torsión es invariante bajo pseudo-isomorfismos y aplicar  $\nu$ .  $\square$

### Ejercicios

**Ejercicio 6.4:** Demuestre que  $\nu: \Lambda(G) \rightarrow \Lambda(G)$  es una involución, es decir  $\nu \circ \nu = \text{id}$ .

**Ejercicio 6.5:** Demuestre que  $\nu(\mu_1) = \lambda_1$  y que  $\nu(h_1)$  es un generador de  $I$ . ¿Qué significa esto para las funciones  $L$   $p$ -ádicas de un carácter de Dirichlet  $\chi$  no trivial? Formule una versión de la existencia y la fórmula de interpolación para esta función  $L$   $p$ -ádica en el estilo del teorema 5.45.

**Ejercicio 6.6:** Demuestre que para cada  $\Lambda(G)$ -módulo tenemos  $(M^\nu)^\pm = (M^\mp)^\nu$ .

**Ejercicio 6.7:** Verifique la afirmación del ejemplo 6.6.

**Ejercicio 6.8:** Verifique que la asociación en el lema 6.11 es compatible con la acción de  $G$ .

## 6.3. Consecuencias de la Conjetura Principal

Aunque la Conjetura Principal conecta la función zeta de Riemann con los módulos de origen aritmético, no es una afirmación fácil de concebir. Para exponer de una manera más concreta la importancia de la Conjetura Principal aquí deducimos algunas implicaciones de ella, las cuales ojalá ilustren su poder. No obstante, hay que reconocer que algunas de estas implicaciones ya eran conocidas antes de la demostración de la Conjetura Principal. Los resultados mas concretos que obtendremos conciernen el grupo de clases  $C_1$  del campo  $K_1 = \mathbb{Q}(\mu_p)$ , la cual denotemos en esta sección simplemente como  $C$ .

Primero queremos deducir el criterio de Kummer (teorema II) de la Conjetura Principal. En este criterio aparece el enunciado de que algunos valores de la función zeta sean divisibles por  $p$ . Si el ideal característico de un módulo es generado por una función  $L$   $p$ -ádica, como dice la Conjetura Principal, y valores de esta función son unidades  $p$ -ádicas, entonces ¿qué significa esto para el módulo?

Empezamos con un lema que contesta esta pregunta en general, y luego lo aplicamos para obtener el criterio de Kummer. En el lema sea  $\Lambda(G)$  el álgebra de Iwasawa de  $G$  con coeficientes en  $\mathcal{O}$ , el anillo de enteros de una extensión finita de  $\mathbb{Q}_p$ .

**Lema 6.16:** *Sea  $\mu \in \Lambda(G)$  y  $X$  un  $\Lambda(G)$ -módulo noetheriano de torsión tal que  $\text{car}_{\Lambda(G)}(X) = (\mu)$ . Sea  $\psi: G \rightarrow \mathcal{O}^\times$  un carácter de la forma  $\psi = \omega^i \kappa_0^s$  con  $i \in \{1, \dots, p-1\}$  y  $s \in \mathbb{Z}_p$ . Sea  $e_i$  el idempotente asociado a  $\omega^i$ . Entonces*

$$\mu(\psi) \in \mathcal{O}^\times \iff e_i X \text{ es finito.}$$

*Si  $X$  no tiene submódulos finitos no triviales entonces*

$$\mu(\psi) \in \mathcal{O}^\times \iff e_i X = 0.$$

*También tenemos afirmaciones análogas si  $X$  es un módulo sobre  $\Lambda(G)^\pm$  e  $i$  es par o impar, respectivamente.*

*Demostración:* Según la proposición 5.31 y (5.6) tenemos la primera equivalencia en

$$\begin{aligned} \mu(\psi) = \mu_i(\kappa_0^s) \in \mathcal{O}^\times &\iff \mu_i \in \Lambda(\Gamma)^\times \\ &\iff \text{car}_{\Lambda(\Gamma)}(e_i X) = \Lambda(\Gamma) \\ &\iff e_i X \sim 0 \\ &\iff e_i X \text{ es finito} \end{aligned}$$

y obtenemos la primera afirmación. El resto de resulta directamente de esto.  $\square$

Aplicando este lema a la situación de la Conjetura Principal nos da el criterio de Kummer. Aquí y también más tarde, utilizaremos el hecho importante de que el módulo  $X_\infty^-$  no tiene submódulos finitos no triviales. Esto es una consecuencia de un resultado de Iwasawa [Iwa59b] cuya demostración usa la teoría de cohomología de Galois, que no queremos usar en este texto. Por eso solo citamos este resultado aquí, una demostración se encuentra en [Sha, Prop. 4.4.2].

**Proposición 6.17:** *La Conjetura Principal implica el criterio de Kummer, que dice*

$$\begin{aligned} p \mid h_{\mathbb{Q}(\mu_p)} &\iff p \mid \zeta(1-n) \text{ para algún } n \in \mathbb{N}_{\geq 1} \text{ par} \\ &\iff p \text{ divide uno de } \zeta(-1), \zeta(-3), \dots, \zeta(4-p). \end{aligned}$$

*Demostración:* Primero explicamos la equivalencia de la segunda y tercera afirmación, que es cierta independientemente de la Conjetura Principal. Si  $p-1 \mid n$  entonces  $\zeta(1-n)$  nunca es divisible por  $p$  según la proposición 5.13 (recuerde que decimos que  $p$  divide a un número racional si divide al numerador en una representación simplificada). Si  $p-1 \nmid n$  entonces por el corolario 5.33, la pregunta si  $p \mid \zeta(1-n)$  para  $n \in \mathbb{N}_{\geq 1}$  solo depende del resto de  $1-n$  módulo  $p-1$ . Los números  $1-n$  con  $n \in \mathbb{N}_{\geq 1}$  par y no divisible por  $p-1$  tienen  $-1, \dots, 4-p$  como representantes módulo  $p-1$ . Esto muestra la equivalencia deseada.

A partir de ahora asumamos la Conjetura Principal. Aplicamos el lema 6.16 con  $\mathcal{O} = \mathbb{Z}_p$ ,  $X = X_\infty^-$  y  $\mu = h_1^{(1)}\mu_1$ . Primero observamos que si ponemos  $\psi = \kappa$  entonces, porque  $h_1^{(1)}\mu_1(\kappa) \in \mathbb{Z}_p^\times$  según el corolario 5.36, el lema nos dice que  $e_1 X_\infty^- = 0$ . Por eso

$$X_\infty^- = \bigoplus_{i=3 \text{ impar}}^{p-1} e_i X_\infty^- = \bigoplus_{n=2 \text{ par}}^{p-3} e_{1-n} X_\infty^-.$$

Ponemos en el lema  $\psi = \kappa^{1-n}$  con  $n \in \{2, 4, \dots, p-3\}$ . Entonces  $n \not\equiv 0 \pmod{p-1}$ , así que  $e_{1-n} h_1^{(1)} = 1$  y pues

$$h_1^{(1)}\mu_1(\kappa^{1-n}) = \mu_1(\kappa^{1-n}) = (1-p^{n-1})\zeta(1-n)$$

(esto resulta del diagrama (5.5)) según la fórmula de interpolación del teorema 5.28. El lema entonces dice que

$$e_{1-n} X_\infty^- = 0 \iff \zeta(1-n) \in \mathbb{Z}_p^\times.$$

Porque  $\{1-n : n = 2, 4, \dots, p-3\} = \{-1, -3, \dots, 4-p\}$ , eso implica que

$$p \text{ divide uno de } \zeta(-1), \zeta(-3), \dots, \zeta(4-p) \iff X_\infty^- \neq 0.$$

Del corolario 4.20 sabemos que  $X_\infty^- \neq 0 \iff X_\infty \neq 0$ , y esto es equivalente a  $p \mid h_{\mathbb{Q}(\mu_p)}$  según el corolario 4.4.  $\square$

Por supuesto, la demostración original de Kummer no utiliza la Conjetura Principal. Una demostración elemental de este criterio se encuentra en [Rib01, §19.2].

Un resultado más fino es el teorema de Herbrand y Ribet. Para esto definimos  $V := \mathbb{F}_p \otimes_{\mathbb{Z}} C = C/(C)^p$ , que es un espacio vectorial de dimensión finita sobre  $\mathbb{F}_p$  con una acción  $\mathbb{F}_p$ -lineal de  $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ . Por eso se descompone en una suma

$$V = \bigoplus_{i=1}^{p-1} V_i$$

donde  $V_i = e_{\omega^i} V$  es el subespacio en que  $\Delta$  actúa por la potencia  $i$ -ésima del carácter de Teichmüller. El teorema de Herbrand y Ribet describe estas partes.

**Teorema 6.18 (Herbrand/Ribet):** *Sea  $i \in \{3, \dots, p-2\}$  impar. Entonces*

$$V_i \neq 0 \iff p \mid \zeta(i+1-p).$$

La implicación « $\implies$ » aquí fue demostrada por Herbrand en 1932, mientras la implicación « $\impliedby$ », que es mucho más difícil, fue demostrada por Ribet en 1976 [Rib76], usando métodos similares a las que más tarde culminaron en la demostración de la Conjetura Principal por Mazur y Wiles.

La Conjetura Principal implica este teorema e incluso nos da una fórmula para los tamaños de los grupos  $e_i C$ , que es un resultado aún más fuerte. Mientras el teorema de Herbrand y Ribet ya era conocido antes de la demostración de la Conjetura Principal, esta fórmula es un resultado nuevo.

La técnica para derivar esta fórmula de la Conjetura Principal es esencialmente una aplicación simple del lema de la serpiente, que funciona en una situación general. Resumamos esto en el lema siguiente antes de aplicarlo a nuestra situación.

**Lema 6.19:** *Sea  $X$  un  $\Lambda(G)$ -módulo noetheriano de torsión sin submódulos finitos no triviales con  $\text{car}_{\Lambda(G)}(X) = (\mu)$  y sea  $\nu \in \Lambda(G)$  tal que  $X/\nu X$  es finito. Para cada  $i \in \{1, \dots, p-1\}$  sean  $\mu_i, \nu_i \in \Lambda(\Gamma)$  las imágenes de  $e_i \mu$  y  $e_i \nu$ , respectivamente, bajo el isomorfismo  $e_i \Lambda(G) \simeq \Lambda(\Gamma)$ . Asumamos que  $\nu_i$  es coprimo a  $\pi$  y cada polinomio distinguido en  $\Lambda(\Gamma) \simeq \mathcal{O}[[T]]$ .*

*Entonces  $\Lambda(\Gamma)/(\mu_i, \nu_i)$  también es finito y*

$$\#(e_i(X/\nu X)) = \#(\Lambda(\Gamma)/(\mu_i, \nu_i)).$$

*Tenemos una afirmación análoga para módulos sobre  $\Lambda(G)^\pm$ .*

*Demostración:* Aquí seguimos [Lango, Appendix, Lem. 8.6].

Sea  $X \rightarrow E$  un pseudo-isomorfo con  $E$  un  $\Lambda(G)$ -módulo elemental, que es inyectivo, y sea  $Z$  el conúcleo. Escribimos  $X[\nu]$  para el núcleo de la multiplicación con  $\nu$  en  $X$ , y similar para otros módulos. Entonces por las definiciones y el lema de la serpiente tenemos un diagrama

conmutativo

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & X[\nu] & \longrightarrow & E[\nu] & \longrightarrow & Z[\nu] \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & X & \longrightarrow & E & \longrightarrow & Z \longrightarrow 0 \\
 & & \downarrow \nu & & \downarrow \nu & & \downarrow \nu \\
 & & X & \longrightarrow & E & \longrightarrow & Z \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & X & \longrightarrow & E & \longrightarrow & Z \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & X/\nu X & \longrightarrow & E/\nu E & \longrightarrow & Z/\nu Z \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

con líneas, columnas y serpientes exactas. De este diagrama obtenemos: Porque  $Z[\nu]$  es finito,  $\text{rg}_{\mathcal{O}} X[\nu] = \text{rg}_{\mathcal{O}} E[\nu]$ , y porque  $X/\nu X$  es finito,  $\text{rg}_{\mathcal{O}} X[\nu] = 0$  (usamos aquí la proposición 3.17), es decir  $\text{rg}_{\mathcal{O}} E[\nu] = 0$ . Según el lema 3.19 entonces  $E[\nu] = 0$ . Porque  $Z$  es finito,  $\#Z[\nu] = \#(Z/\nu Z)$ . El lema de la serpiente entonces implica que  $\#(X/\nu X) = \#(E/\nu E)$ . De la misma manera, si aplicamos  $e_i$  al diagrama entero,<sup>3</sup> obtenemos

$$\#(e_i(X/\nu X)) = \#(e_i(E/\nu E))$$

y lo que falta ver es que  $\#(e_i(E/\nu E)) = \#(\Lambda(\Gamma)/(\mu_i, \nu_i))$ . Es fácil ver que  $e_i(E/\nu E) = e_i E/\nu_i e_i E$ , y  $e_i E$  es un  $\Lambda(\Gamma)$ -módulo elemental, pues de la forma  $\bigoplus_{j=1}^s \Lambda(\Gamma)/(f_j)$ , y  $(\prod_{j=1}^s f_j) = (\mu_i)$ . Por eso es suficiente demostrar que

$$\# \left( \bigoplus_{j=1}^s \Lambda(\Gamma)/(f_j, \nu_i) \right) = \# \left( \Lambda(\Gamma)/(\prod_{j=1}^s f_j, \nu_i) \right).$$

Eso lo demostramos con inducción en  $s$ ; el caso  $s = 1$  es trivial. Sea entonces  $s > 1$ , ponemos  $f = f_1 \cdots f_{s-1}$  y  $g = f_s$ . Hay una sucesión exacta

$$0 \rightarrow (f, \nu_i)/(fg, \nu_i) \rightarrow \Lambda(\Gamma)/(fg, \nu_i) \rightarrow \Lambda(\Gamma)/(f, \nu_i) \oplus \Lambda(\Gamma)/(g, \nu_i) \rightarrow \Lambda(\Gamma)/(g, \nu_i) \rightarrow 0$$

donde el mapeo en el centro es  $r \mapsto (r, 0)$ . Por eso es suficiente demostrar que  $\#(f, \nu_i)/(fg, \nu_i) = \#\Lambda(\Gamma)/(g, \nu_i)$ . Pero el mapeo

$$\Lambda(\Gamma)/(g, \nu_i) \rightarrow (f, \nu_i)/(fg, \nu_i), \quad x \mapsto fx$$

es obviamente sobreyectivo y porque  $f$  es coprimo a  $\nu_i$  también es inyectivo.  $\square$

**Proposición 6.20:** *La Conjetura Principal implica que para cada  $i \in \{3, \dots, p-2\}$  impar tenemos*

$$\#e_i C = p^{v_p(B_{1, \omega^{-i}})}.$$

<sup>3</sup> Aplicar  $e_i$  es lo mismo como aplicar  $-\otimes_{\Lambda(G)} e_i \Lambda(G)$ , y del isomorfismo  $\Lambda(G) \simeq \Lambda(\Gamma)^{p-1}$  (corolario 2.22) es claro que  $e_i \Lambda(G) \simeq \Lambda(\Gamma)$  es plano sobre  $\Lambda(G)$ .

*Demostración:* Asumamos la Conjetura Principal y aplicamos el lema 6.19 con  $X = X_\infty^-$ ,  $\mu = h_1^{(1)}\mu_1$ ,  $\nu = \sigma_{1+p} - 1$  y  $i \in \{3, \dots, p-2\}$  impar. Entonces por el corolario 4.19 tenemos  $e_i(X/\nu X) \simeq e_i C$ . Además,  $\nu_i = \sigma_{1+p} - 1$  y porque  $i \neq 1$  el elemento  $\mu_i$  es la imagen de  $e_i\mu_1$  en  $\Lambda(\Gamma)$ . El lema entonces dice

$$\#e_i C = \#(\Lambda(\Gamma)/(\sigma_{1+p} - 1, \mu_i)).$$

Ahora el morfismo  $\Lambda(\Gamma) \rightarrow \mathbb{Z}_p$  inducido por el carácter trivial  $\kappa_0^0: \Gamma \rightarrow \mathbb{Z}_p^\times$  es sobreyectivo con núcleo generado por  $\sigma_{1+p} - 1$  (si identificamos  $\Lambda(\Gamma)$  con  $\mathbb{Z}_p[[T]]$  usando el generador topológico  $\sigma_{1+p}$  entonces el morfismo es inducido por  $T \mapsto 0$ , cuyo núcleo es generado por  $T$ ). El isomorfismo  $\Lambda(\Gamma)/(\sigma_{1+p} - 1) \xrightarrow{\simeq} \mathbb{Z}_p$  que obtenemos envía  $\mu_i$  a  $\mu_1(\omega^i) = -B_{1,\omega^{-i}}$  (usamos aquí el diagrama (5.5) y el lema 5.34) y pues induce un isomorfismo

$$\Lambda(\Gamma)/(\mu_i\sigma_{1+p} - 1) \xrightarrow{\simeq} \mathbb{Z}_p/B_{1,\omega^{-i}}$$

y esto termina la demostración. □

**Corolario 6.21:** *La Conjetura Principal implica el siguiente caso especial del teorema de Stickelberger. Sea  $\Sigma_p \in \mathbb{Q}[G_p]$  el elemento de Stickelberger y sea  $I$  el ideal  $\Sigma_p \mathbb{Z}[G_p] \cap \mathbb{Z}[G_p]$ . Entonces cada elemento de  $I^-$  anula a  $C^-$ .*

*Demostración:* Se puede demostrar que  $I = \Sigma_p J$ , donde  $J$  es el ideal generado por los elementos de la forma  $\sigma_a - a$  con  $a \in \mathbb{Z}$ ,  $p \nmid a$ . Omitimos esta demostración aquí, véase [Lang0, §1.2, Lemma 2, p. 11] para ella. Usando esto, la afirmación que queremos demostrar es equivalente a: Para cada  $i \in \{1, \dots, p-1\}$  impar, los elementos del ideal  $e_i \Sigma_p J \subseteq \mathbb{Z}_p$  anulan a  $e_1 C$ . El ideal  $e_i J$  es generado por los  $\omega^i(a) - a$  con  $a \in \mathbb{Z}$ ,  $p \nmid a$ , y se verifica fácilmente que esto es igual a  $(p)$  si  $i = 1$  y igual a  $(1)$  si  $i \neq 1$ , véase [Lang0, §1.3, Lemma 1, p. 15]. Entonces el caso de  $i = 1$  ya es claro. En el caso  $i \neq 1$  tenemos  $e_i \Sigma_p J = (B_{1,\omega^{-i}})$  según la nota 5.35, y la afirmación resulta de la proposición 6.20. □

Beispiel mit 691

Finalmente mencionamos que en [NSW08, §XI.6] se encuentran aún más consecuencias de la Conjetura Principal que no vamos a describir aquí.

