Universitat Autònoma
de Barcelona

Invariantes de Iwasawa en $\mathbb{Z}_p$–extensiones

Un trabajo de fin de grado en matemáticas presentado por

Isaac Aarón Jesús Lorenzo

bajo la supervisión de

Dr. Francesc Bars Cortina

en Barcelona, a 20 de junio de 2018.

Resumen

En el primer capítulo de este trabajo introduciremos diversas estructuras algebraicas como son los módulos y los dominios de Dedekind, y desarrollaremos varios conceptos de Teoría de Números como son el número de clases o la ramificación de un ideal. En el segundo capítulo, construiremos el anillo $\mathbb{Z}_p$ de los enteros p–ádicos, que permiten definir ciertas extensiones de cuerpos no finitas, denominadas $\mathbb{Z}_p$–extensiones. A continuación, en el capítulo tercero, consideraremos el conjunto series formales de potencias sobre $\mathbb{Z}_p$, y posteriormente estructuras de módulo sobre el anillo resultante. En este capítulo enunciaremos y demostraremos el Teorema de clasificación de $\mathbb{Z}_p[[T]]$–módulos, que era el objetivo de partida de la presente memoria. En el cuarto capítulo enunciaremos y demostraremos el Teorema de Iwasawa, el resultado principal del trabajo, que permite controlar las variaciones de la p–parte del número de clases de una $\mathbb{Z}_p$–extensión, e introducimos los conceptos de λ, μ y ν–invariantes de Iwasawa, sobre los cuales realizaremos una breve recopilación de resultados.

Quisiera agradecer a Francesc Bars, mi tutor, por el inconmensurable apoyo prestado durante todo el proceso de elaboración de la memoria.

Índice

1. Preliminares. **7**
- 1.1. Módulos. . . . 7
  - 1.1.1. Generadores y relaciones. . . . 8
  - 1.1.2. Rango. . . . 8
  - 1.1.3. Secuencias exactas. . . . 9
- 1.2. Cuerpos de números y anillos de enteros. . . . 10
- 1.3. Grupos de clases de ideales. . . . 10
- 1.4. Ramificación. . . . 12
  - 1.4.1. Discriminante. . . . 13
- 1.5. Teoría de Galois. . . . 14
  - 1.5.1. Teoría de Galois infinita. . . . 14
  - 1.5.2. Grupos de inercia. . . . 15
- 1.6. Límites proyectivos. . . . 15
  - 1.6.1. Grupos profinitos. . . . 16
- 1.7. Completaciones. . . . 16

2. $\mathbb{Z}_p$–extensiones. **18**
- 2.1. Enteros p–ádicos. . . . 18
- 2.2. $\mathbb{Z}_p$–extensiones. . . . 19
- 2.3. $\mathbb{Z}_p$–extensiones ciclotómicas. . . . 20
- 2.4. Conjetura de Leopoldt. . . . 20

3. $\mathbb{Z}_p[[T]]$–módulos. **22**
- 3.1. Álgebra de Iwasawa. . . . 22
- 3.2. Propiedades de $\mathbb{Z}_p[[T]]$. . . . 23
- 3.3. Ejemplo de $\mathbb{Z}_p[[T]]$–módulo. . . . 24
- 3.4. Teorema de clasificación de $\mathbb{Z}_p[[T]]$–módulos. . . . 25
  - 3.4.1. Demostración. . . . 26

4. Invariantes de Iwasawa. **33**
- 4.1. Teorema de Iwasawa. . . . 33
  - 4.1.1. Demostración. . . . 33
- 4.2. μ–invariantes. . . . 41
- 4.3. λ–invariantes. . . . 41

5. Referencias **43**

1. Preliminares.

En este capítulo presentamos numerosos conceptos básicos para el desarrollo posterior de la memoria. Comenzaremos definiendo qué es un módulo sobre un anillo conmutativo y enunciando algunas de sus propiedades, y continuaremos presentando diversos conceptos de Teoría de Números, como son las definiciones de cuerpo de números y grupo de clases, o la idea de ramificación de un ideal. Como trabajaremos con extensiones de cuerpos no finitas, deberemos enunciar el Teorema Fundamental de la Teoria de Galois no finita, así como presentar la definición de límite proyectivo. El lector interesado puede consultar las referencias [14], [6] y [13] para más detalles sobre módulos, Teoría de Números y Teoría de Galois no finita respectivamente.

1.1. Módulos.

Un módulo es una generalización de la estructura de espacio vectorial, en que los escalares son elementos de un anillo. Recordemos que al referirnos a un anillo, nos referimos a un anillo conmutativo y con unidad.

Definición 1.1. Sea A un anillo. Un A–**módulo** es un grupo abeliano M dotado de un producto por escalar que cumple

1. $a(x+y) = ax + ay$,
2. $(a+b)(x) = ax + bx$,
3. $(ab)x = a(bx)$,
4. $1x = x$,

para todo $a, b \in A$, $x, y \in M$.

Así, tenemos que si A es un cuerpo, entonces un A–módulo corresponde a un A–espacio vectorial. Si A es un anillo e I un ideal de A, tenemos que I es un A–módulo.

Definición 1.2. Un **submódulo** M' de M es un subgrupo de M que es cerrado respecto a la multiplicación por escalares de A.

Definición 1.3. Si M' es un submodulo de M, el **cociente** de M por M' es el grupo abeliano M/M' con la estructura de A–módulo heredada.

De igual manera, un morfismo de módulos representa una generalización de una aplicación lineal.

Definición 1.4. Si M, N son A–módulos, una aplicación $f : M \longrightarrow N$ es un **morfismo de módulos** si

1. $f(x+y) = f(x) + f(y)$,
2. $f(ax) = af(x)$,

para todo $a \in A$, $x, y \in M$.

Definición 1.5. Sea $f : M \longrightarrow N$ un morfismo de A–módulos. El **núcleo** o **kernel** de f es

$$\mathrm{Ker}(f) = \{x \in M \,\big|\, f(x) = 0\}, \tag{1}$$

la **imagen** de f es

$$\mathrm{Im}(f) = f(M), \tag{2}$$

y el **conúcleo** o **cokernel** de f es

$$\mathrm{Coker}(f) = N/\,\mathrm{Im}(f). \tag{3}$$

Proposición 1.6. Si $f : M \longrightarrow N$ un morfismo de A–módulos, entonces $\mathrm{Ker}(f)$ es un submódulo de M, $\mathrm{Im}(f)$ es un submódulo de N, y $\mathrm{Coker}(f)$ es un módulo cociente de N.

Teorema 1.7 (Teorema de isomorfía de A–módulos). Sea $f : M \longrightarrow N$ un morfismo de A–módulos. Entonces, se tiene el isomorfismo $M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.

Demostración. Véase la sección *Submodules and Quocient Modules* del capítulo 2 de [5]. □

Notación 1.8. El **orden** de un conjunto finito M es su número de elementos, y lo denotamos por $|M|$.

Definición 1.9. Un elemento m de un A–módulo M se denomina **elemento de torsión** si $am = 0$ para algún $a \in A$ no nulo. Un módulo M se denomina **módulo de torsión** si todos sus elementos son de torsión.

1.1.1. Generadores y relaciones.

Las definiciones de suma directa y sistema de generadores de módulos conducen a los conceptos de módulo libre y módulo de relaciones.

Definición 1.10. Si M, N son A–módulos, su **suma directa** es el conjunto $M \oplus N$ de todos los pares (x, y) con $x \in M$, $y \in N$. Más en general, si $(M_i)_{i\in I}$ es una familia de A–módulos, su **suma directa** es el conjunto $\bigoplus_{i\in I} M_i$ formado por las familias $(x_i)_{i\in I}$ tales que $x_i \in M_i$ y todos los x_i salvo un número finito son cero.

Notemos que la suma directa de A–módulos es un A–módulo con la operación natural.

Definición 1.11. Sea X un subconjunto de un A–módulo M. El **submódulo generado** por X es la intersección de todos los submódulos de M que contienen X. Si este submódulo coincide con M, entonces decimos que X es un **sistema de generadores** de M. Si X es finito, decimos que M es **finitamente generado**.

Si $X = \{x_i\}_{i\in I}$ es un sistema de generadores de M, entonces M puede escribirse como $M = \sum_{i\in I} Ax_i$, con $Ax_i = \{ax_i \,|\, a \in A\}$, de manera que todo elemento de M puede expresarse como combinación lineal de elementos de X.

Definición 1.12. Un A–módulo isomorfo a uno de la forma $\bigoplus_{i\in I} M_i$, en que cada $M_i \cong A$, se denomina **A–módulo libre**. Si M es un A–módulo libre finitamente generado, entonces $M = \bigoplus_{i=1}^{n} A$ para cierto n, de manera que denotamos este módulo por A^n.

Proposición 1.13. Sean M un A–módulo finitamente generado, $X = \{x_1, \ldots, x_n\}$ un sistema de generadores de M y A^n un A–módulo libre. Los elementos $(a_1, \ldots, a_n) \in A^n$ tales que $a_1x_1 + \cdots + a_nx_n = 0$ se denominan **relaciones** entre $x_1, \ldots, x_n$. El conjunto de todas estas relaciones forma un submódulo de A^n, denominado **módulo de relaciones** entre $x_1, \ldots, x_n$.

1.1.2. Rango.

Definición 1.14. Sean M y N dos A–módulos. El **producto tensorial** de M y N es un A–módulo T tal que las aplicaciones A–bilineales $M \times N \longrightarrow P$ se corresponden una a una a las aplicaciones A–lineales $T \longrightarrow P$ para todo A–módulo P, y los denotamos por $M \otimes N$.

La siguiente proposición nos dice que el producto tensorial de dos A–módulos existe y es único.

Proposición 1.15. Sean M, N dos A–módulos. Entonces, existen un A–módulo T y una aplicación A–bilineal $g : M \times N \longrightarrow T$ que cumplen:

1. Dados un A–módulo P y una aplicación A–bilineal $f : M \times N \longrightarrow P$, existe una única aplicación A–lineal $f' : T \longrightarrow P$ tal que $f = f' \circ g$.

2. Si T' y g' también cumplen la propiedad anterior, entonces existe un único isomorfismo $j : T \longrightarrow T'$ tal que $j \circ g = g'$.

Demostración. Véase la proposición 2.12 de [5]. □

La proposición siguiente nos permitirá definir el rango de un módulo.

Proposición 1.16. Sean A un dominio, $Q(A)$ el cuerpo de fracciones de A, y M un A–módulo. Entonces, $M \otimes Q(A)$ es un $Q(A)$–espacio vectorial.

Demostración. El resultado se sigue del ejercicio 2.15 de [5]. □

Definición 1.17. Si M es un A–módulo finitamente generado, definimos el **rango** de M como la dimensión de $M \otimes Q(A)$ como $Q(A)$–espacio vectorial .

1.1.3. Secuencias exactas.

Definición 1.18. Sea $\{A_i\}$ una secuencia de módulos. Una **secuencia exacta** es una secuencia de aplicaciones $\alpha_i : A_i \longrightarrow A_{i+1}$ tales que $\operatorname{Im} \alpha_i = \operatorname{Ker} \alpha_{i+1}$.

Un resultado particular es que las secuencias $0 \to N \to N'$ y $M \to M' \to 0$ son exactas si y sólo si las apliaciones $N \to N'$ y $M \to M'$ son inyectiva y exhaustiva respectivamente.

Lema 1.19. Dada una secuencia exacta de A–módulos finitos, se tiene que el producto alterno de sus órdenes es 1.

Demostración. El resultado se deduce por inducción a partir de la observación de que, si la secuencia $0 \to N_1 \to N_2 \to N_3 \to \dots$ es exacta, también lo es $0 \to N_1/N_2 \to N_3 \to \dots$. □

Lema 1.20 (**Lema de la Serpiente**)**.** Consideremos el diagrama conmutativo siguiente,

$$\begin{array}{ccccccccc} & & N_1 & \xrightarrow{f} & N_2 & \xrightarrow{g} & N_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{f'} & M_2 & \xrightarrow{g'} & M_3 & & \end{array}$$

Si sus filas forman secuencias exactas, entonces se tiene la secuencia exacta siguiente,

$$\operatorname{Ker} f \to \operatorname{Ker} \alpha \to \operatorname{Ker} \beta \to \operatorname{Ker} \gamma \to \operatorname{Coker} \alpha \to \operatorname{Coker} \beta \to \operatorname{Coker} \gamma \to \operatorname{Coker} g. \qquad (4)$$

Demostración. Véase la proposición 1.3.2 de [15]. □

1.2. Cuerpos de números y anillos de enteros.

Definición 1.21. Un **cuerpo de números algebraicos**, o simplemente **cuerpo de números**, es un cuerpo K tal que la extensión $K/\mathbb{Q}$ es finita. Sus elementos se denominan **números algebraicos**.

Al estudiar la aritmética de un cuerpo de números, interesa tener algún anillo que lo tenga como cuerpo de fracciones y que presente buenas propiedades de divisibilidad. De especial interés resulta el anillo de enteros algebráicos, que generaliza las propiedades de $\mathbb{Z}$ dentro de $\mathbb{Q}$.

Definición 1.22. Si K es un cuerpo de números algebraicos, un elemento $b \in K$ se denomina **entero algebraico** si es raiz de algún polinomio mónico a coeficientes en $\mathbb{Z}$. Más en general, si $A \subseteq B$ son dominios, un elemento $b \in B$ se denomina **entero** sobre A si es raiz de algún polinomio mónico a coeficientes en A.

Definición 1.23. Sean A, B dos dominios tales que $A \subseteq B$. La **clausura entera** de A sobre B es el conjunto de elementos de B que son enteros sobre A. Decimos que A es un dominio **íntegramente cerrado** si su clausura entera sobre su cuerpo de fracciones es igual a A.

Por ejemplo, tenemos que $\mathbb{Z}$ es íntegramente cerrado sobre $\mathbb{Q}$.

Definición 1.24. El **anillo de enteros** de un cuerpo de números algebraicos K es la clausura entera de $\mathbb{Z}$ sobre K, y lo denotamos por $\mathcal{O}_K$.

Los anillos de enteros presentan propiedades muy interesantes, como describen el teorema siguiente y el teorema 1.30.

Teorema 1.25. El anillo de enteros de un cuerpo de números algebraicos es un anillo noetheriano[1], íntegramente cerrado, y tal que todo ideal primo no nulo es un ideal maximal.

Demostración. Véase el teorema 3.1 del capítulo 1 de [6]. □

Consideremos los dos ejemplos siguientes. Por un lado, un cuerpo cuadrático, es decir, un cuerpo $\mathbb{Q}(\sqrt{D})$ con D entero y libre de cuadrados, y por otro lado, un cuerpo ciclotómico, es decir, un cuerpo $\mathbb{Q}(\xi_n)$ con ξ_n una raiz primitiva n–ésima de la unidad. Sus anillos de enteros vienen dado por el resultado siguiente.

