Desde Fermat, Lamé y Kummer hasta Iwasawa: Una introducción a la teoría de Iwasawa

por

Álvaro Lozano-Robledo

Resumen. En una conferencia de 1956, Kenkichi Iwasawa presentó la demostración de un teorema que inauguraba lo que hoy llamamos la teoría de Iwasawa. Desde entonces, las ideas de Iwasawa han ido abriendo numerosas nuevas vías de investigación en teoría de números, y sus ideas y sus generalizaciones se han usado en cientos de artículos.

Este artículo es una introducción a la teoría de Iwasawa desde un punto de vista histórico. Los orígenes de esta teoría se remontan al famoso último teorema de Fermat y, en particular, a un célebre intento fallido de demostrarlo por parte de Gabriel Lamé. En la primera parte del artículo hablaremos sobre el intento de Lamé y de cómo Ernst Kummer, que independientemente estaba estudiando ideas similares, logró encontrar una demostración válida del teorema de Fermat para primos regulares. La estrategia de Kummer motivará el estudio del número de clases y grupo de clases de ideales de un cuerpo de números, que son precisamente el centro de atención de la teoría de Iwasawa.

1. Introducción

En una conferencia de 1956, Kenkichi Iwasawa presentó la demostración de un teorema (Teorema 9.2 de este artículo) que inauguraba lo que hoy llamamos teoría de Iwasawa. Desde entonces, las ideas de Iwasawa han ido abriendo numerosas nuevas vías de investigación en teoría de números y tanto ellas como sus múltiples generalizaciones se han usado en cientos de trabajos científicos. Este artículo es una introducción histórica a la teoría de Iwasawa. Está orientado hacia la comunidad matemática en general (y no solo para aquellos interesados en teoría de números) y, por tanto, es parte de nuestro objetivo definir y motivar los conceptos según vayan apareciendo, aunque corramos el riesgo de aburrir a los expertos.

Los orígenes de esta teoría se remontan al famoso último teorema de Fermat y, en particular, a un célebre intento fallido de demostrarlo por parte de Gabriel Lamé. En la primera parte del artículo hablaremos sobre el intento de Lamé (en las secciones 2 y 3) y de cómo Ernst Kummer, que independientemente estaba estudiando ideas similares, logró encontrar una demostración válida del teorema de Fermat para primos regulares (en las secciones 4, 5 y 6). La estrategia de Kummer motivará el estudio del número y grupo de clases de ideales de un cuerpo de números, que son precisamente el centro de atención de la teoría (clásica) de Iwasawa. En la sección 5 repasaremos la definición del número y grupo de clases de un cuerpo de números, y

su relación con factorización única en el anillo de enteros del cuerpo. En la sección 7 trataremos brevemente de las propiedades de divisibilidad de números de clases en extensiones de cuerpos de números. La teoría de Iwasawa describe el crecimiento de la componente p-primaria del grupo de clases en un tipo de extensiones de cuerpos de números llamadas extensiones p-ádicas. En las secciones 8 y 9 describiremos el teorema que Iwasawa presentó en 1956, y hablaremos sobre extensiones p-ádicas en general. En la sección 10, trataremos las consecuencias del teorema de Iwasawa. En concreto, explicaremos el significado de los invariantes λ, μ y ν que aparecen en el enunciado del teorema de Iwasawa, en relación con los grupos de clases de una extensión p-adica. En las últimas tres secciones del artículo, discutiremos una reformulación del teorema de Iwasawa en términos de extensiones sin ramificación (gracias a la teoría de cuerpos de clases), y haremos un resumen de la demostración del teorema, usando la estructura de módulos sobre $\mathbb{Z}_p[[T]]$.

Es necesario aclarar que en este artículo, cuando decimos «teoría de Iwasawa» nos referimos a lo que los expertos denominan teoría de Iwasawa *clásica*, que se centra en el estudio de números y grupos de clases de torres de cuerpos de números. En la actualidad, la teoría de Iwasawa *moderna* abarca el estudio de otros grupos, como el grupo de Shafarevich-Tate, que se asemejan al grupo de clases. La teoría sigue creciendo muy rápido y ahora tiene muchas más aplicaciones, además del estudio de números de clases. Por ejemplo, la teoría moderna de Iwasawa es de gran interés en el estudio de curvas elípticas y funciones L, y es uno de los ingredientes fundamentales en los avances en torno a la conjetura de Birch y Swinnerton-Dyer (uno de los siete «problemas del milenio» elegidos por el Instituto Clay). Por no omitir completamente los nombres de los grandes arquitectos de la teoría de Iwasawa moderna, incluimos aquí algunos de ellos: Burns, Coates, Greenberg, Kato (el cual, precisamente, habló en Madrid sobre la teoría de Iwasawa durante el ICM de 2006), Kolyvagin, Pollack, Rubin, y Wiles, entre muchos otros.

Hay muy buenas referencias (en inglés) sobre la teoría de Iwasawa. El libro de L. C. Washington, [15], es una de las referencias más completas y más recomendables para aquel que esté comenzando en este tema. Muy desafortunadamente, no podemos tratar de abarcar en este artículo la «Conjetura Central» (*Main Conjecture*) de la teoría de Iwasawa (demostrada por B. Mazur y A. Wiles), pero el lector puede leer sobre ella en [15], o en el librito de J. Coates y R. Sujatha, [3]. El autor también recomienda encarecidamente el artículo [6] de R. Greenberg, que explica varias de las nuevas tendencias en la teoría de Iwasawa (por ejemplo, las aplicaciones al estudio de rangos de curvas elípticas).

2. El teorema de Fermat y los acontecimientos de 1847

Los orígenes de la teoría de Iwasawa se remontan a un célebre (o, mejor dicho, tristemente célebre) pero fallido intento de demostrar el último teorema de Fermat.

TEOREMA 2.1 (Último teorema de Fermat, o teorema de Wiles [16]). *La ecuación*

$$x^n + y^n = z^n$$

Figura 1: Pierre de Fermat (1601-1665).

no tiene soluciones con $x, y, z \in \mathbb{Z}$ *y* $xyz \neq 0$*, cuando* $n \geq 3$*.*

El primer día de Marzo de 1847, un excitadísimo Gabriel Lamé presentó sus ideas sobre una posible demostración del último teorema de Fermat, ante la Academia de París. Lamé propuso resolver el problema a través de una factorización de $x^n + y^n$ usando números complejos (explicaremos sus ideas en más detalle luego). De acuerdo con los documentos que han perdurado hasta nuestros días, la presentación de Lamé fue muy poco apropiada para la Academia, pues le faltaban muchos detalles y precisión. De cualquier modo, Lamé proclamó haber resuelto completamente el problema que Fermat había enunciado a finales de la decada de 1630. Sin embargo, Lamé no se quiso atribuir todo el mérito de la demostración durante su charla, y mencionó que la idea se originó tras una conversación con Liouville.

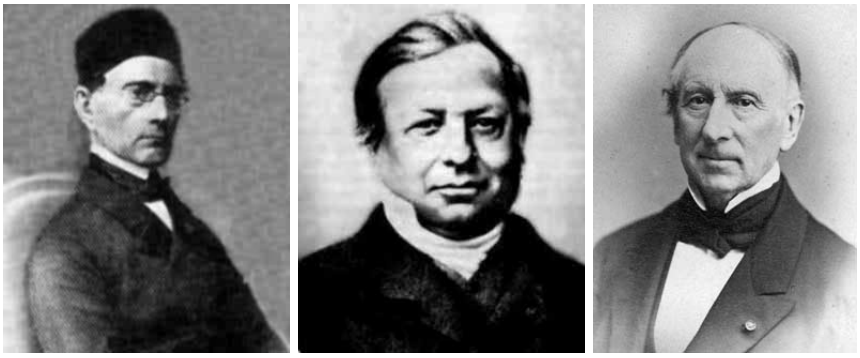


Figura 2: Gabriel Lamé, Joseph Liouville y Augustin Cauchy.

Ese mismo día de 1847, el mismísimo Liouville fue el siguiente orador en la Academia de París, pero su discurso estuvo cargardo de reproches hacia Lamé. Para

empezar, Liouville dijo que la estrategia de Lamé era una de las primeras que se le ocurrirían a cualquier matemático competente al enfrentarse con el problema por primera vez. De hecho, es muy probable que Liouville ya hubiese considerado la misma alternativa, y sabemos que Lagrange ya había mencionado la misma factorización de $x^n + y^n$ en conexión con el último teorema de Fermat. Para acabar de rematar a Lamé en su discurso, Liouville señaló una laguna importante en la demostración: su método asumía la factorización única en un subanillo de números complejos y Lamé no había justificado en ningún momento porqué esta propiedad se tendría que cumplir.

Tras Liouville, sin embargo, tomó la palabra Cauchy y mencionó su optimismo acerca de la estrategia de Lamé, porque él mismo había mandado a la Academia (supuestamente en Octubre de 1846) un bosquejo de una demostración del teorema de Fermat, posiblemente muy parecida a la idea de Lamé.

El debate lo cerró Ernst Kummer, el 24 de Mayo de 1847. En una carta a la Academia de París (leida a la Academia por Liouville), Kummer explicó que *tres años antes* había publicado una memoria en la que demostraba que, desafortunadamente, la factorización única no se cumple en general en los anillos que Lamé (y probablemente Cauchy) consideraba en su trabajo. En la misma carta Kummer proseguía diciendo que la teoría de factorización se puede «salvar» introduciendo una nueva clase de números complejos que él decidió llamar «números complejos ideales». Todos los detalles habían sido publicados en 1846 en las actas de la Academia de Berlín, y una exposición más completa iba a aparecer en la revista de Crelle en breve. El lector que quiera saber más sobre los interesantes y célebres acontecimientos de 1847 puede consultar el Capítulo 4 de [5].

Figura 3: Ernst Eduard Kummer (1810-1893).

3. La «demostración» de Lamé

Es bien sabido, y fácil de demostrar, que para verificar que la ecuación de Fermat no tiene soluciones cuando $n \geq 3$ basta demostrar que no hay soluciones en el caso

$n = 4$ y cuando $n = p \geq 3$ es un número primo. La prueba del caso $n = 4$ fue proporcionada por Fermat (y es una de las únicas demostraciones de Fermat que han perdurado hasta nuestros días). Cuando estudiamos la ecuación $x^p + y^p = z^p$, donde $p \geq 3$ es primo, es conveniente considerar dos casos:

1. primer caso: $x^p + y^p = z^p$ con $\text{mcd}(xyz, p) = 1$, y
2. segundo caso: $x^p + y^p = z^p$ con $\text{mcd}(xyz, p) = p$.