### Ejercicios

**Ejercicio 6.9:** Sea  $K$  un campo de números y  $h = \# \text{Cl}(K)$  su número de clases. Demuestre que  $p \nmid h$  es equivalente a lo siguiente: Para cada ideal fraccional  $I \neq 0$  de  $K$ , si  $I^p$  es un ideal principal entonces  $I$  es un ideal principal.

**Ejercicio 6.10:** Demuestre que la Conjetura Principal implica el teorema de Herbrand y Ribet:

- (a) Demuéstrelo usando argumentos similares a los de la demostración de la proposición 6.17.
- (b) Demuestre que la afirmación de la proposición 6.20 implica el teorema de Herbrand y Ribet, usando el corolario 5.33.

## 6.4. Unos comentarios sobre la demostración de la Conjetura Principal

En esta sección describimos de manera muy escasa los métodos como se puede demostrar la Conjetura Principal, siguiendo principalmente el texto [Kat07, §2.4–5].

Existen esencialmente dos enfoques para demostrar la Conjetura Principal. El enfoque original de Mazur y Wiles usa formas modulares y es una extensión de métodos usados por Ribet en su demostración del teorema 6.18. El segundo enfoque, hallado por Rubin

usando ideas de Kolyvagin y Thaine, usa algo que se llama *sistemas de Euler*. Por su naturaleza, el enfoque con formas modulares demuestra la inclusión  $\text{car}_{\Lambda(G)^-}(X_\infty^-) \subseteq (h_1\mu_1)$  en la conjetura principal (o la inclusión análoga en la otra versión) y el método de sistemas de Euler demuestra la inclusión opuesta. En el caso de la Conjetura Principal original de Iwasawa, de hecho una de estas inclusiones ya implica la otra (esto es una consecuencia de la fórmula de clases). Sin embargo, en las generalizaciones de la Conjetura Principal que vamos a explicar en la sección 7.2 este lujo ya no existe, así que hay que usar ambos métodos para demostrarlas.

La relación entre las formas modulares y la Conjetura Principal es, muy a manera de esbozo, la siguiente. Como vimos en la sección 5.4, la función zeta  $p$ -ádica tiene que ver con congruencias módulo  $p$  entre valores especiales de la función zeta. Estos valores también aparecen como coeficiente constante en la expansión  $q$  de series de Eisenstein: para  $k \geq 4$  la series de Eisenstein  $E_k$  de peso  $k$  tiene la expansión de Fourier

$$E_k = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n$$

donde  $\sigma_{k-1}(n)$  es la suma de las potencias  $(k-1)$ -ésimas de los divisores de  $n$ . Por eso, si  $\zeta(1-k)$  es divisible por  $p$  entonces  $E_k \pmod{p}$  parece una forma modular cuspidal, y de hecho existe una forma cuspidal  $f$  congruente a  $E_k \pmod{p}$ . Esta congruencia implica que los representaciones de Galois de  $E_k$  y  $f$  son relacionados módulo  $p$ , más precisamente tienen las mismas semisimplificaciones. La representación de  $E_k$  es conocida explícita y es reducible, así que la de  $f$  módulo  $p$  es una extensión de los componentes irreducibles de la de  $E_k$ . Finalmente, estas extensiones son relacionados a grupos de clases por la teoría de campos de clases. Para más detalles, véase [Kat07, §2.4] y el artículo original de Mazur y Wiles [MW84].

Un sistema de Euler es una colección de elementos de grupos de cohomología de Galois de la forma  $c_m \in H^1(\mathbb{Q}(\mu_m), T)$  para cada  $m \in \mathbb{N}_{\geq 1}$ , donde  $T$  es un retículo estable en una representación  $V$  de  $\text{Gal}_{\mathbb{Q}}$  con coeficientes en  $\mathbb{Q}_p$ , tal que los  $c_m$  cumplen algunas relaciones de compatibilidad con respecto al mapeo de la corestricción. Esta definición probablemente parece poco iluminador, pero la razón por que uno se interesa en este tipo de colección es que su sola existencia produce anuladores de grupos de clases (o objetos más generales) que permiten acotar el exponente o incluso el orden de dichos grupos. Por otro lado los sistemas de Euler son relacionados a valores especiales de funciones  $L$ : existe un mapeo llamado el mapeo de Coleman del límite de los  $H^1(\mathbb{Q}(\mu_m), T)$  al álgebra de Iwasawa enviando el sistema de Euler a la función zeta  $p$ -ádica. Esto implica relaciones entre los órdenes de los grupos de clases y los valores especiales. De esta manera el sistema de Euler permite conectar los dos objetos que aparecen en la Conjetura Principal.

Existe una teoría bastante general de sistemas de Euler. La dificultad principal en este ámbito es *construir* sistemas de Euler, es decir demostrar que existen y que son no triviales. Aquí no hay un método general y hasta ahora conocemos solo unos pocos sistemas de Euler. En el caso de la Conjetura Principal, el sistema de Euler que se usa es construido usando las unidades ciclotómicas de la definición 5.39.

Textos introductorios a la teoría de sistemas de Euler son [Loe17] y [Rub00]. Una demostración completa de la Conjetura Principal usando sistemas de Euler se encuentra en [Lango, Appendix] y en [CS06].

# Capítulo 7

## Generalizaciones

### 7.1. Teoría de Iwasawa para aritmética logarítmica

- El corolario 4.4 aplica
- El teorema de Ferrero-Washington

### 7.2. Generalizaciones de la Conjetura Principal: Curvas elípticas, Motivos y la Conjetura Equivariante de los Números de Tamagawa

En esta sección final contamos de qué manera los fenómenos alrededor de la Conjetura Principal que conocimos en los capítulos precedentes se extienden a nuevos terrenos. Paso a paso vamos a ver como reinterpretarlas y generalizarlas hasta alcanzar una ampliación sustancial. En este camino no siempre podemos ser completamente exactos porque esto nos obligaría a introducir bastantes nociones nuevas que probablemente llenarían otro libro. Nuestro objetivo es que el lector pueda tener una intuición del camino a seguir.

En (casi) toda esta sección sea  $K_r = \mathbb{Q}(\mu_{p^r})$  para  $r \in \mathbb{N}_{\geq 0} \cup \{\infty\}$  y  $G = \text{Gal}(K_\infty/\mathbb{Q})$  como en el capítulo 6.

#### 7.2.1. Proemio

La Conjetura Principal conecta una función « $L$ » compleja – la función zeta de Riemann – a un objeto aritmético – los grupos de clases. Existen muchas funciones complejas más que se llaman funciones  $L$  ... ¿Tendrán estas funciones también un par  $p$ -ádico? ¿Estarán relacionadas con objetos aritméticos? En caso de afirmativo ¿Cuáles son estos objetos aritméticos?

Una de las primeras generalizaciones propuestas es la formulación de una Conjetura Principal para curvas elípticas hecha por Mazur en los años 1970. En este caso tenemos la función  $L$  de Hasse y Weil, que de hecho tiene un análogo  $p$ -ádico que veremos más adelante. En el lado algebraico, el papel de los grupos de clases será jugado por grupos de Selmer de la curva elíptica. Esta formulación, que además es paralela a la Conjetura Principal original de Iwasawa, resultó correcta: fue demostrada en muchos casos por Skinner y Urban en 2003. Este proceso no se detuvo en las curvas elípticas, en realidad se podía formular una Conjetura Principal para objetos mucho más generales: los denominados motivos, que vamos a mencionar a grandes rasgos más adelante. En el lado algebraico, Greenberg, Bloch y Kato definieron grupos de Selmer en gran generalidad alrededor de 1990. Por otro lado, en 1988 Coates y Perrin-Riou formularon conjeturas sobre la existencia de funciones  $L$   $p$ -ádicas para ciertos motivos. Estos desarrollos llevaron a la formulación de una Conjetura Principal para motivos hecha por Greenberg y a una versión mucho más general hecha por Fukaya y

Kato en 2006. Sin embargo, de la mayoría de estas generalizaciones hasta ahora no tenemos demostraciones.

En este capítulo primero vamos a estudiar grupos de Selmer, que son los protagonistas del lado algebraico de la Teoría de Iwasawa, y explicaremos su conexión con objetos clásicos como grupos de clases. Luego hablaremos sobre funciones  $L$  complejas en gran generalidad. Como primer contacto con estos conceptos expondremos la aplicación a curvas elípticas, que son un objeto de gran interés en la geometría aritmética, y veremos cómo formular una Conjetura Principal para ellas. Después de esto discutiremos las funciones  $L$   $p$ -ádicas en esta situación porque aquí entrarán las formas modulares en el cuadro. Finalmente esbozamos las generalizaciones de todo lo anterior y la manera en que sumergen en un océano aún más grande.

Hay que tener un poco de cuidado con algunos encajes, por eso aclaramos esto inmediatamente. Sea  $K$  un campo de números con un encaje en  $\overline{\mathbb{Q}}$ , y recuerde que ya fijamos encajes  $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$  para cada primo  $\ell$  y  $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ . Estas elecciones inducen varias más, como explicamos ahora. Primero, ya mencionamos que vía restricción obtenemos inclusiones de grupos  $G_{\mathbb{R}} \hookrightarrow G_{\mathbb{Q}}$  y  $G_{\mathbb{Q}_\ell} \hookrightarrow G_{\mathbb{Q}}$ . Esto entonces fija un subgrupo de inercia de  $G_{\mathbb{Q}}$  para cada primo  $\ell$ , que es el núcleo de la aplicación de  $G_{\mathbb{Q}_\ell}$  al grupo absoluto de Galois del campo residual  $\mathbb{F}_\ell$ . Lo denotamos como  $I_\ell$ ; su campo fijo es la máxima extensión no ramificada  $\mathbb{Q}_\ell^{\text{nr}}$ . El encaje  $K \hookrightarrow \overline{\mathbb{Q}}$  fija encajes  $K \hookrightarrow \mathbb{C}$  y  $K \hookrightarrow \overline{\mathbb{Q}}_\ell$ , además para cada primo  $\ell$  el núcleo de

$$\mathcal{O}_K \hookrightarrow \mathcal{O}_{\overline{\mathbb{Q}}_\ell} \twoheadrightarrow \overline{\mathbb{F}}_\ell$$

es un ideal primo de  $\mathcal{O}_K$  y por lo tanto una plaza  $\lambda \mid \ell$  de  $K$ . Los encajes también fijan inclusiones de grupos  $\text{Gal}(\overline{\mathbb{Q}}/K) \hookrightarrow G_{\mathbb{Q}}$  y  $\text{Gal}(\overline{\mathbb{Q}}_\ell/K_\lambda) \hookrightarrow G_{\mathbb{Q}_\ell}$ . Dicho esto, a partir de ahora siempre asumiremos que cada campo de números está encajado en  $\overline{\mathbb{Q}}$ , y recordaremos estas elecciones.

### 7.2.2. Representaciones de Galois y grupos de Selmer

Los grupos de Selmer fueron originalmente introducidos para curvas elípticas (o variedades abelianas), pero ahora existe una definición bastante general. Al especializar esta definición con los parámetros correctos recobramos la definición de los grupos de clases, esto motiva naturalmente el uso de grupos de Selmer para las generalizaciones de la Conjetura Principal.

A partir de aquí suponemos algunos conocimientos extras, por ejemplo asumimos que el lector conozca la teoría de cohomología de Galois, es decir la cohomología de cocadenas continuas de grupos de Galois con coeficientes en módulos topológicos, como es explicada por ejemplo en [NSWo8, Cap. I, II, esp. II.7]. Si  $K$  es un campo entonces escribimos la cohomología de su grupo absoluto de Galois  $G_K$  como  $H^*(K, -)$  en lugar de  $H^*(G_K, -)$ . Si  $K$  es una extensión finita de  $\mathbb{Q}$  o de  $\mathbb{Q}_\ell$  entonces denotamos  $K^{\text{nr}}$  su máxima extensión no ramificada. Es decir, en el caso de una extensión  $K_\lambda/\mathbb{Q}_\ell$  la cohomología  $H^*(K_\lambda^{\text{nr}}, -)$  es la cohomología del subgrupo de inercia  $I_\lambda$  en  $G_{K_\lambda}$ .

**Definición 7.1:** Sea  $V$  un espacio vectorial de dimensión finita sobre algún campo topológico  $L$  con una acción continua de  $G_{\mathbb{Q}}$ . Entonces  $V$  se llama una *representación de Galois*  $L$ -lineal (o con coeficientes en  $L$ ). Después de escoger una base, esto puede ser visto como un morfismo continuo de grupos

$$\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_n(L)$$

con  $n = \dim V$ .

Sea  $L/\mathbb{Q}_p$  una extensión finita con anillo de enteros  $\mathcal{O}$ . Un  $\mathcal{O}$ -submódulo  $T$  de  $V$  se llama *retículo estable* si  $T$  es compacto, estable bajo la acción de  $G_{\mathbb{Q}}$  y  $V = L \otimes_{\mathcal{O}} T$ . La representación  $V$  se llama *no ramificada* en una plaza  $v$  de  $K$  si el subgrupo de inercia  $I_v$  actúa trivialmente en  $V$ . Se llama *no ramificada en casi todos lados* si es ramificada solo en una cantidad finita de plazas de  $K$ .

Por continuidad, cada representación de Galois con coeficientes en una extensión finita de  $\mathbb{Q}_p$  contiene un retículo estable (ejercicio 7.1)

En esta sección en la mayoría de los casos tendremos  $L = \mathbb{Q}_p$ . Además, normalmente el retículo es canónicamente dado – de hecho, primero conocemos el retículo  $T$  y luego definimos  $V = L \otimes_{\mathcal{O}} T$ .

**Observación:** Vía restricción obtenemos acciones de  $G_{\mathbb{Q}_\ell}$  y de  $G_{\mathbb{R}}$  en  $V$  y  $T$ .

**Ejemplo 7.2:** Un ejemplo muy importante es el siguiente. Sea

$$\mathbb{Z}_p(1) = \varprojlim_{r \in \mathbb{N}_{\geq 1}} \mu_{p^r}$$

como en la nota 1.47, que es un  $\mathbb{Z}_p$ -módulo compacto que es no canónicamente isomorfo a  $\mathbb{Z}_p$  con una acción continua de  $G_{\mathbb{Q}}$ . Definimos  $\mathbb{Q}_p(1) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$ . Entonces  $V = \mathbb{Q}_p(1)$  y  $T = \mathbb{Z}_p(1)$  es un ejemplo de una representación de Galois  $\mathbb{Q}_p$ -lineal y un retículo estable. Esta representación es ramificada solo en  $p$ , así que es no ramificada en casi todos lados.

Ahora introducimos los grupos de Selmer. La idea es que queremos un grupo que mide «la diferencia entre el comportamiento local y global de un objeto aritmético». Por ejemplo, si  $K$  es un campo de números entonces cada ideal de  $\mathcal{O}_K$  se vuelve un ideal principal en cada completación  $\mathcal{O}_{K_v}$  para los primos  $v$  de  $K$ , pero en general no debe ser un ideal principal en  $\mathcal{O}_K$ . La diferencia entre la situación local y global es medida por el grupo de clases (que esencialmente es un grupo de Selmer, véase la proposición 7.5 abajo). Los objetos aritméticos generales para cuales introducimos grupos de Selmer son representaciones de Galois, y usamos la cohomología de Galois local y global para definirlos.

**Definición 7.3:** Sea  $L/\mathbb{Q}$  una extensión finita con anillo de enteros  $\mathcal{O}$ . Sea  $V$  una representación de Galois con coeficientes en  $L$  que es no ramificada en casi todos lados y  $T$  un retículo estable. Para un campo de números  $K$ , encajado en  $\overline{\mathbb{Q}}$  de tal manera que su grupo absoluto de Galois  $G_K$  sea un subgrupo de  $G_{\mathbb{Q}}$ , definimos los siguientes grupos.

- (a) Sea  $v$  una plaza de  $K$ . Definimos un subgrupo del grupo  $H^1(K_v, V)$  de la cohomología local de Galois como

$$H_f^1(K_v, V) = \begin{cases} \ker(H^1(K_v, V) \rightarrow H^1(K_v^{\text{nr}}, V)), & v \nmid p\infty, \\ \ker(H^1(K_v, V) \rightarrow H^1(K_v, V \otimes_{\mathbb{Q}_p} B_{\text{cris}})), & v \mid p, \\ 0, & v \mid \infty \end{cases}$$

los mapeos siendo la restricción. Aquí,  $B_{\text{cris}}$  es un cierto anillo sobre cual no podemos decir mucho.<sup>1</sup> Usando esto definimos un subgrupo de  $H^1(K_v, V/T)$  para cada plaza  $v$  como

$$H_f^1(K_v, V/T) = \text{im}(H_f^1(K_v, V) \rightarrow H^1(K_v, V/T)).$$

- (b) Definimos un subgrupo del grupo  $H^1(K, V/T)$  de la cohomología global de Galois como

$$\begin{aligned} \text{Sel}(K, V/T) &= \{c \in H^1(K, V/T) \mid \forall v \text{ plaza: } \text{res}_v(c) \in H_f^1(K_v, V/T)\} \\ &= \ker \left( H^1(K, V/T) \longrightarrow \prod_{v \text{ plaza}} \frac{H^1(K_v, V/T)}{H_f^1(K_v, V/T)} \right) \end{aligned}$$

<sup>1</sup> El anillo  $B_{\text{cris}}$  fue definido por Fontaine y es uno de los *anillos de períodos  $p$ -ádicos* de la teoría de Hodge  $p$ -ádica, que no explicamos aquí (remitimos a [BCog] para esto). Es una  $\mathbb{Q}_p$ -álgebra topológica completa con una acción continua de  $G_{\mathbb{Q}_p}$  y algunas estructuras más, de manera que  $V \otimes_{\mathbb{Q}_p} B_{\text{cris}}$  tiene una acción de  $G_{\mathbb{Q}_p}$  diagonalmente.

con  $\text{res}_v : H^1(K, V/T) \rightarrow H^1(K_v, V/T)$  el mapeo de restricción. Esto es un  $\mathcal{O}$ -módulo discreto que se llama el *grupo de Selmer* de  $V/T$  (sobre  $K$ ).

Más precisamente estos grupos de Selmer a veces se llaman *grupos de Selmer de Bloch y Kato* porque ellos los introdujeron en [BK90]; también existen otras variantes con diferentes subgrupos locales en lugar de los  $H_f^1$ , pero los de Bloch y Kato se comportan bien y son los que se usan en las generalizaciones de la Conjetura Principal.