Proposición 1.26.
1. Si $K = \mathbb{Q}(\sqrt{D})$ es un cuerpo cuadrático, su anillo de enteros es el anillo $\mathcal{O}_K = \mathbb{Z}[\omega]$, con $\omega = \sqrt{D}$ si $D \not\equiv 1 \mod 4$, y $\omega = (D + \sqrt{D})/2$ si $D \equiv 1 \mod 4$.
2. Si $K = \mathbb{Q}(\xi_n)$ es un cuerpo ciclotómico, su anillo de enteros es el anillo $\mathcal{O}_K = \mathbb{Z}[\xi_n]$.

Demostración. Véanse la proposición 2.2 y el teorema 9.9 de [12]. □

1.3. Grupos de clases de ideales.

Los dominos de Dedekind son la estructura sobre la que se desarrolla la teoría de divisibilidad de ideales, y pueden entenderse como una generalización de los dominios de ideales principales.

Definición 1.27. Un **dominio de Dedekind** es un dominio noetheriano e íntegramente cerrado, en que todo ideal primo no nulo es maximal.

En virtud del teorema 1.25, vemos que el anillo de enteros de un cuerpo de números algebraicos es un dominio de Dedekind.

[1] Recordemos que un anillo es **noetheriano** si para toda cadena creciente de ideales $I_1 \subseteq I_2 \subseteq \ldots$ existe un $n \in \mathbb{N}$ tal que $I_n = I_{n+1} = \ldots$, o equivalentemente, si todo ideal es finitamente generado.

Observación 1.28. Dado un A–módulo finitamente generado, el número mínimo de generadores tiene cierto interés, pero en general no coincide con el rango de A. Por ejemplo, $\mathbb{Z}[\sqrt{-5}]$ es un dominio de Dedekind pero no es un dominio de ideales principales. El ideal $I = (2, 1+\sqrt{5})$, que es un $\mathbb{Z}[\sqrt{-5}]$–módulo, es un ideal primo no principal de $\mathbb{Z}[\sqrt{-5}]$, por lo que el número mínimo de generadores de I es 2. Sin embargo, en este caso tendríamos $I \otimes \mathbb{Q}(\sqrt{-5}) \cong \mathbb{Q}(\sqrt{-5})$, por lo que el rango de I es 1. Para más información sobre este ejemplo, véase el ejemplo 4.3 de [4].

Sean $\mathcal{O}$ un dominio de Dedekind, K su cuerpo de fracciones, L/K una extensión de cuerpos finita y B la clausura entera de $\mathcal{O}$ en L.

Proposición 1.29. Bajo las condiciones anteriores, B es un anillo de Dedekind.

Demostración. Véase la proposición 8.1 del capítulo 1 de [6]. □

Una propiedad fundamental de los dominios de Dedekind es la siguiente.

Teorema 1.30. Todo ideal $\mathfrak{a}$ de $\mathcal{O}$ diferente de (0) y (1) admite una factorización $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ en ideales primos no nulos $\mathfrak{p}_i$ de $\mathcal{O}$, que es única salvo por el orden de los factores.

Demostración. Véase el teorema 3.3 del capítulo 1 de [6]. □

Los ideales fraccionarios permiten obtener inversos de ideales en dominios de Dedekind.

Definición 1.31. Sean $\mathcal{O}$ un dominio de Dedekind y K su cuerpo de fracciones. Un **ideal fraccionario** de K es un $\mathcal{O}$–submódulo finitamente generado $\mathfrak{a} \neq 0$ de K. Un **ideal entero** es un ideal usual de $\mathcal{O}$.

Proposición 1.32. Los ideales fraccionarios de K forman un grupo multiplicativo abeliano, que denominamos **grupo ideal** de K y que denotamos por J_K.

Demostración. Véase la proposición 3.8 del capítulo 1 de [6]. □

El grupo de clases de ideales constituye una medida de cuánto se aparta $\mathcal{O}$ de ser un dominio de ideales principales.

Definición 1.33. Denotamos por P_K el subgrupo de J_K formado por los ideales fraccionarios principales. El grupo cociente J_K/P_K se denomina **grupo de clases de ideales** o **grupo de clases** de K, y lo denotamos por $\mathrm{Cl}(K)$. El orden del grupo de clases de ideales se denomina **número de clases** de K.

Si $\mathcal{O}$ es un dominio de Dedekind y K su cuerpo de fracciones, habitualmente nos referiremos a $\mathrm{Cl}(K)$ como $\mathrm{Cl}(\mathcal{O})$.

Proposición 1.34. Si $\mathcal{O}$ es un dominio de Dedekind, entonces $\mathrm{Cl}(\mathcal{O}) = \{1\}$ si y sólo si $\mathcal{O}$ es un dominio de ideales principales.

Demostración. Véase el lema 2.4 del capítulo 5 de [4]. □

Como $\mathbb{Z}$ es un dominio de ideales principales, del resultado anterior se deduce que su número de clases es 1.

Teorema 1.35. Si $\mathcal{O}$ es un anillo de enteros, entonces $\mathrm{Cl}(\mathcal{O})$ es un grupo finito.

Demostración. Véase el teorema 3.10 del capítulo 5 de [4]. □

1.4. Ramificación.

Sean A un anillo de Dedekind, K su cuerpo de fracciones, L/K una extensión de cuerpos finita y B la clausura entera de A en L. De la proposición 1.29 y el teorema 1.30 se deduce que dado un ideal primo $\mathfrak{p} \subseteq A$ no nulo, su extensión $\mathfrak{p}B \subseteq B$ es un ideal no nulo que descompone en producto de ideales primos de B de manera única. Sea

$$\mathfrak{p}B = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\dots\mathfrak{B}_g^{e_g} \tag{5}$$

esta descomposición en factores primos en B, de manera que los ideales $\mathfrak{B}_i$ son ideales primos no nulos y diferentes de B, y que los $e_i \geq 1$ son enteros.

Definición 1.36. El **índice de ramificación** de $\mathfrak{B}_i$ sobre $\mathfrak{p}$ es el entero e_i, y se designa por $e(\mathfrak{B}_i/\mathfrak{p})$.

Dado un ideal primo no nulo $\mathfrak{p} \subseteq A$, el anillo cociente $A/\mathfrak{p}$ es un cuerpo y se denomina **cuerpo residual** de A en $\mathfrak{p}$. Si $\mathfrak{B}$ es un ideal primo no nulo de B y $\mathfrak{p} = \mathfrak{B} \cap A$ es su contracción en A, entonces la extensión de cuerpos residuales $A/\mathfrak{p} \subseteq B/\mathfrak{B}$ es una extensión finita de grado $[B/\mathfrak{B} : A/\mathfrak{p}] \leq [L : K]$.

Definición 1.37. El grado $[B/\mathfrak{B} : A/\mathfrak{p}]$ se denomina **grado residual** o **grado de inercia** de la extensión B/A en $\mathfrak{B}$, y se designa por $f(\mathfrak{B}/\mathfrak{p})$.

A continuación, consideremos la descomposición (5) y sea $f_i = f(\mathfrak{B}_i/\mathfrak{p})$.

Definición 1.38. Decimos que el ideal primo $\mathfrak{B}_i$ está **no ramificado** sobre A si $e_i = 1$ y si la extensión de cuerpos residuales es separable. En caso contrario, decimos que está **ramificado**. Si además $f_i = 1$, decimos que está **totalmente ramificado**.

En el caso de las extensiones separables, y en especial en las de Galois, resultan útiles los siguientes resultados.

Proposición 1.39. Si la extensión $K \subseteq L$ es separable, entonces

$$\sum_{i=1}^{g} e_i f_i = [L : K]. \tag{6}$$

Demostración. Véase la proposición 8.2 del capítulo 1 de [6]. □

La siguiente proposición limita el número ideales primos que ramifican en extensiones separables.

Proposición 1.40. Sea L/K una extensión separable. Entonces, solo hay un número finito de ideales primos de K que ramifican en L.

Demostración. Véase la proposición 8.4 del capítulo 1 de [6]. □

Proposición 1.41. Sean K, L cuerpos de números. Si la extensión $K \subseteq L$ es de Galois, entonces todos los índices de ramificación e_i y grados de inercia f_i son iguales. Si los designamos por e y f respectivamente, entonces se cumple

$$efg = [L : K] \tag{7}$$

Demostración. Véase la proposición 5.2 de [12]. □

1.4.1. Discriminante.

Dada una extensión finita de cuerpos L/K, para todo elemento $x \in L$ puede definirse una aplicación K–lineal $m_x : L \longrightarrow L$ dada por $m_x(y) = xy$. Esta aplicación lineal tiene asociada una matriz $(a_{ij}) \in \mathcal{M}_n(K)$, con $\mathcal{M}_n(K)$ el espacio vectorial de las matrices cuadradas $n \times n$ a coeficientes en K. El polinomio característico de la matriz (a_{ij}) no depende de la base escogida, por lo que tampoco lo hacen su traza y su determinante.

Definición 1.42. Las aplicaciones $T_{L/K} : L \longrightarrow K$ y $N_{L/K} : L \longrightarrow K$ dadas respectivamente por $T_{L/K} = \sum_{i=1}^{n} a_{ii}$ y $N_{L/K} = \det(a_{ij})$ se denominan **traza** y **norma** de la extensión L/K.

El estudio de los ideales primos que ramifican en una extensión finita puede hacerse, en el caso separable, con ayuda de un invariante asociado a la extensión: el discriminante. Sean A un anillo de Dedekind, K su cuerpo de fracciones, L/K una extensión de cuerpos finita y B la clausura entera de A en L.

Definición 1.43. Dada una K–base $\{b_1, \ldots, b_n\}$ de L, su **discriminante** es el determinante de la matriz de la forma bilineal traza en esta base, es decir, $\det(T_{L/K}(b_i b_j))$. El **discriminante** de la extensión B/A es el ideal de A generado por todos los discriminantes que recorren las K–bases de L formadas por elementos de B, y lo designamos por $\Delta(B/A)$.

La relación entre ramificación y discriminante viene dada por el resultado siguiente.

Proposición 1.44. Supongamos que la extensión L/K es separable, y sea $\mathfrak{p}$ un ideal primo no nulo de A. Entonces, el ideal $\mathfrak{p}$ ramifica en la extensión B/A si y sólo si el discriminante $\Delta(B/A)$ es divisible por $\mathfrak{p}$.

Demostración. Véase la proposición 7.1 de [12]. □

Por ejemplo, en un cuerpo cuadrático se tiene que el discriminante es el siguiente.

Ejemplo 1.45. Sea $K = \mathbb{Q}(\sqrt{D})$ con D entero y libre de cuadrados. Entonces, el discriminante de la extensión $K/\mathbb{Q}$ es $4D$ si $D \not\equiv 1 \mod 4$, y D si $D \equiv 1 \mod 4$.

Demostración. Véase la proposición 8.1 de [12]. □

Si $K = \mathbb{Q}(\sqrt{D})$, de los dos resultados anteriores se tiene que los ideales primos de $\mathbb{Z}$ que ramifican en $K/\mathbb{Q}$ son los primos que dividen a D, y en el caso en que $D \not\equiv 1 \mod 4$, a 2. Como los cuerpos residuales son separables y la extensión es de Galois y de grado 2, de la proposición 1.41 tenemos que la extensión a K de estos primos es el cuadrado de un ideal primo de K. Para la descomposición del resto de primos de $\mathbb{Z}$ en K solo quedan dos opciones; o bien que el primo de $\mathbb{Z}$ continue siendo un ideal primo tras extenderlo a K, o bien que este primo descomponga como producto de dos ideales diferentes de K. El resultado siguiente explica cómo descomponen todos los primos de $\mathbb{Z}$ en la extensión cuadrática $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

Proposición 1.46. Sea $\mathcal{O}_K$ el anillo de enteros de $K = \mathbb{Q}(\sqrt{D})$ y p un número primo. Si p divide al discriminante de la extensión cuadrática $K/\mathbb{Q}$, entonces $p\mathcal{O}_K = \mathfrak{p}^2$, con $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ de grado residual 1. Si $p \neq 2$ y D es un residuo cuadrático módulo p, entonces $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, el producto de dos ideales primos diferentes de $\mathcal{O}_K$ de grado residual 1. Si $p \neq 2$ y D no es un residuo[2] cuadrático módulo p, entonces $p\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$ de grado residual 2. Finalmente, $2\mathcal{O}_K$ es el producto de dos ideales primos diferentes de $\mathcal{O}_K$ de grado residual 1 si $D \equiv 1 \mod 8$, mientras que $2\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$ de grado residual 2 si $D \equiv 5 \mod 8$.

Demostración. Véase la proposición 8.2 de [12]. □

[2]El número b en la congruencia $a \equiv b \mod n$ se denomina **residuo** de a módulo n.

1.5. Teoría de Galois.

Recordemos la definición de extensión de Galois.

Definición 1.47. Una extensión de cuerpos F/K es **de Galois** si es normal sobre K y está generada por raices de polinomios separables sobre K.

Resultarán de especial interés los dos tipos de extensiones de Galois siguientes.

Definición 1.48. Sean p un primo y K un cuerpo. Una **p–extensión** de K es una extensión F/K de Galois tal que $[F : K] = p^n$ para algún $n \in \mathbb{Z}$.

Definición 1.49. Una **extensión abeliana** de cuerpos F/K es una extensión de Galois tal que $\mathrm{Gal}(F/K)$ es un grupo abeliano.

Recordemos el resultado siguiente de Teoría de Galois, que resultará de utilidad más adelante.

Lema 1.50. Sean L/K y F/K dos extensiones finitas de cuerpos, con L/K de Galois. Entonces, $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L \cap F)$.

El siguiente teorema relaciona ciertos grupos de Galois sobre un cuerpo de números K con grupos de clases de ideales de K.

Teorema 1.51. Sean K un cuerpo de números y L su máxima extensión abeliana no ramificada. Entonces, $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K)$.

Demostración. Véase el apéndice 3 de [14]. □

1.5.1. Teoría de Galois infinita.

La topología utilizada en Teoría de Galois infinita es la siguiente.

Definición 1.52. Sea F/K una extensión de cuerpos y $G = \mathrm{Gal}(F/K)$. La **topología de Krull** sobre G se define de manera que un subconjunto $X \subseteq G$ es abierto si es el conjunto vacío o si cumple $X = \bigcup_{i \in I} \sigma_i N_i$ para ciertos $\sigma_i \in G$ y $N_i \leq G$, en que los N_i son tales que $N_i = \mathrm{Gal}(F/E)$ para alguna subextensión de Galois finita E de K.

El Teorema fundamental de la Teoría de Galois es el siguiente.