En general, el primer caso del último teorema de Fermat es más fácil de tratar, mientras que el segundo caso es, habitualmente, más difícil de demostrar. En este artículo nos limitamos al primer caso por simplicidad aunque la «demostración» de Lamé, en principio, hubiera tratado ambos casos.

La estrategia propuesta por Lamé se basaba en una factorización de $x^p + y^p$, usando números complejos. Comencemos calculando las raíces de $x^p + y^p$, considerándolo como un polinomio en la variable x. La igualdad $x^p + y^p = 0$ implica que $x^p = -y^p = (-y)^p$. Por tanto, se debe cumplir que $x = \zeta \cdot (-y)$, donde ζ es una raíz p-ésima de la unidad.[1] Sea ζ_p una raíz primitiva de la unidad, dada por:

$$\zeta_p = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi}{p}\right) + i\,\text{sen}\left(\frac{2\pi}{p}\right).$$

Las raíces p-ésimas de la unidad son las raíces de $x^p = 1$, y todas ellas vienen dadas por ζ_p^i con $i = 0, \ldots, p-1$. Por consiguiente, las raíces de $x^p + y^p$ son $x = \zeta_p^i \cdot (-y) = -\zeta_p^i \cdot y$ para $i = 0, \ldots, p-1$. Así que el polinomio $x^p + y^p$ se puede factorizar como

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y),$$

y, por tanto,

$$z^p = x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y) = (x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y). \tag{1}$$

Ejemplo 3.1. Sea $p = 3$. Entonces

$$\begin{aligned} x^3 + y^3 &= (x + y)(x^2 - xy + y^2) \\ &= (x + y)\left(x + \left(\frac{1 + \sqrt{3}}{2}\right) y\right)\left(x + \left(\frac{1 - \sqrt{3}}{2}\right) y\right), \end{aligned}$$

donde $\zeta_3 = \frac{1+\sqrt{-3}}{2}$ y $\zeta_3^2 = \frac{1-\sqrt{-3}}{2}$.

Consideraremos la ecuación (1) como una factorización de $x^p + y^p$ sobre el anillo

$$\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} : a_i \in \mathbb{Z}\}.$$

[1] ¡léase pe-ésima, y no pésima!

Lamé demostró correctamente que, en el anillo $\mathbb{Z}[\zeta_p]$, dos números cualquiera de la forma $x + \zeta_p^i y$ y $x + \zeta_p^j y$ son relativamente primos entre sí, siempre que $i \neq j$. Pero su error fue concluir que si estos números son relativamente primos y tenemos la ecuación (1), entonces cada $x + \zeta_p^i y$ tiene que ser una potencia p-ésima de otro elemento de $\mathbb{Z}[\zeta_p]$. Es decir, Lamé afirmó que existe un $\beta_i \in \mathbb{Z}[\zeta_p]$ tal que $x+\zeta_p^i y = \beta_i^p$, y después deduciría una contradicción con la existencia de tales β_i.

Tal y como señaló Liouville, el problema con este argumento es que, para concluir que cada $x + \zeta_p^i y$ es una potencia p-ésima, Lamé estaba afirmando implícitamente que $\mathbb{Z}[\zeta_p]$ es un dominio de factorización única o DFU (es decir, todos los elementos del anillo tienen una factorización única como producto de elementos primos). Pero no hay ninguna razón obvia por la que $\mathbb{Z}[\zeta_p]$ tenga que ser un DFU y, de hecho, Ernst Kummer ya había demostrado que algunos de estos anillos *no tienen* la propiedad de factorización única. (Véase [12], Capítulo I, Ejercicios 19-27.)

4. Los «números complejos ideales» de Kummer

Anteriormente, y de manera independiente, Kummer había descubierto la estrategía que Lamé intentaba seguir y había llegado a la conclusión de que este método tenía un fallo fundamental. Sin embargo, Kummer encontró una manera de salvar esta idea (en ciertos casos) definiendo los que él llamó «números complejos ideales» (y que hoy en día llamamos ideales de un anillo). Esta nueva construcción le permitió demostrar el último teorema de Fermat en un gran número de casos.

Sean $\alpha_1, \ldots, \alpha_n$ elementos en $\mathbb{Z}[\zeta_p]$. Definimos el *ideal* generado por $\{\alpha_i : i = 1, \ldots, n\}$ en $\mathbb{Z}[\zeta_p]$ como

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = \{\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n : \beta_i \in \mathbb{Z}[\zeta_p]\}.$$

Por ejemplo, el ideal $\mathfrak{A} = (\alpha)$ es el conjunto de números de la forma $\alpha \cdot \beta$, donde $\beta \in \mathbb{Z}[\zeta_p]$. Decimos que un ideal $\mathfrak{A}$ en $\mathbb{Z}[\zeta_p]$ es *principal* si hay un $\delta \in \mathbb{Z}[\zeta_p]$ tal que $\mathfrak{A} = (\delta)$.

Sea $\mathfrak{A}_i = (x + \zeta_p^i y)$ para cada $i = 0, \ldots, p-1$. Entonces, como en la ecuación (1) de la sección 3, la igualdad:

$$(x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1}) = z^p$$

implica una factorización de la p-ésima potencia del ideal (z) como producto de ideales:

$$(z)^p = \mathfrak{A}_0 \cdot \mathfrak{A}_1 \cdots \mathfrak{A}_{p-1}.$$

Kummer comprendió que los ideales en $\mathbb{Z}[\zeta_p]$ tienen una estructura multiplicativa (la única unidad es el anillo entero $(1) = \mathbb{Z}[\zeta_p]$), y que cada ideal tiene una factorización única como producto de ideales primos. Además, demostró que los ideales $\mathfrak{A}_i$ son primos entre sí. Por tanto, se puede concluir que $\mathfrak{A}_i = \mathfrak{B}_i^p$ para cada $i = 0, \ldots, p-1$, i. e., cada ideal $\mathfrak{A}_i$ es una potencia p-ésima de otro ideal $\mathfrak{B}_i$. Pero Kummer indicó que $\mathfrak{B}_i$ no es necesariamente principal. Si *asumimos* que el anillo $\mathbb{Z}[\zeta_p]$ es un dominio

de ideales principales (DIP), entonces todos los ideales son principales, y existen elementos $\beta_i \in \mathbb{Z}[\zeta_p]$ tales que $\mathfrak{B}_i = (\beta_i)$.

Por consiguiente,

$$(x + \zeta_p^i y) = \mathfrak{A}_i = \mathfrak{B}_i^p = (\beta_i)^p.$$

Esto conlleva que existen unidades $\xi_i \in \mathbb{Z}[\zeta_p]^\times$ tales que

$$x + \zeta_p^i y = \xi_i \beta_i^p,$$

y Kummer probó que esta igualdad es imposible, lo cual demuestra el último teorema de Fermat para todos aquellos primos p tales que $\mathbb{Z}[\zeta_p]$ es un DIP. No entraremos en este artículo en más detalles del resto de la demostración de Kummer, pero el lector interesado puede encontrarlos en el Capítulo 1 de [15], o en [4], por ejemplo.

Las aportaciones de Kummer en esta área no terminan aquí, porque él era consciente de que la condición «$\mathbb{Z}[\zeta_p]$ es un DIP» es demasiado fuerte,[2] así que se propuso encontrar una manera de sortear esta hipótesis tan restrictiva. Para medir lo lejos que un anillo dado está de ser un DIP, definió un *grupo de clases de ideales*que, como veremos en la siguiente sección, es, esencialmente, el grupo cociente de ideales, módulo ideales principales.

5. El grupo y número de clases de ideales

En esta sección explicamos (y procuramos motivar) la definición del grupo de clases de ideales y el número de clases de un cuerpo de números K. Como ya hemos visto, estamos interesados en el caso particular de $K = \mathbb{Q}(\zeta_p)$, pero también necesitaremos hablar de grupos de clases de otros cuerpos más adelante. Recordamos al lector que un cuerpo de números K es simplemente una extensión finita (y por tanto algebraica) de $\mathbb{Q}$, y el anillo de enteros de K, denotado por $\mathcal{O}_K$, es el anillo formado por todos los elementos de K que son raíces de polinomios mónicos con coeficientes enteros.

Ejemplo 5.1. Sea $d \in \mathbb{Z}$ un entero libre de cuadrados, y definamos un cuerpo de números $K = \mathbb{Q}(\sqrt{d})$. La extensión $K/\mathbb{Q}$ es cuadrática (grado 2) y

$$\mathcal{O}_K \cong \begin{cases} \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}, \text{ si } d \equiv 1 \text{ mód } 4, \\ \mathbb{Z} + \sqrt{d}\,\mathbb{Z}, \text{ s } d \equiv 2, 3 \text{ mód } 4. \end{cases}$$

En otras palabras, si definimos

$$\tau = \begin{cases} \frac{1+\sqrt{d}}{2}, \text{ si } d \equiv 1 \text{ mód } 4, \\ \sqrt{d}, \text{ si } d \equiv 2, 3 \text{ mód } 4 \end{cases}$$

entonces $\mathcal{O}_K = \mathbb{Z}[\tau] = \{n + m\tau : n, m \in \mathbb{Z}\}$. Por ejemplo, si $K = \mathbb{Q}(\sqrt{-3})$, entonces $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Por cierto, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}\left(\frac{1+\sqrt{-3}}{2}\right) = \mathbb{Q}(\zeta_3)$.

[2] De hecho, Montgomery y Uchida han demostrado (independientemente) que $\mathbb{Z}[\zeta_p]$ es un DIP si y solo si $p \leq 19$. Véase [14], por ejemplo.

EJEMPLO 5.2. El cuerpo $K = \mathbb{Q}(\zeta_p)$ es un cuerpo de números. La extensión $K/\mathbb{Q}$ es de Galois y su grado es $[K : \mathbb{Q}] = p - 1$. El anillo de enteros es $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. En general, si $n \geq 2$ y $\zeta_n = e^{2\pi i/n}$ es una raíz n-ésima de la unidad, entonces la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es de Galois, de grado $\varphi(n)$ y su anillo de enteros es $\mathbb{Z}[\zeta_n]$. Aquí φ representa la función de Euler.

A continuación, definimos el grupo de clases de ideales de un cuerpo de números. Primero, definimos una relación de equivalencia entre ideales.