Notemos que aunque los llamamos «grupos de Selmer», realmente son  $\mathcal{O}$ -módulos.

**Nota 7.4:** En la definición de arriba, se podría preguntar por qué no definimos

$$\tilde{H}_f^1(K_v, V/T) = \ker(H^1(K_v, V/T) \rightarrow H^1(K_v^{\text{nr}}, V/T))$$

en lugar de

$$H_f^1(K_v, V/T) = \text{im}(H_f^1(K_v, V) \rightarrow H^1(K_v, V/T))$$

para  $v \nmid p\infty$ . Estos dos grupos en general son diferentes. El segundo es un subgrupo del primero y siempre es divisible porque  $H_f^1(K_v, V)$  es un  $L$ -espacio vectorial. De hecho se cumple que

$$H_f^1(K_v, V/T) = \tilde{H}_f^1(K_v, V/T)_{\text{div}},$$

donde escribimos  $(\cdot)_{\text{div}}$  como los elementos  $p$ -divisibles en un  $\mathbb{Z}_p$ -módulo abeliano [Rub00, Lem. I.3.5 (i)]. En particular, si  $\tilde{H}_f^1(K_v, V/T)$  es divisible entonces sí tenemos la igualdad

$$H_f^1(K_v, V/T) = \ker(H^1(K_v, V/T) \rightarrow H^1(K_v^{\text{nr}}, V/T)).$$

En este caso podemos describir el grupo de Selmer como

$$\text{Sel}(K, V/T) = \ker \left( H^1(K, V/T) \longrightarrow \prod_{v \nmid p\infty} H^1(I_v, V/T) \times \prod_{v|\infty} H^1(K_v, V/T) \times \prod_{v|p} \frac{H^1(K_v, V/T)}{H_f^1(K_v, V/T)} \right). \quad (7.1)$$

Para explicar las relaciones de todo esto con lo anterior, empecemos con calcular el grupo de Selmer en el caso más simple posible. Sea  $\mathcal{O} = \mathbb{Z}_p$ ,  $L = \mathbb{Q}_p$ ,  $T = \mathbb{Z}_p$  y  $V = \mathbb{Q}_p$  con la acción trivial de  $G_{\mathbb{Q}}$ .

**Proposición 7.5:** *Sea  $K$  un campo de números. Entonces tenemos un isomorfismo canónico*

$$\text{Sel}(K, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \text{Cl}(K)(p)^\vee,$$

donde  $\text{Cl}(K)(p)$  es la  $p$ -parte del grupo de clases de  $K$ .

*Demostración:* Usamos el teorema 1.38 que dice que el grupo de clases  $\text{Cl}(K)$  es canónicamente isomorfo al grupo de Galois  $\text{Gal}(H/K)$  del campo de clases de Hilbert  $H$  de  $K$ , que es la extensión máxima abeliana no ramificada. Por definición tenemos una sucesión exacta de grupos profinitos

$$\bigoplus_{v \text{ plaza}} I_v \rightarrow G_K^{\text{ab}} \rightarrow \text{Gal}(H/K) \rightarrow 0$$

donde  $I_v$  es el grupo de inercia en la plaza  $v$  de  $K$  (si  $v$  es una plaza arquimedea entonces  $I_v$  es de orden 2 generado por la conjugación compleja en esta plaza).

Aplicamos el funtor  $\text{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$  a esta sucesión y usamos que esto es lo mismo que  $H^1(-, \mathbb{Q}_p/\mathbb{Z}_p)$  porque la acción de todos los grupos en  $\mathbb{Q}_p/\mathbb{Z}_p$  es trivial. Además usamos

que para cada abeliano grupo finito  $A$  tenemos que  $\text{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p) = \text{Hom}(A(p), \mathbb{Q}_p/\mathbb{Z}_p)$ . Así obtenemos

$$0 \rightarrow \text{Gal}(H/K)(p)^\vee \rightarrow H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow \prod_v H^1(I_v, \mathbb{Q}_p/\mathbb{Z}_p). \quad (*)$$

Queremos usar la descripción en (7.1). Para esto tenemos que verificar que  $\ker(H^1(K_v, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(K_v^{\text{nr}}, \mathbb{Q}_p/\mathbb{Z}_p))$  es divisible para los primos  $v \nmid p$ . Pero porque  $H^1(-, \mathbb{Q}_p/\mathbb{Z}_p) = \text{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ , los elementos en este núcleo son los homomorfismos de  $G_{K_v}$  a  $\mathbb{Q}_p/\mathbb{Z}_p$  que son triviales en  $I_v$ , es decir son los que se factorizan a través de  $G_{K_v}/I_v \cong \widehat{\mathbb{Z}}$ . Pero  $\text{Hom}_{\mathbb{Z}_p}(\widehat{\mathbb{Z}}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p$  porque cada tal homomorfismo es únicamente determinado por la imagen de  $1 \in \widehat{\mathbb{Z}}$ . Este grupo es claramente divisible.

Es decir, la sucesión  $(*)$  es casi la misma que (7.1), las diferencias están en las plazas  $v \mid p$  y  $v \mid \infty$ . Para las plazas  $v \mid \infty$  observamos que en el producto a la derecha en ambas sucesiones los grupos son triviales porque  $I_v$  es de orden 2 en este caso y  $p \neq 2$ , y  $G_{K_v}$  es de orden 1 o 2. Falta ver que para las plazas  $v \mid p$  tenemos

$$\ker(H^1(K_v, \mathbb{Q}_p) \rightarrow H^1(I_v, \mathbb{Q}_p)) = \ker(H^1(K_v, \mathbb{Q}_p) \rightarrow H^1(K_v, B_{\text{cris}})).$$

Una demostración de esto se encuentra en [BK90, Ex. 3.9] (teniendo en cuenta el ejercicio 7.2); la omitimos aquí porque ni siquiera explicamos que es  $B_{\text{cris}}$ .  $\square$

**Definición 7.6:** Sea  $(K_r)_r$  la torre infinita de campos que usamos también en el capítulo 6, es decir  $K_r = \mathbb{Q}(\mu_{p^r})$  para  $r \in \mathbb{N}_{\geq 0} \cup \{\infty\}$ , y sea  $G = \lim_r \text{Gal}(K_r/\mathbb{Q})$  su grupo de Galois. Fijamos encajes compatibles de todos los  $K_r$  en  $\mathbb{Q}$ . Además sea  $V$  una representación de Galois con coeficientes en  $L$  y  $T$  un retículo estable. Entonces definimos

$$X(V/T) = \varprojlim_{r \in \mathbb{N}_{\geq 1}} \text{Sel}(K_r, V/T)^\vee = (\varinjlim_{r \in \mathbb{N}_{\geq 1}} \text{Sel}(K_r, V/T))^\vee$$

donde los mapeos  $\text{Sel}(K_r, V/T) \rightarrow \text{Sel}(K_{r+1}, V/T)$  son las restricciones (véase el ejercicio 7.3). Esto es un  $\Lambda(G)$ -módulo compacto (aquí  $\Lambda(G)$  es el álgebra de Iwasawa con coeficientes en  $\mathcal{O}$ , los enteros de  $L$ ).

De la proposición 7.5 obtenemos inmediatamente:

**Corolario 7.7:**  $X(\mathbb{Q}_p/\mathbb{Z}_p) = X_\infty$  es el módulo de la sección 6.1.

*Demostración:* Lo que falta verificar es que los mapeos con respecto a cuales tomamos los límites son los mismos, es decir, que el diagrama

$$\begin{array}{ccc} H^1(K_{r+1}, \mathbb{Q}_p/\mathbb{Z}_p) & \supseteq \text{Sel}(K_{r+1}, \mathbb{Q}_p/\mathbb{Z}_p) \simeq & \text{Cl}(K_{r+1})(p)^\vee \\ = \text{Hom}(G_{K_{r+1}}, \mathbb{Q}_p/\mathbb{Z}_p) & & \simeq \text{Hom}(\text{Gal}(H_{r+1}/K_{r+1}), \mathbb{Q}_p/\mathbb{Z}_p) \\ \downarrow \text{res} & & \downarrow \text{res} \\ \text{Hom}(G_{K_r}, \mathbb{Q}_p/\mathbb{Z}_p) & & \text{Hom}(\text{Gal}(H_r/K_r), \mathbb{Q}_p/\mathbb{Z}_p) \simeq \\ = H^1(K_r, \mathbb{Q}_p/\mathbb{Z}_p) & \supseteq \text{Sel}(K_r, \mathbb{Q}_p/\mathbb{Z}_p) \simeq & \text{Cl}(K_r)(p)^\vee \end{array}$$

conmuta para  $r$  suficientemente grande (donde  $H_r$  es el campo de clases de Hilbert de  $K_r$ ). Lo dejamos como ejercicio.  $\square$

También podemos obtener el otro módulo  $Y_\infty$  como un módulo  $X(-)$  de esta forma. En la siguiente proposición escribimos  $\mathbb{Q}_p/\mathbb{Z}_p(1)$  para  $\mathbb{Q}_p(1)/\mathbb{Z}_p(1)$ .

**Proposición 7.8:** Sea  $K$  un campo de números. Entonces tenemos un isomorfismo canónico

$$\text{Sel}(K, \mathbb{Q}_p/\mathbb{Z}_p(1)) \simeq \text{Gal}(M/K)^\vee,$$

donde  $M$  es su extensión máxima abeliana pro- $p$  no ramificada fuera de  $p$ . En particular,  $X(\mathbb{Q}_p/\mathbb{Z}_p(1)) = Y_\infty$  es el módulo de la sección 6.1.

*Demostración:* Benutze  $H^1(K, \mu_m(K)) = K^\times / (K^\times)^m$  und proposición 6.7. Oder Referenz? □

Estas observaciones ya insinúan cómo la Conjetura Principal podría ser generalizada. Sin embargo, quedan muchas preguntas: ¿Para cuáles tipos de representaciones de Galois podemos esperar una generalización? ¿Qué tendría que ser la función  $L$   $p$ -ádica? Y antes que nada, ¿cómo definimos una función  $L$  compleja? Vamos a indicar las respuestas a estas preguntas en los siguientes apartados.

### Ejercicios

**Ejercicio 7.1:** Demuestre que cada representación de Galois con coeficientes en una extensión finita de  $\mathbb{Q}_p$  contiene un retículo estable. Para esto tome cualquier retículo, no necesariamente estable, y considere sus traslados bajo la acción de  $G_{\mathbb{Q}}$ . Use la continuidad de la representación y el hecho de que  $\mathcal{O}$  es compacto.

**Ejercicio 7.2:** Demuestre que para cada plaza  $v \mid p$  de un campo de números  $K$  el espacio vectorial

$$\ker(H^1(K_v, \mathbb{Q}_p) \rightarrow H^1(I_v, \mathbb{Q}_p))$$

tiene dimensión 1 sobre  $\mathbb{Q}_p$ . Para esto use que  $H^1(-, \mathbb{Q}_p) = \text{Hom}(-, \mathbb{Q}_p)$  (porque la acción en  $\mathbb{Q}_p$  es trivial) y la teoría local de campos de clases para describir estos homomorfismos.

**Ejercicio 7.3:** Sea  $V$  una representación de Galois con coeficientes en una extensión finita  $L/\mathbb{Q}_p$  y  $T$  un retículo estable. Demuestre que si  $K \subseteq K'$  son campos de números entonces el mapeo de restricción  $H^1(K, V/T) \rightarrow H^1(K', V/T)$  envía  $\text{Sel}(K, V/T)$  a  $\text{Sel}(K', V/T)$ .

**Ejercicio 7.4:** Verifique que el diagrama en la demostración del corolario 7.7 es conmutativo. Use la conmutatividad del diagrama (4.5) para esto.

### 7.2.3. Funciones $L$ para sistemas compatibles de representaciones

Recordemos algunos aspectos de las funciones  $L$  complejas. Las que conocimos en la sección 5.1 tenían un producto de Euler, es decir un producto de la forma

$$L(s) = \prod_{\ell \text{ primo}} P_\ell(\ell^{-s})^{-1} \quad (s \in \mathbb{C}, \text{Re } s \gg 0)$$

donde  $P_\ell \in \overline{\mathbb{Q}}[T]$  es un polinomio: en el caso de la función zeta de Riemann tenemos  $P_\ell = 1 - T$  para cada primo  $\ell$  y en el caso de la función  $L$  de un carácter de Dirichlet  $\chi$  tenemos  $P_\ell = 1 - \chi(\ell)T \in \mathbb{Q}(\chi)[T]$  – véase la definición 5.8. Notemos que la función zeta de Riemann es un caso especial de una función  $L$  de Dirichlet, es decir, la del carácter trivial. El camino a generalizar la conexión de los polinomios  $P_\ell$  y el carácter  $\chi$  se aclara cuando vemos el carácter como una representación de Galois.

Para explicar esto necesitamos usar los *elementos de Frobenius* en  $G_{\mathbb{Q}}$ . Si  $\ell$  es un primo entonces tenemos el subgrupo (gracias a los encajes que fijamos)  $G_{\mathbb{Q}_\ell} \subseteq G_{\mathbb{Q}}$  que tiene una sobreyección al grupo de Galois absoluto del campo residual  $\mathbb{F}_\ell$  de  $\mathbb{Q}_\ell$ . Este grupo de Galois  $G_{\mathbb{F}_\ell}$  es canónicamente isomorfo a  $\widehat{\mathbb{Z}}$  con  $1 \in \widehat{\mathbb{Z}}$  correspondiendo al automorfismo Frobenius

(ejercicio 1.1). Porque  $G_{\mathbb{Q}_\ell} \rightarrow G_{\mathbb{F}_\ell}$  es sobreyectivo podemos escoger un levantamiento que llamamos  $\text{Frob}_\ell \in G_{\mathbb{Q}_\ell} \subseteq G_{\mathbb{Q}}$ . Este elemento no es único, pero es bien definido salvo a multiplicación del grupo de inercia  $I_\ell$ , que es el núcleo de la aplicación  $G_{\mathbb{Q}_\ell} \rightarrow G_{\mathbb{F}_\ell}$ ; esto será suficiente para lo que queremos hacer. A partir de ahora fijemos elementos de Frobenius  $\text{Frob}_\ell \in G_{\mathbb{Q}}$  para cada primo  $\ell$ .

Ahora tomamos un carácter de Dirichlet  $\chi$  de conductor  $N \in \mathbb{N}_{\geq 1}$  y lo vemos como una representación de Galois  $\mathbb{C}$ -lineal vía

$$G_{\mathbb{Q}} \twoheadrightarrow \text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \overline{\mathbb{Q}}^\times \subset \mathbb{C}^\times \quad (7.2)$$

(llamamos este mapeo  $G_{\mathbb{Q}} \rightarrow \mathbb{C}^\times$  también  $\chi$ ), que define una acción de  $G_{\mathbb{Q}}$  en el  $\mathbb{C}$ -espacio vectorial  $V = \mathbb{C}$  en que  $g \in G_{\mathbb{Q}}$  actúa por multiplicación con  $\chi(g)$ . Esta representación es ramificada en un primo  $\ell$  si y solo si  $\ell \mid N$ , es decir si y solo si  $\chi(\ell) = 0$ . La acción de un elemento de Frobenius  $\text{Frob}_\ell$  en  $V$  en general no es bien definida porque  $\text{Frob}_\ell$  solo es bien definido salvo elementos de  $I_\ell$  y  $I_\ell$  podría actuar no trivialmente. Pero si escribimos  $V^{I_\ell}$  como el subespacio de  $V$  donde  $I_\ell$  actúa trivialmente, entonces la acción de  $\text{Frob}_\ell$  en  $V^{I_\ell}$  sí es bien definida; en particular, su polinomio característico lo es. Si definimos  $P_\ell(\chi, T)$  como el polinomio<sup>2</sup>

$$P_\ell(\chi, T) := \det(1 - \chi(\text{Frob}_\ell)T, V^{I_\ell})$$

entonces de hecho tenemos

$$P_\ell(\chi, T) = 1 - \chi(\ell)T,$$

es decir ¡reconstruimos los polinomios que definen el producto de Euler a partir de la representación de Galois! Le sugerimos urgentemente al lector que verifique todas estas afirmaciones.

Las representaciones que estudiamos al principio de esta sección tuvieron coeficientes en  $\mathbb{Q}_p$  o una extensión finita  $L$ . Si usamos la misma fórmula como arriba para definir polinomios  $P_\ell$  para ellas tenemos un problema – los coeficientes serán en  $L$ , que no podemos encajar en  $\mathbb{C}$  para definir una función  $L$  compleja. Sin embargo, para las representaciones  $\mathbb{Q}_p$  (con la acción trivial) y  $\mathbb{Q}_p(1)$  que estudiamos antes este problema no aparece: por supuesto, para la representación trivial tenemos

$$P_\ell(\mathbb{Q}_p, T) := \det(1 - T, \mathbb{Q}_p^{I_\ell}) = 1 - T$$

para cada primo  $\ell$  y en el otro caso tenemos

$$P_\ell(\mathbb{Q}_p(1), T) := \det(1 - T, \mathbb{Q}_p(1)^{I_\ell}) = 1 - \ell T$$

al menos para los primos  $\ell \neq p$ , mientras para  $\ell = p$  obtenemos  $P_p(\mathbb{Q}_p(1), T) = 1$ . ¡Otra vez el lector debería verificar estas afirmaciones! Es decir, estos polinomios de hecho tienen coeficientes en  $\overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}_p}$ , que encajamos en  $\mathbb{C}$ . Por supuesto hay representaciones para cuales esto no sea verdad, por eso sólo vamos a usar representaciones donde los coeficientes de los polinomios que obtengamos estén en  $\overline{\mathbb{Q}}$  (véase la siguiente definición).

Si ahora definimos una función  $L$  para las representaciones  $\mathbb{Q}_p$  y  $\mathbb{Q}_p(1)$  usando la fórmula del producto de Euler obtenemos la función zeta de Riemann para  $\mathbb{Q}_p$  y obtenemos

$$(1 - p^{-(s+1)})\zeta(s+1)$$

para  $\mathbb{Q}_p(1)$ , es decir la función zeta trasladada por 1 y con un factor de Euler faltante. Esto es un poco raro . . . queremos tener también el factor de Euler en  $p$ . Notemos que también existen las representaciones  $\mathbb{Q}_q(1)$  para todos los otros primos  $q \neq p$ , y si usamos éstas en

<sup>2</sup> Aquí y en lo siguiente, la notación  $\det(\varphi, V)$  significa el determinante de un endomorfismo  $\varphi$  de un espacio vectorial  $V$ .

lugar de  $\mathbb{Q}_p(1)$  para definir el polinomio  $P_\ell$  entonces obtenemos lo mismo para  $\ell \neq p, q$ , pero para  $\ell = p$  obtenemos el polinomio que corresponde al factor de Euler que hacía falta. Es decir, las representaciones  $\mathbb{Q}_q(1)$  para todos los primos  $q$  son compatibles de alguna manera, y para definir  $P_\ell$  podemos usar cualquiera de ellas salvo  $\mathbb{Q}_\ell(1)$ . Esto nos lleva a la siguiente definición.