Teorema 1.53 (Teorema fundamental de la Teoría de Galois). Sea F/K una extensión de Galois y $G = \mathrm{Gal}(F/K)$ con la topología de Krull. Sean

$$\mathcal{A} = \{L \text{ cuerpo } \big| \, K \subseteq L \subseteq F\}, \tag{8}$$

$$\mathcal{B} = \{H \leq G \big| \, H \text{ cerrado en } G\}. \tag{9}$$

Consideremos las aplicaciones $\Psi : \mathcal{A} \longrightarrow \mathcal{B}$ tal que $\Psi(L) = \mathrm{Gal}(F/L)$ y $\Theta : \mathcal{B} \longrightarrow \mathcal{A}$ tal que $\Theta(H) = F^H$, con F^H el subcuerpo fijo de F por H. Entonces, Ψ y Θ son biyecciones, y si $L_1 \subseteq L_2$, entonces $\Psi(L_2) \leq \Psi(L_1)$. Además, si $L \in \mathcal{A}$ se corresponde con $H \in \mathcal{B}$, entonces

1. $|G : H| < \infty \Leftrightarrow [L : K] < \infty \Leftrightarrow H$ es abierto. Además, $|G : H| = [L : K]$.
2. H es subgrupo normal de $G \Leftrightarrow L$ es de Galois sobre K.

Además, si sucede lo anterior, tenemos $G/H \cong \mathrm{Gal}(L/K)$.

Demostración. Véase el teorema 3.3.1 de [13]. □

1.5.2. Grupos de inercia.

Si K/k es una extensión de cuerpos abeliana y de Galois arbitraria, en general $\mathcal{O}_K$ y $\mathcal{O}_k$ no serán dominios de Dedekind, por lo que no podemos definir ramificación vía factorización de primos. Para solucionar este inconveniente, se utilizan los grupos de inercia. Sean $\mathfrak{p} \in \mathcal{O}_k$ y $\mathscr{P} \in \mathcal{O}_K$ primos tales que $\mathfrak{p} = \mathscr{P} \cap \mathcal{O}_k$.

Definición 1.54. El **grupo de descomposición** de $\mathscr{P}$ sobre $\mathfrak{p}$ es

$$D(\mathscr{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K/k) \,\big|\, \sigma\mathscr{P} = \mathscr{P}\}. \tag{10}$$

Definición 1.55. El **grupo de inercia** de $\mathscr{P}$ sobre $\mathfrak{p}$ es

$$I(\mathscr{P}/\mathfrak{p}) = \{\sigma \in D(\mathscr{P}/\mathfrak{p}) \,\big|\, \sigma(\alpha) \equiv \alpha \mod \mathscr{P}, \forall \alpha \in \mathcal{O}_K\}. \tag{11}$$

Observación 1.56. Tenemos la secuencia exacta siguiente:

$$1 \longrightarrow I(\mathscr{P}/\mathfrak{p}) \longrightarrow D(\mathscr{P}/\mathfrak{p}) \longrightarrow \mathrm{Gal}((\mathcal{O}_K/\mathscr{P})/(\mathcal{O}_k/\mathfrak{p})) \longrightarrow 1. \tag{12}$$

Sean K/k una extensión algebraica y $\bar{\mathbb{Q}}$ la clausura algebraica de $\mathbb{Q}$. Las extensiones $\bar{\mathbb{Q}}/K$ y $\bar{\mathbb{Q}}/k$ son extensiones de Galois.[3] Sean $\mathfrak{p} \in \mathcal{O}_k$ y $\mathscr{P} \in \mathcal{O}_K$ primos tales que $\mathfrak{p} = \mathscr{P} \cap \mathcal{O}_k$. Sea $\mathfrak{D} \in \mathcal{O}_{\bar{\mathbb{Q}}}$ un primo tal que $\mathscr{P} = \mathfrak{D} \cap \mathcal{O}_K$.

Definición 1.57. Con la notación anterior, el índice de ramificación de $\mathscr{P}$ sobre $\mathfrak{p}$ se define como $e(\mathscr{P}/\mathfrak{p}) = [T(\mathfrak{D}/\mathfrak{p}) : T(\mathfrak{D}/\mathscr{P})]$.

Notemos que la definición anterior no depende del $\mathfrak{D}$ escogido.

Proposición 1.58. Si la extensión de cuerpos residuales es separable, entonces el índice de ramificación de $\mathscr{P}$ es igual al orden del grupo de inercia de $\mathscr{P}$ sobre $\mathfrak{p}$, es decir,

$$e(\mathscr{P}/\mathfrak{p}) = |I(\mathscr{P}/\mathfrak{p})| \tag{13}$$

Demostración. Véase el apéndice 2 de [14]. □

1.6. Límites proyectivos.

Definición 1.59. Un **sistema proyectivo** de conjuntos es una colección de conjuntos X_i y aplicaciones $\varphi_{ij} : X_j \longrightarrow X_i$ que existen siempre que $i \leq j$, cumpliendo que $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ para todo $i \leq j \leq k$. Lo denotamos por $\{X_i, \varphi_{ij}\}$.

Definición 1.60. Sean X un conjunto, $\{X_i, \varphi_{ij}\}$ un sistema proyectivo de conjuntos, y sean $\psi_i : X \longrightarrow X_i$ aplicaciones. Decimos que las aplicaciones ψ_i son **compatibles** si $\varphi_{ij}\psi_j = \psi_i$ siempre que $i \leq j$. Decimos que (X, ψ_i) forma un **sistema compatible** con $\{X_i, \varphi_{ij}\}$.

Definición 1.61. Sea (X, φ_i) un sistema compatible con el sistema proyectivo $\{X_i, \varphi_{ij}\}$. Decimos que X es un **límite proyectivo** del sistema si cumple que, dado un sistema (Y, ψ_i) compatible con $\{X_i, \varphi_{ij}\}$, entonces existe una única aplicación $\psi : Y \longrightarrow X$ tal que $\varphi_i\psi = \psi_i$. Denotamos $X = \varprojlim X_i$.

El teorema siguiente garantiza la existencia del límite proyectivo, así como su unicidad salvo biyección.

[3] Véase el apéndice 2 de [14].

Teorema 1.62. Si $\{X_i, \varphi_{ij}\}$ es un sistema proyectivo, entonces existe $X = \varprojlim X_i$. Además, si (X, φ_i) y (X', φ_i') son límites proyectivos del sistema, entonces existe una única aplicación biyectiva $\psi : X \longrightarrow X'$ tal que $\varphi_i' \psi = \varphi_i$.

Demostración. Véase el apéndice A de [13]. □

Una propiedad interesante del límite proyectivo es que conserva las estructuras de grupo, anillo y módulo del sistema proyectivo $\{X_i, \varphi_{ij}\}$. Además, presenta la propiedad topológica siguiente.

Proposición 1.63. Si $\{X_i, \varphi_{ij}\}$ es un sistema proyectivo en que los X_i son compactos, entonces $\varprojlim X_i$ también es compacto.

Demostración. Véase el apéndice A de [13]. □

1.6.1. Grupos profinitos.

Una estructura dada por un límite proyectivo es la de grupo proyectivo.

Definición 1.64. Sea $\{G_i, \varphi_{i,j}\}$ un sistema proyectivo, en que los G_i son grupos finitos con la topología discreta y los φ_{ij} son morfismos continuos de grupos. Un grupo G se denomina **grupo profinito** si es un grupo topológico[4] y existen morfismos de grupo φ_i tales que $\{G, \varphi_i\}$ es un sistema compatible con $\{G_i, \varphi_{i,j}\}$ isomorfo al límite proyectivo del sistema $\{G_i, \varphi_{i,j}\}$.

De hecho, el teorema siguiente nos dice que todo grupo profinitio es el grupo de Galois de alguna extensión de cuerpos.

Teorema 1.65 (Teorema de Waterhouse). Sea G un grupo profinito. Entonces, existe una extensión de cuerpos F/K que es de Galois y tal que $G \cong \mathrm{Gal}(F/K)$.

Demostración. Véase el teorema 3.4.1 de [13]. □

1.7. Completaciones.

Definición 1.66. Una **valoración** multiplicativa de un cuerpo K es una función $|\cdot| : K \longrightarrow \mathbb{R}$ que cumple

1. $|x| \geq 0$, y $|x| = 0 \Leftrightarrow x = 0$,
2. $|xy| = |x||y|$,
3. $|x + y| \leq |x| + |y|$.

Decimos que K es un **cuerpo valorado**.

Proposición 1.67. Sea K un cuerpo valorado. Entonces, $\bar{\mathcal{O}}_K = \{x \in K \,\big|\, |x| \geq 1\}$ es un anillo, al que denominamos **anillo de la valoración** $|\cdot|$, $\mathfrak{p}_K = \{x \in K \,\big|\, |x| > 1\}$ es el único ideal máximal de $\bar{\mathcal{O}}_K$, al que denominamos **ideal máximo**, de manera que el cociente $\bar{\mathcal{O}}_K/\mathfrak{p}_K$ es un cuerpo, al que denominamos **cuerpo residual** de K.

Demostración. Véase la proposición 3.8 del capítulo 2 de [6]. □

Definición 1.68. Sea K un cuerpo valorado. Decimos que K es **completo** si toda sucesión de Cauchy $\{a_n\}_{n\in\mathbb{N}}$ converge a un elemento $a \in K$.

[4] Un **grupo topológico** es un grupo equipado con una topología tal que la multiplicación y la inversión son contínuas.

De manera análoga a como $\mathbb{R}$ se obtiene a partir de $\mathbb{Q}$ respecto al valor absoluto, podemos realizar un proceso de **completación** sobre K respecto a una valoración $|\cdot|$ para obtener un cuerpo valorado $\hat{K}$ que sea completo respecto $|\cdot|$.

Definición 1.69. Un **cuerpo global** es una extensión finita de $\mathbb{Q}$ o de $\mathbb{F}_p(t)$. Un **cuerpo local** L es todo cuerpo con una valoración $|\cdot|$ tal que L sea completo respecto a $|\cdot|$ y tal que su cuerpo residual sea finito.

De hecho, podemos caracterizar un cuerpo local en base a la proposición siguiente.

Proposición 1.70. Una extensión finita de $\mathbb{Q}_p$ o de $\mathbb{F}_p((t))$ es un cuerpo local.

Demostración. Véase la proposición 5.2 del capítulo 2 de [6]. □

Sea K un cuerpo de números. Dado un primo $\mathfrak{p} \in \mathcal{O}_K$, éste permite definir una valoración[5], y por ello, realizar una completación de K, que denotamos por $K_\mathfrak{p}$. Además, $K_\mathfrak{p}$ tiene cuerpo residual finito, por lo que es un cuerpo local.

Definición 1.71. Sea L un cuerpo local. El grupo de **unidades locales** de L es

$$U = \{x \in L \,\big|\, |x| = 1\}. \tag{14}$$

El grupo de **unidades principales** de L es

$$U_1 = 1 + \mathfrak{p}_L = \{x \in \bar{\mathcal{O}}_L \,\big|\, x \equiv 1 \mod \mathfrak{p}_L\}. \tag{15}$$

Definición 1.72. Sea K un cuerpo de números. El grupo de **unidades globales** de K es $\mathcal{O}_K^\times$.

Teorema 1.73 (Teorema de Dirichlet). Sean K un cuerpo de números y $\mathcal{O}_K^\times$ el grupo de unidades del anillo de enteros de K. Entonces, $\mathcal{O}_K^\times$ es un grupo abeliano finitamente generado isomorfo a $\mathbb{Z}^{r_1+r_2-1} \oplus \mu(K)$, con $\mu(K)$ el grupo cíclico de las raíces de la unidad de K, r_1 el número de inmersiones reales de K y r_2 el número de inmersiones complejas.

Demostración. Véase el teorema 7.4 del capítulo 1 de [6]. □

[5]Dado un elemento $x \in \mathcal{O}_K$, el teorema 1.30 nos da una descomposición $(x) = \mathfrak{p}^n\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\cdots$ para ciertos $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ primos de $\mathcal{O}_K$. Esto nos permite definir una valoración dada por $|x|_\mathfrak{p} = 1/|\mathcal{O}_K/\mathfrak{p}|^n$.

2. $\mathbb{Z}_p$–extensiones.

En este capítulo construimos el anillo $\mathbb{Z}_p$ de los enteros p–ádicos, interpretándolo como el límite proyectivo de los anillos $\mathbb{Z}/p^n\mathbb{Z}$. A continuación, definimos una $\mathbb{Z}_p$–extensión de un cuerpo de números y vemos que todo cuerpo de números tiene siempre almenos una de estas extensiones, la extensión ciclotómica. Finalmente, enunciamos la conjetura de Leopold, que nos permite determinar el número de $\mathbb{Z}_p$-extensiones independientes que puede tener un cuerpo de números.

2.1. Enteros p–ádicos.

Los números p–ádicos surgen con la finalidad de incorporar las expansiones en series de potencias dentro de la teoría de números cuando pensamos en la valoración dada por el ideal (p) de $\mathbb{Z}$ y por un límite de sucesiones de Cauchy en $\mathbb{Z}$ con la valoración dada por (p).

Sea p un primo fijo y consideremos $\mathbb{Q}$ con la valoración $|\cdot|_p$ dada por el ideal (p). Denotamos por $\mathbb{Q}_p$ la completación de $\mathbb{Q}$ respecto $|\cdot|_p$. Consideremos en $\mathbb{Q}_p$ una expansión

$$f = \sum_{i=0}^{\infty} a_i p^i, \tag{16}$$

con $0 \leq a_i \leq p-1$. Notemos que la expansión anterior tiene sentido en $\mathbb{Q}_p$, pues ésta es el límite por $|\cdot|_p$ de la sucesión $\{s_n\}_{n\in\mathbb{N}}$ dada por

$$s_n = \sum_{i=0}^{n} a_i p^i \in \mathbb{N} \tag{17}$$

Definición 2.1. El conjunto de todos los elementos f obtenidos de la manera anterior se denota por $\mathbb{Z}_p$, y sus elementos se denominan **enteros p–ádicos**.

Lema 2.2. $\mathbb{Z}_p$ es la completación de $\mathbb{Z}$ respecto a la valoración $|\cdot|_p$.

Demostración. Como $\{s_n\}_{n\in\mathbb{N}}$ es una sucesión de Cauchy respecto (p), es suficiente demostrar que $\mathbb{Z} \subseteq \mathbb{Z}_p$. Para ello, es suficiente observar que $-1 = \sum_{i=0}^{\infty}(p-1)p^i$. □

Los elementos de $\mathbb{Z}_p$ pueden interpretarse, por un lado, como secuencias de sumas de enteros,

$$s_n = \sum_{i=0}^{n} a_i p^i, \tag{18}$$

y por otro, como secuencias de clases de residuos,

$$\bar{s}_n = s_n \bmod p^n. \tag{19}$$

Los elementos de esta última secuencia pertenecen a diferentes anillos $\mathbb{Z}/p^n\mathbb{Z}$ con $n > 0$, que se relacionan mediante proyecciones canónicas

$$\begin{aligned} \lambda_n : \mathbb{Z}/p^{n+1}\mathbb{Z} &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ \bar{s}_{n+1} &\longmapsto \bar{s}_n \end{aligned} \tag{20}$$

Si consideramos elementos $(x_n)_{n\in\mathbb{N}}$ del espacio producto $\prod_{n=1}^{\infty}\mathbb{Z}/p^n\mathbb{Z}$ tales que $\lambda_n(x_{n+1}) = x_n$, obtenemos el límite proyectivo de los anillos $\mathbb{Z}/p^n\mathbb{Z}$.