DEFINICIÓN 5.3. Sea K un cuerpo de números y sea $\mathcal{O}_K$ el anillo de enteros de K. Decimos que dos ideales $\mathfrak{A}$ y $\mathfrak{B}$ de $\mathcal{O}_K$ pertenecen a la misma *clase de ideales* si existen α y $\beta \in \mathcal{O}_K$ tales que $(\alpha)\mathfrak{A} = (\beta)\mathfrak{B}$. En tal caso, escribiremos $[\mathfrak{A}] = [\mathfrak{B}]$. Por tanto:

$$[\mathfrak{A}] = \{\text{ideales } \mathfrak{B} \subseteq \mathcal{O}_K : \text{ existen } \alpha, \beta \in \mathcal{O}_K \text{ con } (\alpha)\mathfrak{A} = (\beta)\mathfrak{B}\}.$$

Definimos el *grupo de clases de ideales* de K, denotado por $\mathrm{Cl}(K)$, como el grupo multiplicativo de clases de ideales de $\mathcal{O}_K$.[3]

NOTA 5.4. El grupo de clases de ideales de un cuerpo de números K es un grupo *abeliano*. El elemento identidad en $\mathrm{Cl}(K)$ es la clase $[(1)] = [\mathcal{O}_K]$ que también denominaremos como la clase trivial. La clase de un ideal $\mathfrak{A}$ es la clase trivial si y solo si $\mathfrak{A}$ es principal. En efecto, si $\mathfrak{A} = (\alpha)$ entonces $(1)\mathfrak{A} = (\alpha)\mathcal{O}_K$, y por tanto $[\mathfrak{A}] = [\mathcal{O}_K]$. Por otra parte, si $[\mathfrak{A}] = [\mathcal{O}_K]$ entonces existen $\alpha, \beta \in \mathcal{O}_K$ tales que $(\alpha)\mathfrak{A} = (\beta)\mathcal{O}_K = (\beta)$. Así que α debe ser un divisor de β, i. e. hay un $\delta \in \mathcal{O}_K$ tal que $\alpha\delta = \beta$, y por tanto $\mathfrak{A} = (\delta)$ es principal.

NOTA 5.5. El grupo de clases de un cuerpo de números K es un grupo finito (ni la finitud del grupo ni la existencia del inverso multiplicativo de cualquier clase de ideales son propiedades obvias). El orden (o cardinal) del grupo de clases se denomina el *número de clases* de K, y normalmente lo denotamos por h_K o $h(K)$. En el caso particular de $K = \mathbb{Q}(\zeta_p)$, escribiremos h_p en vez de h_K para recalcar la dependencia de la elección del primo p.

NOTA 5.6. El número de clases de K es $h_K = 1$ si y solo si K es un DIP. En efecto, supongamos primero que $h_K = 1$. Entonces $\mathrm{Cl}(K)$ solo tiene un elemento, la clase trivial, y todo ideal $\mathfrak{A}$ satisface $[\mathfrak{A}] = [\mathcal{O}_K]$. Por la nota 5.4, $\mathfrak{A}$ es principal. A la inversa, si todos los ideales son principales, entonces todos pertenecen a la clase trivial $[\mathcal{O}_K]$ y, por tanto, $\mathrm{Cl}(K)$ tiene un único elemento.

NOTA 5.7. Todo DIP es también un dominio de factorización única (DFU). Además, si R es un *dominio de Dedekind* entonces DFU y DIP son condiciones equivalentes. Afortunadamente, el anillo de enteros de un cuerpo de números es un dominio de Dedekind y, por tanto, DFU y DIP son sinónimos en los casos que nos interesan.

EJEMPLO 5.8. El anillo $\mathbb{Z}[\sqrt{-5}]$ no es un DFU. En efecto:

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

[3]En libros de texto recientes, el grupo de clases es simplemente definido como el cociente de los ideales fraccionales de K, módulo los ideales fraccionales principales.

son dos factorizaciones distintas de 6 como producto de factores irreducibles. Por tanto, $\mathbb{Z}[\sqrt{-5}]$ no es tampoco un DIP. Se puede demostrar fácilmente que el ideal $\mathfrak{P} = (2, 1 + \sqrt{-5})$ no es principal. De hecho, el grupo de clases de $K = \mathbb{Q}(\sqrt{-5})$ consiste en dos elementos, a saber $\{[\mathcal{O}_K], [\mathfrak{P}]\}$, y el número de clases de K es 2.

6. El criterio de Kummer

En la sección 4 hemos indicado que si $\mathbb{Z}[\zeta_p]$ es un DIP entonces el último teorema de Fermat es cierto para el exponente primo p. Sea $K_p = \mathbb{Q}(\zeta_p)$. ¿Cuándo es el número de clases de K_p igual a 1? Kummer identificó esta pregunta como interesante pero difícil de reponder, así que intentó buscar una solución alternativa. Recordemos que, para que su demostración funcionase, Kummer necesitaba precisamente que lo siguiente fuera cierto:

$$\text{si } (x + \zeta_p y) = \mathfrak{B}^p \text{ entonces existe } \beta \in \mathbb{Z}[\zeta_p] \text{ tal que } \mathfrak{B} = (\beta).$$

Supongamos que $(x + \zeta_p y) = \mathfrak{B}^p$. Entonces, $[\mathfrak{B}]^p = [(x + \zeta_p y)] = [\mathcal{O}_{K_p}]$ porque $(x + \zeta_p y)$ es un ideal principal. Por consiguiente, la p-ésima potencia de $\mathfrak{B}$ es el elemento identidad en $\mathrm{Cl}(K_p)$ y, por tanto, el orden del elemento $[\mathfrak{B}]$ en el grupo es 1 ó p. De este modo, si $\mathrm{Cl}(K_p)$ no tiene elementos de orden p, el orden de $[\mathfrak{B}]$ tiene que ser 1, y $\mathfrak{B}$ tiene que ser principal. Gracias al teorema de Lagrange sabemos que $\mathrm{Cl}(K_p)$ tiene un elemento de orden p si y solo si p es un divisor del orden de $\mathrm{Cl}(K_p)$ o, en otras palabras, si y solo si h_p, el número de clases de K_p, es divisible por p.

Teorema 6.1 (Kummer, 1846). *Sea $p \geq 3$ un número primo. Si el número de clases de $\mathbb{Q}(\zeta_p)$ no es divisible por p, entonces el último teorema de Fermat se cumple para el exponente primo p.*

Definición 6.2. Decimos que un número primo es *irregular* si $h_p = \#\,\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ es divisible por p. Si $\mathrm{mcd}(h_p, p) = 1$, entonces decimos que p es un primo *regular*.

Esta definición propicia una pregunta obvia:

Pregunta 6.3. *¿Cuándo es p un primo regular? O de otro modo, ¿cuándo son p y h_p primos entre sí?*

Kummer fue capaz de encontrar una respuesta magnífica a esta pregunta. Antes de ver su teorema, necesitamos definir los números de Bernoulli.

Definición 6.4. Los *números de Bernoulli* B_k, así llamados en honor de Jacob Bernoulli (figura 4), son números racionales definidos por la siguiente expansión en serie

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

Se pueden calcular fácilmente usando la fórmula recursiva $\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$. Hemos incluido los primeros números de Bernoulli en el cuadro 1. Si $k \geq 3$ es impar, el número de Bernoulli B_k es cero.

k	0	1	2	4	6	8	10	12	14	16
B_k	1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$

Cuadro 1: Los primeros números de Bernoulli

Figura 4: Jacob Bernoulli (1654-1705).

TEOREMA 6.5 (Criterio de Kummer, 1847). *Un número primo p es irregular si y sólo si p divide al numerador del número de Bernoulli B_k para algún índice par $2k$ en el intervalo $2 \leq 2k \leq p-3$.*

EJEMPLO 6.6. El cuadro 1 muestra que el primo $p = 5$ es regular. En efecto, por el criterio de Kummer, sólo tenemos que verificar que el numerador de $B_2 = -1/2$ no es divisible por 5. De modo similar, la misma tabla muestra que $p = 7, 11, 13, 17$ y 19 son regulares, porque ninguno de estos primos aparecen como factores de uno de los numeradores de B_{2k} con $2 \leq 2k \leq p-3 \leq 16$.

Sin embargo, la misma tabla nos dice que $p = 691$ es irregular, porque el numerador de B_{12} es precisamente -691. Por tanto, el número de clases de $\mathbb{Q}(\zeta_{691})$ es un múltiplo de 691. Igualmente, el primo 3617 es irregular.

NOTA 6.7. Los primeros primos irregulares son $37, 59, 67, 101, 103, 131, \ldots$. Sabemos demostrar que hay infinitos primos irregulares pero, sorprendentemente, nadie ha sido capaz de demostrar que hay infinitos primos regulares. Se cree que alrededor de un 39 % de todos los primos son irregulares (véase [15], p. 62, 63).

NOTA 6.8. Si p es irregular, el criterio de Kummer nos dice que h_p, el número de clases de $\mathbb{Q}(\zeta_p)$ es un múltiplo de p, pero el criterio no nos dice nada del resto de divisores primos de h_p. Por ejemplo, para $p = 37$, el número de clases h_{37} es

precisamente igual a 37. Indicamos a continuación la factorización de h_p para los tres primeros primos irregulares:

$$h_{37} = 37,\ h_{59} = 3 \cdot 59 \cdot 233, \quad \text{y} \quad h_{67} = 67 \cdot 12739.$$

Nota 6.9. Si p es un primo que es divisor de los numeradores de n números de Bernoulli B_{2k} distintos, todos con $2 \leq 2k \leq p-3$, entonces h_p es un múltiplo de p^n. Por ejemplo, los numeradores de B_{62} y B_{110} son divisibles por 157 (y ningún otro numerador de un número de Bernoulli entre $2 \leq 2k \leq 154$ es divisible por 157). Por tanto, h_{157} es divisible por 157^2 (pero no es divisible por 157^3).

Un siglo después de que Kummer resolviera el último teorema de Fermat para primos regulares, Martin Eichler (véase la figura 5) extendió las ideas de Kummer a números primos que no son «demasiado irregulares». Definimos el índice de irregularidad de un primo p, que denotamos por $i(p)$, como el cardinal del conjunto de números de Bernoulli B_{2k}, con $2 \leq 2k \leq p-3$, cuyos numeradores son múltiplos de p. Por ejemplo, el índice de irregularidad de $p = 5, 7, 11, 13, 17$ ó 19 es $i(p) = 0$ (véase el ejemplo 6.6). Sin embargo, las notas 6.8 y 6.9 nos dicen que $i(37) = i(59) = i(67) = 1$, pero $i(157) = 2$. He aquí el teorema de Eichler (recordamos al lector que la distinción entre el primer y segundo caso de Fermat aparece al principio de la Sección 3):

Teorema 6.10 (Eichler, 1965). *Supongamos que p es irregular con un índice de irregularidad $i(p) < \sqrt{p} - 2$. Entonces el primer caso del último teorema de Fermat es cierto para el exponente p.*

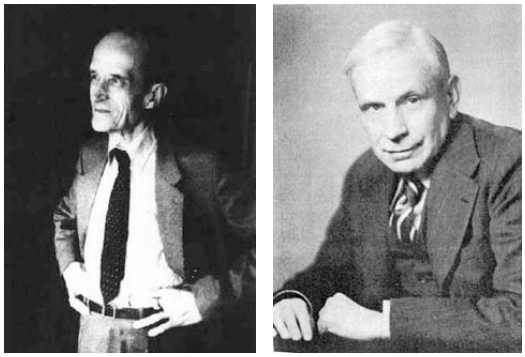


Figura 5: Martin Eichler (1912-1992) y Harry Vandiver (1882 - 1973).