**Definición 7.9:** Un *sistema compatible de representaciones de Galois* es una colección  $V = (V_q)_q$  de representaciones de  $G_{\mathbb{Q}}$ , donde  $V_q$  es un espacio vectorial sobre  $\mathbb{Q}_q$ , para cada primo  $q$ , tal que las siguientes condiciones sean ciertas.

- (a) Existe un conjunto finito  $S$  de primos tal que cada  $V_q$  no es ramificado fuera de  $S \cup \{q\}$ .
- (b) Para cada primo  $\ell$  y cada otro primo  $q \neq \ell$  el polinomio

$$P_\ell(V, T) := \det(1 - \text{Frob}_\ell T, V_q^{I_\ell})$$

que a priori tiene coeficientes en  $\mathbb{Q}_q$  de hecho tiene coeficientes en  $\mathbb{Q}$  y no depende de  $q$ .

Un poco más general, si  $K$  es un campo de números entonces definimos un sistema compatible de representaciones de Galois con coeficientes en  $K$  como es una colección de representaciones  $V = (V_q)_q$  de  $G_{\mathbb{Q}}$  indexada por todos los primos de  $K$ , donde  $V_q$  es un espacio vectorial sobre  $K_q$  con las condiciones análogos (en este caso los polinomios  $P_\ell(V, T)$  deben tener coeficientes en  $K$ ).

Si  $V$  es un sistema compatible de representaciones de Galois entonces definimos su función  $L$  como

$$L(V, s) := \prod_{\ell \text{ primo}} P_\ell(V, \ell^{-s})^{-1}.$$

De momento, esto sólo es una expresión formal, porque todavía no sabemos nada sobre convergencia.

Queremos dar una heurística por qué esta definición es interesante. El teorema de Brauer y Nesbitt dice que dos representaciones de un grupo profinito son iguales (salvo a semisimplificación, que no vamos a explicar aquí) si y solo si los polinomios característicos de los imágenes de todos elementos del grupo bajo las dos representaciones son iguales. Además, el teorema de densidad de Chebotarev implica que los elementos Frobenius son densos en  $G_{\mathbb{Q}}$ , así que por continuidad la igualdad de los polinomios característicos de ellos ya es suficiente. Es decir, en la formula que define la función  $L(V, s)$  multiplicamos expresiones que juntos determinan  $V$  únicamente (salvo a semisimplificación). Véase [CR06, Thm. 30.16]<sup>3</sup> y [Neu99, Thm. 13.4].

**Ejemplo 7.10:** (a) Poniendo  $V_q = \mathbb{Q}_q$  con la acción trivial de  $G_{\mathbb{Q}}$  para cada primo  $q$  nos da un sistema compatible de representaciones de Galois. Su función  $L$  es la función zeta de Riemann.

(b) Poniendo  $V_q = \mathbb{Q}_q(1)$  nos da también un sistema compatible de representaciones de Galois. Su función  $L$  es  $\zeta(s + 1)$ .

(c) Sea  $\chi$  un carácter de Dirichlet y  $K = \mathbb{Q}(\chi)$ . Entonces si ponemos  $V_q = K_q$  para cada primo  $q$  de  $K$  con  $g \in G_{\mathbb{Q}}$  actuando en  $V_q$  como multiplicación con  $\chi(g)$  entonces esto también es un sistema compatible de representaciones de Galois, esta vez con coeficientes en  $K$ . Su función  $L$  es la función  $L$  de Dirichlet  $L(\chi, s)$ .

<sup>3</sup> El teorema de Brauer y Nesbitt allá es formulado para un grupo finito, pero examinando la demostración se puede ver que la demostración sigue funcionando para un grupo profinito.

Un sistema compatible de representaciones de Galois todavía no es la noción final a la cual se puede generalizar los fenómenos de la Teoría de Iwasawa, pero para nuestros ejemplos básicos es suficiente (la verdadera noción son los motivos, que mencionamos en la sección 7.2.6). Resumiendo, tenemos lo siguiente para el sistema compatible de representaciones de Galois  $(\mathbb{Q}_q)_q$ :

- La función  $L$  del sistema (la función zeta de Riemann) es meromorfa en todo de  $\mathbb{C}$  y algunos valores especiales son algebraicos.
- Fijamos un primo  $p$ . Entonces estos valores especiales pueden ser interpolados  $p$ -ádicamente, esto conduce a la existencia de una función  $L$   $p$ -ádica, que (esencialmente) es un elemento del álgebra de Iwasawa  $\Lambda(G)$ , donde  $G$  es el grupo de Galois de la torre infinita  $(K_r)_r = (\mathbb{Q}(\mu_{p^r}))_r$  de campos de números.
- Para el mismo primo  $p$ , si consideramos el módulo  $X(\mathbb{Q}_p/\mathbb{Z}_p)$  para el miembro en  $p$  del sistema de representaciones y un retículo estable obtenemos un módulo noetheriano de torsión sobre  $\Lambda(G)$ , y por lo tanto tiene un ideal característico gracias a la teoría de estructura de tales módulos.
- Este ideal característico es generado por la función  $L$   $p$ -ádica del sistema – esto es la Conjetura Principal.<sup>4</sup>

Algo similar ocurre para el sistema  $(\mathbb{Q}_q(1))_q$ , dándonos la otra versión de la Conjetura Principal. La relación entre estas dos formulaciones y el hecho de que son equivalentes la discutiremos más tarde (pie de página 15 en la página 139).

### Ejercicios

**Ejercicio 7.5:** Para los siguientes campos de números  $K$ , ¿cuáles primos de  $\mathbb{Q}$  son ramificados y cuáles son los elementos de Frobenius?

- (a)  $K = \mathbb{Q}(\sqrt{d})$  para  $d \in \mathbb{Z}$  libre de cuadrados;
- (b)  $K = \mathbb{Q}(\mu_m)$  con  $m \in \mathbb{N}_{\geq 1}$ .

Use los resultados para deducir el ley de reciprocidad cuadrática

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

para primos impares  $p, q$ .

**Ejercicio 7.6:** Para un carácter de Dirichlet que vemos como representación de Galois como en (7.2), ¿en cuáles primos es ramificado?

**Ejercicio 7.7:** Demuestre que si  $V$  es un espacio vectorial de dimensión 1 sobre  $\mathbb{C}$  con una acción de  $G_{\mathbb{Q}}$  dada por un carácter de Dirichlet  $\chi$  como en (7.2) entonces tenemos

$$\det(1 - \chi(\text{Frob}_{\ell})T, V^{\ell}) = 1 - \chi(\ell)T,$$

para cada primo  $\ell$  (no importa si sea ramificado o no).

**Ejercicio 7.8:** Sea  $V = (V_q)_q$  un sistema compatible de representaciones de Galois. Demuestre que entonces

$$V(1) := (V_q \otimes_{\mathbb{Q}_q} \mathbb{Q}_q(1))_q$$

también es un sistema compatible de representaciones de Galois y que

$$L(V(1), s) = L(V, s + 1).$$

<sup>4</sup> Salvo a que tenemos que restringir a la parte  $(\cdot)^-$  del módulo y multiplicar la función  $L$   $p$ -ádica con su denominador. Vamos a ignorar estos detalles aquí y en lo que sigue. De hecho, en las generalizaciones estas dos fenómenos no ocurren.

### 7.2.4. La Conjetura Principal para curvas elípticas

Como prometido ahora explicamos como curvas elípticas se insertan en la imagen que esbozamos hasta ahora. Para eso asumimos que el lector sea familiar con la teoría básica de curvas elípticas como es explicada por ejemplo en [Silog]. Para toda la sección fijamos una curva elíptica  $E$  sobre  $\mathbb{Q}$  y un primo  $p$ , además, suponemos que la curva tiene buena reducción ordinaria en  $p$ .

Al lector interesado en aprender más sobre la Teoría de Iwasawa de curvas elípticas le recomendamos el texto [Gre01a] de Greenberg y también [Wut14, §2].

Escribimos  $E(K)$  para los puntos de  $E$  con coeficientes en un campo  $K/\mathbb{Q}$ . Si  $m \in \mathbb{N}_{\geq 1}$  entonces escribimos  $E(K)[m]$  para los elementos de  $E(K)$  cuyo orden es divisible por  $m$ , es decir los que son anulados por la multiplicación por  $m$ , que denotamos  $[m]$ . Se sabe que  $E(\mathbb{Q})[m]$  es isomorfo a  $(\mathbb{Z}/m\mathbb{Z})^2$ , aunque el isomorfismo no es canónico. Para cada primo  $q$ , el *módulo de Tate*  $q$ -ádico de  $E$  está definido como

$$T_q E := \varprojlim_{l \in \mathbb{N}_{\geq 1}} E(\overline{\mathbb{Q}})[q^l],$$

los mapeos  $E(\overline{\mathbb{Q}})[q^{l+1}] \rightarrow E(\overline{\mathbb{Q}})[q^l]$  siendo  $P \mapsto [q]P$ . Esto es no canónicamente isomorfo a  $\mathbb{Z}_q^2$ . También definimos

$$V_q E = \mathbb{Q}_q \otimes_{\mathbb{Z}_q} T_p E$$

que es un espacio vectorial de dimensión 2 sobre  $\mathbb{Q}_q$ . La acción de  $G_{\mathbb{Q}}$  en  $E(\overline{\mathbb{Q}})$  induce acciones continuas en  $E(\overline{\mathbb{Q}})[q^l]$ ,  $T_q E$  y  $V_q E$ , y por eso  $V_q E$  es una representación de Galois  $\mathbb{Q}_q$ -lineal y  $T_q E$  es un retículo estable.

Sea  $p$  un primo. A continuación resumimos cómo se define el grupo de Selmer de una curva elíptica clásicamente. Fijamos un campo de números y  $l \in \mathbb{N}_{\geq 1}$  y seguimos [Silog, §X.4] poniendo allá  $E = E'$  y  $\phi = [p^l]$ . Para cada plaza  $v$  de  $K$  tenemos una sucesión exacta

$$0 \rightarrow E[p^l](\overline{K}_v) \rightarrow E(\overline{K}_v) \xrightarrow{[p^l]} E(\overline{K}_v) \rightarrow 0$$

de grupos abelianos discretos con acción de  $G_{K_v}$ . Tomando la sucesión exacta larga en cohomología obtenemos

$$0 \rightarrow E[p^l](K_v) \rightarrow E(K_v) \xrightarrow{[p^l]} E(K_v) \xrightarrow{\partial} H^1(K_v, E[p^l](\overline{K}_v)) \rightarrow \dots$$

El morfismo de borde  $\partial$  induce un morfismo inyectivo

$$\kappa_{r,v}: E(K_v)/p^l E(K_v) \hookrightarrow H^1(K_v, E[p^l](\overline{K}_v))$$

que se llama el *morfismo de Kummer* (en [Silog, §X.4] lo denotan  $\delta$ ). Entonces se define el grupo de Selmer de nivel  $p^l$  sobre  $K$  como las clases en cohomología de Galois global que localmente están en la imagen del morfismo de Kummer, es decir

$$S^{(p^l)}(E/K) := \{c \in H^1(K, E[p^l](\overline{K})) \mid \forall v \nmid \infty: \text{res}_v(c) \in \text{im } \kappa_{l,v}\}$$

y luego

$$S^{(p^\infty)}(E/K) := \varinjlim_{l \in \mathbb{N}_{\geq 1}} S^{(p^l)}(E/K) \subseteq \varinjlim_{l \in \mathbb{N}_{\geq 1}} H^1(K, E[p^l](\overline{K})) = H^1(K, E[p^\infty](\overline{K}))$$

(aquí la última igualdad sigue de [NSW08, (1.2.5)] y el hecho de que cada  $E[p^l](\overline{K})$  es finito, así que su estabilizador en  $G_K$  es abierto). Además, se puede ver fácilmente que  $E[p^\infty](\overline{K}) \simeq V_p E/T_p E$  canónicamente (véase el ejercicio 7.9). La siguiente proposición dice que, usando esta identificación, el grupo de Selmer clásico de hecho es lo mismo que el grupo de Selmer de la definición 7.3 en esta situación.

**Proposición 7.11:** *Para cada campo de números  $K$  tenemos una igualdad*

$$S^{(p^\infty)}(E/K) = \text{Sel}(K, V_p E/T_p E)$$

de subgrupos de  $H^1(K, V_p E/T_p E)$ .

*Demostración:* [Rub00, Prop. 1.6.7] □

Aplicando la definición 7.6 en nuestra situación obtenemos un  $\Lambda(G)$ -módulo compacto  $X(V_p E/T_p E)$  que simplemente denotamos  $X(E)$ . Se sabe que este módulo es noetheriano [Wut14, Lem. 13], que es importante para poder aplicar la teoría de estructura a este módulo. Como los módulos que aparecen en la Conjetura Principal clásica tenemos incluso el siguiente resultado, que era sospechado por Mazur:

**Teorema 7.12 (Kato):** *El  $\Lambda(G)$ -módulo  $X(E)$  es de torsión.*

*Demostración:* [Kat04, Thm. 17.4 (1)] □

Como consecuencia de esto se puede aplicar las mismas técnicas que llevaron a la demostración del teorema I de Iwasawa sobre el crecimiento de los grupos de clases para obtener un resultado análogo sobre los ordenes de los  $p$ -partes de los grupos de Tate-Shafarevich, véase [Wut14, Prop. 14].

Ahora toca el turno de hablar de la función  $L$  asociada. Para la curva elíptica  $E$  tenemos la función  $L$  de Hasse y Weil

$$L(E, s) = \prod P_\ell(E, \ell^{-s})^{-1}$$

con

$$P_\ell(E, s) = \begin{cases} (1 - (\ell + 1 - \#E(\mathbb{F}_\ell))\ell^{-s} + \ell^{1-2s}) & \text{si } E \text{ tiene buena reducción en } \ell, \\ (1 - \ell^{-s}) & \text{si } E \text{ tiene reducción multiplicativa escindida en } \ell, \\ (1 + \ell^{-s}) & \text{si } E \text{ tiene reducción multiplicativa no escindida en } \ell, \\ 1 & \text{si } E \text{ tiene reducción aditiva en } \ell \end{cases}$$

que es introducida en [Sil09, §C.16] (por ahora, esto es sólo una expresión formal; hablamos de convergencia en la siguiente sección). Esta función  $L$  es un caso especial de la función  $L$  general de la definición 7.9: El sistema compatible de representaciones de Galois que hay que usar es  $(V_q E)_q$ , es decir está formado por todos los módulos de Tate. La primera condición sobre la ramificación de las representaciones es cierta por el criterio de Néron, Ogg y Shafarevich [Sil09, Thm. VII.7.1]. En [Hid12, §2.7.2] es demostrado que los polinomios de la definición 7.9 coinciden con los de la definición arriba, esto explica las fórmulas anteriores; en particular, la segunda condición sobre la compatibilidad también es cierta.

La discusión de esta función  $L$  y la pregunta sobre la existencia de una función  $L$   $p$ -ádica asociada la posponemos a la siguiente sección para la claridad de la exposición. Por ahora mencionamos el resultado sólo en una forma provisional, la versión precisa se encuentra en el teorema 7.18.

**Teorema 7.13 (Mazur/Swinnerton-Dyer):** *Existe un elemento  $\mu_E \in \Lambda(G)$  que interpola valores especiales de la función  $L(E, s)$   $p$ -ádicamente.*

Es decir, curvas elípticas (sobre  $\mathbb{Q}$  con buena reducción ordinaria en  $p$ ) también tienen una función  $L$   $p$ -ádica. Con estas preparaciones debería ser claro como formular la Conjetura Principal para curvas elípticas.

**Conjetura 7.14 (Conjetura Principal de Mazur para curvas elípticas):** *Tenemos la igualdad de ideales en  $\Lambda(G)$*

$$\text{car}_{\Lambda(G)} X(E) = (\mu_E).$$

Al día de hoy, esta conjetura es demostrada en muchos casos. El caso de una curva con multiplicación compleja la conjetura fue demostrada por Rubin [Rub91]. En el caso general, suponiendo algunas condiciones técnicas menudas, Kato [Kat04] demostró la inclusión « $\supseteq$ » en la igualdad y Skinner y Urban [SU14] demostraron la otra. Véase también [Kat07, §2.3.3, §2.4.4, §2.5.5] para una discusión de las ideas detrás de estas demostraciones.

### Ejercicios

**Ejercicio 7.9:** Sea  $A$  un grupo abeliano. Use el hecho de que el producto tensorial es compatible con colímites para demostrar que canónicamente

$$A \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \simeq \varinjlim_{l \in \mathbb{N}_{\geq 1}} A/p^l A$$

donde los mapeos  $A/p^l A \rightarrow A/p^{l+1} A$  en el colímite a la derecha son  $a \mapsto pa$ . Aplique esto al módulo de Tate  $A = T_p E$  de una curva elíptica  $E$  para demostrar que

$$V_p E/T_p E \simeq E[p^\infty](\overline{K}).$$

### 7.2.5. Funciones $L$ $p$ -ádicas para formas modulares

En la sección anterior dejamos pendiente la pregunta de cómo debe ser la función  $L$   $p$ -ádica de una curva elíptica. En el caso de la función zeta  $p$ -ádica, esta interpolaba valores especiales de la función zeta en enteros negativos, que eran algebraicos. ¡Recuerde que en los enteros negativos la serie que define la función zeta no converge! Además, no obtuvimos estos valores sino hasta que continuamos la función zeta analíticamente. Por lo tanto, antes de que podamos pensar en una función de Hasse y Weil  $p$ -ádica, tenemos que preguntarnos:

- ¿Dónde converge la serie que define la función  $L$  de Hasse y Weil?
- ¿Tiene una continuación meromorfa o analítica a todo  $\mathbb{C}$ ?
- ¿También tenemos valores especiales que son algebraicos? ¿Cuáles son estos valores?