Proposición 2.3. La asociación de elementos de $\mathbb{Z}_p$ con secuencias de clases de residuos en $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ constituye una biyección, de manera que

$$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}. \tag{21}$$

Demostración. Véase la proposición 1.3 del capítulo 2 de [6]. □

Notemos que $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ es un subanillo de $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ en que las operaciones suma y productos se definen componente a componente, por lo que $\mathbb{Z}_p$ también es un anillo. Además, se puede demostrar que todo elemento $f \in \mathbb{Q}_p$ admite una representación $f = p^{-m}g$ para ciertos $m \in \mathbb{Z}$ y $g \in \mathbb{Z}_p$, de donde se tiene que $\mathbb{Q}_p$ es el cuerpo de fracciones de $\mathbb{Z}_p$.

2.2. $\mathbb{Z}_p$–extensiones.

Definición 2.4. Sea K un cuerpo de números. Una extensión K_∞/K es una **$\mathbb{Z}_p$–extensión** si $\mathrm{Gal}(K_\infty/K) \cong (\mathbb{Z}_p, +)$.

Tener una $\mathbb{Z}_p$–extensión es equivalente a tener una cadena de cuerpos

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \cup K_n, \tag{22}$$

tales que $\mathrm{Gal}(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z}, +)$. Además, las aplicaciones $\mathrm{Gal}(K_n/K) \longrightarrow \mathrm{Gal}(K_{n-1}/K)$ dadas por $\sigma \mapsto \sigma_{K_{n-1}}$ corresponden a los morfismos de proyección $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}$.

Para ver un ejemplo de $\mathbb{Z}_p$ extensión, consideremos $\mathbb{F}_p$ el cuerpo finito de p elementos, $\bar{\mathbb{F}}_p$ su clausura algebraica y $\mathbb{F}_{p^n} = \{x \in \bar{\mathbb{F}}_p \mid x^{p^n} = x\}$. Recordemos que el endomorfismo de Frobenius $F_n : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ es un morfismo de cuerpos dado por $F_n(x) = x^p$.

Lema 2.5. $\mathbb{F}_{p^n}/\mathbb{F}_p$ es una extensión de Galois no finita, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ está generado por el endomorfismo de Frobenius y $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si $n|m$.

Demostración. Véanse los lemas 3.1.3 y 3.1.4 de [13]. □

Si definimos $\mathbb{F}_{p^{p^\infty}} = \cup_n \mathbb{F}_{p^{p^n}}$, la proposición siguiente nos dice que la extensión $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ es una $\mathbb{Z}_p$–extensión.

Proposición 2.6. Se cumple que

$$\mathrm{Gal}(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p) \cong \varprojlim \mathrm{Gal}(\mathbb{F}_{p^{p^n}}/\mathbb{F}_p) \cong (\mathbb{Z}_p, +). \tag{23}$$

Demostración. Para el primer isomorfismo, véase la proposición 3.1.6 de [13].

Para el segundo, notemos que $[\mathbb{F}_{p^{p^n}} : \mathbb{F}_p] = p^n$, por lo que $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong (\mathbb{Z}/p^n\mathbb{Z}, +)$, de manera que $\varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong (\mathbb{Z}_p, +)$. □

El lema siguiente proporciona información sobre la ramificación en $\mathbb{Z}_p$–extensiones de cuerpos de números.

Lema 2.7. Sean K un cuerpo de números y K_∞/K una $\mathbb{Z}_p$–extensión. Entonces, al menos un primo ramifica en esta extensión, y existe un $n \geq 0$ tal que todo primo que ramifica en K_∞/K_n está totalmente ramificado.

Demostración. Véase la proposición 13.1 de [14]. □

Notemos que el lema anterior sólo es válido para cuerpos de números, pues por ejemplo la extensión $\mathbb{F}_{p^n}/\mathbb{F}_p$ no ramifica en ningún primo.

2.3. $\mathbb{Z}_p$–extensiones ciclotómicas.

Si K es un cuerpo de números, veremos a continuación que éste tiene siempre al menos una $\mathbb{Z}_p$–extensión, la $\mathbb{Z}_p$–extensión ciclotómica. Sea $\bar{\mathbb{Q}}$ la clausura algebraica de $\mathbb{Q}$, y consideremos $\mu_m = \{x \in \bar{\mathbb{Q}} \,|\, x^m = 1\}$ el grupo de raíces m–ésimas de la unidad, que es un grupo cíclico de orden m generado por las raíces primitivas. Sea $\mu_{p^\infty} = \{x \in \bar{\mathbb{Q}} \,|\, x \in \mu_{p^n} \text{ para algún } n \in \mathbb{N}\}$.

La extensión $K(\mu_{p^\infty})/K$ es una extensión de Galois, pues es separable por estar en característica cero y normal por ser $K(\mu_{p^\infty})$ el cuerpo de descomposición de la familia de polinomios $\{x^{p^n} - 1\}_{n\in\mathbb{N}}$. Si $K = \mathbb{Q}$, es conocido que $[\mathbb{Q}(\mu_{p^n}) : \mathbb{Q}] = \deg \Phi_n(x)$, donde $\Phi_n(x)$ es el n–ésimo polinomio ciclotómico, que puede obtenerse a partir de la igualdad $x^n - 1 = \prod_{d|n} \Phi_d(x)$. De ello se deduce que $K(\mu_{p^\infty})/K$ es una extensión no finita.

Pensemos ahora $K = \mathbb{Q}$ y sea p un primo impar. Sea ξ_{p^n} una raiz primitiva p^n–ésima de la unidad y consideremos la aplicación $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$ tal que si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$ es tal que $\sigma(\xi_{p^n}) = \xi_{p^n}^a$ cumpliendo $\mathrm{mcd}(a, p^n) = 1$, ya que entonces $\xi_{p^n}^a$ también es una raiz primitiva p^n–ésima de la unidad, entonces la imagen de σ por la aplicación es a. La aplicación anterior es, de hecho, un isomorfismo de grupos. Además, la aplicación es compatible con el límite proyectivo, de manera que

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \cong (\mathbb{Z}_p^\times, *). \tag{24}$$

Puede verse que el grupo multiplicativo $(\mathbb{Z}_p^\times, *)$ es isomorfo a $(\mathbb{Z}/(p-1)\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)$, o equivalentemente a $(\mathbb{Z}/(p)\mathbb{Z})^\times \times (\mathbb{Z}_p, +)$, con este último isomorfismo dado vía logaritmo p–ádico[6]. Por ello, los subgrupos cerrados de $\mathbb{Z}_p^\times$ no finitos serán de la forma $H \times (0)$, con $H \leq (\mathbb{Z}/(p)\mathbb{Z})^\times$. Si escogemos $H = (\mathbb{Z}/p\mathbb{Z})^\times$ y pasamos a $\hat{H} \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ vía isomorfismo, escogiendo el cociente $H_\infty = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})/\hat{H}$ tenemos que $H_\infty \cong (\mathbb{Z}_p, +)$, y si consideramos el cuerpo fijo por H_∞, vemos que $\mathbb{Q}(\mu_{p^\infty})$ contiene un único subcuerpo $\mathbb{Q}_\infty$ tal que $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. Decimos que $\mathbb{Q}_\infty$ es la **$\mathbb{Z}_p$–extensión ciclotómica** de $\mathbb{Q}$.

Para K un cuerpo de números cualquiera, el morfismo $\mathrm{Gal}(K(\mu_{p^\infty})/K) \longrightarrow \mathbb{Z}_p^\times$ será inyectivo, y en consecuencia, $\mathrm{Gal}(K(\mu_{p^\infty})/K)$ será isomorfo a un subgrupo cerrado e infinito de $\mathbb{Z}_p^\times$. A partir de ello, es fácil ver que $K(\mu_{p^\infty})$ contiene un único subcuerpo K_∞ tal que $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Éste K_∞ es la **$\mathbb{Z}_p$–extensión ciclotómica** de K, que cumple $K_\infty = K\mathbb{Q}_\infty$.

2.4. Conjetura de Leopoldt.

Sea K un cuerpo de números y p un primo impar. Sea $\mathfrak{p}$ un primo sobre p, es decir, tal que $\mathfrak{p} \cap \mathcal{O}_K = (p)$, y consideremos el cuerpo $K_\mathfrak{p}$. Para cada $\mathfrak{p}$, sean $U_\mathfrak{p}$ el grupo de unidades locales de $K_\mathfrak{p}$ y $U_{1,\mathfrak{p}}$ el grupo de unidades principales. Sean

$$U = \prod_{\mathfrak{p}|p} U_\mathfrak{p}, \qquad U_1 = \prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}. \tag{25}$$

Sea E el grupo de unidades globales de K, y consideremos la inmersión $E \longrightarrow U$ tal que $\varepsilon \mapsto (\varepsilon, \ldots, \varepsilon)$. Sea E_1 el subgrupo de E cuyos elementos tienen imagen en U_1 por la aplicación anterior. Del teorema de Dirichlet se deduce que E_1 es un grupo abeliano de rango $r = r_1 + r_2 - 1$,

[6] Dado un cuerpo de números K, existe un único morfismo continuo $\log : K^\times \longrightarrow K$ tal que $\log p = 0$ y que viene dado en sus unidades principales por la serie formal $\log(1+x) = \sum_{i=1}^\infty \frac{(-1)^{i+1}x^i}{i}$. A esta función se la denomina **logaritmo p–ádico**. Véase la proposición 5.4 de [6].

con r_1 el número de inmersiones reales de K y r_2 el número de inmersiones complejas.

Notemos que U_1 es un grupo abeliano y profinito. Tenemos el teorema siguiente.

Teorema 2.8. Sea G un grupo abeliano profinito y $m \in G$ un elemento de torsión. Entonces, $G \cong \prod_p (\prod_{m(p)} \mathbb{Z}_p)$, donde p recorre todos los primos de p y $m(p)$ es un número cardinal. Si G es finitamente generado, entonces $m(p)$ es un natural que vale cero para cualquier p. En este caso, el $\mathbb{Z}_p$–rango de G es $m(p)$.

Demostración. Véase [10]. □

Si consideramos $\bar{E}_1$ la clausura de E_1 por la topología en U_1 tenemos la conjetura siguiente.

Conjetura 2.9 (Conjetura de Leopoldt). El $\mathbb{Z}_p$–rango de $\bar{E}_1$ es $r_1 + r_2 - 1$.

Puede verse[7] que existe una aplicación natural $f_p : E \otimes \mathbb{Z}_p \longrightarrow U$. El **defecto de Leopoldt** δ se define como el $\mathbb{Z}_p$–rango de $\operatorname{Ker} f_p$. La conjetura de Leopoldt es equivalente a suponer que $\delta = 0$. El resultado siguiente resulta fundamental a la hora de contar $\mathbb{Z}_p$–extensiones.

Proposición 2.10. El número de $\mathbb{Z}_p$–extensiones independientes[8] de K es $1 + r_2 + \delta$.

Suponiendo cierta la Conjetura de Leopoldt, la proposición anterior nos dice que hay exactamente $1 + r_2$ $\mathbb{Z}_p$–extensiones independientes de K.

Como ejemplo de este resultado, consideremos el cuerpo de números cuadrático $\mathbb{Q}(\sqrt{D})$, con $D > 0$ y libre de cuadrados. En este caso, las únicas inmersiones posibles de $\mathbb{Q}(\sqrt{D})$ son aquellas tales que $\sqrt{D}$ va a parar a una raíz de $\operatorname{Irr}(\sqrt{D}, \mathbb{Q}) = x^2 - D$, es decir, a $\sqrt{D}$ o a $-\sqrt{D}$. Por tanto, ambas inmersiones serán reales, de manera que tenemos $r_1 = 2$ y $r_2 = 0$. Así, el número de $\mathbb{Z}_p$–extensiones independientes de $\mathbb{Q}(\sqrt{D})$ es 1. Como en todo cuerpo de números, podemos considerar la $\mathbb{Z}_p$–extensión ciclotómica, por lo que ésta será la única $\mathbb{Z}_p$–extensión de $\mathbb{Q}(\sqrt{D})$.

[7] Véase el teorema 10.3.6 de [7].

[8] Dado un cuerpo de números K y una extensión abeliana no finita de K, su parte libre de torsión es un grupo abeliano profinito finitamente generado. Sea $m(p)$ como en el teorema 2.8. La p–parte del grupo anterior corresponde a $\prod_{m(p)} \mathbb{Z}_p$ y da $m(p)$ $\mathbb{Z}_p$–extensiones, que decimos que son independientes.

3. $\mathbb{Z}_p[[T]]$–módulos.

Comenzaremos este capítulo definiendo el conjunto de series formales sobre un anillo de enteros, que nos permitirá considerar módulos sobre el anillo $\mathbb{Z}_p[[T]]$. El resultado principal del capítulo, que demostraremos extendidamente, nos permitirá clasificar los $\mathbb{Z}_p[[T]]$–módulos mediante una relación estructural especial, el pseudo–isomorfismo.

3.1. Álgebra de Iwasawa.

Definición 3.1. El conjunto de series formales en T sobre $\mathbb{Z}_p$ es

$$\mathbb{Z}_p[[T]] = \left\{ \sum_{i=0}^{\infty} a_i T^i \,\middle|\, a_i \in \mathbb{Z}_p \right\}. \tag{26}$$

Estructuralmente, $\mathbb{Z}_p[[T]]$ es un álgebra conmutativa, es decir, un grupo abeliano dotado de una multiplicación y un producto tal que, considerando la multiplicación, $\mathbb{Z}_p[[T]]$ es un anillo conmutativo, y considerando el producto, es un módulo.

Definición 3.2. Llamamos a $\mathbb{Z}_p[[T]]$ **álgebra de Iwasawa**, y lo denotamos por Λ.

La proposición siguiente caracteriza el algoritmo de la división en $\mathbb{Z}_p[[T]]$.

Proposición 3.3. Sean $f, g \in \mathbb{Z}_p[[T]]$ y supongamos que $f = a_0 + a_1 T + \ldots$ es tal que para algún n se tiene que todos los coeficientes a_i con $0 \leq i \leq n-1$ son divisibles por p, pero que a_n no lo es. Entonces, podemos escribir de manera única $g = qf + r$ con $q \in \mathbb{Z}_p[[T]]$ y $r \in \mathbb{Z}_p[T]$ un polinomio de grado menor o igual a $n-1$.