7. El máximo subcuerpo real y la conjectura de Vandiver

En esta sección mencionaremos brevemente algunas de las relaciones entre los números de clases en extensiones (finitas) de cuerpos de números. Antes de enunciar el tipo de problemas a los que nos referimos, recordemos la definición de ramificación en una extensión de cuerpos de números F/K. Sea $\wp$ un ideal primo de $\mathcal{O}_K$, el anillo

de enteros de K. Entonces $\wp\mathcal{O}_F$ es un ideal de $\mathcal{O}_F$ y tiene una factorización (¡única!) como un producto de ideales primos de $\mathcal{O}_F$. Es decir, $\wp\mathcal{O}_F = P_1^{e_1} \cdot P_2^{e_2} \cdots P_r^{e_r}$, donde los $P_i \subseteq \mathcal{O}_F$ son ideales primos distintos. Decimos que $\wp$ se ramifica en F/K si existe un índice $1 \leq i \leq r$ tal que $e_i > 1$. Si $e_i = 1$ para todo i, entonces decimos que $\wp$ no se ramifica. Si $\wp\mathcal{O}_K = P^e$, entonces decimos que $\wp$ (y también F/K) se ramifica totalmente. Una extensión F/K es no ramificada si ningún ideal primo de F se ramifica.

TEOREMA 7.1 ([15], Prop. 4.11). *Sea F/K una extensión de cuerpos de números tal que, si L/K es una extensión de Galois intermedia, con $K \subsetneq L \subsetneq F$, existe por lo menos un primo (finito o infinito) que se ramifica en la extensión L/K. Entonces, h_K, el número de clases de K, es un divisor del número de clases de F, h_F.*

Más tarde, también haremos uso del siguiente teorema de divisibilidad de números de clases:

TEOREMA 7.2 (Teorema de «empujar hacia abajo», o *push-down*; [9]). *Sea F/K una p-extensión de cuerpos de números (i. e. el grado de F/K es una potencia de p) y supongamos que sólo un ideal primo de K ramifica en F y la ramificación es total. Entonces, si p es un divisor de h_F, también lo es de h_K.*

NOTA 7.3. Para poder usar el Teorema 7.1, el lector ha de recordar lo siguiente acerca de extensiones ciclotómicas: el ideal primo (p) de $\mathbb{Z}$ ramifica totalmente en la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. En efecto, el ideal (p) en $\mathbb{Z}[\zeta_p]$ es la $(p-1)$-ésima potencia del ideal primo $\wp = (\zeta_p - 1)$. Como la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es de Galois y abeliana (i. e. el grupo de Galois es abeliano), cualquier cuerpo intermediario $\mathbb{Q} \subsetneq L \subsetneq \mathbb{Q}(\zeta_p)$ es de Galois sobre $\mathbb{Q}$, y el primo p ramifica en $L/\mathbb{Q}$ y también en $\mathbb{Q}(\zeta_p)/L$. Por tanto, el número de clases de L es un divisor del número de clases de $\mathbb{Q}(\zeta_p)$, i. e. h_L es un divisor de h_p.

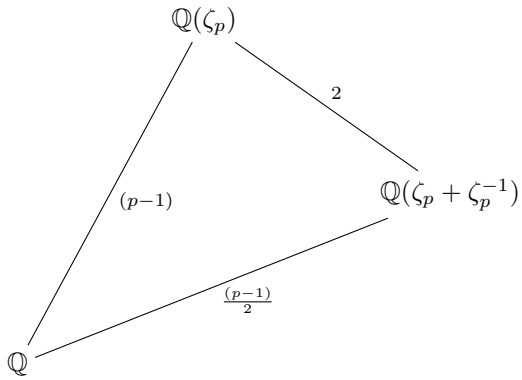
En particular, el número de clases de $\mathbb{Q}(\zeta_p)$ esta íntimamente relacionado con los números de clases de sus subcuerpos. Uno de los subcuerpos de mayor interés es el *máximo subcuerpo real* de $\mathbb{Q}(\zeta_p)$, que viene dado por

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

de modo que, $\mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{R}$. Recordemos además que la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es de grado $p-1$, y el estimado lector puede verificar fácilmente que ζ_p es una raíz del polinomio

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

Por tanto, la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ es cuadrática, y el grado de $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$ es $(p-1)/2$.



Como antes, sea h_p el número de clases de $\mathbb{Q}(\zeta_p)$ y sea h_p^+ el de $\mathbb{Q}(\zeta_p)^+$. El número h_p^+ es un divisor de h_p (véase la nota 7.3). La siguiente famosa conjectura apareció por primera vez en una carta de 1849 de Kummer a Kronecker, pero Harry Vandiver propusó está pregunta en público frecuentemente, y lleva su nombre:

Conjetura 7.4 (La conjetura de Vandiver). *El número de clases de* $\mathbb{Q}(\zeta_p)^+$ *nunca es divisible por* p*, i. e.* $\mathrm{mcd}(p, h_p^+) = 1$.

Esta misteriosa conjectura de Vandiver se ha verificado, por lo menos, para todos los primos $p < 12\ 000\ 000$ (véase [1]).

8. Torres ciclotómicas y el teorema de Iwasawa

Hasta ahora, nos hemos concentrado en el grupo de clases del cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$, para cada primo p. Es natural extender nuestro estudio a otros cuerpos ciclotómicos. En concreto, estamos interesados en números de clases de cuerpos ciclotómicos de tipo $\mathbb{Q}(\zeta_{p^n})$, donde $\zeta_{p^n} = e^{2\pi i/p^n}$ es una raíz p^n-ésima de la unidad, y $n \geq 1$. Los cuerpos $\mathbb{Q}(\zeta_{p^n})$, para cada $n \geq 1$, forman lo que llamamos una *torre de cuerpos*:

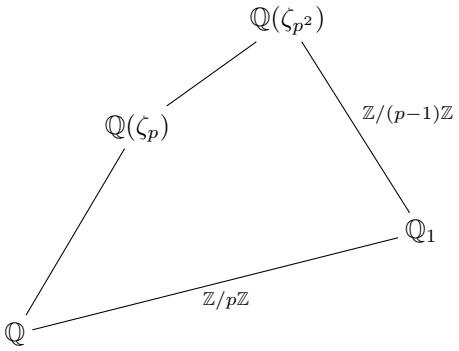
$$\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^n}) \subset \cdots$$

Para cada $n \geq 1$, la extensión $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ es de Galois, y el grupo de Galois es isomorfo a $(\mathbb{Z}/p^n\mathbb{Z})^\times$ y, por tanto, el grado de la extensión es $\varphi(p^n) = p^{n-1}(p-1)$. Por su parte, la extensión $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}(\zeta_{p^n})$ es de Galois, de grado p.

Sea h_{p^n} el número de clases de $\mathbb{Q}(\zeta_{p^n})$. El primo p ramifica totalmente en la extensión $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$, y por tanto ramifica totalmente en la torre $\bigcup_{n\geq 1}\mathbb{Q}(\zeta_{p^n})$. El teorema 7.1 implica que h_{p^k} es un divisor de h_{p^j}, para todo $k \leq j$.

El primer paso de Kenkichi Iwasawa hacia lo que hoy llamamos la teoría de Iwasawa fue demostrar un teorema muy interesante acerca de los números de clases en una torre de ciertos subcuerpos de $\bigcup_{n\geq 1}\mathbb{Q}(\zeta_{p^n})$ que definimos a continuación. Primero, consideremos $G_2 = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})$ que es un grupo abeliano (cíclico) isomorfo a $(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p\mathbb{Z}$. Por tanto, G_2 tiene un único subgrupo (normal)

H_1 de orden $(p-1)$ tal que G_2/H es isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Definimos $\mathbb{Q}_1$ como el subcuerpo de $\mathbb{Q}(\zeta_{p^2})$ fijo por H, i. e. $\mathbb{Q}_1 = \mathbb{Q}(\zeta_{p^2})^H$. Por consiguiente, $\mathbb{Q}_1/\mathbb{Q}$ es una extensión de Galois y abeliana de grado p.



Podemos generalizar esta construcción como sigue. Para cada $n \geq 1$, sea $G_{n+1} = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ que es un grupo abeliano (cíclico) isomorfo a $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^n\mathbb{Z}$. Por tanto, G_{n+1} tiene un único subgrupo (normal) H de orden $(p-1)$, tal que G_{n+1}/H es isomorfo a $\mathbb{Z}/p^n\mathbb{Z}$. Definimos $\mathbb{Q}_n$ como el subcuerpo de $\mathbb{Q}(\zeta_{p^{n+1}})$ fijo por H, i. e. $\mathbb{Q}_n = \mathbb{Q}(\zeta_{p^{n+1}})^H$. Así que $\mathbb{Q}_n/\mathbb{Q}$ es una extensión abeliana de grado p^n, tal que $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$ y

$$\mathbb{Q} \subsetneq \mathbb{Q}_1 \subsetneq \mathbb{Q}_2 \subsetneq \cdots \subsetneq \mathbb{Q}_n \subset \cdots \subset \bigcup_{n\geq 1} \mathbb{Q}_n \subsetneq \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^n}).$$

He aquí nuestra primera versión del teorema de Iwasawa:

TEOREMA 8.1 (Iwasawa, 1956). *Sea p^{e_n} la mayor potencia de p que es un divisor del número de clases de $\mathbb{Q}_n$. Existen $n_0 \geq 0$ y enteros no negativos $\lambda, \mu, \nu \in \mathbb{Z}$ tales que $e_n = \lambda n + \mu p^n + \nu$ para todo $n \geq n_0$.*

Figura 6: Kenkichi Iwasawa (1917-1998).

En el resto del artículo primero explicamos el teorema de Iwasawa en toda la generalidad en la que fue demostrado originalmente (ver [10]), pues el teorema 8.1 es sólo un caso particular. Para ello, repasaremos la teoría de extensiones p-ádicas, mencionaremos algunas de las consecuencias del teorema y, finalmente, trataremos de esbozar una demostración.