Estas preguntas se pueden formular también para funciones  $L$  más generales como las de la definición 7.9, y lo que pasa es que en esta generalidad no se sabe casi nada (aunque hay algunas conjeturas que mencionaremos en la sección 7.2.6). El problema es que las funciones  $L$  son definidas por polinomios de origen aritmético (esencialmente polinomios característicos de elementos de Frobenius en una representación de Galois), y esta definición no dice mucho sobre el comportamiento analítico de dichas funciones. Necesitamos alguna herramienta para sobreponernos a estos obstáculos.

Aquí entra el famoso Programa de Langlands en el escenario. Esto es un tema enorme sobre el que se podría escribir otro libro, así que sólo indicamos algunas pocas ideas detrás del Programa de Langlands. La filosofía es que para cada «objeto aritmético» (más precisamente, un motivo<sup>5</sup>) debería existir un objeto «automorfo» (más precisamente, una representación automorfa), que es de origen analítico, con la misma función  $L$ . Sobre las funciones  $L$  de origen automorfo sabemos mucho más y en casos favorables tenemos por ejemplo la continuación analítica. Esto debería generalizar la teoría de campos de clases, es decir, la teoría de

<sup>5</sup> Por ahora nos imaginamos un motivo como un sistema compatible de representaciones de Galois aunque en realidad es algo más específico: conjeturalmente, cada motivo lleva a un tal sistema, pero no al revés. Diremos un poco más sobre esto en la siguiente sección 7.2.6.

campos de clases debería de ser una especialización del Programa de Langlands. Sobre  $\mathbb{Q}$  tenemos lo siguiente: El teorema de Kronecker y Weber dice que cada extensión abeliana está contenida en una extensión ciclotómica  $\mathbb{Q}(\mu_m)$  para un  $m \in \mathbb{N}_{\geq 1}$ , y el isomorfismo de Artin de la teoría de campos de clases en este caso simplemente es  $\text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ . En particular, las representaciones de Galois que se factorizan a través de  $\text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$  corresponden únicamente a los caracteres de Dirichlet de conductor un divisor de  $m$ . Bajo esta correspondencia, la función  $L$  de tal representación de Galois es la función  $L$  del carácter de Dirichlet correspondiente, como mencionamos antes. Esto es el caso más sencillo de una correspondencia tipo Langlands: los objetos aritméticos son las representaciones de  $G_{\mathbb{Q}}$  de orden finito y dimensión uno, y los objetos automorfos son los caracteres de Dirichlet. Tienen la misma función  $L$  y esta afirmación es equivalente al isomorfismo de Artin. Porque sabemos propiedades como continuación analítica de las funciones  $L$  de Dirichlet, lo obtenemos también para las funciones  $L$  de dichas representaciones de Galois. Aunque esto parece casi trivial en este caso básico, de hecho es una encarnación del Programa de Langlands.

En el caso de curvas elípticas el objeto automorfo que corresponde a ellas son ciertas formas modulares. En este caso tenemos el siguiente famoso resultado que implica el Último Teorema de Fermat. A partir de ahora hasta el fin de la sección suponemos que el lector conozca la teoría básica de formas modulares como es explicada por ejemplo en [DS05] o [Shi94]. Antes de citar el resultado resumimos la definición de la función  $L$  de formas modulares.

Sea  $f \in S_k(N, \chi)$  una forma modular cuspidal nueva<sup>6</sup> de peso  $k \geq 2$ , nivel  $N \in \mathbb{N}_{\geq 1}$  y nebentipo  $\chi$ ; en particular  $f$  es una forma propia para todos los operadores de Hecke. Si la vemos como función en el semiplano superior  $\mathbb{H}$  entonces se escribe como una serie de Fourier

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi iz} \quad (z \in \mathbb{H}).$$

La función  $L$  en este caso es definida como

$$L(f, s) = \sum_{n=1}^{\infty} a_n n^s.$$

Más generalmente, si  $\psi$  es un carácter de Dirichlet cualquiera entonces se define

$$L(f, \psi, s) = \sum_{n=1}^{\infty} a_n \psi(n) n^s.$$

Esta función se llama la función de  $f$  chanfleada por  $\psi$ . El siguiente resultado clásico describe sus propiedades básicas analíticas.

**Proposición 7.15:** *La serie que define  $L(f, \psi, s)$  converge absolutamente para  $\text{Re}(s) > \frac{k}{2} + 1$  y la función holomorfa que define tiene una continuación analítica a todo  $\mathbb{C}$ . Además tiene un producto de Euler*

$$L(f, \psi, s) = \prod_{\ell \text{ primo}} (1 - \psi(\ell) a_{\ell} \ell^{-s} + \chi \psi^2(\ell) \ell^{k-1-2s})^{-1} \quad (\text{Re}(s) > \frac{k}{2} + 1)$$

*Demostración:* [Shi94, Thm. 3.66], [DS05, Thm. 5.9.2] □

El Teorema de Modularidad entonces es el siguiente.

---

<sup>6</sup> *cuspidal newform*

**Teorema 7.16 (Wiles, Taylor, Breuil, Conrad, Diamond):** Sea  $E/\mathbb{Q}$  una curva elíptica. Entonces existe una forma modular nueva  $f$  de peso 2 con nebentipo trivial cuya función  $L$  es la misma que la de  $E$ , es decir

$$L(E, s) = L(f, s) \quad \forall s \in \mathbb{C}.$$

En particular  $L(E, -)$  tiene una continuación analítica a todo de  $\mathbb{C}$ .

Este resultado también es una encarnación del Programa de Langlands, y nos provee de la herramienta deseada para responder a las preguntas planteadas del inicio de esta sección. En general, no hay ninguna esperanza a responder a estas preguntas directamente sin pasar por el mundo automorfo, y esto ilustra la enorme importancia del Programa de Langlands para la Teoría de Iwasawa.

Es decir, la existencia de una función  $L$   $p$ -ádica para una curva elíptica ahora es equivalente a la existencia de una tal función para formas modulares nuevas de peso 2 con nebentipo trivial. De hecho, no es mucho más difícil explicar esto para formas modulares nuevas en general, así que desde ahora ya no hablaremos de curvas elípticas sino de formas modulares.

A partir de ahora fijamos una forma modular cuspidal nueva  $f \in S_k(N, \chi)$  como arriba. La pregunta de algebraicidad de valores especiales es contestada por el siguiente resultado.

**Teorema 7.17 (Shimura):** Sea  $K_f$  el campo de números generado por los coeficientes de Fourier de  $f$ . Existen dos números  $\Omega_f^\pm \in \mathbb{C}^\times$  tal que para cada carácter de Dirichlet  $\psi$  para  $n = 1, \dots, k-1$  tenemos

$$\frac{G(\psi^{-1})}{(2\pi i)^n \Omega_f^\pm} L(f, \psi, n) \in K_f(\psi).$$

Aquí el superíndice de  $\Omega_f^\pm$  debe ser el signo de  $(-1)^n \psi(-1)$  y

$$G(\psi^{-1}) = \sum_{j=1}^c \psi^{-1}(j) e^{2\pi i j/c}$$

es la suma de Gauß (con  $c$  siendo el conductor de  $\psi$ ).

*Demostración:* [Shi77, Thm. 1 (ii)] □

Como se puede ver de este teorema, los valores especiales en general ya no son algebraicos (porque los números  $\Omega_f^\pm$  en general son trascendentes), pero al menos podemos describir y controlar su parte trascendente con dos números. Otra diferencia, con el resultado análogo de la proposición 5.9 para caracteres de Dirichlet, es que sólo tenemos valores algebraicos para una cantidad finita de enteros  $n$ , pero para una cantidad infinita de caracteres. Este fenómeno tiene explicación en una conjetura de Deligne que abordaremos en la siguiente sección.

Para el siguiente resultado sobre la función  $L$   $p$ -ádica tenemos que suponer que  $f$  es ordinaria en  $p$ , esto significa que  $|a_p|_p = 1$  (esto es el valor absoluto  $p$ -ádico). Es fácil ver que en este caso el polinomio

$$X^2 - a_p X + \chi(p)p^{k-1},$$

que se llama el *polinomio de Hecke*  $p$ -ésimo de  $f$ , tiene una única raíz  $\alpha \in \overline{\mathbb{Q}}$  tal que  $|\alpha|_p = 1$ . Este  $\alpha$  aparece en el siguiente resultado. La condición ordinaria aquí es análoga a la condición en la sección 5.3 que pide que el conductor del carácter  $\chi$  no sea divisible por  $p$ .

La forma modular asociada a una curva elíptica de buena reducción ordinaria en  $p$  es ordinaria. Mencionamos además que en este caso el campo  $K_f$  es  $\mathbb{Q}$ .

Aquí y en los siguientes resultados,  $\Lambda(G)$  denota el álgebra de Iwasawa con coeficientes en el anillo de enteros  $\mathcal{O}$  de la completación de  $K_f$  en la plaza arriba de  $p$  fijada por nuestros encajes (es decir, para una curva elíptica  $\mathcal{O} = \mathbb{Z}_p$ ).

**Teorema 7.18 (Mazur/Swinnerton-Dyer, Mazur/Tate/Teitelbaum):** Sean  $K_f$  y  $\Omega_f^\pm$  como arriba.

Entonces existe un único elemento  $\mu_f \in \Lambda(G)$  tal que para  $n = 1, \dots, k-1$  y cada carácter de Dirichlet  $\psi$  de conductor  $p^m$  con  $m \in \mathbb{N}_{\geq 0}$  tenemos

$$\int_G \psi^{-1} \kappa^n d\mu_f = (n-1)! (1 - \alpha^{-1} \psi^{-1}(p) p^{n-1}) (1 - \alpha^{-1} \chi \psi(p) p^{k-n}) \frac{p^{m(n-1)} G(\psi^{-1})}{\alpha^m (2\pi i)^n \Omega_f^\pm} L(f, \psi, n),$$

donde otra vez el superíndice de  $\Omega_f^\pm$  es el signo de  $(-1)^n \psi(-1)$ .

*Demostración:* [MTT86] (y [MS74] para  $k = 2$ ) □

La fórmula de interpolación en este teorema se ve mucho menos elegante que la del teorema 5.24 – no simplemente quitamos un factor de Euler, sino que aparecen muchas «expresiones de corrección» que la desproveen de belleza. Sin embargo, hay una explicación satisfactoria por la cual cada una de estas expresiones debe aparecer y por qué esta fórmula de hecho es consistente con la del teorema 5.24. Esbozaremos esta explicación en la siguiente sección.

Finalmente podemos formular una Conjetura Principal también para formas modulares. Un resultado famoso de Deligne asocia a una forma modular nueva como antes un sistema compatible de representaciones de Galois cuya función  $L$  es la función  $L$  de  $f$ . Más precisamente, tenemos lo siguiente.

**Teorema 7.19 (Deligne):** Sea  $f$  una forma modular nueva como antes y  $K_f$  el campo generado por los coeficientes de Fourier. Entonces para cada primo  $\mathfrak{q}$  de  $K_f$  existe una representación de Galois

$$\rho_{f,\mathfrak{q}}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(K_{f,\mathfrak{q}})$$

que es no ramificada fuera de  $N$ ,  $\infty$  y el primo  $q$  de  $\mathbb{Q}$  abajo de  $\mathfrak{q}$  y tal que para primo  $\ell \neq q$  tenemos

$$\det(1 - \rho_{f,\mathfrak{q}}(\mathrm{Frob}_\ell) T, V_{\mathfrak{q}}^{I_\ell}) = 1 - a_\ell T + \chi(\ell) \ell^{k-1} T^2$$

(donde  $V_{\mathfrak{q}} = K_{f,\mathfrak{q}}^2$  con la acción de  $G_{\mathbb{Q}}$  definida por  $\rho_{f,\mathfrak{p}}$ )

En el caso en que  $f$  corresponde a una curva elíptica  $E$  la representación del teorema anterior es la misma que la representación  $V_{\mathfrak{q}} E$  construida con los módulos de Tate.

Sea  $\mathfrak{p} | p$  el primo de  $K_f$  arriba de  $p$  fijado por nuestros encajes. Después de escoger un retículo estable  $T_{\mathfrak{p}}$  en  $V_{\mathfrak{p}}$  tenemos el grupo de Selmer  $\mathrm{Sel}(V_{\mathfrak{p}}/T_{\mathfrak{p}})$  y el módulo  $X(V_{\mathfrak{p}}/T_{\mathfrak{p}})$  de la definición 7.6, que denotamos como  $X(f)$ . El teorema 7.12 de Kato de hecho todavía es válido en esta situación más general y dice que el  $\Lambda(G)$ -módulo  $X(f)$  es noetheriano y de torsión. La Conjetura Principal para formas modulares entonces es la afirmación siguiente (note que la conjetura 7.14 para curvas elípticas es un caso especial).

**Conjetura 7.20 (Conjetura Principal para formas modulares):** Sea  $f$  como antes. Entonces tenemos la igualdad de ideales en  $\Lambda(G)$

$$\mathrm{car}_{\Lambda(G)} X(f) = (\mu_f).$$

Los resultados de Kato, Skinner y Urban que citamos después de la conjetura 7.14 de hecho son más generales: no sólo funcionan para curvas elípticas (es decir con  $k = 2$ ) sino para cualquier forma modular  $f$  como arriba (con las mismas pequeñas condiciones técnicas que mencionamos). Es decir, también esta conjetura es demostrada en muchos casos.

## Ejercicios

**Ejercicio 7.10:** Sea  $f$  una forma modular ordinaria. Demuestre que el polinomio de Hecke  $p$ -ésimo de  $f$

$$X^2 - a_p X + \chi(p)p^{k-1},$$

tiene una única raíz  $\alpha \in \overline{\mathbb{Q}}$  tal que  $|\alpha|_p = 1$ .

**Ejercicio 7.11:** Demuestre la unicidad en el teorema 7.18. Es decir, aunque la fórmula de interpolación sólo es verdad para una cantidad finita de  $n \in \mathbb{N}_{\geq 1}$  (al contrario del teorema 5.24) aún así el elemento  $\mu_f \in \Lambda(G)$  es determinado únicamente por la fórmula. Esta demostración es análoga a la de la proposición 5.29.

**Ejercicio 7.12:** ¿Que significa la existencia de  $\mu_f$  del teorema 7.18 para los valores especiales de la función  $L$ ? Use las proposiciones 5.30 y 5.31 para deducir resultados análogos a los corolarios 5.32 y 5.33.

**Ejercicio 7.13:** ¿Que significa la Conjetura Principal para los grupos de Selmer? Use los lemas 6.16 y 6.19 para deducir resultados análogos a las proposiciones 6.17 y 6.20 (también para curvas elípticas).

### 7.2.6. Motivos y la Conjetura Equivariante de Números de Tamagawa

Hasta ahora hemos conocido varias «Conjeturas Principales»: dos versiones de la clásica, la de curvas elípticas y más generalmente aquella para formas modulares. ¿Cómo se pueden uniformar estas en una sola afirmación general? En esta última sección tratamos de esbozar algunas ideas de cómo hacerlo.

Aquí entran los motivos que ya mencionamos varias veces. Ellos son de alguna manera «el objeto más general de interés aritmético». En la introducción a este texto escribimos que la pregunta que queremos estudiar es «cómo se comportan los números enteros o algebraicos y ecuaciones entre ellos en diferentes situaciones». Ecuaciones (de polinomios) entre números enteros o algebraicos llevan a un objeto geométrico: una variedad algebraica.<sup>7</sup> Entonces, los motivos son como «pedazos» o «componentes» de tales variedades que son aritméticamente interesantes. Son objetos muy generales que incluyen los objetos que estudiamos hasta ahora y muchos más. Intentamos a explicar esto un poco más, pero el lector está en libertad de simplemente pensar en variedades (o ecuaciones).

De manera ligeramente más precisa, la idea es la siguiente. Escribimos  $\mathcal{V}ar(\mathbb{Q})$  para la categoría de variedades lisas proyectivas sobre  $\mathbb{Q}$  (esto se puede hacer para campos más generales como por ejemplo campos de números, pero para simplificar sólo tratamos el caso de  $\mathbb{Q}$ ). De una variedad se puede considerar su cohomología de diferentes maneras: existen varios funtores de  $\mathcal{V}ar(\mathbb{Q})$  a categorías de espacios vectoriales con estructuras adicionales que tienen propiedades similares aunque son construidos de maneras muy diferentes. Por ejemplo, tomando los puntos en  $\mathbb{C}$  de una variedad algebraica lleva a una variedad analítica compleja, de la cual podemos tomar la cohomología singular de la topología algebraica. También existe la cohomología de de Rham (algebraica). Además existe para cada primo  $q$  la cohomología étale  $q$ -ádica. Todas estas cohomologías tienen propiedades comunes (por ejemplo, sus dimensiones son iguales, existen resultados de dualidad, ...), aunque ni siquiera son espacios vectoriales sobre el mismo campo. El deseo que estimuló la teoría de motivos era el de una «teoría de cohomología universal», que debería existir un funtor  $h: \mathcal{V}ar(\mathbb{Q}) \rightarrow \mathcal{M}ot(\mathbb{Q})$  a una categoría de motivos sobre  $\mathbb{Q}$  tal que todos los funtores de cohomología de factoricen a través de  $h$ , y tal que  $\mathcal{M}ot(\mathbb{Q})$  se encuentre «más cerca» de las categorías de espacios vectoriales – idealmente debería ser una categoría abeliana. Si algo así existe, entonces la categoría  $\mathcal{M}ot(\mathbb{Q})$  claramente tiene que tener más objetos que  $\mathcal{V}ar(\mathbb{Q})$  que no es una categoría abeliana

<sup>7</sup> Para nosotros, una *variedad* es un esquema integral y separado de tipo finito sobre un campo.

– por eso el motivo  $h(X)$  asociado a una variedad  $X$  se puede descomponer aunque  $X$  sea irreducible. Esto es lo que quisimos decir cuando hablamos de «pedazos» de variedades. Vamos a ilustrar este fenómeno en el ejemplo 7.24 (e).

Hasta hoy no se ha podido demostrar que una categoría  $\mathcal{M}ot(\mathbb{Q})$  con las propiedades deseadas existe, pero se han construido algunos candidatos. Para que estas realmente tengan dichas propiedades falta que demostrar algunas conjeturas difíciles (las «conjeturas estándar» de Grothendieck). No vamos a explicar más detalles aquí. Simplemente nos imaginamos que la categoría existe, como de hecho lo hacen muchos textos en la literatura. Lo que pasa es que, aunque no sea posible hacer todo lo que Grothendieck soñaba que se pudiera hacer con los motivos, lo que necesitamos para la Teoría de Iwasawa sí es posible, por eso este enfoque pragmático funciona bien. Lo que necesitamos es «tomar cohomología de un motivo», es decir aplicar los funtores que mencionamos antes como cohomología singular (que se llama también cohomología de Betti), de Rham o étale  $q$ -ádica a un motivo para obtener espacios vectoriales. Estos se llaman las *realizaciones* del motivo. Si  $M$  es un motivo, las denotamos como  $M_B$ ,  $M_{dR}$  y  $M_q$ , respectivamente.