Demostración. Véase la proposición 7.2 de [14]. □

La proposición anterior resulta de especial interés si f es un polinomio distinguido.

Definición 3.4. Un polinomio en $\mathbb{Z}_p[T]$ es **distinguido** si es mónico y todos los coeficientes salvo el de mayor grado son divisibles por p.

Corolario 3.5. Sean $g \in \mathbb{Z}_p[[T]]$ y $f \in \mathbb{Z}_p[T]$ un polinomio distinguido. Entonces, podemos escribir de manera única $g = qf + r$ con $q \in \mathbb{Z}_p[[T]]$ y $r \in \mathbb{Z}_p[T]$ un polinomio tal que $\deg r < \deg f$.

El teorema siguiente resulta de especial utilidad.

Teorema 3.6 (Teorema de Preparación de Weierstrass). Sea

$$f(T) = \sum_{i=0}^{\infty} a_i T^i \tag{27}$$

una serie de potencias en $\mathbb{Z}_p[[T]]$ tal que para algún n se tiene que todos los a_i con $0 \leq i \leq n-1$ son divisibles por p, pero a_n no lo es (por lo que $a_n \in \mathbb{Z}_p^{\times}$). Entonces, f puede escribirse de manera única de la forma

$$f(T) = P(T)U(T), \tag{28}$$

con $U(T) \in \mathbb{Z}_p[[T]]$ una unidad y $P(T) \in \mathbb{Z}_p[T]$ un polinomio distinguido de grado n. Más en general, si $f \in \mathbb{Z}_p[[T]]$ es no nulo y arbitrario, entonces puede escribirse de manera única de la forma

$$f(T) = p^{\mu} P(T) U(T) \tag{29}$$

con $U(T) \in \mathbb{Z}_p[[T]]$ una unidad, $P(T) \in \mathbb{Z}_p[T]$ un polinomio distinguido y $\mu \geq 0$.

Demostración. Véase el teorema 7.3 de [14]. □

Notemos que si en el teorema anterior $f(T)$ es un polinomio, entonces $U(T)$ también lo es.

3.2. Propiedades de $\mathbb{Z}_p[[T]]$.

Sea Γ un grupo topológico multiplicativo, isomorfo al grupo aditivo $\mathbb{Z}_p$ y γ un generador topológico fijo de Γ tal que el ismorfismo $\mathbb{Z}_p \cong \Gamma$ venga dado por $x \mapsto \gamma^x$. Sea $\Gamma_n = \Gamma/\Gamma^{p^n}$, que es un grupo cíclico de orden p^n generado por la imagen de γ.

Proposición 3.7. Por un lado, se tiene que

$$\varprojlim \mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[[\Gamma]]. \tag{30}$$

Por otro lado, se tiene el isomorfismo

$$\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]], \tag{31}$$

dado por $\gamma \mapsto 1 + T$.

Demostración. A continuación, relizaremos unos breves comentarios sobre la demostración. Para más, véase la demostración teorema 7.1 en [14].

Respecto al primer isomorfismo, notemos que si $m \geq n \geq 0$, el morfismo natural $\Gamma_m \longrightarrow \Gamma_n$ induce una aplicación $\phi_{m,n} : \mathbb{Z}_p[\Gamma_m] \longrightarrow \mathbb{Z}_p[\Gamma_n]$, de manera que $\{\Gamma_n, \phi_{m,n}\}$ forman un sistema proyectivo, cuyo límite proyectivo es, en efecto, $\mathbb{Z}_p[[\Gamma]]$.

Respecto al segundo isomorfismo, sea $P_n(T) = (1+T)^{p^n} - 1$, que es un polinomio distinguido. Notemos que $\mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[T]/(P_n(T))$, de manera que $\gamma \mod \Gamma^{p^n} \mapsto 1 + T \mod (P_n(T))$. Aplicando el primer isomorfismo, tenemos $\mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[T]/(P_n(T))$. Mediante un proceso de inducción puede verse que $P_n(T) \in (p, T)^{n+1}$, y aplicando el corolario 3.5 se tienen aplicaciones naturales f_n de $\mathbb{Z}_p[[T]]$ a $\mathbb{Z}_p[T] \mod P_n(T)$ para cada n, tales que si $m \geq n \geq 0$, entonces $f_m \equiv f_n \mod P_n$ como polinomios, de donde se deduce que $(f_0, f_1, \dots) \in \varprojlim \mathbb{Z}_p[T]/(P_n(T))$. Esto da una aplicación de $\mathbb{Z}_p[[T]]$ a $\mathbb{Z}_p[T]/(P_n(T))$ que puede verse que es bijectiva, obteniéndose así el isomorfismo. □

Es conocido que Λ es un dominio de factorización única. La proposición siguiente determina los elementos irreductibles, las unidades y los ideales primos de Λ.

Proposición 3.8.

1. Los elementos irreductibles de Λ son p y los polinomios distinguidos e irreductibles.
2. Las unidades de Λ son las series de potencias de término constante en $\mathbb{Z}_p^\times$.
3. Los ideales primos de Λ son 0, (p, T), (p), y los ideales $(P(T))$ con $P(T)$ un polinomio distinguido e irreductible. El ideal (p, T) es el único ideal maximal.

Demostración. Véase la proposición 13.9 de [14]. □

La proposición 3.7 nos permite identificar $\Lambda = \mathbb{Z}_p[[T]]$ con el límite proyectivo de los anillos de polinomios $\mathbb{Z}_p[\Gamma_n]$, de manera que

$$\varprojlim \mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[[T]] \tag{32}$$

Otras propiedades de Λ que nos serán de utilidad posteriormente vienen dadas por el lema siguiente.

Lema 3.9. Sean $f, g \in \Lambda$ coprimos.

1. Λ es un anillo noetheriano.

2. El ideal (f, g) es de índice finito en Λ.

3. La aplicación natural
$$\Lambda/(fg) \longrightarrow \Lambda/(f) \oplus \Lambda/(g) \tag{33}$$
es inyectiva y tiene cokernel finito. Además, existe una aplicación inyectiva
$$\Lambda/(f) \oplus \Lambda/(g) \longrightarrow \Lambda/(fg) \tag{34}$$
con cokernel finito.

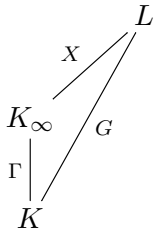
Demostración. Véanse los lemas 13.11, 13.7 y 13.8 de [14]. □

3.3. Ejemplo de $\mathbb{Z}_p[[T]]$–módulo.

Sea K un cuerpo de números y consideremos una $\mathbb{Z}_p$–extensión K_∞/K. Sea $\Gamma = \mathrm{Gal}(K_\infty/K) \cong (\mathbb{Z}_p, +)$ y γ_0 un generador topológico fijo de Γ tal que el isomorfismo $\mathbb{Z}_p \cong \Gamma$ venga dado por $x \mapsto \gamma^x$. La $\mathbb{Z}_p$–extensión K_∞/K es equivalente a la cadena de cuerpos
$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \cup K_n, \tag{35}$$
en que los K_n cumplen que $\mathrm{Gal}(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z}, +)$. Sea L_n la máxima p–extensión abeliana no ramificada de cada K_n, y sea $X_n = \mathrm{Gal}(L_n/K_n)$. Definimos $L = \bigcup_{n\geq 0} L_n$ y $X = \mathrm{Gal}(L/K_\infty)$. Notemos que existe una cadena de cuerpos
$$L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \cdots \subseteq L = \cup L_n. \tag{36}$$

Veamos que cada extensión L_n/K es de Galois. Por un lado, la extensión es separable porque las extensiones finitas K_n/K y L_n/K_n lo son. Por otro lado, sea $\bar{K}$ la clausura algebraica de K, y pensemos en todas las extensiones F de K dentro de $\bar{K}$. Dado $\sigma \in \mathrm{Aut}_K(\bar{K})$, la extensión finita F/K es normal si y solo si $\sigma(F) = F$. La extensión $\sigma(L_n)/K_n$ es una p–extensión abeliana no ramificada, pero como la extensión L_n/K_n es la máxima p–extensión no abeliana no ramificada, entonces debe ser $\sigma(L_n) = L_n$, por lo que L_n/K es una extensión normal, y por tanto, de Galois.

Como cada L_n/K es de Galois, la extensión L/K también lo es, así que sea $G = \mathrm{Gal}(L/K)$. Tenemos el siguiente diagrama



Por el Teorema fundamental de la Teoría de Galois, tenemos $\Gamma = G/X$. Realicemos la suposición siguiente.

Suposición: Todos los primos que están ramificados en K_∞/K están totalmente ramificados.

Consideremos la torre de cuerpos $K_n \subseteq L_n \cap K_{n+1} \subseteq K_{n+1}$. Como la extensión K_{n+1}/K_n es de grado p, entonces la extensión $L_n \cap K_{n+1}/K_n$ solo puede tener grados 1 o p. Si la extensión

tiene grado 1, entonces $L_n \cap K_{n+1} = K_n$, mientras que si tiene grado p, $L_n \cap K_{n+1} = K_{n+1}$. Por el lema 2.7, existe un primo $\mathfrak{p} \in K_n$ que ramifica en K_{n+1}, y por la Suposición este primo ramifica totalmente. Sin embargo, L_n es una extensión no ramificada de K_n, por lo que p no puede ramificar en $L_n \cap K_{n+1}$, de manera que $L_n \cap K_{n+1} \neq K_{n+1}$, por lo que debe ser

$$L_n \cap K_{n+1} = K_n. \tag{37}$$

Aplicando el lema 1.50, tenemos

$$X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_{n+1}/K_{n+1}). \tag{38}$$

Notemos que X_n es un cociente de $X_{n+1} = \mathrm{Gal}(L_{n+1}/K_{n+1})$, pues por el teorema fundamental de la Teoría de Galois tenemos $\mathrm{Gal}(L_nK_{n+1}/K_{n+1}) \cong \mathrm{Gal}(L_{n+1}/K_{n+1})/\mathrm{Gal}(L_{n+1}/L_nK_{n+1})$, es decir, $X_n \cong X_{n+1}/\mathrm{Gal}(L_{n+1}/L_nK_{n+1})$.

De manera análoga obtendríamos $X_n \cong \mathrm{Gal}(L_nK_{n+1}K_{n+2}/K_{n+2}) = \mathrm{Gal}(L_nK_{n+2}/K_{n+2})$, e iterando el proceso, $X_n \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$.

Consideremos el sistema proyectivo formado por los grupos X_i y, cuando $i \leq j$, las aplicaciones $\pi_{ij} : X_j \longrightarrow X_i$ definidas como la composición de las proyecciones al cociente $X_j \to \ldots \to X_i$. Consideremos aplicaciones $\varphi_i : X \longrightarrow X_i$, pensadas como $\varphi_i : \mathrm{Gal}(L/K_\infty) \longrightarrow \mathrm{Gal}(L_iK_\infty/K_\infty)$, definidas por $\varphi_i(\sigma) = \sigma|_{L_iK_\infty}$. Estas aplicaciones cumplen $\pi_{ij}\varphi_j = \varphi_i$, por lo que el sistema (X, φ_i) forma un sistema compatible con $\{X_i, \pi_{ij}\}$. Sea (Y, ψ_i) otro sistema compatible con $\{X_i, \pi_{ij}\}$. Si $y \in Y$, para cada i tenemos $\psi_i(y) = \sigma_i$ para cierto $\sigma_i \in X_i$, cumpliendo $\pi_{ij}\psi_j = \psi_i$. Definiendo $\psi : Y \longrightarrow X$ según $\psi(y) = \sigma$, con $\sigma \in X$ tal que $\sigma|_{X_i} = \sigma_i$ para cada i, tenemos que $\psi_i = \varphi_i\psi$. Por tanto, tenemos que (X, φ_n) es el límite proyectivo de $\{X_n, \pi_{ij}\}$, por lo que

$$\varprojlim X_n \cong \varprojlim \mathrm{Gal}(L_nK_\infty/K_\infty) = \mathrm{Gal}(L/K_\infty) = X \tag{39}$$

Sean $\Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z} \cong \mathrm{Gal}(K_n/K)$ y $\gamma \in \Gamma_n$. Extendemos γ a $\tilde{\gamma} \in \mathrm{Gal}(L_n/K)$, de manera que la acción de $\gamma \in \Gamma_n$ sobre $x \in X_n = \mathrm{Gal}(L_n/K_n)$ viene dada por $x^\gamma = \tilde{\gamma}x(\tilde{\gamma})^{-1}$. Veamos que x^γ está bien definido. Por un lado, como $\mathrm{Gal}(L_n/K) \subseteq \mathrm{Gal}(L_n/K_n)$, tenemos que $x^\gamma \in X_n = \mathrm{Gal}(L_n/K_n)$. Por otro lado, si $\hat{\gamma}_1, \hat{\gamma}_2$ son dos extensiones de γ, como $\mathrm{Gal}(L_n/K_n)$ es abeliano tenemos

$$\hat{\gamma}_2^{-1}\hat{\gamma}_1 x \hat{\gamma}_1^{-1}\hat{\gamma}_2 = (\hat{\gamma}_2^{-1}\hat{\gamma}_1)(\hat{\gamma}_1^{-1}\hat{\gamma}_2)x = (\hat{\gamma}_1^{-1}\hat{\gamma}_2)^{-1}(\hat{\gamma}_1^{-1}\hat{\gamma}_2)x = x, \tag{40}$$

de donde se deduce que $\hat{\gamma}_1 x \hat{\gamma}_1^{-1} = \hat{\gamma}_2 x \hat{\gamma}_2^{-1}$, por lo que x^γ no depende de la elección de $\hat{\gamma}$. Notemos que el producto por escalares inducido por la acción anterior permite ver X_n como un $\mathbb{Z}_p[\Gamma_n]$–módulo.

Si representamos un elemento de $X \cong \varprojlim X_n$ como un vector $(x_0, x_1, \ldots)$, con $x_n \in X_n$, y dejando $\mathbb{Z}_p[\Gamma_n]$ actuar en la n–ésima componente, puede verse que X se vuelve un módulo sobre $\varprojlim \mathbb{Z}_p[\Gamma_n]$, y por (32), sobre $\Lambda = \mathbb{Z}_p[[T]]$. Por tanto, hemos visto que X es un Λ–módulo.

3.4. Teorema de clasificación de $\mathbb{Z}_p[[T]]$–módulos.

Un pseudo–isomorfismo permite establecer una relación de estructura menos restrictiva que el isomorfismo.

Definición 3.10. Decimos que dos Λ–módulos M y M' son **pseudo–isomorfos**, y lo denotamos por $M \sim M'$, si existe un morfismo de Λ–módulos $M \longrightarrow M'$ con kernel y cokernel finitos.