9. Extensiones p-ádicas de cuerpos de números

Fijemos un número primo p y sea $\mathbb{Q}_n/\mathbb{Q}$ la extensión abeliana definida en la sección 8, que está completamente caracterizada por las condiciones $\mathbb{Q}_n \subset \mathbb{Q}(\zeta_{p^{n+1}})$ y $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. Recordemos que $\mathbb{Q}_n \subset \mathbb{Q}_{n+1}$ y definamos $\mathbb{Q}_\infty = \bigcup_{n\geq 1} \mathbb{Q}_n$. Entonces, $\mathbb{Q}_\infty/\mathbb{Q}$ es una extensión de Galois y

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

donde $\varprojlim$ denota el límite inverso de grupos via morfismos de conexión $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, que vienen dados como reducción módulo p^n. Por tanto, $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ es isomorfo a $\mathbb{Z}_p$, los enteros p-ádicos. Podemos definir extensiones p-ádicas de otros cuerpos de números como sigue.

Definición 9.1. Sea K un cuerpo de números y sea p un primo fijo. Supongamos que, para cada $n \geq 1$, existe una extensión K_n/K tal que $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$, y $K_n \subset K_{n+1}$. Entonces decimos que $K_\infty = \bigcup_{n\geq 1} K_n$ es una $\mathbb{Z}_p$-extensión, o una extensión p-ádica, de K.

En realidad, Iwasawa demostró el teorema 8.1 para *todas* las $\mathbb{Z}_p$-extensiones de un cuerpo de números K, y a continuación reformulamos el enunciado en toda su generalidad.

Teorema 9.2 (Iwasawa, 1956). *Sea p un número primo, sea K un cuerpo de números y sea $K_\infty = \bigcup_{n\geq 1} K_n$ una $\mathbb{Z}_p$-extensión de K. Sea p^{e_n} la mayor potencia de p que divide al número de clases de K_n. Entonces existe un $n_0 \geq 0$ y enteros no negativos $\lambda, \mu, \nu \in \mathbb{Z}$ tales que $e_n = \lambda n + \mu p^n + \nu$ para todo $n \geq n_0$.*

Antes de adentrarnos en la demostración del teorema de Iwasawa, necesitamos algunos resultados de la teoría de $\mathbb{Z}_p$-extensiones.

Ejemplo 9.3. La extensión $\mathbb{Q}_\infty/\mathbb{Q}$ definida al principio de esta sección es una $\mathbb{Z}_p$-extensión de $\mathbb{Q}$, que llamamos la $\mathbb{Z}_p$-extensión ciclotómica de $\mathbb{Q}$. Si K es un cuerpo de números entonces el cuerpo $K_\infty = K\mathbb{Q}_\infty$ se conoce como la $\mathbb{Z}_p$-extensión ciclotómica de K. En efecto, sea $m \geq 1$ el mayor entero tal que $\mathbb{Q}_m \subseteq K$. Entonces $K_1 = K\mathbb{Q}_{m+1}$ es una extensión abeliana de K de grado p y $K_n = K\mathbb{Q}_{m+n}/K$ es una extensión abeliana con grupo de Galois isomorfo a $\mathbb{Z}/p^n\mathbb{Z}$, para todo $n \geq 1$. Por tanto, K_∞/K es una $\mathbb{Z}_p$-extensión.

Ejemplo 9.4. Sea $p = 5$. La extensión 5-ádica ciclotómica $\mathbb{Q}_\infty$ de $\mathbb{Q}$ está contenida en la extensión ciclotómica $\bigcup_{n\geq 1} \mathbb{Q}(\zeta_{5^n})$. Sea $q = 11$ y consideremos la extensión $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ de grado 10, con grupo de Galois isomorfo a $\mathbb{Z}/10\mathbb{Z}$. Gracias a la teoría de Galois, sabemos que hay un subcuerpo (único) F_1 de $\mathbb{Q}(\zeta_{11})$ tal que $F_1/\mathbb{Q}$ es

abeliano con grado 5. ¿Es F_1 el primer nivel de una $\mathbb{Z}_5$-extensión F_∞ de $\mathbb{Q}$, distinta de $\mathbb{Q}_\infty$?

En este ejemplo, hemos escogido el primo 11 porque $11 \equiv 1$ mód 5. Por el teorema de Dirichlet sobre primos en progresiones aritméticas, y si fijamos un entero $n \geq 1$, existen infinitos números primos q tales que $q \equiv 1$ mód 5^n (por ejemplo, $q = 101 \equiv 1$ mód 25). Por tanto, podemos encontrar infinitas extensiones distintas de $\mathbb{Q}$, con grupo de Galois $\mathbb{Z}/5^n\mathbb{Z}$, cada una dentro de un cuerpo $\mathbb{Q}(\zeta_q)$, y cada una con un primo q diferente. ¿Quiere esto decir que existen infinitas $\mathbb{Z}_5$-extensiones distintas de $\mathbb{Q}$? La respuesta es *no* y el teorema 9.5 explica el porqué (véase también el ejemplo 9.8 más abajo).

Antes de enunciar el teorema, recordamos al lector que el grado de una extensión $K/\mathbb{Q}$ puede expresarse como $[K : \mathbb{Q}] = r_1 + 2r_2$, donde r_1 es el número de homomorfismos inyectivos distintos de K en $\mathbb{R}$ y $2r_2$ es el número de homomorfismos inyectivos distintos de K en $\mathbb{C}$, cuya imagen no esta incluida en $\mathbb{R}$ (que aparecen en pares conjugados).

TEOREMA 9.5 ([15], Teorema 13.4). *Sea K un cuerpo de números y sea p un número primo. Sea $\widehat{K}$ la composición de todas las $\mathbb{Z}_p$-extensiones de K. Existe un entero $d \geq 1$ tal que* $\mathrm{Gal}(\widehat{K}/K) \cong \mathbb{Z}_p^d$ *y*

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

Nótese que el entero d en el teorema es el rango del $\mathbb{Z}_p$-módulo $\mathrm{Gal}(\widehat{K}/K)$. El número d es pues el número de $\mathbb{Z}_p$-extensiones linealmente independientes de K, y hay una famosa conjetura de H. W. Leopoldt que asegura que d es siempre $r_2 + 1$.

CONJETURA 9.6 (Conjetura de Leopoldt). *Sean K, $\widehat{K}$ y d definidos como en el teorema 9.5. Entonces $d = r_2 + 1$.*

En mayo del 2009, Preda Mihăilescu anunció una demostración de la conjetura que, hasta esta fecha, está todavía siendo verificada. Desde que se propuso la conjetura ha habido numerosos anuncios de demostraciones, pero siempre se han encontrado errores en la prueba y, como consecuencia, la comunidad matemática está siendo muy cautelosa con la verificación de esta nueva demostración. El indicio más claro que tenemos a nuestra disposición para creer que la conjetura es cierta es que lo es si $K/\mathbb{Q}$ es una extensión abeliana.

TEOREMA 9.7 (Brumer, 1967, [2]). *Sea $K/\mathbb{Q}$ una extensión finita de Galois y abeliana. Entonces la conjetura de Leopoldt es cierta para K.*

EJEMPLO 9.8. Sea $K = \mathbb{Q}$. Entonces $r_1 = 1$ y $r_2 = 0$, y

$$d = \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q}) = 0 + 1 = 1.$$

Por tanto, el teorema 9.7 nos dice que hay *solo una* extensión p-ádica de $\mathbb{Q}$. Es decir, $\mathbb{Q}_\infty$, la extensión p-ádica ciclotómica del ejemplo 9.3 es la única $\mathbb{Z}_p$-extensión de $\mathbb{Q}$.

EJEMPLO 9.9. Sea K una extensión cuadrática de $\mathbb{Q}$. Como todas las extensiones cuadráticas son galoisianas (pues $K = \mathbb{Q}(\sqrt{m})$, para algún entero m libre de cuadrados), el teorema 9.7 se puede utilizar en este caso. Hay que considerar dos casos:

- Supongamos que $K/\mathbb{Q}$ es un cuerpo real cuadrático, i. e. $K = \mathbb{Q}(\sqrt{m})$, donde $m > 0$. El número de inyecciones reales y complejas de K son $r_1 = 2$ y $r_2 = 0$, respectivamente, y $\operatorname{rank}_{\mathbb{Z}_p} \operatorname{Gal}(\widehat{K}/K) = 0+1 = 1$. Por tanto K tiene una única $\mathbb{Z}_p$-extensión, una para cada primo p, que es $K_\infty = K\mathbb{Q}_\infty$, la extensión p-ádica ciclotómica de K.
- Supongamos que $K/\mathbb{Q}$ es un cuerpo cuadrático imaginario. Entonces $r_1 = 0$, $r_2 = 1$ y $\operatorname{rank}_{\mathbb{Z}_p} \operatorname{Gal}(\widehat{K}/K) = 1 + 1 = 2$. Por consiguiente, K tiene dos $\mathbb{Z}_p$-extensiones linealmente independientes. Una de ellas es la extensión ciclotómica. La *otra* extensión aparece de manera natural en la teoría de curvas elípticas (se puede obtener al añadir a K las coordenadas de los puntos de torsión de orden p^n de una curva elíptica con multiplicación compleja por K). La otra extensión se denomina la $\mathbb{Z}_p$-extensión *anticiclotómica* de K, y normalmente escribimos $K_\infty^{\mathrm{ac}} = \bigcup_{n\geq 1} K_n^{\mathrm{ac}}$. Los cuerpos intermedios K_n^{ac} están caracterizados como las únicas extensiones abelianas de K tales que el grupo de Galois de K_n^{ac}/K es el grupo dihedral de orden $2p^n$.

10. Acerca de los invariantes λ, μ y ν de una $\mathbb{Z}_p$-extensión

En esta sección queremos explicar la importancia del teorema de Iwasawa y para ello describiremos la relación entre los invariantes λ y μ y el grupo de clases de ideales de cuerpos intermedios de una $\mathbb{Z}_p$-extensión.