Al lector que quiera aprender más (y de una manera precisa) sobre los motivos le recomendamos el maravilloso texto [Mil13] y para más detalles el libro [Ando4].

Entonces ¿cómo extendemos las ideas de las secciones anteriores a los motivos? Para esto lo más importante son las realizaciones étales de un motivo. Si  $X$  es una variedad lisa proyectiva sobre  $\mathbb{Q}$  y  $q$  es un primo entonces la cohomología étale  $q$ -ádica

$$H_{\text{ét}}^i(X \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_q)$$

es un espacio vectorial sobre  $\mathbb{Q}_q$  con una acción continua de  $G_{\mathbb{Q}}$ , así que es una representación de Galois. Por eso, si  $M$  es un motivo sobre  $\mathbb{Q}$ , su realización étale  $q$ -ádica  $M_q$  también es una representación de Galois. Por supuesto, podemos hacer esto para cada primo  $q$ , y la siguiente conjetura salta a la vista.

**Conjetura 7.21:** *Sea  $M$  un motivo sobre  $\mathbb{Q}$ . Entonces  $(M_q)_q$  es un sistema compatible de representaciones de Galois.*

Suponemos que esta conjetura sea cierta.<sup>8</sup> En esta sección vamos a explicar más y más conjeturas cada una planteada sobre las anteriores. Esto quizás parezca un poco tambaleante, pero todas estas conjeturas sí son conocidas en algunos casos (por ejemplo para curvas elípticas), así que lo peor sería que fueran válidas solamente en estos casos, pero al menos sabemos que no son vacías.

Con el sistema compatible podemos definir (casi) todos los objetos que necesitamos para una Conjeturas Principal, como la función  $L$  y los grupos de Selmer. No se cree que cada sistema compatible viene de un motivo – para esto conjeturalmente se necesita una condición extra al sistema, que en este caso se llama «geométrico»; esto es el contenido de la conjetura de Fontaine y Mazur [FM95]. La Conjetura Principal conjeturalmente es verdad para motivos, y esto explica para cuales sistemas compatibles esperamos una Conjetura Principal: los que vienen de motivos, o si la conjetura de Fontaine y Mazur es verdad, equivalentemente los geométricos.

**Definición 7.22:** La función  $L$  de un motivo  $M$  sobre  $\mathbb{Q}$  es la función  $L$  del sistema compatible  $(M_q)_q$ . La denotamos  $L(M, -)$ .

La siguiente conjetura entonces sería una consecuencia de las conjeturas en el Programa de Langlands.

<sup>8</sup> En general esta conjetura está abierta, pero algunos casos especiales son conocidos (por ejemplo los de curvas elípticas o formas modulares). A más, las famosas Conjeturas de Weil (véase por ejemplo [FK88]) implican que al menos para *casi todas* plazas la compatibilidad de la definición 7.9 (b) es cierta.

**Conjetura 7.23:** La función  $L(M, -)$  tiene una continuación meromorfa a todo de  $\mathbb{C}$ .

Antes de continuar mencionamos algunos ejemplos.

- Ejemplo 7.24:**
- (a) El caso más sencillo es el de la variedad  $X = \text{Spec } \mathbb{Q}$ , que geométricamente es un punto. Su cohomología étale  $q$ -ádica es un espacio vectorial de dimensión 1 con la acción trivial de  $G_{\mathbb{Q}}$ . Por eso, su función  $L$  es la función zeta de Riemann. Este motivo lo denotamos como  $\mathbb{Q}$ .
  - (b) El sistema de representaciones  $(\mathbb{Q}_q(1))_q$  también viene de un motivo, que se denota  $\mathbb{Q}(1)$ . Por supuesto, su función  $L$  es  $L(\mathbb{Q}(1), s) = \zeta(s + 1)$  ( $s \in \mathbb{C}$ ).
  - (c) Mencionamos que para cada carácter de Dirichlet  $\chi$  existe un motivo  $[\chi]$  cuya función  $L$  es la de  $\chi$ . Más generalmente para cada *representación de Artin*  $\rho$ , es decir una representación de  $G_{\mathbb{Q}}$  con imagen finita, existe un motivo  $[\rho]$  cuyo función  $L$  es la función  $L$  de Artin de  $\rho$ .
  - (d) Una curva elíptica  $E$  sobre  $\mathbb{Q}$  es una variedad proyectiva lisa y por eso da lugar a un motivo.<sup>9</sup> Aquí la cohomología étale  $q$ -ádica  $H_{\text{ét}}^1(E \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_q)$  *no* es lo mismo que  $V_q E$  (que usamos para definir la función  $L$ ) sino dual a esto, que gracias al apareamiento de Weil en la curva es isomorfo a  $V_q E \otimes_{\mathbb{Q}_q} \mathbb{Q}_q(1)$ . Por eso la función  $L$  del motivo asociado a  $E$  es  $s \mapsto L(E, s + 1)$  ( $s \in \mathbb{C}$ ).
  - (e) Un ejemplo bastante interesante es el asociado a la variedad  $\text{Spec } K$  sobre  $\mathbb{Q}$  para un campo de números  $K$ . Se puede verificar que la función  $L$  asociada a su motivo es la función zeta de Dedekind  $\zeta_K$  del campo, que es también la función  $L$  de Artin de la representación trivial de  $\text{Gal}(K/K)$ . Suponemos que  $K/\mathbb{Q}$  es Galois. Entonces el formalismo de Artin (es decir el hecho de que la función de Artin es invariante bajo inducción de representaciones, véase [Del73, Prop. 3.8]) dice que  $\zeta_K$  es la función  $L$  de la representación regular de  $\text{Gal}(K/\mathbb{Q})$ . De la teoría de representaciones de grupos finitos sabemos que esta representación se descompone en irreducibles: si  $\rho_1, \dots, \rho_k$  son todas las representaciones irreducibles de  $\text{Gal}(K/\mathbb{Q})$  entonces la representación regular es isomorfa a  $\rho_1^{\dim \rho_1} \oplus \dots \oplus \rho_k^{\dim \rho_k}$ . Su función  $L$  entonces se escribe como un producto de funciones de  $L$  de Artin

$$\zeta_K(s) = \prod_{i=1}^k L(\rho_i^{\dim \rho_i}, s).$$

Esta descomposición de la función  $L$  del motivo  $\text{Spec } K$  es la presencia, en el lado de las funciones  $L$ , del fenómeno de que el motivo  $\text{Spec } K$  se puede descomponer en  $\mathcal{M}ot(\mathbb{Q})$  aunque geométricamente es irreducible (¡es un punto!): cada una de las funciones  $L(\rho_i, s)$  de hecho es la función  $L$  de un submotivo. Esto ilustra la idea de que un motivo es un «pedazo» de una variedad e ilustra la utilidad de motivos: realmente nos dan un panorama más fino que las variedades.

- (f) Finalmente mencionamos que para formas modulares (más precisamente, formas nuevas) también existe un motivo cuya función  $L$  es la asociada a la forma modular. Esto es un teorema de Scholl [Sch90].<sup>10</sup>

Ahora, la pregunta importante es la de algebraicidad de valores especiales, que necesitamos para funciones  $L$   $p$ -ádicas. Esto es el contenido de una conjetura de Deligne [Del79, Conj.

<sup>9</sup> Más precisamente, aquí usamos el motivo  $h^1(E)$ .

<sup>10</sup> Estrictamente, para formas modulares necesitamos más generalmente motivos con coeficientes en un campo de números (en lugar de sólo  $\mathbb{Q}$ ), que en el caso de una forma nueva  $f$  es el campo  $K_f$ . Para estos, las realizaciones son espacios vectoriales sobre  $K_f$  o sus completaciones en lugar de sobre  $\mathbb{Q}$  o  $\mathbb{Q}_q$ .

tensar o tensorizar?

1.8]. Antes de poder explicarla tenemos que hablar sobre *isomorfismos de comparación* para motivos. Las diferentes maneras de tomar cohomología de una variedad proyectiva lisa son relacionados de manera tal que los espacios vectoriales que obtenemos son canónicamente isomorfos después de tensorarlos con un campo más grande. Por ejemplo, la cohomología singular y de Rham son canónicamente isomorfas al aplicar el producto tensorial con  $\mathbb{C}$ . Similarmente, la cohomología singular y la  $p$ -ádica son canónicamente isomorfas al tensorar la primera con  $\mathbb{Q}_p$ . Entre la de de Rham y la  $p$ -ádica también existe un tal isomorfismo después de tensorar con  $B_{dR}$ , que es un campo de la teoría  $p$ -ádica de Hodge que no vamos a explicar aquí (remitimos a [BC09] para esto). Estos isomorfismos se extienden a los motivos, así que tenemos lo siguiente para cada motivo  $M$ : Existen isomorfismos canónicos

$$\begin{aligned} \text{cp}_\infty &: M_B \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\cong} M_{dR} \otimes_{\mathbb{Q}} \mathbb{C}, \\ \text{cp}_{ét} &: M_B \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\cong} M_p, \\ \text{cp}_{dR} &: M_p \otimes_{\mathbb{Q}_p} B_{dR} \xrightarrow{\cong} M_{dR} \otimes_{\mathbb{Q}} B_{dR} \end{aligned}$$

(los últimos dos para cada primo  $p$ ) que son compatibles con las varias estructuras extras que tenemos en ambos lados.

Parte de estas estructuras extras son subespacios canónicos  $M_B^+ \subseteq M_B$  y  $M_{dR}^0 \subseteq M_{dR}$ .<sup>11</sup> Con esto podemos definir:

**Definición 7.25:** Un motivo  $M$  se llama *crítico* si la composición

$$M_B^+ \otimes_{\mathbb{Q}} \mathbb{C} \hookrightarrow M_B \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\text{cp}_\infty} M_{dR} \otimes_{\mathbb{Q}} \mathbb{C} \twoheadrightarrow M_{dR}/M_{dR}^0 \otimes_{\mathbb{Q}} \mathbb{C}$$

es un isomorfismo. En este caso, si escogemos bases de los  $\mathbb{Q}$ -espacios vectoriales  $M_B^+$  y  $M_{dR}/M_{dR}^0$  definimos  $\Omega_\infty(M) \in \mathbb{C}^\times$  como el determinante de este morfismo con respecto a estas bases. Por supuesto, esto depende de las bases, es decir  $\Omega_\infty(M)$  solo está bien definido salvo a elementos de  $\mathbb{Q}^\times$ , pero esto será suficiente. El número  $\Omega_\infty(M)$  se llama el *período complejo* de  $M$ .

La conjetura de Deligne entonces es la siguiente. Obviamente su validez no depende de las bases que escogemos.

**Conjetura 7.26 (Deligne):** Si  $M$  es un motivo crítico entonces

$$\frac{L(M, 0)}{\Omega_\infty(M)} \in \mathbb{Q}^\times.$$

El teorema 7.17 para formas modulares es una instancia de esta conjetura que está demostrada.<sup>12</sup> También las proposiciones 5.6 y 5.9 son casos especiales de esta conjetura.

Ahora estamos casi listos para explicar cómo debería ser en general una función  $L$   $p$ -ádica. Antes de esto tenemos que introducir la siguiente notación, que usa el hecho de que la categoría de motivos tiene un producto tensorial y duales (los cuales en realizaciones se convierten en el producto tensorial y el dual usual).

<sup>11</sup> Más precisamente, en  $M_B$  tenemos una acción de  $G_R$  y  $M_B^+$  es el espacio fijo por esta acción, y en  $M_{dR}$  tenemos una filtración descendiente que se llama la filtración de Hodge, y  $M_{dR}^0$  es el paso 0 de esta filtración. Estas estructuras vienen directamente de las estructuras análogas en la cohomología de una variedad.

<sup>12</sup> Como mencionamos en la pie de página 10 en la página 134, para formas modulares necesitamos motivos con coeficientes en un campo de números  $K$  en lugar de  $\mathbb{Q}$ . La conjetura de Deligne que mencionamos es la versión para motivos con coeficientes en  $\mathbb{Q}$ , la versión más general afirma que la expresión está en  $K^\times$ . El teorema 7.17 es la conjetura de Deligne para el motivo  $M(f)(\psi)(n)$  con la notación que introducimos en la definición 7.27.

**Definición 7.27:** Sea  $M$  un motivo.

- (a) Sea  $n \in \mathbb{Z}$ . Si  $n \geq 1$  entonces definimos  $\mathbb{Q}(n) := \mathbb{Q}(1)^{\otimes n}$ . Para  $n = -1$  definimos  $\mathbb{Q}(-1) = \mathbb{Q}(1)^*$  (el dual de  $\mathbb{Q}(1)$ ) y para  $n \leq 1$  definimos  $\mathbb{Q}(n) = \mathbb{Q}(-1)^{\otimes(-n)}$ . (Aquí  $\mathbb{Q}(1)$  es como en el ejemplo 7.24 (b).)
- (b) Definimos  $M(n) := M \otimes \mathbb{Q}(n)$  para  $n \in \mathbb{Z}$ .
- (c) Si  $\psi$  es un carácter de Dirichlet entonces definimos  $M(\psi) := M \otimes [\psi]$ . Más generalmente, si  $\rho$  es una representación de Artin entonces definimos  $M(\rho) := M \otimes [\rho]$ . (Aquí  $[\psi]$  y  $[\rho]$  son como en el ejemplo 7.24 (c).)

Se ve fácilmente que  $L(M(n), s) = L(M, s + n)$  para  $s \in \mathbb{C}$ . La respuesta a la pregunta cuales valores de una función  $L$  compleja conjeturalmente pueden ser interpolados  $p$ -ádicamente entonces es: los valores  $L(M(n)(\chi), 0) = L(M(\chi), n)$  para  $n \in \mathbb{Z}$  y caracteres de Dirichlet  $\chi$  tal que el motivo  $M(n)(\chi)$  es crítico. Por ejemplo, se puede verificar que para una forma modular nueva  $f$  de peso  $k$ , un entero  $n \in \mathbb{Z}$  y un carácter de Dirichlet  $\chi$  el motivo  $M(f)(\chi)(n)$  es crítico si y solo si  $1 \leq n \leq k - 1$ , que es compatible con el teorema 7.17.

En las conjeturas sobre funciones  $L$   $p$ -ádicas los motivos deben cumplir una condición adicional que muchas veces se llama la *condición de Panchishkin*. No la explicamos aquí, se encuentra por ejemplo en [Greg94, §3] o [FKo6, §4.2.3]. Para una forma modular, esta condición es equivalente a la condición que la forma sea ordinaria.

Similarmente como definimos el período complejo en la definición 7.25 se puede definir también un período  $p$ -ádico, que esencialmente es el determinante de

$$M_{\mathbb{B}}^+ \otimes_{\mathbb{Q}} \mathbb{B}_{\text{dR}} \hookrightarrow M_{\mathbb{B}} \otimes_{\mathbb{Q}} \mathbb{B}_{\text{dR}} \xrightarrow{\text{cpét}} M_p \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{dR}} \xrightarrow{\text{cpdR}} M_{\text{dR}} \otimes_{\mathbb{Q}} \mathbb{B}_{\text{dR}} \rightarrow M_{\text{dR}}/M_{\text{dR}}^0 \otimes_{\mathbb{Q}} \mathbb{B}_{\text{dR}}$$

salvo a una pequeña modificación que omitimos aquí. Siempre suponemos que calculamos este determinante con respecto a las mismas bases que usamos para calcular  $\Omega_{\infty}(M)$ . Esto lleva a un número  $\Omega_p(M) \in (\hat{\mathbb{Q}}_p^{\text{nr}})^{\times}$ , es decir en la completación de la máxima extensión no ramificada de  $\mathbb{Q}_p$ .<sup>13</sup> Con esta definición podemos esbozar la conjetura. En ella escribimos  $\tilde{\Lambda}(G) := \tilde{\mathcal{O}}[[G]]$  para el álgebra de Iwasawa con coeficientes en  $\tilde{\mathcal{O}}$ , que denota el anillo de enteros en  $\hat{\mathbb{Q}}_p^{\text{nr}}$ , y escribimos  $\tilde{\Phi}(G)$  para el anillo de cocientes de  $\tilde{\Lambda}(G)$  (eso es la localización donde invertimos todos los elementos que no son divisores de cero). En general las funciones  $L$   $p$ -ádicas están en  $\tilde{\Phi}(G)$  y no en  $\tilde{\Lambda}(G)$ , como vimos en el ejemplo de la función zeta  $p$ -ádica de Riemann. La función  $L$   $p$ -ádica conjeturalmente tiene valores en  $\tilde{\mathcal{O}}$ .

**Conjetura 7.28:** *Sea  $M$  un motivo que cumple la condición de Panchishkin. Entonces existe un único elemento  $\mu_M \in \tilde{\Phi}(G)$  tal que para cada carácter de Dirichlet  $\psi$  cuyo conductor es una potencia de  $p$  y cada  $n \in \mathbb{Z}$  tal que  $M(\chi)(n)$  es crítico tenemos*

$$\int_G \psi^{-1} \kappa^n d\mu_M = (\text{factores de corrección}) \cdot \frac{\Omega_p(M(\chi)(n))}{\Omega_{\infty}(M(\chi)(n))} L(M(\chi)(n), 0).$$

En esta forma la conjetura es un caso especial de una conjetura de Fukaya y Kato de [FKo6], pero ya antes conjeturas similares han sido formuladas por Coates y Perrin-Riou [CP89; Coa89].

**Nota 7.29:** El anillo  $\tilde{\Lambda}(G)$  que aparece aquí es mucho más grande que  $\Lambda(G)$ , donde las funciones  $L$   $p$ -ádicas anteriores vivían. En las versiones de esta conjetura de Coates y Perrin-Riou la función  $L$   $p$ -ádica vive en  $\Lambda(G)$  o su anillo de cocientes (que denotamos  $\Phi(G)$ ), pero

<sup>13</sup> La modificación que mencionamos garantiza que de hecho  $\Omega_p(M) \neq 0$ ; como lo definimos arriba puede pasar que la composición de mapeos no es un isomorfismo. Además la modificación garantiza también que el período de hecho está en el subcampo  $\hat{\mathbb{Q}}_p^{\text{nr}} \subseteq \mathbb{B}_{\text{dR}}$ .

en su fórmula de interpolación no aparece el período  $p$ -ádico. La versión de aquí de Fukaya y Kato incluye el período  $p$ -ádico y por eso es un poco más elegante y conceptual (como explicamos al final de esta sección), pero para incluirla hay que aumentar el anillo.