Notemos que el kernel y el cokernel de un pseudo–isomorfismo también son Λ–módulos. En general, $M \sim M'$ no implica $M' \sim M$, aunque en determinadas circunstancias, como que M y M' sean Λ–módulos de torsión finitamente generados, sí se tiene que $M \sim M'$ implica $M' \sim M$.

El teorema siguiente permite clasificar los Λ–módulos finitamente generados vía pseudo–isomorfismos.

Teorema 3.11 (**Teorema de clasificación de Λ–módulos**). Sea M un Λ–módulo finitamente generado. Entonces,

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

con $r, s, t, n_i, m_j \in \mathbb{Z}$ y f_j distinguidos e irreductibles.

3.4.1. Demostración.

Sea $\{u_1 \ldots, u_n\}$ un sistema de n generadores de M, que es un Λ–módulo finitamente generado. Sea

$$R = \{(\lambda_1, \ldots, \lambda_n) \in \Lambda^n \,\big|\, \lambda_1 u_1 + \cdots + \lambda_n u_n = 0\} \tag{41}$$

el módulo de relaciones entre $u_1 \ldots, u_n$, que corresponde al núcleo de la aplicación exhaustiva $\varphi : \Lambda^n \longrightarrow M$ definida por $\varphi(\lambda_1, \ldots, \lambda_n) = \lambda_1 u_1 + \cdots + \lambda_n u_n$. Notemos que, por el Teorema de Isomorfía, tenemos $M \cong \Lambda^n / R$. Por el lema 3.9–1, Λ es un módulo noetheriano, por lo que también lo es Λ^n, y como todo submódulo de un módulo noetheriano finitamente generado es finitamente generado, entonces R es finitamente generado. Esto nos permite representar M como una matriz finita, que denotaremos por $\hat{R}$, cuyas filas son relaciones de la forma $(\lambda_1, \ldots, \lambda_n)$ que generan R.

Las transformaciones por filas y columnas sobre la matriz $\hat{R}$ corresponden cambiar los generadores de R y M respectivamente. Recordemos a continuación las transformaciones usuales, que conservan la estructura del módulo mediante un isormorfismo.

Transformación A: Podemos permutar dos filas (o columnas).
Transformación B: Podemos añadir a una fila (o columna) un múltiplo de otra fila (o columna).
Transformación C: Podemos multiplicar una fila (o columna) por un elemento de $\Lambda^\times$.

A estas transformaciones añadiremos tres más, que resultan permisibles al considerar el pseudo-isomorfismo, de manera que si $\hat{R}$ transforma en $\hat{R}'$, entonces $M \sim M'$.

Transformación 1: Si $\hat{R}$ contiene una fila de la forma $(\lambda_1, p\lambda_2, \ldots, p\lambda_n)$ en que p no divide a λ_1, entonces podemos cambiar $\hat{R}$ por la matriz $\hat{R}'$ cuya primera fila es $(\lambda_1, \ldots, \lambda_n)$ y sus otras filas corresponden al resto de filas de $\hat{R}$, pero con sus primeros elementos multiplicados por p.

Demostración. La fila $(\lambda_1, p\lambda_2, \ldots, p\lambda_n)$ corresponde con la relación

$$\lambda_1 u_1 + p(\lambda_2 u_2 + \cdots + \lambda_n u_n) = 0. \tag{42}$$

Sea $M' = M \oplus v\Lambda$, con $v \in M$ un nuevo generador, módulo las relaciones adicionales

$$(-u_1, pv) = 0, \tag{43}$$
$$(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) = 0. \tag{44}$$

Consideremos la aplicación natural $\varphi : M \longrightarrow M'$ tal que $m \mapsto (m, 0)$ módulo las relaciones adicionales. Si $m \in M$ es tal que $m \mapsto (0, 0)$, entonces m pertenece al módulo de relaciones de M', por lo que debe ser combinación lineal de las dos relaciones adicionales (43) y (44), de manera que

$$(m, 0) = a(-u_1, pv) + b(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v), \tag{45}$$

con $a, b \in \Lambda$. En componentes,

$$m = -au_1 + b(\lambda_2 u_2 + \cdots + \lambda_n u_n), \tag{46}$$
$$ap = -b\lambda_1. \tag{47}$$

Ahora bien, como p es primo y no divide a λ_1 por hipótesis, tenemos que p y λ_1 son coprimos. De (47) se deduce que λ_1 debe dividir a a, lo que nos permite reescribir (46) como

$$m = -\frac{a}{\lambda_1}\lambda_1 u_1 - \frac{a}{\lambda_1}p(\lambda_2 u_2 + \cdots + \lambda_n u_n) = -\frac{a}{\lambda_1}(\lambda_1 u_1 + p(\lambda_2 u_2 + \cdots + \lambda_n u_n)). \tag{48}$$

Aplicando la relación (42) obtenemos $m = 0$, por lo que φ es una aplicación inyectiva y $\operatorname{Ker}\varphi = \{0\}$ es finito.

De la relación (43) se deduce que $pv = 0$ en M'/M, y de la relación (44) se deduce que $\lambda_1 v = 0$ en M'/M. Como M'/M está únicamente generado por v, de lo anterior se sigue que el ideal (p, λ_1) aniquila M'/M, de manera que M'/M es un $\Lambda/(p, \lambda_1)$–módulo. Como p y λ_1 son coprimos, por el lema 3.9–2 se tiene que el ideal (p, λ_1) es de índice finito, por lo que $\Lambda/(p, \lambda_1)$ es finito. Consecuentemente, como M'/M es un $\Lambda/(p, \lambda_1)$–módulo finitamente generado y $\Lambda/(p, \lambda_1)$ es finito, entonces M'/M es finito. Finalmente, como $\operatorname{Im}\varphi = M$, entonces $\operatorname{Coker}\varphi = M'/M$ es finito. Por tanto, tenemos que $M \sim M'$.

El nuevo módulo M' tiene generadores $v, u_2, \ldots, u_n$, pues la relación (43) nos permite eliminar u_1 del sistema de generadores. Toda relación $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0$ cambia a $p\alpha_1 v + \cdots + \alpha_n u_n = 0$, por lo que la primera columna de $\hat{R}'$ queda multiplicada por p. Debemos añadir también la relación (44), es decir, la fila $(\lambda_1, \ldots, \lambda_n)$. Además, la fila $(\lambda_1, p\lambda_2, \ldots, p\lambda_n)$ cambia a $(p\lambda_1, p\lambda_2, \ldots, p\lambda_n)$, que es equivalente a la fila $(\lambda_1, \ldots, \lambda_n)$, por lo que podemos eliminarla. Por tanto, la matriz $\hat{R}'$ tiene la forma buscada. □

Transformación 2: Si todos los elementos en la primera columna de $\hat{R}$ son divisibles por p^k y hay una fila $(p^k\lambda_1, \ldots, p^k\lambda_n)$ en que p no divide a λ_1, entonces podemos cambiar $\hat{R}$ por la matriz $\hat{R}'$ que coincide con $\hat{R}$, salvo en que la fila $(p^k\lambda_1, \ldots, p^k\lambda_n)$ cambia por $(\lambda_1, \ldots, \lambda_n)$.

Demostración. Sea $M' = M \oplus v\Lambda$, con $v \in M$ un nuevo generador, módulo las relaciones adicionales

$$(p^k u_1, -p^k v) = 0, \tag{49}$$
$$(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) = 0. \tag{50}$$

Al igual que en la demostración de la Transformación 1, que p divida a λ_1 nos permite concluir que la aplicación natural $\varphi : M \longrightarrow M'$ es inyectiva. También de manera análoga podemos ver

que el ideal (p^k, λ_1) aniquila M'/M y que este cociente es finito, por lo que tenemos que $M \sim M'$.

Notemos que podemos escribir M' como

$$M' = u_1\Lambda + \cdots + u_n\Lambda + v\Lambda = (u_1 - v)\Lambda + v\Lambda + u_2\Lambda + \cdots + u_n\Lambda + v\Lambda, \tag{51}$$

módulo las relaciones (49) y (50). Si escogemos M'' como el Λ–módulo generado por $v, u_2, \ldots, u_n$, tenemos $M' = (u_1 - v)\Lambda + M'' + v\Lambda$. Ahora bien, como $v\Lambda \subseteq M''$, tenemos $M' = (u_1 - v)\Lambda + M''$. Veamos a continuación que la descomposición $M' = (u_1 - v)\Lambda + M''$ determina una suma directa. Para ello, dado un elemento $m' \in M'$, debemos ver que si puede escribirse como

$$m' = m_1'' + (u_1 - v)\gamma_1 = m_2'' + (u_1 - v)\gamma_2, \tag{52}$$

con $m_1'', m_2'' \in M''$ y $\gamma_1, \gamma_2 \in \Lambda$, entonces $m_1'' = m_2''$ y $\gamma_1 = \gamma_2$.

Supongamos $m_1'' \neq m_2''$, o equivalentemente, $m_1'' - m_2'' \neq 0$, y procedamos por reducción al absurdo. Como $m_1'' - m_2'' \in M''$ y M'' está generado por $v, u_2, \ldots, u_n$, entonces existen $\lambda_1, \lambda_2, \ldots, \lambda_n$ tales que $m_1'' - m_2'' = \lambda_1 v + \lambda_2 u_2 + \cdots + \lambda_n u_n \neq 0$. De (52) tenemos

$$(m_1'' - m_2'') - (u_1 - v)(\gamma_2 - \gamma_1) = 0, \tag{53}$$

o equivalentemente,

$$\lambda_2 u_2 + \cdots + \lambda_n u_n - (\gamma_2 - \gamma_1)u_1 + (\gamma_2 - \gamma_1 + \lambda_1)v = 0. \tag{54}$$

La única forma de eliminar u_1 en la expresión anterior es según la relación (49), por lo que debe ser $(\gamma_2 - \gamma_1) = \gamma p^k$, con $\gamma \in \Lambda$. Pero entonces, en (53) tendríamos $(m_1'' - m_2'') - (u_1 - v)p^k\gamma = 0$, y dada la relación (49), que $m_1'' - m_2'' = 0$, llegando así a contradicción. Por tanto, debe ser $m_1'' = m_2''$, y en consecuencia, $\gamma_1 = \gamma_2$.

Tenemos pues que $M' = (u_1 - v)\Lambda \oplus M''$, donde M'' está generado por $v, u_2, \ldots, u_n$ y tiene relaciones generadas por $\hat{R}$ y, según (50), por $(\lambda_1, \ldots, \lambda_n)$. Notemos que podemos eliminar de $\hat{R}$ la fila $(p^k\lambda_1, p^k\lambda_2, \ldots, p^k\lambda_n)$, pues es equivalente a la fila $(\lambda_1, \ldots, \lambda_n)$. Por ello, las relaciones de M'' vienen dadas por $\hat{R}'$, que tiene la forma buscada.

Consideremos la proyección $\varphi : \Lambda \longrightarrow (u_1 - v)\Lambda$ tal que $\lambda \mapsto \lambda(u_1 - v)$, que es una aplicación exhaustiva. Por un lado, $(p^k) \subseteq \operatorname{Ker}\varphi = \{\lambda \in \Lambda \,\big|\, \lambda(u_1 - v) = 0\}$ debido a la relación (49). Como por hipótesis los primeros coeficientes de todas las relaciones que involucran u_1 son divisibles por p^k, debe ser $\lambda \in (p^k)$, por lo que $\operatorname{Ker}\varphi \subseteq (p^k)$, y en consecuencia, $\operatorname{Ker}\varphi = (p^k)$. Aplicando el Teorema de Isomorfía, tenemos que

$$(u_1 - v)\Lambda \simeq \Lambda/(p^k), \tag{55}$$

que ya está en la forma establecida por el teorema. Tenemos entonces $M' = M'' \oplus \Lambda/(p^k)$, por lo que en lo que sigue es suficiente trabajar con M'' y $\hat{R}'$. □

Transformación 3: Si $\hat{R}$ contiene una fila $(p^k\lambda_1, \ldots, p^k\lambda_n)$ y para algún $\lambda \in \Lambda$ tal que p no divide a λ se tiene que $(\lambda\lambda_1, \ldots, \lambda\lambda_n)$ también es una relación, entonces podemos cambiar la fila $(p^k\lambda_1, \ldots, p^k\lambda_n)$ por $(\lambda_1, \ldots, \lambda_n)$.

Demostración. Sea $M' = M/(\lambda_1 u_1 + \cdots + \lambda_n u_n)\Lambda$ y consideremos la proyección $\varphi : M \longrightarrow M'$, que es exhaustiva, de manera que $\operatorname{Im}\varphi = M'$, por lo que $\operatorname{Coker}\varphi = M'/M' = \{0\}$ es finito.

Por un lado, $(p^k\lambda_1, \ldots, p^k\lambda_n)$ y $(\lambda\lambda_1, \ldots, \lambda\lambda_n)$ son relaciones por hipótesis, por lo que $\operatorname{Ker}\varphi$ es aniquilado por el ideal (λ, p^k), de manera que $\operatorname{Ker}\varphi$ es un $\Lambda/(p^k, \lambda)$–módulo. Por otro lado, como p es primo y no divide a λ por hipótesis, tenemos que p^k y λ son coprimos. Por el lema 3.9–2 se tiene que el ideal (p^k, λ) es de índice finito, por lo que $\Lambda/(\lambda, p^k)$ es finito. Además, como M es finitamente generado, también lo es $\operatorname{Ker}\varphi$. Consecuentemente, como $\operatorname{Ker}\varphi$ es un $\Lambda/(p^k, \lambda)$–módulo finitamente generado y $\Lambda/(\lambda, p^k)$ es finito, entonces $\operatorname{Ker}\varphi$ es finito. Por tanto, tenemos que $M \sim M'$. Claramente las relaciones de M' vienen dadas por $\hat{R}'$, pues la fila $(p^k\lambda_1, \ldots, p^k\lambda_n)$ se vuelve en el cociente equivalente a $(\lambda_1, \ldots, \lambda_n)$. □

Notación 3.12. Las seis transformaciones anteriores (A,B,C,1,2,3) se denominan **transformaciones admisibles**.

Sea $f \in \Lambda$ no nulo. Por el Teorema de Preparación de Weierstrass, f puede escribirse como $f(T) = p^\mu P(T)U(T)$, con $U(T) \in \Lambda^\times$, $P(T) \in \mathbb{Z}_p[T]$ un polinomio distinguido y $\mu \geq 0$.