Sea K un cuerpo de números y sea $K_\infty = \bigcup_{n\geq 1} K_n$ una $\mathbb{Z}_p$-extensión de K. Por el teorema de Iwasawa 9.2, existen invariantes

$$\lambda = \lambda(K_\infty/K), \quad \mu = \mu(K_\infty/K) \quad \text{y} \quad \nu = \nu(K_\infty/K)$$

tales que, si p^{e_n} es la mayor potencia de p que divide el orden de $\mathrm{Cl}(K_n)$, entonces

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

para todo $n \geq n_0$. De esto se desprende que, si μ o λ no es nulo, entonces el tamaño de la parte p-primaria del grupo de clases $\mathrm{Cl}(K_n)$ crece con n (¡y si $\mu \neq 0$ muy rápidamente!). De ahora en adelante llamaremos A_n a la componente p-primaria de $\mathrm{Cl}(K_n)$. Es decir, A_n es el subgroup de $\mathrm{Cl}(K_n)$ formado por todos los elementos cuyo orden es una potencia de p. Con esta notación, el teorema de Iwasawa nos dice que el órden del grupo A_n es precisamente p^{e_n} y, por tanto, si μ o λ no es nulo, A_n crece con n. Pero, ¿cual es la estructura de A_n como grupo abeliano? ¿$\mathbb{Z}/p^{e_n}\mathbb{Z}$, o $(\mathbb{Z}/p\mathbb{Z})^{e_n}$, o ...? El teorema de Iwasawa, y la teoría que Iwasawa inició con este trabajo [10], describe precisamente la estructura de A_n. A continuación ofrecemos ejemplos de resultados que conocemos acerca de esta cuestión.

Teorema 10.1 ([6], Prop. 2.1). *Sea K un cuerpo de números con número de clases h_K. Supongamos que h_K no es divisible por p y que en K sólo hay un ideal primo sobre p. Entonces $\lambda = \mu = \nu = 0$ para toda $\mathbb{Z}_p$-extensión de K.*

Ejemplo 10.2. Pongamos $K = \mathbb{Q}$ en el teorema 10.1. Claramente, el número de clases de $\mathbb{Q}$ es 1 (pues $\mathbb{Z}$ es un DIP) y sólo hay un ideal primo en $\mathbb{Z}$ sobre p.

Por consiguiente $\lambda = \mu = \nu = 0$ para toda $\mathbb{Z}_p$-extensión de $\mathbb{Q}$. En el ejemplo 9.8 hemos visto que, si fijamos el primo p, sólo hay una $\mathbb{Z}_p$-extensión de $\mathbb{Q}$, la extensión ciclotómica $\mathbb{Q}_\infty/\mathbb{Q}$. Así que $\lambda = \mu = \nu = 0$ en esta extensión.

Que los invariantes λ, μ, ν se anulan en este caso también se puede deducir de la conjetura de Vandiver. En efecto, sea $\mathbb{Q}_n$ el n-ésimo cuerpo de la $\mathbb{Z}_p$-extensión ciclotómica de $\mathbb{Q}$. Como $\mathbb{Q}_n$ es el subcuerpo de $\mathbb{Q}(\zeta_{p^{n+1}})$ fijo por H, donde H es el subgrupo de orden $p-1$ en el grupo de Galois $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, sabemos que $\mathbb{Q}_n$ está contenido en $\mathbb{Q}(\zeta_{p^{n+1}})^+$ porque el máximo subcuerpo real es el cuerpo fijo de un subgrupo de H de orden 2. La extensión $\mathbb{Q}(\zeta_{p^{n+1}})^+/\mathbb{Q}_n$ es abeliana, de grado $(p-1)/2$ y p ramifica totalmente. Por el teorema 7.1, $h(\mathbb{Q}_n)$, el número de clases de $\mathbb{Q}_n$, es un divisor del número de clases $h(\mathbb{Q}(\zeta_{p^{n+1}})^+)$.

Supongamos que p divide a $h(\mathbb{Q}_n)$. En el parrafo anterior hemos visto que, entonces, p también divide a $h(\mathbb{Q}(\zeta_{p^{n+1}})^+)$. Además, $\mathbb{Q}(\zeta_{p^{n+1}})^+/\mathbb{Q}(\zeta_p)^+$ es una extensión de grado p^n y, por tanto, por el teorema de *push-down* (Teorema 7.2), el primo p es un divisor de $h(\mathbb{Q}(\zeta_p)^+)$, en contradicción con la conjetura de Vandiver (Conj. 7.4). Así que si creemos que la conjetura de Vandiver es cierta, entonces p no puede ser un divisor de $h(\mathbb{Q}_n)$, para ningún $n \geq 1$, lo cual implica que $\lambda = \mu = \nu = 0$ en la $\mathbb{Z}_p$-extensión ciclotómica de $\mathbb{Q}$.

Si combinamos el teorema 10.1 con el criterio de Kummer (teorema 6.5) obtenemos el siguiente resultado:

COROLARIO 10.3. *Supongamos que p no es divisor del numerador de ningún número de Bernoulli B_{2k} con $2 \leq 2k \leq p-3$. Entonces $\lambda = \mu = \nu = 0$ para todas las $\mathbb{Z}_p$-extensiones de $K = \mathbb{Q}(\zeta_p)$.*

La $\mathbb{Z}_p$-extensión ciclotómica de un cuerpo de números es un tanto especial, pues tiene propiedades que no tienen por qué ocurrir en otras extensiones p-ádicas. La siguiente conjetura fue propuesta por Iwasawa.

CONJETURA 10.4 (Iwasawa). *Sea K un cuerpo de números y sea $K_\infty = K\mathbb{Q}_\infty$ la $\mathbb{Z}_p$-extensión ciclotómica de K. Entonces $\mu(K_\infty/K) = 0$.*

Sabemos que esta conjetura es cierta cuando $K/\mathbb{Q}$ es una extensión abeliana (este resultado es un teorema de Ferrero y Washington; véase [15], Teorema 7.15). Iwasawa encontró ejemplos de otras $\mathbb{Z}_p$-extensiones, distintas de la ciclotómica, tales que $\mu(K_\infty/K) \neq 0$ (véase [11]). Si $K/\mathbb{Q}$ es totalmente real, i. e. el número de inyecciones de K en $\mathbb{R}$ es igual al grado de $K/\mathbb{Q}$, entonces se cree que el invariante λ de la $\mathbb{Z}_p$-extensión ciclotómica es también nulo. Esto último es una conjetura que apareció en la tesis de Ralph Greenberg (figura 7), uno de los grandes expertos en este campo en la actualidad. Greenberg fue estudiante de Iwasawa, ha explorado muchas cuestiones en la teoría de Iwasawa y continúa atrayendo a muchos matemáticos hacia este tipo de preguntas.

CONJETURA 10.5 ([7]). *Sea $K/\mathbb{Q}$ un cuerpo de números totalmente real y sea $K_\infty = \bigcup_{n\geq 1} K_n$ la $\mathbb{Z}_p$-extensión ciclotómica de K. Entonces $\lambda(K_\infty/K) = \mu(K_\infty/K) = 0$. Es decir, la mayor potencia de p que divide al número de clases de K_n está acotada por $p^{e_n} \leq p^\nu = p^{\nu(K_\infty/K)}$, para todo $n \geq 1$.*

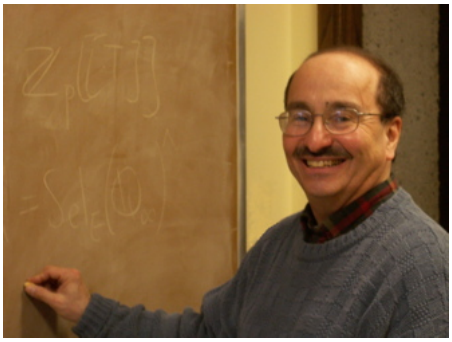


Figura 7: Ralph Greenberg.

¿Qué ocurre cuando el invariante μ es nulo en una $\mathbb{Z}_p$-extensión? El siguiente teorema responderá a esta pregunta, pero primero necesitamos introducir el concepto de p-rango de un grupo abeliano.

Definición 10.6. Sea G un grupo abeliano finito y sea $G[p^\infty]$ la componente p-primaria de G. Como $G[p^\infty]$ es un grupo abeliano finito tal que el orden de cada uno de sus elementos es una potencia de p, tenemos que existen enteros $r \geq 0$ y $e_1, \ldots, e_r \geq 1$ tales que:

$$G[p^\infty] \cong (\mathbb{Z}/p^{e_1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{e_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{e_r}\mathbb{Z}).$$

Si $r = 0$ entonces $G[p^\infty]$ es trivial (con un solo elemento, la identidad). Por tanto, $G[p^\infty]/pG[p^\infty] \cong (\mathbb{Z}/p\mathbb{Z})^r$ y el entero $r \geq 0$ es llamado el p-rango de G. O lo que es lo mismo, r es la dimensión de G/pG como espacio vectorial sobre $\mathbb{Z}/p\mathbb{Z}$ y decimos que $r = \operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(G/pG)$. Nótese que $G/pG \cong G[p^\infty]/pG[p^\infty] \cong (\mathbb{Z}/p\mathbb{Z})^r$, así que r también se puede calcular directamente desde G.

Teorema 10.7 ([15], Prop. 13.23). *Sea K un cuerpo de números y sea K_∞/K una $\mathbb{Z}_p$-extensión. Entonces $\mu(K_\infty/K) = 0$ si y sólo si el p-rango de $\mathrm{Cl}(K_n)$ está acotado cuando $n \to \infty$.*

Este teorema nos dice que $\mu = 0$ si y sólo si existe un r_0 tal que $\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(A_n) \leq r_0$ para todo $n \geq 1$ donde, como antes, A_n es la componente p-primaria de $\mathrm{Cl}(K_n)$. Es decir, existen constantes $e_{n,i} \geq 1$ para cada $i = 1, \ldots, r_0$ tales que

$$A_n \cong (\mathbb{Z}/p^{e_{n,1}}\mathbb{Z}) \oplus (\mathbb{Z}/p^{e_{n,2}}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{e_{n,r_0}}\mathbb{Z})$$

y $e_{n,i} \leq e_{n+1,i}$ (porque la norma de A_{n+1} a A_n es sobreyectiva). Por tanto, para cada $i = 1, \ldots, r_0$, tenemos una sucesión ascendente de enteros positivos $\beta_i = \{e_{n,i}\}_{n \geq 1}$. ¿Se cumple que $e_{n,i} \to \infty$ cuando $n \to \infty$, o es $\{e_{n,i}\}$ una sucesión acotada? Es aquí donde el invariante λ entra en juego. Definimos $A = \varprojlim A_n$ donde los morfismos de conexión vienen dados por la norma.

Teorema 10.8 ([15], Prop. 13.25). *Sea K un cuerpo de números y sea K_∞/K una $\mathbb{Z}_p$-extensión tal que $\mu(K_\infty/K) = 0$. Sea A_n la componente p-primaria de $\mathrm{Cl}(K_n)$,*

donde K_n es la n-ésima capa de K_∞/K. Entonces

$$A = \varprojlim A_n \cong \mathbb{Z}_p^\lambda \oplus G$$

donde $\lambda = \lambda(K_\infty/K)$ y G es un grupo finito abeliano cuyo orden es una potencia de p.