Sin embargo, mencionamos que el elemento conjetural  $\mu_M$  se puede escribir como  $\mu_M = \lambda \mu'_M$  con  $\lambda \in \tilde{\Lambda}(G)$  y  $\mu'_M \in \Phi(G)$  de una manera esencialmente única, es decir si  $\mu_M = \lambda' \mu''_M$  es otra tal descomposición entonces  $\mu'_M$  y  $\mu''_M$  sólo difieren por una unidad en  $\Lambda(G)^\times$ .

Es decir, la conjetura tiene la forma

$$\frac{\text{valor de la función } L \text{ } p\text{-ádica}}{\text{período } p\text{-ádico}} = (\text{factores de corrección}) \cdot \frac{\text{valor de la función } L \text{ compleja}}{\text{período complejo}}.$$

Los factores de corrección son expresiones sencillas como factores de Euler y factoriales. En particular son algebraicos, así que lo de arriba es una igualdad en  $\overline{\mathbb{Q}}$  y el período  $p$ -ádico describe la parte transcendente del valor de la función  $L$   $p$ -ádica, justamente como el período complejo describe la parte transcendente del valor de la función  $L$  compleja.

Notemos que, aunque los períodos no son bien definidos (sólo salvo a un factor en  $\mathbb{Q}^\times$ ), si cambiamos la base con respeto a cual los definimos entonces ambos cambian por el mismo factor. Es decir, el valor de la integral en la conjetura arriba no depende de las bases que escogemos.

En general, no es nada fácil verificar que una función  $L$   $p$ -ádica construida sea compatible con esta conjetura. Esto se debe a que por definición los períodos son difíciles de calcular, mientras que para construir una función  $L$   $p$ -ádica no existe una manera estándar y las fórmulas de interpolación que uno obtiene muchas veces contienen expresiones que son más bien artefactos del método de construcción y a priori no tienen un significado conceptual. Por lo tanto, no queda claro si estas expresiones de hecho están relacionadas con los períodos. Sin embargo, para todas las funciones  $L$   $p$ -ádicas que hemos visto hasta ahora, esto sí es cierto. Para los de caracteres de Dirichlet esto es fácil de ver porque los motivos y los isomorfismos de comparación tienen descripciones muy explícitas. Para las formas modulares esto es mucho más difícil, pero también es conocido.

Ahora podemos enunciar la Conjetura Principal para motivos. Una conjetura de este estilo fue formulada por Greenberg en [Gre89] y [Gre94, §3, 3.1]. Para esto sea  $M$  un motivo cumpliendo la condición de Panchishkin. Además escojamos un retículo estable  $T_p$  en la realización  $M_p$ , con el cual podemos definir el módulo  $X(M) := X(M_p/T_p)$ , que según un resultado de [Gre94] es noetheriano<sup>14</sup> y conjeturalmente es de torsión. Escribimos  $\mu_M = \lambda \mu'_M$  con  $\lambda \in \tilde{\Lambda}(G)$  y  $\mu'_M \in \Phi(G)$  como en la nota 7.29. Según esta nota la veracidad de la siguiente afirmación no depende de esta descomposición.

**Conjetura 7.30 (Conjetura Principal para motivos):** *Existe  $h \in \Lambda(G)$  tal que tenemos la igualdad de ideales en  $\Lambda(G)$*

$$\text{car}_{\Lambda(G)} X(M) = (h \mu'_M)$$

y  $(h)$  también es el ideal característico de un cierto módulo (que omitimos aquí).

En particular, si  $\mu_M \in \tilde{\Lambda}(G)$  entonces tenemos la igualdad de ideales en  $\Lambda(G)$

$$\text{car}_{\Lambda(G)} X(M) = (\mu'_M).$$

El lector debería comparar esta Conjetura Principal (en el caso  $\mu'_M \notin \tilde{\Lambda}(G)$ ) con la interpretación de la Conjetura Principal clásica que damos en la nota 6.3. En cuyo caso explicamos el módulo cuyo ideal característico es generado por  $h$ .

<sup>14</sup> En los textos de Greenberg la definición del grupo de Selmer es ligeramente diferente, el subgrupo  $H_f^1(K_v, -)$  para las plazas  $v \mid p$  difiere de nuestra definición; sin embargo, se puede demostrar que bajo la condición de Panchishkin la versión de Greenberg de hecho es la misma que la de Bloch y Kato.

Esta conjetura claramente generaliza todas las que hemos visto antes, pero todavía no es el fin de la historia. Quedan dos direcciones principales en cuales podemos generalizar.

Primero, podemos cambiar el campo de base  $\mathbb{Q}$  a un campo de números  $F$ . Esto significaría estudiar (sistemas de) representaciones de  $G_F$  y motivos sobre  $F$  (como por ejemplo curvas elípticas). Esto es posible y las generalizaciones en este caso han sido formuladas, pero esto no cambia mucho conceptualmente, sólo hace que la notación es menos clara. Por eso ninguneamos esta dirección.

Segundo, es posible cambiar la torre de campo de números  $(K_r)_r$  a otra torre, por ejemplo una más grande. Esto cambia el grupo  $G$  y también el álgebra de Iwasawa  $\Lambda(G)$ . Incluso se puede estudiar el caso en que  $G$  no es conmutativo. La Teoría de Iwasawa no conmutativa fue fundada por Harris, Coates, Howson, Ochi y Venjakob y trae algunos nuevos fenómenos. Por ejemplo, en el lado algebraico la teoría de estructura ya no funciona porque el anillo  $\Lambda(G)$  entonces se comporta peor en general. En particular, ya no tenemos ideales característicos, que eran esenciales para formular la Conjetura Principal. Se puede arreglar esto usando la teoría  $K$  algebraica para definir *elementos característicos* – estos son elementos de una modificación de  $K_1$  del álgebra de Iwasawa que son enviados al módulo por el morfismo de borde a  $K_0$ . Para formular una Conjetura Principal, las funciones  $L$   $p$ -ádicas también son elementos de este  $K_1$  y se sospecha que son elementos característicos de grupos de Selmer. En su fórmula de interpolación entonces aparecen no sólo los chaffles del motivo por caracteres de Dirichlet sino de representaciones de Artin del grupo  $G$  (que para  $G \simeq \mathbb{Z}_p^\times$  como antes, son justamente los caracteres de Dirichlet que usamos). Para una curva elíptica la teoría es descrita en [CFKSV05]. También queremos mencionar [Ven05] que es una introducción muy bonita a estas ideas. Para motivos más generales, la Teoría de Iwasawa no conmutativa, es un caso especial de las ideas que indicamos enseguida.

Las últimas generalizaciones de las que hablaremos son la denominada *Conjetura Equivariante de Números de Tamagawa* y la *conjetura equivariante de los  $\varepsilon$ -isomorfismos*, formuladas por Burns, Flach, Fukaya y Kato después de trabajos de Deligne, Beilinson, Bloch, Kato, Perrin-Riou, Fontaine, Huber, Kings y otros. En la introducción mencionamos dos resultados sobre conexiones entre valores especiales de funciones  $L$  y la aritmética que todavía relucen en el cuadro: la fórmula analítica de números de clases y la Conjetura de Birch y Swinnerton-Dyer. Estas dos afirmaciones de hecho no son « $p$ -ádicas», por eso su relación con las Conjeturas Principales no es clara a primera vista. La Conjetura Equivariante de Números de Tamagawa y la conjetura equivariante de los  $\varepsilon$ -isomorfismos son diseñadas como una generalización común de estas conexiones. Describen de una manera satisfactoria el significado de valores de funciones  $L$  de motivos mediante invariantes cohomológicas del motivo.

Explicamos las ideas de estas conjeturas; aquí seremos muy vagos. La Conjetura de Números de Tamagawa (todavía no equivariante), también conocida como la conjetura de Bloch y Kato, es una generalización común de la fórmula analítica de números de clases y la Conjetura de Birch y Swinnerton-Dyer. En estas dos afirmaciones tenemos una función  $L$  de un motivo  $M$ , meromorfa en  $\mathbb{C}$ , que podemos escribir como serie de potencia

$$L(M, s) = L^*(M)s^{r(M)} + \text{expresiones de orden más alto}$$

donde  $L^*(M) \in \mathbb{C}^\times$  es el coeficiente principal y  $r(M) \in \mathbb{Z}$  es el orden de cero de la función en  $s = 0$  (para la fórmula analítica de números de clases tomamos  $M = K(1)$  para un campo de números  $K$  y para la Conjetura de Birch y Swinnerton-Dyer tomamos un motivo construido de la curva elíptica). Las afirmaciones entonces describen los números  $r(M)$  y  $L^*(M)$  usando invariantes del motivo (el número de clases, la orden del grupo de Tate y Shafarevich, el rango del grupo de Mordell y Weil, ...). La Conjetura de Números de Tamagawa es una generalización de esto para cada motivo, expresando  $r(M)$  y  $L^*(M)$  con invariantes del motivo. Entonces la Conjetura de Números de Tamagawa Equivariante filosóficamente predice que los valores de  $r(M)$  y  $L^*(M)$  «varían continuamente con el motivo

$M$ ». Finalmente, conjeturalmente la función  $L$  de un motivo  $M$  tiene una ecuación funcional que relaciona  $L(M, s)$  con  $L(M^*(1), -s)$  para  $s \in \mathbb{C}$ . Esta ecuación funcional da una relación entre  $L^*(M)$  y  $L^*(M^*(1))$  y también  $r(M)$  y  $r(M^*(1))$ , por eso debería haber también una relación entre las Conjeturas de Números de Tamagawa para  $M$  y  $M^*(1)$ . La conjetura de los  $\varepsilon$ -isomorfismos (no equivariante) describe tal relación de una manera muy sutil y la conjetura equivariante de los  $\varepsilon$ -isomorfismos afirma que estas relaciones también varían continuamente con el motivo. Una introducción a estas ideas se encuentra en [Ven07] o [Flao4].

¿Qué tiene todo esto que ver con la Conjetura Principal? Esto es explicado por el siguiente teorema. Aquí ya no aparecen grupos de Selmer sino complejos de Selmer, que son generalizaciones de grupos de Selmer apropiados para esta situación general. El «otro módulo» que apareció en la conjetura 7.30 ahora está incluido en el complejo de Selmer.

**Teorema 7.31 (Fukaya/Kato):** *Supongamos que la Conjetura Equivariante de los Números de Tamagawa y la conjetura equivariante de los  $\varepsilon$ -isomorfismos sean ciertas.*

*Sea  $M$  un motivo que cumple la condición de Panchishkin. Fijemos una torre  $K_\infty/\mathbb{Q}$  tal que  $G = \text{Gal}(K_\infty/\mathbb{Q})$  tenga un subgrupo normal de índice finito que es pro- $p$  y topológicamente finitamente generado.*

*Entonces:*

- (a) *Existe una función  $L$   $p$ -ádica, que es un elemento de un cierto grupo  $K_1$ , que interpola los valores  $L(M(\rho)(n), 0)$ , donde  $\rho$  es una representación de Artin de  $G$  y  $n \in \mathbb{Z}$  tal que  $M(\rho)(n)$  es crítico.*
- (b) *Esta función es un elemento característico del complejo de Selmer de  $M$  (esto es la Conjetura Principal).*

Para más detalles sobre esto remitimos al texto original [FK06] de Fukaya y Kato y también al texto introductorio [Ven07] de Venjakob que explica algunas de las ideas con más detalles.

El elemento conjetural  $\mu_M$  de la conjetura 7.28 es el de la afirmación (a) del teorema 7.31 en el caso especial  $K_\infty = \mathbb{Q}(\mu_{p^\infty})$ . La conjetura 7.30 entonces es equivalente a la afirmación (b) en este caso especial. Es decir, ¡la Conjetura Equivariante de los Números de Tamagawa y la conjetura equivariante de los  $\varepsilon$ -isomorfismos implican toda la Teoría de Iwasawa! En particular, implican la existencia de funciones  $L$   $p$ -ádicas para muchos motivos, y también proporcionan la fórmula de interpolación. Así le dan una explicación más profunda: es una consecuencia de estas dos conjeturas, y en particular es compatible con la fórmula analítica de números de clases y la Conjetura de Birch y Swinnerton-Dyer. Además, la Conjetura Principal, incluso no conmutativa, también es una consecuencia; por ende, son todas las Conjeturas Principales que aparecieron en este texto. Así la Conjetura Equivariante de los Números de Tamagawa y la conjetura equivariante de los  $\varepsilon$ -isomorfismos unifican toda la Teoría de Iwasawa e implican esencialmente todo lo que uno podría querer saber sobre funciones  $L$  y sus conexiones a la aritmética.<sup>15</sup> Por supuesto queda un largo camino por demostrar, no obstante, la amplia impresión dada por estas ideas es de una elegancia peculiar, que ojalá persuada al lector de continuar estudiando la Teoría de Iwasawa.

<sup>15</sup> Mencionamos que la equivalencia de las dos formulaciones de la Conjetura Principal que damos en la sección 6.1 es una encarnación de la conjetura equivariante de los  $\varepsilon$ -isomorfismos – note que la ecuación funcional en este caso conecta  $\zeta(s)$  y  $\zeta(1-s)$ !



## Bibliografía

- [Ando4] Yves André. *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*. Vol. 17. Panoramas et Synthèses [Panoramas and Syntheses]. Société Mathématique de France, Paris, 2004, págs. xii+261. ISBN: 2-85629-164-3 (vid. pág. 133).
- [BC09] Olivier Brinon y Brian Conrad. *CMI Summer School notes on  $p$ -adic Hodge theory. Preliminary version*. 2009. URL: <http://math.stanford.edu/~conrad/papers/notes.pdf> (vid. págs. 119, 135).
- [BK90] Spencer Bloch y Kazuya Kato. *L-functions and Tamagawa numbers of motives*. En: *The Grothendieck Festschrift, Vol. I*. Vol. 86. Progr. Math. Birkhäuser Boston, Boston, MA, 1990, págs. 333-400 (vid. págs. 120 s.).
- [CFKSV05] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha y Otmar Venjakob. *The  $GL_2$  main conjecture for elliptic curves without complex multiplication*. En: *Publ. Math. Inst. Hautes Études Sci.* 101 (2005), págs. 163-208. ISSN: 0073-8301. DOI: 10.1007/s10240-004-0029-3. URL: <https://doi.org/10.1007/s10240-004-0029-3> (vid. pág. 138).
- [Coa89] John Coates. *On  $p$ -adic  $L$ -functions attached to motives over  $\mathbf{Q}$ . II*. En: *Bol. Soc. Brasil. Mat. (N.S.)* 20.1 (1989), págs. 101-112. ISSN: 0100-3569. DOI: 10.1007/BF02585471. URL: <https://doi.org/10.1007/BF02585471> (vid. pág. 136).
- [Col79] Robert F. Coleman. *Division values in local fields*. En: *Invent. Math.* 53.2 (1979), págs. 91-116. ISSN: 0020-9910. DOI: 10.1007/BF01390028. URL: <https://doi.org/10.1007/BF01390028> (vid. pág. 98).
- [CP89] John Coates y Bernadette Perrin-Riou. *On  $p$ -adic  $L$ -functions attached to motives over  $\mathbf{Q}$* . En: *Algebraic number theory*. Vol. 17. Adv. Stud. Pure Math. Academic Press, Boston, MA, 1989, págs. 23-54 (vid. pág. 136).
- [CR06] Charles W. Curtis e Irving Reiner. *Representation theory of finite groups and associative algebras*. Reprint of the 1962 original. AMS Chelsea Publishing, Providence, RI, 2006, págs. xiv+689. ISBN: 0-8218-4066-5. DOI: 10.1090/chel/356. URL: <https://doi.org/10.1090/chel/356> (vid. pág. 124).
- [CS06] J. Coates y R. Sujatha. *Cyclotomic fields and zeta values*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006, págs. x+113. ISBN: 978-3-540-33068-4; 3-540-33068-2 (vid. págs. 5, 98-100, 102, 105 s., 116).
- [Del73] P. Deligne. *Les constantes des équations fonctionnelles des fonctions  $L$* . En: (1973), 501-597. *Lecture Notes in Math.*, Vol. 349 (vid. pág. 134).
- [Del79] P. Deligne. *Valeurs de fonctions  $L$  et périodes d'intégrales*. En: *Automorphic forms, representations and  $L$ -functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*. Proc. Sympos. Pure Math., XXXIII. With an appendix by N. Koblitz and A. Ogus. Amer. Math. Soc., Providence, R.I., 1979, págs. 313-346 (vid. pág. 134).
- [DS05] Fred Diamond y Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, págs. xvi+436. ISBN: 0-387-23229-X (vid. pág. 129).