Definición 3.13. Si $f \in \Lambda$ no nulo se escribe de la forma anterior, definimos el **grado de Weierstrass** de f como

$$\deg_W f = \begin{cases} \infty & \text{si } \mu > 0 \\ \deg P(T) & \text{si } \mu = 0 \end{cases}. \tag{56}$$

Definición 3.14. Dada una matriz $\hat{R} = (a_{ij})$, definimos

$$\deg^{(k)}(\hat{R}) = \min_{i,j \geq k}\{\deg_W(a'_{ij})\}, \tag{57}$$

en que (a'_{ij}) varía sobre todas las matrices obtenidas a partir de $\hat{R}$ vía transformaciones admisibles que dejan las primeras $k-1$ filas iguales.

Definición 3.15. Sean $r \geq 1$ y

$$D_{r-1} = \begin{pmatrix} \lambda_{11} & & 0 \\ & \ddots & \\ 0 & & \lambda_{r-1,r-1} \end{pmatrix}. \tag{58}$$

Decimos que $\hat{R}$ está en **forma** $(r-1)$**–normal** si es de la forma

$$\hat{R} = \begin{pmatrix} D_{r-1} & 0 \\ \hat{A} & \hat{B} \end{pmatrix}, \tag{59}$$

y para $1 \leq k \leq r-1$ se tiene que λ_{kk} son distinguidos y cumplen

$$\deg \lambda_{kk} = \deg_W \lambda_{kk} = \deg^{(k)}(\hat{R}). \tag{60}$$

Lema 3.16. Si la submatriz $\hat{B}$ anterior es no nula, entonces $\hat{R}$ puede transformarse, via transformaciones admisibles, en una matriz en forma r–normal que tenga los primeros $r-1$ elmentos de la diagonal iguales.

Demostración. Si consideramos una fila con un único elemento no nulo, la Transformación 1 nos permite multiplicar el resto de elementos de su columna por una potencia arbitraria de p. De esta manera, podemos asumir que todos los elementos λ_{ij} que conforman la submatriz $\hat{A}$ son divisibles por una potencia arbitraria de p, es decir, que p^N divide a todos los elementos de $\hat{A}$, con N que escogemos suficientemente grande como para que no divida a todos los elementos

de $\hat{B}$.

Sea k el menor entero tal que p^k no divide a todos los elementos de $\hat{B}$ y λ_{ij} uno de los elementos de $\hat{B}$ no divisible por p^k. La Transformación 2, en combinación con la Transformación A, nos permite reemplazar la fila i de manera que el nuevo elemento λ_{ij} no sea divisible por p. Por tanto, podemos asumir que $\hat{B}$ contiene un elemento λ_{ij} tal que $\deg_W \lambda_{ij} = \deg^{(r)}(\hat{R}) < \infty$, y la Transformación A nos permite suponer que este elemento es λ_{rr}. Si λ_{rr} se escribe como $\lambda_{rr} = P(T)U(T)$ según el Teorema de Preparación de Weierstrass, la Transformación C nos permite multiplicar la r–ésima columna de $\hat{R}$ por U^{-1}, de manera que el nuevo λ_{rr} es un polinomio distinguido tal que $\deg \lambda_{rr} = \deg_W \lambda_{rr} = \deg^{(r)}(\hat{R})$. Aplicando la Transformación B, el algoritmo de la división dado por el corolario 3.5 nos permite asumir que los λ_{rj} son polinomios tales que $\deg \lambda_{rj} < \deg \lambda_{rr}$ si $j \neq r$, y que $\deg \lambda_{rj} < \deg \lambda_{jj}$ si $j < r$. Ahora bien, como $\deg \lambda_{rr} = \deg_W \lambda_{rr} = \deg^{(r)}(\hat{R})$ es mínimo en $\hat{B}$, entonces p debe dividir a λ_{rj} para todo $j > r$, pues en caso contrario tendríamos $\deg_W \lambda_{rj} < \deg_W \lambda_{rr} = \deg^{(r)}(\hat{R})$, que no es posible. Además, la Transformación 1 nos permite asumir que p^N divide a cada λ_{rj} si $j < r$.

A continuación, supongamos que algún λ_{rj} con $j > r$ es no nulo y procedamos por reducción al absurdo. La Transformación 1 nos permite eliminar toda potencia de p para algún elemento λ_{rj} no nulo, de manera que $\deg_W \lambda_{rj} = \deg \lambda_{rj}$. Ahora bien, como hemos visto que $\deg \lambda_{rj} < \deg \lambda_{rr}$ si $j \neq r$ y que $\deg \lambda_{rr} = \deg_W \lambda_{rr}$ por ser λ_{rr} un polinomio distinguido, obtenemos $\deg_W \lambda_{rj} < \deg_W \lambda_{rr}$, que no es posible pues $\deg_W \lambda_{rr} = \deg^{(r)}(\hat{R})$ es mínimo. Por tanto, todo λ_{rj} con $j > r$ debe ser nulo.

Ahora, supongamos que algún λ_{rj} con $j < r$ es no nulo y procedamos por reducción al absurdo. Nuevamente la Transformación 1 nos permite eliminar toda potencia de p para algún elemento λ_{rj} no nulo, de manera que $\deg_W \lambda_{rj} = \deg \lambda_{rj}$. Ahora bien, como hemos visto que $\deg \lambda_{rj} < \deg \lambda_{jj}$ si $j < r$ y que $\deg \lambda_{rr} = \deg_W \lambda_{rr}$ por ser λ_{rr} un polinomio distinguido, obtenemos $\deg_W \lambda_{rj} < \deg_W \lambda_{jj}$, que no es posible pues $\deg_W \lambda_{jj} = \deg^{(j)}(\hat{R})$ es mínimo. Por tanto, todo λ_{rj} con $j < r$ debe ser nulo.

De esta manera, tenemos que el único elemento no nulo de la r–ésima fila es λ_{rr}, que es un polinomio distinguido que cumple $\deg \lambda_{rr} = \deg_W \lambda_{rr} = \deg^{(r)}(\hat{R})$. Por tanto, la matriz $\hat{R}$ está ahora en forma r–normal. □

Comenzando con la matriz $\hat{R}$, podemos aplicar sucesivamente el lema anterior a $\hat{R}$ hasta obtener una matriz

$$\hat{R}' = \begin{pmatrix} \lambda_1 & & 0 & \\ & \ddots & & \hat{0} \\ 0 & & \lambda_{r,r} & \\ & \hat{A} & & \hat{0} \end{pmatrix}. \tag{61}$$

en forma r–normal.

Lema 3.17. La submatriz $\hat{A}$ anterior es nula.

Demostración. Aplicando la Transformación B, el algoritmo de la división dado por el corolario 3.5 nos permite asumir que los λ_{ij} que conforman la submatriz $\hat{A}$ son polinomios tales que $\deg \lambda_{ij} < \deg \lambda_{jj}$.

A continuación, supongamos que algún λ_{ij} es no nulo, fijemos i y procedamos por reducción al absurdo. Como $\deg \lambda_{jj} = \deg^{(j)}(\hat{R}')$ es mínimo, entonces p debe dividir a λ_{ij}, pues en caso

contrario tendríamos $\deg_W \lambda_{ij} < \deg_W \lambda_{jj} = \deg^{(j)}(\hat{R})$, que no es posible. Por tanto, tenemos una relación no nula $(\lambda_{i1}, \ldots, \lambda_{ir}, 0, \ldots, 0)$ que es divisible por p. Como los λ_{jj} son distinguidos, tenemos que p no divide a ningún λ_{jj}, por lo que p no divide a $\lambda = \lambda_{11} \cdots \lambda_{rr}$. Ahora bien, la matriz $\hat{R}'$ muestra que tenemos relaciones dadas por $\lambda_{jj} u_j = 0$, por lo que $\lambda u_j = 0$, y también $\lambda \lambda_{ij} u_j = 0$, de manera que $\lambda \lambda_{i1} u_1 + \cdots + \lambda \lambda_{in} u_n = 0$, y por ello $(\lambda \lambda_{i1}, \ldots, \lambda \lambda_{ir}, 0, \ldots, 0)$ es una relación. Aplicando ahora la Transformación 3 podemos asumir que p no divide a alguno de los nuevos λ_{ij}, de manera que

$$\deg_W \lambda_{ij} \leq \deg \lambda_{ij} < \deg \lambda_{jj} \tag{62}$$

que no es posible porque $\deg \lambda_{jj} = \deg_W \lambda_{jj} = \deg^{(j)}(\hat{R}')$ es mínimo. Por tanto, todos los λ_{ij} deben ser nulos, por lo que $\hat{A}$ es una submatriz nula. □

De esta manera, la matriz $\hat{R}'$ queda en la forma

$$\hat{R}' = \begin{pmatrix} \lambda_{11} & & 0 & \\ & \ddots & & \hat{0} \\ 0 & & \lambda_{rr} & \\ & \hat{0} & & \hat{0} \end{pmatrix}. \tag{63}$$

Lema 3.18. La matriz $\hat{R}'$ anterior corresponde, en términos de Λ–módulos, con

$$M \sim \Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r} \tag{64}$$

Demostración. Para entender la mátriz $\hat{R}'$ en términos de Λ–módulos, consideremos aplicaciones φ y ψ definidas según

$$\begin{array}{ccccc} \Lambda^n & \xrightarrow{\varphi} & \Lambda^n & \xrightarrow{\psi} & u_1\Lambda + \cdots + u_n\Lambda \\ (\alpha_1, \ldots, \alpha_n) & \longmapsto & (\lambda_{11}\alpha_1, \ldots, \lambda_{rr}\alpha_r, 0, \ldots, 0) & & \\ & & (\beta_1, \ldots, \beta_n) & \longmapsto & \beta_1 u_1 + \cdots + \beta_n u_n \end{array} \tag{65}$$

donde $u_1\Lambda + \cdots + u_n\Lambda$ lo consideramos módulo las relaciones dadas por $\hat{R}'$. Notemos que φ es una aplicación inyectiva y ψ una aplicación exhaustiva. La matriz $\hat{R}'$ muestra que tenemos relaciones $\lambda_{11} u_1 = 0, \ldots, \lambda_{rr} u_r = 0$, de manera que

$$\psi(\varphi(\alpha_1, \ldots, \alpha_n)) = \lambda_{11}\alpha_1 u_1 + \cdots + \lambda_{rr}\alpha_r u_r = 0, \tag{66}$$

de donde se deduce que $\operatorname{Im}\varphi = \lambda_{11}\Lambda + \cdots + \lambda_{rr}\Lambda \subseteq \operatorname{Ker}\psi$. Además, $\operatorname{Ker}\psi = R'$ está generado por las filas de $\hat{R}'$, por lo que dado $(\beta_1, \ldots, \beta_n) \in \operatorname{Ker}\psi$ existen $\alpha_1, \ldots, \alpha_r \in \Lambda$ tales que $(\beta_1, \ldots, \beta_n) = \alpha_1(\lambda_{11}, 0, \ldots, 0) + \cdots + \alpha_r(0, \ldots, \lambda_{rr}, \ldots, 0)$, de manera que tenemos $\varphi(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0) = (\beta_1, \ldots, \beta_n)$, por lo que $\operatorname{Ker}\psi \subseteq \operatorname{Im}\varphi$, y por tanto, $\operatorname{Ker}\psi = \operatorname{Im}\varphi$.

Por el Teorema de Isomorfia, tenemos

$$\operatorname{Im}\psi \cong \Lambda^n/\operatorname{Ker}\psi = \Lambda^n/(\lambda_{11}\Lambda + \cdots + \lambda_{rr}\Lambda) \tag{67}$$

Por ello, los elementos de $\operatorname{Im}\psi$ pueden pensarse como los elementos de Λ^n módulo la relación de equivalencia $(\alpha_1, \ldots, \alpha_n) \sim (\alpha'_1, \ldots, \alpha'_n) \Leftrightarrow (\alpha_1 - \alpha'_1, \ldots, \alpha_n - \alpha'_n) \in (\lambda_{11}, \ldots, \lambda_{rr}, 0 \ldots, 0)\Lambda \Leftrightarrow \alpha_1 - \alpha'_1 \equiv 0 \mod \lambda_{11}, \ldots, \alpha_r - \alpha'_r \equiv 0 \mod \lambda_{rr}$, $\alpha_{r+1} - \alpha'_{r+1} = 0, \ldots, \alpha_n - \alpha'_n = 0 \Leftrightarrow \alpha_1 = \alpha'_1$ en $\Lambda/(\lambda_{11}), \ldots, \alpha_r = \alpha'_r$ en $\Lambda/(\lambda_{rr})$, $\alpha_{r+1} = \alpha'_{r+1}$ en $\Lambda, \ldots, \alpha_n = \alpha'_n$ en Λ. Por tanto, tenemos

$$\operatorname{Im}\psi \cong \Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r} \tag{68}$$

Como M es pseudo–isomorfo a $\operatorname{Im}\psi$, tenemos lo que buscabamos. □

Recuperando los factores $\Lambda/(p^k)$ que fueron descartados en la Transformación 2, obtenemos

$$M \sim \Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r} \oplus \Lambda/(p^{n_1}) \oplus \cdots \oplus \Lambda/(p^{n_s}) \tag{69}$$

para ciertos $n_1, \ldots, n_s \in \mathbb{N}$. Notemos que los λ_{jj} son polinomios distinguidos, y como Λ es un módulo noetheriano, descomponen en producto de polinomios distinguidos e irreductibles f_k. El lema 3.9–3 nos permite obtener

$$M \sim \Lambda/(f_1^{m_1}) \oplus \cdots \oplus \Lambda/(f_t^{m_t}) \oplus \Lambda^{n-r} \oplus \Lambda/(p^{n_1}) \oplus \cdots \oplus \Lambda/(p^{n_s}) \tag{70}$$

para ciertos $m_1, \ldots, m_t$. Agrupando y reordenando, tenemos

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j^{m_j}) \right) \tag{71}$$

tal y como queríamos ver.

4. Invariantes de Iwasawa.

En este capítulo enunciamos y demostramos un teorema de Iwasawa correspondiente a los invariantes de una $\mathbb{Z}_p$–extensión, conocidos actualmente como invariantes de Iwasawa. Al final del capítulo, recopilamos algunos resultados sobre los invariantes de Iwasawa en determinadas $\mathbb{Z}_p$–extensiones sobre cuerpos de números.

4.1. Teorema de Iwasawa.

El teorema siguiente permite obtener información sobre la p–parte de los números de clases en $\mathbb{Z}_p$–extensiones.

Teorema 4.1 (**Teorema de Iwasawa**). Sean K un cuerpo de números y K_∞/K una $\mathbb{Z}_p$–extensión. Sea p^{e_n} la potencia exacta de p que divide el número de clases de K_n. Entonces, existe enteros $\lambda \geq 0$, $\mu \geq 0$ y ν independientes de n, y un entero n_0 tales que

$$e_n = \lambda n + \mu p^n + \nu \quad \text{para todo } n \geq n_0. \tag{72}$$

A los enteros λ, μ y ν del teorema anterior se les denomina **invariantes de Iwasawa**. Antes de proceder a la demostración del teorema, consideremos los lemas siguientes.