En general, es muy difícil calcular los valores exactos de los invariantes μ, λ y ν de una $\mathbb{Z}_p$-extensión dada. Sin embargo, en algunos casos particulares, tenemos cotas para estos invariantes.

TEOREMA 10.9 ([6], Prop. 2.2). *Sea K un cuerpo de números y p un primo que se descompone completamente en $K/\mathbb{Q}$ (i. e. $p\mathcal{O}_K = \wp_1\wp_2\cdots\wp_r$, donde todos los $\wp_i$ son ideales primos distintos y $r = [K:\mathbb{Q}]$). Sea K_∞/K una $\mathbb{Z}_p$-extensión en la cual todos los ideales primos de $\mathcal{O}_K$ sobre p ramifican. Entonces $\lambda(K_\infty/K) \geq r_2$, donde, como siempre, $[K:\mathbb{Q}] = r_1 + 2r_2$.*

También se ha conjeturado que, si fijamos el cuerpo de números K, el invariante λ de la $\mathbb{Z}_p$-extensión ciclotómica de K no puede ser arbitrariamente grande al variar el primo p.

CONJETURA 10.10 ([6], p. 13). *Sea K un cuerpo de números y, para cada primo p, sea $K_{\infty,p}/K$ la $\mathbb{Z}_p$-extensión ciclotómica de K. Entonces existe un número $N > 0$ tal que $\lambda(K_{\infty,p}/K) \leq N$ para todos los primos $p \geq 2$.*

11. EL CUERPO DE CLASES DE HILBERT

Antes de comenzar nuestra discusión de la demostración del teorema de Iwasawa necesitamos un ingrediente más, que es la sorprendente conexión entre el número de clases de un cuerpo de números y sus extensiones sin ramificación en ningún primo.

Figura 8: David Hilbert (1862 - 1943).

TEOREMA 11.1 (Hilbert, 1897). *Sea K un cuerpo de números y sea $\mathrm{Cl}(K)$ el grupo de clases de ideales de K. Existe un cuerpo de números H (conocido en la actualidad como el cuerpo de clases de Hilbert de K) tal que:*

1. *$K \subseteq H$, la extensión H/K es de Galois, y* $\mathrm{Gal}(H/K)$ *es abeliano, isomorfo a* $\mathrm{Cl}(K)$*, y*
2. *H es la máxima extensión abeliana de K sin ramificación en ningún primo.*

Este teorema, y los fundamentos de lo que hoy conocemos como *la teoría de cuerpos de clases*, aparecieron en el libro de Hilbert [8], también conocido como su *Zahlbericht*. El teorema 11.1 constituye un diccionario entre grupos de clases de ideales y extensiones abelianas no ramificadas y, en particular nos dice que el número de clases de K es divisible por un primo p si y sólo si existe una extensión F/K abeliana no ramificada de grado p.

Supongamos que K es un cuerpo de números y $K_\infty = \bigcup_{n\geq 1} K_n$ es una extensión p-ádica de K. Sea H_n el cuerpo de clases de Hilbert de K_n y sea L_n la máxima p-extensión de K_n que es abeliana y no ramificada (véase la figura 9). Por la definición de H_n, sabemos que hay una inclusión $L_n \subseteq H_n$. También definimos:

$$K_\infty = \bigcup_{n\geq 1} K_n, \quad L_\infty = \bigcup_{n\geq 1} L_n, \quad \text{y} \quad H_\infty = \bigcup_{n\geq 1} H_n.$$

Sea $X_n = \mathrm{Gal}(L_n/K_n)$. Por el Teorema 11.1, sabemos que $\mathrm{Gal}(H_n/K_n) \cong \mathrm{Cl}(K_n)$ y el grupo de Galois $\mathrm{Gal}(L_n/K_n)$ es isomorfo a A_n, la componente p-primaria de $\mathrm{Cl}(K_n)$. Como L_n/K es de Galois, la extensión L_∞/K también es de Galois, es decir normal y separable. Si definimos $X = \mathrm{Gal}(L_\infty/K_\infty)$ entonces sabemos que

$$\mathrm{Gal}(L_\infty/K)/X \cong \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p.$$

A partir de ahora asumiremos, por simplicidad que la extensión K_∞/K está totalmente ramificada en cada primo que ramifica. Bajo esta hipótesis, tenemos que $K_{n+1} \cap L_n = K_n$ porque K_{n+1}/K_n está totalmente ramificada y L_n/K_n no se ramifica. Por tanto,

$$\mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_{n+1}/K_{n+1})$$

y $X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$ y también

$$X = \mathrm{Gal}(L_\infty/K_\infty) \cong \varprojlim \mathrm{Gal}(L_nK_\infty/K_\infty) = \varprojlim X_n.$$

Por consiguiente, está claro que nos interesa mucho conocer la estructura de $X = \mathrm{Gal}(L_\infty/K_\infty)$ porque resume la estructura de $X_n \cong A_n$, para cada $n \geq 1$.

12. La estructura de X como un módulo sobre $\mathbb{Z}_p[[T]]$

En esta sección describimos como se puede dotar a $X = \mathrm{Gal}(L_\infty/K_\infty)$ con una estructura de módulo sobre $\mathbb{Z}_p[[T]]$ y también hablaremos de $\mathbb{Z}_p[[T]]$-módulos en general. Por abreviar, llamaremos $\Lambda = \mathbb{Z}_p[[T]]$ al anillo de series en la variable T con coeficientes en $\mathbb{Z}_p$.

(a) Primero, sabemos que $X = \varprojlim X_n$ es un límite inverso de p-grupos abelianos finitos, porque X_n es isomorfo a A_n, la componente p-primaria de $\mathrm{Cl}(K_n)$ y, por tanto, podemos considerar X como un $\mathbb{Z}_p$-módulo de modo natural.

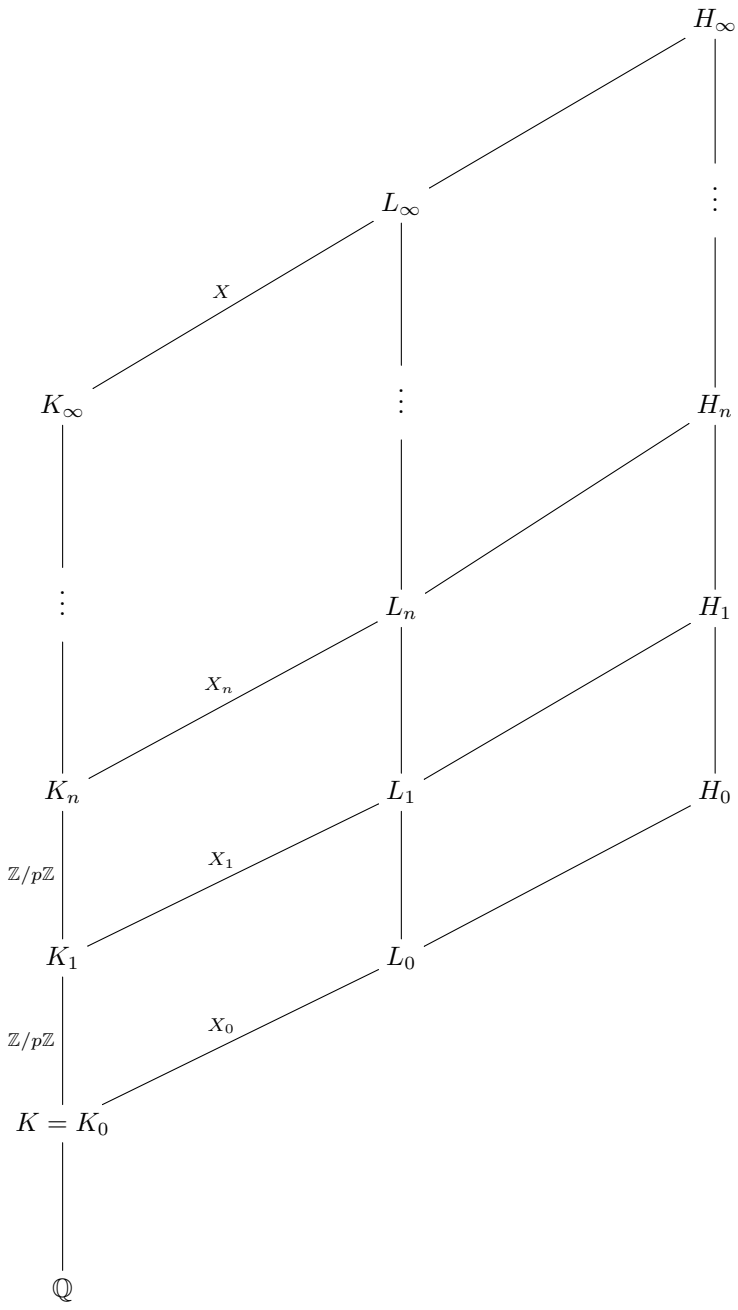


Figura 9: La $\mathbb{Z}_p$-extensión K_∞/K, la máxima p-extensión abeliana sin ramificación de la capa K_n, y sus cuerpos de clases de Hilbert.

Ejemplo 12.1. Supongamos que $X \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}_p$. Definimos la acción natural de $k \in \mathbb{Z}_p$ sobre un elemento $x = (a \bmod p, b \bmod p^2, c) \in X$, donde $a, b \in \mathbb{Z}$ y $c \in \mathbb{Z}_p$, como

$$k \cdot x = (ka \bmod p, kb \bmod p^2, kc).$$

(b) También hay una acción natural de $\Gamma = \mathrm{Gal}(K_\infty/K)$ sobre $X = \mathrm{Gal}(L_\infty/K_\infty)$. En efecto, sea $\gamma \in \Gamma$ y sea $\widetilde{\gamma}$ cualquier elemento de $\mathrm{Gal}(L_\infty/K)$ que extiende a γ (es decir, la restricción de $\widetilde{\gamma}$ a K_∞ es γ) y sea $x \in X$. Definimos la acción de $\gamma \in \Gamma$ sobre $x \in X$ como

$$\gamma \cdot x = \widetilde{\gamma} x \widetilde{\gamma}^{-1}.$$

Esta acción está bien definida porque, si $\widetilde{\gamma}'$ es otra extensión de γ a todo $\mathrm{Gal}(L_\infty/K)$, entonces $\widetilde{\gamma}'$ y $\widetilde{\gamma}$ difieren en ϕ, un automorfismo de L_∞/K_∞ (i. e. $\phi \in X$). De esto se deduce que

$$\widetilde{\gamma}' x (\widetilde{\gamma}')^{-1} = \widetilde{\gamma}\phi x (\widetilde{\gamma}\phi)^{-1} = \widetilde{\gamma}\phi x \phi^{-1}\widetilde{\gamma}^{-1} = \widetilde{\gamma} x \widetilde{\gamma}^{-1}$$

porque X es abeliano, $\phi, x \in X$ y, por tanto, $\phi x \phi^{-1} = x$.