- [Eis95] David Eisenbud. *Commutative algebra*. Vol. 150. Graduate Texts in Mathematics. With a view toward algebraic geometry. Springer-Verlag, New York, 1995, págs. xvi+785. ISBN: 0-387-94268-8; 0-387-94269-6. DOI: 10.1007/978-1-4612-5350-1. URL: <https://doi.org/10.1007/978-1-4612-5350-1> (vid. pág. 46).
- [FK06] Takako Fukaya y Kazuya Kato. *A formulation of conjectures on  $p$ -adic zeta functions in noncommutative Iwasawa theory*. En: *Proceedings of the St. Petersburg Mathematical Society. Vol. XII*. Vol. 219. Amer. Math. Soc. Transl. Ser. 2. Amer. Math. Soc., Providence, RI, 2006, págs. 1-85. DOI: 10.1090/trans2/219/01. URL: <https://doi.org/10.1090/trans2/219/01> (vid. págs. 106, 136, 139).
- [FK88] Eberhard Freitag y Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*. Vol. 13. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné. Springer-Verlag, Berlin, 1988, págs. xviii+317. ISBN: 3-540-12175-7. DOI: 10.1007/978-3-662-02541-3. URL: <https://doi.org/10.1007/978-3-662-02541-3> (vid. págs. 103, 133).
- [Fla04] Matthias Flach. *The equivariant Tamagawa number conjecture: a survey*. En: *Stark's conjectures: recent work and new directions*. Vol. 358. Contemp. Math. With an appendix by C. Greither. Amer. Math. Soc., Providence, RI, 2004, págs. 79-125. DOI: 10.1090/conm/358/06537. URL: <https://doi.org/10.1090/conm/358/06537> (vid. pág. 139).
- [FM95] Jean-Marc Fontaine y Barry Mazur. *Geometric Galois representations*. En: *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*. Ser. Number Theory, I. Int. Press, Cambridge, MA, 1995, págs. 41-78 (vid. pág. 133).
- [Gre01a] Ralph Greenberg. *Introduction to Iwasawa theory for elliptic curves*. En: *Arithmetic algebraic geometry (Park City, UT, 1999)*. Vol. 9. IAS/Park City Math. Ser. Amer. Math. Soc., Providence, RI, 2001, págs. 407-464 (vid. pág. 126).
- [Gre01b] Ralph Greenberg. *Iwasawa theory—past and present*. En: *Class field theory—its centenary and prospect (Tokyo, 1998)*. Vol. 30. Adv. Stud. Pure Math. Math. Soc. Japan, Tokyo, 2001, págs. 335-385 (vid. págs. 5 s.).
- [Gre89] Ralph Greenberg. *Iwasawa theory for  $p$ -adic representations*. En: *Algebraic number theory*. Vol. 17. Adv. Stud. Pure Math. Academic Press, Boston, MA, 1989, págs. 97-137 (vid. pág. 137).
- [Gre94] Ralph Greenberg. *Iwasawa theory and  $p$ -adic deformations of motives*. En: *Motives (Seattle, WA, 1991)*. Vol. 55. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI, 1994, págs. 193-223 (vid. págs. 136 s.).
- [Hid12] Haruzo Hida. *Geometric modular forms and elliptic curves*. Second. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012, págs. xiv+454. ISBN: 978-981-4368-64-3; 981-4368-64-4 (vid. pág. 127).
- [Hid93] Haruzo Hida. *Elementary theory of  $L$ -functions and Eisenstein series*. Vol. 26. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1993, págs. xii+386. ISBN: 0-521-43411-4; 0-521-43569-2. DOI: 10.1017/CBO9780511623691. URL: <https://doi.org/10.1017/CBO9780511623691> (vid. págs. 34, 97).

- [Hub94] R. Huber. *A generalization of formal schemes and rigid analytic varieties*. En: Math. Z. 217.4 (1994), págs. 513-551. ISSN: 0025-5874. DOI: 10.1007/BF02571959. URL: <https://doi.org/10.1007/BF02571959> (vid. pág. 97).
- [Iwa59a] Kenkichi Iwasawa. *On  $\Gamma$ -extensions of algebraic number fields*. En: Bull. Amer. Math. Soc. 65 (1959), págs. 183-226. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1959-10317-7. URL: <https://doi.org/10.1090/S0002-9904-1959-10317-7> (vid. pág. 6).
- [Iwa59b] Kenkichi Iwasawa. *On the theory of cyclotomic fields*. En: Ann. of Math. (2) 70 (1959), págs. 530-561. ISSN: 0003-486X. DOI: 10.2307/1970328. URL: <https://doi.org/10.2307/1970328> (vid. pág. 112).
- [Iwa64] Kenkichi Iwasawa. *On some modules in the theory of cyclotomic fields*. En: J. Math. Soc. Japan 16 (1964), págs. 42-82. ISSN: 0025-5645. DOI: 10.2969/jmsj/01610042. URL: <https://doi.org/10.2969/jmsj/01610042> (vid. pág. 6).
- [Iwa69a] Kenkichi Iwasawa. *Analogies between number fields and function fields*. En: *Some Recent Advances in the Basic Sciences, Vol. 2 (Proc. Annual Sci. Conf., Belfer Grad. School Sci., Yeshiva Univ., New York, 1965-1966)*. Belfer Graduate School of Science, Yeshiva Univ., New York, 1969, págs. 203-208 (vid. págs. 6, 103).
- [Iwa69b] Kenkichi Iwasawa. *On  $p$ -adic  $L$ -functions*. En: Ann. of Math. (2) 89 (1969), págs. 198-205. ISSN: 0003-486X. DOI: 10.2307/1970817. URL: <https://doi.org/10.2307/1970817> (vid. pág. 6).
- [Iwa72] Kenkichi Iwasawa. *Lectures on  $p$ -adic  $L$ -functions*. Annals of Mathematics Studies, No. 74. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972, págs. vii+106 (vid. págs. 83, 87).
- [Iwa73] Kenkichi Iwasawa. *On  $\mathbf{Z}_l$ -extensions of algebraic number fields*. En: Ann. of Math. (2) 98 (1973), págs. 246-326. ISSN: 0003-486X. DOI: 10.2307/1970784. URL: <https://doi.org/10.2307/1970784> (vid. págs. 6, 52).
- [Kato04] Kazuya Kato.  *$p$ -adic Hodge theory and values of zeta functions of modular forms*. En: Astérisque 295 (2004). Cohomologies  $p$ -adiques et applications arithmétiques. III, págs. ix, 117-290. ISSN: 0303-1179 (vid. págs. 127 s.).
- [Kato07] Kazuya Kato. *Iwasawa theory and generalizations*. En: *International Congress of Mathematicians. Vol. I*. Eur. Math. Soc., Zürich, 2007, págs. 335-357. DOI: 10.4171/022-1/14. URL: <https://doi.org/10.4171/022-1/14> (vid. págs. 5, 115 s., 128).
- [KL64] Tomio Kubota y Heinrich-Wolfgang Leopoldt. *Eine  $p$ -adische Theorie der Zetawerte. I. Einführung der  $p$ -adischen Dirichletschen  $L$ -Funktionen*. En: J. Reine Angew. Math. 214/215 (1964), págs. 328-339. ISSN: 0075-4102 (vid. pág. 73).
- [Koc97] H. Koch. *Algebraic number theory*. Russian. Reprint of the 1992 translation. Springer-Verlag, Berlin, 1997, págs. iv+269. ISBN: 3-540-63003-1. DOI: 10.1007/978-3-642-58095-6. URL: <https://doi.org/10.1007/978-3-642-58095-6> (vid. pág. 19).
- [Lan02] Serge Lang. *Algebra*. third. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002, págs. xvi+914. ISBN: 0-387-95385-X. DOI: 10.1007/978-1-4613-0041-0. URL: <https://doi.org/10.1007/978-1-4613-0041-0> (vid. págs. 45, 60).

- [Lang0] Serge Lang. *Cyclotomic fields I and II*. second. Vol. 121. Graduate Texts in Mathematics. With an appendix by Karl Rubin. Springer-Verlag, New York, 1990, págs. xviii+433. ISBN: 0-387-96671-4. DOI: 10.1007/978-1-4612-0987-4. URL: <https://doi.org/10.1007/978-1-4612-0987-4> (vid. págs. 5, 60, 79, 97, 105, 107, 113, 115 s.).
- [Loe17] David Loeffler. *Euler systems. Iwasawa 2017 notes*. 2017. URL: [https://warwick.ac.uk/fac/sci/math/people/staff/david\\_loeffler/iwasawanotes.pdf](https://warwick.ac.uk/fac/sci/math/people/staff/david_loeffler/iwasawanotes.pdf) (vid. pág. 116).
- [Mil13] James S. Milne. *Motives—Grothendieck’s dream*. En: *Open problems and surveys of contemporary mathematics*. Vol. 6. Surv. Mod. Math. Int. Press, Somerville, MA, 2013, págs. 325-342 (vid. pág. 133).
- [MS74] B. Mazur y P. Swinnerton-Dyer. *Arithmetic of Weil curves*. En: *Invent. Math.* 25 (1974), págs. 1-61. ISSN: 0020-9910. DOI: 10.1007/BF01389997. URL: <https://doi.org/10.1007/BF01389997> (vid. pág. 131).
- [MTT86] B. Mazur, J. Tate y J. Teitelbaum. *On  $p$ -adic analogues of the conjectures of Birch and Swinnerton-Dyer*. En: *Invent. Math.* 84.1 (1986), págs. 1-48. ISSN: 0020-9910. DOI: 10.1007/BF01388731. URL: <https://doi.org/10.1007/BF01388731> (vid. pág. 131).
- [MW84] B. Mazur y A. Wiles. *Class fields of abelian extensions of  $\mathbf{Q}$* . En: *Invent. Math.* 76.2 (1984), págs. 179-330. ISSN: 0020-9910. DOI: 10.1007/BF01388599. URL: <https://doi.org/10.1007/BF01388599> (vid. pág. 116).
- [Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, págs. xviii+571. ISBN: 3-540-65399-6. DOI: 10.1007/978-3-662-03983-0. URL: <https://doi.org/10.1007/978-3-662-03983-0> (vid. págs. 14-17, 19-22, 105, 124).
- [NSWo8] Jürgen Neukirch, Alexander Schmidt y Kay Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2008, págs. xvi+825. ISBN: 978-3-540-37888-4. DOI: 10.1007/978-3-540-37889-1. URL: <https://doi.org/10.1007/978-3-540-37889-1> (vid. págs. 5, 25, 45, 48, 55, 64, 103, 106, 115, 118, 126).
- [Pan97] A. A. Panchishkin. *Non-Archimedean Mellin transform and  $p$ -adic  $L$ -functions*. En: *Vietnam J. Math.* 25.3 (1997), págs. 179-202. ISSN: 0866-7179 (vid. pág. 81).
- [Ribo1] Paulo Ribenboim. *Classical theory of algebraic numbers*. Universitext. Springer-Verlag, New York, 2001, págs. xxiv+681. ISBN: 0-387-95070-2. DOI: 10.1007/978-0-387-21690-4. URL: <https://doi.org/10.1007/978-0-387-21690-4> (vid. pág. 113).
- [Rib76] Kenneth A. Ribet. *A modular construction of unramified  $p$ -extensions of  $\mathbf{Q}(\mu_p)$* . En: *Invent. Math.* 34.3 (1976), págs. 151-162. ISSN: 0020-9910. DOI: 10.1007/BF01403065. URL: <https://doi.org/10.1007/BF01403065> (vid. pág. 113).

- [Rub00] Karl Rubin. *Euler systems*. Vol. 147. Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000, págs. xii+227. ISBN: 0-691-05075-9; 0-691-05076-7. DOI: 10.1515/9781400865208. URL: <https://doi.org/10.1515/9781400865208> (vid. págs. 116, 120, 127).
- [Rub91] Karl Rubin. *The “main conjectures” of Iwasawa theory for imaginary quadratic fields*. En: *Invent. Math.* 103.1 (1991), págs. 25-68. ISSN: 0020-9910. DOI: 10.1007/BF01239508. URL: <https://doi.org/10.1007/BF01239508> (vid. pág. 128).
- [RZ10] Luis Ribes y Pavel Zalesskii. *Profinite groups*. Second. Vol. 40. *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2010, págs. xvi+464. ISBN: 978-3-642-01641-7. DOI: 10.1007/978-3-642-01642-4. URL: <https://doi.org/10.1007/978-3-642-01642-4> (vid. págs. 9-11, 13).
- [Sch90] A. J. Scholl. *Motives for modular forms*. En: *Invent. Math.* 100.2 (1990), págs. 419-430. ISSN: 0020-9910. DOI: 10.1007/BF01231194. URL: <https://doi.org/10.1007/BF01231194> (vid. pág. 134).
- [Sha] Romyar Sharifi. *Iwasawa Theory*. Lecture notes. URL: <http://math.ucla.edu/~sharifi/iwasawa.pdf> (vid. págs. 5, 52, 112).
- [Shi77] Goro Shimura. *On the periods of modular forms*. En: *Math. Ann.* 229.3 (1977), págs. 211-221. ISSN: 0025-5831. DOI: 10.1007/BF01391466. URL: <https://doi.org/10.1007/BF01391466> (vid. pág. 130).
- [Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 11. *Publications of the Mathematical Society of Japan*. Reprint of the 1971 original, Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994, págs. xiv+271. ISBN: 0-691-08092-5 (vid. pág. 129).
- [Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009, págs. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: <https://doi.org/10.1007/978-0-387-09494-6> (vid. págs. 126 s.).
- [SU14] Christopher Skinner y Eric Urban. *The Iwasawa main conjectures for  $GL_2$* . En: *Invent. Math.* 195.1 (2014), págs. 1-277. ISSN: 0020-9910. DOI: 10.1007/s00222-013-0448-1. URL: <https://doi.org/10.1007/s00222-013-0448-1> (vid. pág. 128).
- [SV16] Peter Schneider y Otmar Venjakob. *Coates-Wiles homomorphisms and Iwasawa cohomology for Lubin-Tate extensions*. En: *Elliptic curves, modular forms and Iwasawa theory*. Vol. 188. *Springer Proc. Math. Stat.* Springer, Cham, 2016, págs. 401-468 (vid. pág. 53).
- [Ven05] Otmar Venjakob. *From classical to non-commutative Iwasawa theory: an introduction to the  $GL_2$  main conjecture*. En: *European Congress of Mathematics*. Eur. Math. Soc., Zürich, 2005, págs. 861-879 (vid. pág. 138).
- [Ven07] Otmar Venjakob. *From the Birch and Swinnerton-Dyer conjecture to non-commutative Iwasawa theory via the equivariant Tamagawa number conjecture— a survey*. En: *L-functions and Galois representations*. Vol. 320. *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 2007, págs. 333-380. DOI: 10.1017/CBO9780511721267.010. URL: <https://doi.org/10.1017/CBO9780511721267.010> (vid. pág. 139).

## Bibliografía

- [Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, págs. xiv+487. ISBN: 0-387-94762-0. DOI: 10.1007/978-1-4612-1934-7. URL: <https://doi.org/10.1007/978-1-4612-1934-7> (vid. págs. 4 s., 16-18, 60, 64, 66, 79, 87, 97).
- [Wut14] Christian Wuthrich. *Overview of some Iwasawa theory*. En: *Iwasawa theory 2012*. Vol. 7. Contrib. Math. Comput. Sci. Springer, Heidelberg, 2014, págs. 3-34 (vid. págs. 5, 126 s.).
- [Zag81] D. B. Zagier. *Zetafunktionen und quadratische Körper*. Eine Einführung in die höhere Zahlentheorie. [An introduction to higher number theory], Hochschultext. [University Text]. Springer-Verlag, Berlin-New York, 1981, págs. viii+144. ISBN: 3-540-10603-0 (vid. págs. 74, 77).

# Índice

## A

abscisa de convergencia, 73  
adjunto de Iwasawa, 55  
adjuntos de Iwasawa, 52  
álgebra de Iwasawa, 25, 29  
álgebra profinito, 9  
anillo de grupos profinito, 11  
anillo noetheriano, 39  
anillo profinito, 9  
anillos de períodos  $p$ -ádicos, 119  
anulador, 39  
apareamiento de Kummer, 19  
arriba, 15, 16

## C

campo de números, 13  
carácter, 20  
carácter ciclotómico, 22  
carácter de Dirichlet, 76  
carácter de Teichmüller, 22  
condición de Panchishkin, 136  
conductor, 76  
congruencias de Kummer, 81  
Conjetura de Leopoldt, 64  
conjetura equivariante de los  
     $\varepsilon$ -isomorfismos, 138  
Conjetura Equivariante de Números de  
    Tamagawa, 138  
criterio de Kummer, 3  
crítico, 135

## D

de buena fe, 83  
debajo, 15, 16  
distinguido, 26  
dual de Pontryagin, 52

## E

el  $m$ -ésimo campo ciclotómico, 17  
elemental, 51  
elemento de Stickelberger de nivel  $m$ , 87  
elementos característicos, 138  
elementos de Frobenius, 122  
espacios ádicos, 97  
esquemas formales, 97

extensión  $\mathbb{Z}_p$ , 62  
extensión ciclotómica  $\mathbb{Z}_p$ , 62  
extensión de Kummer, 19

## F

fórmula de Bernoulli, 79  
fórmula de interpolación, 86  
fórmula de transformación de Mellin, 75  
función  $\Gamma$ , 75  
función  $L$   $p$ -ádica, 88  
función  $L$  de Dirichlet de  $\chi$ , 77  
función zeta de Riemann, 74  
functor exacto, 53

## G

generador topológico, 11  
grado de inercia, 15  
grado de ramificación, 15  
grado de Weierstraß, 26  
grupo abeliano pro- $p$  libre, 11  
grupo de clases, 14  
grupo de descomposición, 15, 16  
grupo de inercia, 16  
grupo de Selmer, 120  
grupo profinito, 9  
grupos de Selmer de Bloch y Kato, 120

## I

ideal característico, 50  
ideal de aumentación, 32  
ideal fraccional principal, 13  
ideal inverso, 13  
idempotente asociado a  $\chi$ , 35  
idempotentes ortogonales, 35  
invariantes  $\mu$  y  $\lambda$ , 47  
isomorfismos de comparación, 135

## L

Lema de división, 26  
Lema de Nakayama Topológico, 48  
Lema de Representación, 21  
libre de torsión, 39  
localmente profinito, 11

## M

medidas, 31

## Índice

módulo de Tate, 126  
módulo elemental, 46, 47  
módulo noetheriano, 39  
módulo profinito, 9  
módulo pseudo-nulo, 40  
módulo sobre  $\Lambda$ , 39  
morfismo de Kummer, 126  
morfismo pseudo-inyectivo, 40  
morfismo pseudo-sobreyectivo, 40  
motivo, 3

**N**  
no ramificada, 118  
no ramificada en casi todos lados, 118  
no ramificado, 16  
norma relativa de ideales, 16  
número de clases, 14  
números de Bernoulli, 76  
números de Bernoulli generalizados por  $\chi$ ,  
77

**O**  
ordinaria, 130

**P**  
período complejo, 135  
plaza, 14  
plazas arquimedeanas, 14  
plazas complejas, 14  
plazas no arquimedeanas, 14  
plazas reales, 14  
polinomio característico, 47  
polinomio ciclotómico, 28  
polinomio de Bernoulli, 77  
polinomio de Hecke, 130  
polinomio de Weierstraß, 26  
polinomio distinguido, 27  
primitivo, 76

pro- $p$ , 9  
producto de Euler, 73  
pseudo-generator, 28  
pseudo-isomorfismo, 40  
pseudo-medida, 32

**R**  
radical de un ideal, 41  
ramificada, 15  
ramificado, 15, 16  
rango sobre  $\mathbb{F}_p$ , 63  
rango sobre  $\mathbb{Z}_p$ , 63  
realizaciones, 133  
representación de Artin, 134  
representación de Galois, 118  
representación de un grupo, 12  
retículo estable, 118

**S**  
serie de Dirichlet, 73  
sistema compatible de representaciones de  
Galois, 124  
sistemas de Euler, 116  
soporte de un módulo, 41

**T**  
Teorema de Estructura, 47  
teorema de Stickelberger, 87  
topología de Krull, 10  
torsión, 39  
totalmente ramificado, 15, 16

**U**  
unidades ciclotómicas, 98  
unidades principales, 21

**V**  
variedad, 132