Juntando (a) y (b) hemos construido una estructura natural para X como $\mathbb{Z}_p[\Gamma]$-módulo. Nótese que $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Sea γ_0 un generador topológico fijo de Γ y definamos la acción de un parámetro T sobre X como $T \cdot X = (\gamma_0 - 1)X$ (esto hace que consideremos la acción como aditiva, en vez de multiplicativa). Entonces X se puede considerar como un $\mathbb{Z}_p[T]$-módulo. Además, la acción de T sobre X es *topológicamente nilpotente*, i. e. cualquier subgrupo abierto de X contiene a $T^n X$ para todo $n > 0$ suficientemente grande. Por consiguiente, X es un $\mathbb{Z}_p[[T]]$-módulo, o un Λ-módulo por abreviar.

El siguiente teorema es la clave de toda la teoría:

Teorema 12.2 (Serre, [13]). *$X = \mathrm{Gal}(L_\infty/K_\infty)$ es un Λ-módulo finitamente generado, y X es Λ-torsión, i. e. para todo $x \in X$ existe un $\lambda \in \Lambda$, con $\lambda \neq 0$, tal que $\lambda x = 0$.*

El anillo Λ no es un dominio de ideales principales pero, de todos modos, tenemos un teorema sobre la estructura de Λ-módulos, análogo al de módulos finitamente generados sobre un DIP.

Definición 12.3. Decimos que dos Λ-módulos X y Y son pseudoisomorfos, y escribimos $X \sim Y$, si existe un homomorfismo de Λ-módulos $X \to Y$ cuyo núcleo y conúcleo son finitos.

El siguiente teorema fue demostrado primero por Iwasawa ([15], Thm. 13.12), pero Serre y Cohen encontraron demostraciones más sencillas.

Teorema 12.4 (Teorema de estructura para Λ-módulos finitamente generados). *Sea X un Λ-módulo finitamente generado. Entonces X es pseudoisomorfo a un Λ-módulo Y tal que*

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

donde $r, s, t, n_i, m_j \in \mathbb{Z}$ *y* $f_j(T)$ *son polinomios distinguidos en* $\mathbb{Z}_p[T]$.

Recordamos al lector que un polinomio $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in \mathbb{Z}_p[T]$ es *distinguido* si a_i es divisible por p para todo $i = 0, \ldots, n-1$.

13. La demostración del teorema de Iwasawa

En esta última sección vamos a ensamblar todas las piezas para esbozar una demostración del teorema de Iwasawa (Teorema 9.2). El objetivo es calcular el tamaño de A_n, para todo $n \geq n_0$. Por la teoría de cuerpos de clases, $A_n \cong X_n$, y hemos demostrado en la sección 11 que $X = \mathrm{Gal}(L_\infty/K_\infty) \cong \varprojlim X_n$.

PREGUNTA 13.1. *Si conocieramos la estructura de* X *como* Λ*-módulo, ¿podemos deducir la estructura de* X_n*?*

Respondamos primero esta pregunta. Recordemos que hemos elegido un elemento γ_0, que es un generador topológico de $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, así que el elemento $\gamma_n = \gamma_0^{p^n}$ es un generador topológico de $\Gamma_n = \mathrm{Gal}(K_\infty/K_n) \cong p^n\mathbb{Z}_p$. No es difícil demostrar que L_nK_∞ es la máxima extensión abeliana de K_n que está incluida en L_∞. Por tanto, $H_n = \mathrm{Gal}(L_\infty/L_nK_\infty)$ es el mayor subgrupo de $G_n = \mathrm{Gal}(L_\infty/K_n)$ tal que el subcuerpo fijo de H_n es abeliano sobre K_n. Deducimos, pues, que H_n es el subgrupo conmutador de G_n (por las propiedades de subgrupos conmutadores). Es decir, $H_n = \mathrm{Gal}(L_\infty/L_nK_\infty) = [G_n, G_n]$. Además, es fácil demostrar que el subgrupo conmutador $[G_n, G_n] = \{aba^{-1}b^{-1} : a, b \in G_n\}$ también se puede describir como

$$[G_n, G_n] = \{\widetilde{\gamma_n} x \widetilde{\gamma_n}^{-1} x^{-1} : x \in X,\ \widetilde{\gamma_n} \text{ extiende } \gamma_n \in \Gamma_n \text{ a } G_n\}.$$

Si recordamos que la acción de γ_n sobre $x \in X$ viene precisamente definida por $\gamma_n \cdot x = \widetilde{\gamma_n} x \widetilde{\gamma_n}^{-1}$, si cambiamos a la notación aditiva y si ponemos $w_n = \gamma_n - 1$, entonces el subgrupo conmutador de G_n es igual a $[G_n, G_n] = (\gamma_n - 1)X = w_nX$. Concluimos que

$$X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_\infty/K_\infty) \cong \mathrm{Gal}(L_\infty/K_\infty)/[G_n, G_n] \cong X/w_nX.$$

Por tanto, hemos demostrado el siguiente resultado.

PROPOSICIÓN 13.2. *Sea* $X = \mathrm{Gal}(L_\infty/K_\infty)$ *y* $X_n = \mathrm{Gal}(L_n/K_n)$. *Sea* γ_0 *un generador topológico de* $\Gamma = \mathrm{Gal}(K_\infty/K)$. *También, sea* $\gamma_n = \gamma_0^{p^n}$ *y* $w_n = \gamma_n - 1$. *Entonces*

$$X_n \cong X/w_nX.$$

Ahora podemos reescribir el isomorfismo $X_n \cong X/w_nX$ en función de la acción de $\Lambda = \mathbb{Z}_p[[T]]$ sobre X. Recordemos que hemos definido $T \cdot x = (\gamma_0 - 1)x$ y, así pues,

$$w_nx = (\gamma_n - 1)x = (\gamma_0^{p^n} - 1)x = ((1+T)^{p^n} - 1)x.$$

Por tanto, $X_n \cong X/((1+T)^{p^n} - 1)X$ y esto constituye una respuesta afirmativa a nuestra pregunta 13.1.

Esbozo de la demostración del teorema 9.2. El teorema 12.2 nos dice que $X = \mathrm{Gal}(L_\infty/K_\infty)$ es un Λ-módulo finitamente generado y, por el teorema de estructura 12.4, existe un Λ-módulo Y tal que

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

y los módulos X e Y son pseudoisomorfos. Por el Teorema 12.2, X es Λ-torsión, y esto significa que $r = 0$ en la ecuación anterior y, por tanto:

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

Ahora sólo nos queda contar el número de elementos en los grupos cocientes indicados en la proposición 13.2. Dejamos que el lector verifique que existe un entero N_1 tal que, poniendo $m = \sum_{i=1}^{s} n_i$ y $\ell = \sum_{j=1}^{t} \deg(f_j) m_j$,

$$|Y/((1+T)^{p^n} - 1)Y| = p^{mp^n + \ell n + c}$$

para todo $n > N_1$ y para alguna constante $c \geq 0$. Además, si $X \sim Y$ entonces existe un entero $N_2 \geq 0$ tal que

$$|X/((1+T)^{p^n} - 1)X| = p^{c'} |Y/((1+T)^{p^n} - 1)Y|$$

para todo $n > N_2$, donde $c' \geq 0$ es constante. Por consiguiente, si definimos

$$\mu = \mu(K_\infty/K) = m, \quad \lambda = \lambda(K_\infty/K) = \ell \quad \text{y} \quad \nu = c + c'$$

entonces existe un número $n_0 = \max(n_1, n_2)$ tal que

$$|A_n| = |X_n| = |X/((1+T)^{p^n} - 1)X| = p^{\mu p^n + \lambda n + \nu}$$

para todo $n \geq n_0$, lo cual concluye la demostración del teorema de Iwasawa. □

Referencias

[1] J. Buhler, R. Crandall, R. Ernwall, T. Metsänkylä, M. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, *J. Symbolic Comp* **31** (2001), 89–96.

[2] A. Brumer, On the units of algebraic number fields, *Mathematika*, **14** (1967), 121–124.

[3] J. Coates, R. Sujatha, *Cyclotomic Fields and Zeta Values*, Springer, 2009.

[4] K. E. Conrad, *FermatŠs last theorem for regular primes*, disponible en su página: `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/fltreg.pdf`

[5] H. M. EDWARDS, *Fermat's last theorem: A genetic introduction to algebraic number theory*, GTM 50, Springer, 1977.

[6] R. GREENBERG, *Iwasawa Theory - Past and Present*, disponible en su página: `http://www.math.washington.edu/~greenber/research.html`

[7] R. GREENBERG, *On some questions concerning the Iwasawa invariants*, Princeton University thesis, 1971.

[8] D. HILBERT, *Theorie der algebraischen Zahlkrper (The theory of algebraic number fields)*, Springer, 1998 (publicado originalmente en 1897).

[9] K. IWASAWA, A note on Class Numbers of Algebraic Number Fields, *Abh. Math. Sem. Univ. Hamburg*, 20 (1956), 257-258.

[10] K. IWASAWA, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183-226.

[11] K. IWASAWA, On the μ-invariants of $\mathbb{Z}_\ell$-extensions, *Number theory, Algebraic Geometry, and Commutative Algebra (in honor of Y. Akizuki)*, Kinokuniya: Tokyo, 1973, pp. 1-11.

[12] D. LORENZINI, *An invitation to Arithmetic Geometry*, Graduate Studies in Mathematics, Vol 9, American Mathematical Society, 1996.

[13] J. P. SERRE, Classes des corpes cyclotomique (d'après K. Iwasawa), *Seminaire Bourbaki*, **174** (1959).

[14] K. UCHIDA, Class numbers of imaginary abelian number fields, I, II y III, *Tôhoku Math. J.* (2) **23** (1971), 97-104, 335-348 y 573-580.

[15] L. C. WASHINGTON, *Introduction to cyclotomic fields*, Second Edition, GTM 83, Springer, 1997.

[16] A. WILES, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), no. 3, 443–551.

ÁLVARO LOZANO-ROBLEDO, DEPT. OF MATHEMATICS, UNIVERSITY OF CONNECTICUT, STORRS, CT 06269, USA

Correo electrónico: `alvaro.lozano-robledo@uconn.edu`

Página web: `http://www.math.uconn.edu/~alozano`