Lema 4.2. Si $f \in \Lambda$, entonces $\Lambda/(f)$ es infinito.

Demostración. Si asumimos que $f \neq 0$, del Teorema de preparación de Weierstrass tenemos que $f = p^\mu PU$, con $U \in \mathbb{Z}[[T]]$ una unidad y $P \in \mathbb{Z}[T]$ un polinomio distinguido, por lo que basta con considerar los casos en que $f = p$ y f un polinimio distinguido. Si $f = p$, tenemos $\Lambda/(f) \cong \mathbb{Z}/p\mathbb{Z}[[T]]$, que es infinito. Si f es distinguido, por el corolario 3.5 tenemos que si $g \in \Lambda$, entonces $g = fq + r$ para ciertos $q \in \mathbb{Z}[[T]]$ y $r \in \mathbb{Z}[T]$, por lo que $\Lambda/(f) \cong \mathbb{Z}[T]$, que es infinito. □

Lema 4.3. (**Lema de Nakayama**) Sea X un Λ–módulo compacto. Entonces, X es finitamente generado sobre Λ si y sólo si $X/(p,T)X$ es finito. Si $x_1, \ldots, x_n$ generan $X/(p,T)X$ sobre $\mathbb{Z}$, entonces también generan X como Λ–módulo.

Demostración. Véase el lema 13.16 de [14]. □

4.1.1. Demostración.

Como en la sección 3.3, sea $\Gamma = \mathrm{Gal}(K_\infty/K) \cong (\mathbb{Z}_p, +)$ y γ_0 un generador topológico fijo de Γ tal que el isomorfismo $\mathbb{Z}_p \cong \Gamma$ venga dado por $x \mapsto \gamma^x$. La $\mathbb{Z}_p$–extensión K_∞/K es equivalente a la cadena de cuerpos

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \cup K_n, \tag{73}$$

en que los K_n cumplen que $\mathrm{Gal}(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z}, +)$. Sea L_n la máxima p–extensión abeliana no ramificada de K_n, y sea $X_n = \mathrm{Gal}(L_n/K_n)$. Notemos que del teorema 1.51 sabemos que $X_n \cong A_n$, con A_n el p–subgrupo de Sylow de $\mathrm{Cl}(K_n)$. si definimos $L = \bigcup_{n\geq 0} L_n$, existe una cadena de cuerpos

$$L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \cdots \subseteq L = \cup L_n. \tag{74}$$

Sean $G = \mathrm{Gal}(L/K)$, y recordemos que $\Gamma = G/X$.

Suposición: Todos los primos que están ramificados en K_∞/K están totalmente ramificados.

En la sección 3.3 vimos que en estas condiciones, $X = \mathrm{Gal}(L/K_\infty)$ es un Λ–módulo.

Según (31), el polinomio $1+T \in \Lambda$ actúa como $\gamma_0 \in \Gamma$, de manera que $1+T$ es un generador topológico de Λ. Extendemos ahora $\gamma \in \Gamma$ a $\tilde{\gamma} \in G = \mathrm{Gal}(L/K)$, de manera que la acción de $\gamma \in \Gamma$ sobre $x \in X$ venga dada por

$$x^\gamma = \tilde{\gamma} x (\tilde{\gamma})^{-1}. \tag{75}$$

De la proposición 1.40, tenemos que hay un número finito de ideales que ramifican en K_∞/K. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ estos primos, y para cada i fijemos un primo $\tilde{\mathfrak{p}}_i \in \mathcal{O}_L$ tal que $\mathfrak{p}_i = \tilde{\mathfrak{p}}_i \cap \mathcal{O}_K$. Sea $I_i \subseteq G = \mathrm{Gal}(L/K)$ el grupo de inercia de $\tilde{\mathfrak{p}}_i$ sobre $\mathfrak{p}_i$. Como la extensión L/K_∞ es no ramificada, de la proposición 1.58 tenemos $I_i \cap X = 1$.

De ello se deduce que la aplicación $I_i \longrightarrow G/X = \Gamma = \mathrm{Gal}(K_\infty/K)$ dada por $\sigma \mapsto \sigma|_{K_\infty}$ es inyectiva. Para cada $\mathfrak{p}_i \in \mathcal{O}_K$ consideremos $\mathfrak{p}_{i,n} \in \mathcal{O}_{K_n}$ tal que $\mathfrak{p}_{i,n} \cap K = \mathfrak{p}_i$. Como los $\mathfrak{p}_i$ están totalmente ramificados, entonces $\mathfrak{p}_i \mathcal{O}_{K_n} = \mathfrak{p}_{i,n}^{p^n}$. Por un lado, si $\sigma \in \mathrm{Gal}(K_n/K)$, como $\sigma|_K = id$, tenemos que $\sigma(\mathfrak{p}_i) = \mathfrak{p}_i$. Además, como $\sigma(\mathfrak{p}_{i,n})$ es un primo de $\mathcal{O}_{K_n}$ sobre $\mathfrak{p}_i$ y $\mathfrak{p}_i$ está totalmente ramificado, debe ser $\sigma(\mathfrak{p}_{i,n}) = \mathfrak{p}_{i,n}$, Ahora bien, como $\mathfrak{p}_i \mathcal{O}_{K_n} = \mathfrak{p}_{i,n}^{p^n}$, por la proposición 1.41 tenemos que $|I(\mathfrak{p}_{i,n}/\mathfrak{p}_i)| = e(\mathfrak{p}_{i,n}/\mathfrak{p}_i) = p^n$, por lo que $I(\mathfrak{p}_{i,n}/\mathfrak{p}_i) \cong \mathbb{Z}/p^n\mathbb{Z} \cong \mathrm{Gal}(K_n/K)$, de manera que tenemos $I(\mathfrak{p}_{i,n}/\mathfrak{p}_i) = \mathrm{Gal}(K_n/K)$. Por tanto,

$$\varprojlim I(\mathfrak{p}_{i,n}/\mathfrak{p}_i) = \varprojlim \mathrm{Gal}(K_n/K) = \mathrm{Gal}(K_\infty/K) = \Gamma. \tag{76}$$

Por otro lado, tenemos que $I_i|_{K_n} = I(\mathfrak{p}_{i,n}/\mathfrak{p}_i)$. Dado $\sigma \in \mathrm{Gal}(K_\infty/K)$ y un elemento $x \in K_\infty$, como tenemos $K_\infty = \cup K_n$, existe un n_x tal que $x \in K_{n_x}$. Así, $\sigma(x)$ queda determinado por $\sigma|_{K_{n_x}}(x) \in \mathrm{Gal}(K_{n_x}/K) = I(\mathfrak{p}_{i,n_x}/\mathfrak{p}_i) = I_i|_{K_{n_x}}$, por lo que existe un cierto $i \in I_i$ tal que $i|_{K_{n_x}} = \sigma|_{K_{n_x}}$, de manera que la aplicación $I_i \longrightarrow \Gamma$ es exhaustiva, y por tanto, biyectiva, de manera que $I_i \cong \Gamma$. De ello se deduce que

$$G = I_i X = X I_i \tag{77}$$

para todo $i = 1, \ldots, s$.

Sea $\sigma_i \in I_i$ tal que su imagen por la aplicación anterior sea γ_0, de manera que σ_i es un generador topológico de I_i. Como $G = XI_i$ y $I_i \subseteq G$ para todo $i = 1, \ldots, s$, entonces tenemos $I_i \subseteq XI_1$, por lo que

$$\sigma_i = a_i \sigma_1 \tag{78}$$

para algún $a_i \in X$. Notemos que, como $\sigma_1 = a_1 \sigma_1$, debe ser $a_1 = 1$.

Lema 4.4. Tomemos como cierta la Suposición. Sea G' la clausura del subgrupo conmutador de G. Entonces,

$$G' = X^{\gamma_0 - 1} = TX. \tag{79}$$

Demostración. Recordemos que el subgrupo conmutador de G es $\{[a,b] = aba^{-1}b^{-1} \,\big|\, a, b \in G\}$. Antes hemos visto $I_i \cong \Gamma$, por lo que $I_1 \subseteq G$ es isomorfo a $\Gamma = G/X$. Esto nos permite pasar pasar $\gamma \in \Gamma$ a su elemento correspondiente en I_1 para definir la acción de Γ en X. Identificando Γ e I_1, tenemos que la acción de γ sobre $x \in X$ viene dada por $x^\gamma = \gamma x \gamma^{-1}$.

Sean $a = \alpha x$, $b = \beta y$ elementos arbitrarios de $G = I_1 X \cong \Gamma X$, con $\alpha, \beta \in \Gamma$ y $x, y \in X$. Entonces,

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^{\alpha} \alpha \beta x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^{\alpha} (y x^{-1})^{\alpha\beta} (\alpha\beta) \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^{\alpha} (y x^{-1})^{\alpha\beta} (y^{-1})^{\beta} \qquad (\Gamma \text{ es abeliano}) \\ &= (x^{\alpha})^{1-\beta} (y^{\beta})^{\alpha-1} \qquad (X \text{ es abeliano}). \end{aligned} \tag{80}$$

(81)

Escogiendo $\beta = 1$ y $\alpha = \gamma_0$, tenemos que $aba^{-1}b^{-1} = y^{\gamma_0 - 1} \in G'$, por lo que $X^{\gamma_0 - 1} \subseteq G'$.

Si mantenemos $\beta \in \Gamma$ arbitrario, como γ_0 es generador de Γ, entonces existe un $c \in \mathbb{Z}_p$ tal que $\beta = \gamma_0^c$, y como $\gamma_0 \in \Gamma$ es equivalente a $1 + T \in \Lambda$, entonces

$$1 - \beta = 1 - \gamma_0^c = 1 - (1+T)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n = \sum_{n=1}^{\infty} \binom{c}{n} T^n \in T\Lambda \tag{82}$$

Como $T = \gamma_0 - 1$, entonces $(x^{\alpha})^{1-\beta} \in X^{\gamma_0 - 1}$. Análogamente, $(y^{\beta})^{1-\alpha} \in X^{\gamma_0 - 1}$. Notemos que $Tx = (\gamma_0 - 1)x = x^{\gamma_0 - 1}$, por lo que $X^{\gamma_0 - 1} = TX$.

Como X es el límite proyectivo de los X_n, que son conjuntos compactos por ser finitos, entonces X también es compacto, y como $X^{\gamma_0 - 1}$ es la imagen de un compacto, entonces es cerrado. Por tanto tenemos $G' \subseteq X^{\gamma_0 - 1}$, y en consecuencia, $G' = X^{\gamma_0 - 1}$, tal y como queríamos ver. □

Lema 4.5. Tomemos como cierta la Suposición. Sea Y_0 el $\mathbb{Z}_p$–submódulo de X generado por $\{a_i \,\big|\, 2 \leq i \leq s\}$ y por $X^{\gamma_0 - 1} = TX$. Sea $Y_n = v_n Y_0$, con

$$v_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1+T)^{p^n} - 1}{T}. \tag{83}$$

Entonces, $X_n \cong X / Y_n$ para todo $n \geq 0$.

Demostración. Comencemos por el caso $n = 0$, en que tenemos $K \subseteq L_0 \subseteq L$. Como L/K es una p–extensión y L_0 es la máxima p–extensión abeliana no ramificada de K, entonces L_0/K es la máxima subextensión abeliana no ramificada de L/K.

Por un lado, se tiene que $I_i \subseteq \mathrm{Gal}(L/L_0)$. Por otro lado, por el Teorema fundamental de la Teoría de Galois, tenemos que $G/\mathrm{Gal}(L/L_0) \cong \mathrm{Gal}(L_0/K)$, y como $\mathrm{Gal}(L_0/K)$ es abeliano, entonces $G/\mathrm{Gal}(L/L_0)$ es abeliano. Ahora bien, G' es el menor subgrupo H de G tal que G/H es abeliano, de manera que debe ser $G' \subseteq \mathrm{Gal}(L/L_0)$. Por tanto, $I_i G' \subseteq \mathrm{Gal}(L/L_0)$.

Si consideramos $L^{G'}$ el cuerpo fijo por G', tenemos $L_0 \subseteq L^{G'} \subseteq L$. Sean $\sigma \in \mathrm{Gal}(L/L_0)$ y $\tau = \sigma|_{L^{G'}} \in \mathrm{Gal}(L^{G'}/L_0)$. Sea $\tilde{\tau} \in \mathrm{Gal}(L/L_0)$ tal que $\tilde{\tau}|_{L^{G'}} = \tau$. Así, tenemos $\sigma = u\tilde{\tau}$ para cierto $u \in G'$. La extensión $L^{G'}/L_0$ es abeliana, y debe ser ramificada porque L_0/K es la máxima subextensión abeliana no ramificada. De ello se deduce que $\tau \in I_i$, y en consecuencia, que $\sigma = u\tilde{\tau} \in G' I_i$, por lo que $\mathrm{Gal}(L/L_0) \subseteq G' I_i$.

Por tanto, $\mathrm{Gal}(L/L_0)$ es el subgrupo cerrado de G generado por G' y todos los grupos de inercia I_i, con $1 \leq i \leq s$. Por el lema 4.4 y (78), $\mathrm{Gal}(L/L_0)$ es la clausura del grupo generado por X^{γ_0-1}, I_1 y $a_2, \ldots, a_s$. Por el Teorema fundamental de la Teoría de Galois, tenemos $\mathrm{Gal}(L_0/K) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_0)$, es decir, $X_0 = G/\mathrm{Gal}(L/L_0)$, y aplicando (77), tenemos $X_0 = XI_1/\mathrm{Gal}(L/L_0)$. Esto, junto a lo anterior, conduce a

$$X_0 = XI_1/\mathrm{Gal}(L/L_0) \cong XI_1/\overline{\langle X^{\gamma_0-1}, I_1, a_2, \ldots, a_s\rangle} \cong X/\overline{\langle X^{\gamma_0-1}, a_2, \ldots, a_s\rangle} = X/Y_0. \quad (84)$$

Consideremos ahora $n \geq 1$. Reemplazando K por K_n y γ_0 por $\gamma_0^{p^n}$, tenemos que σ_i se vuelve $\sigma_i^{p^n}$. Aplicando (78) y (75), tenemos

$$\sigma_i^{k+1} = (a_i\sigma_1)^{k+1} = a_i\sigma_1 a_i \sigma_1^{-1}\sigma_1^2 a_i \sigma_1^{-2} \ldots \sigma_1^k a_i \sigma_1^{-k}\sigma_1^{k+1} = a_i^{1+\sigma_1+\cdots+\sigma_1^k}\sigma_1^{k+1}. \quad (85)$$

Escogiendo $k = p^n - 1$, y como $a_i^{1+\sigma_1+\cdots+\sigma_1^{p^n-1}} = (1 + \gamma_0 + \cdots + \gamma_0^{p^n-1})a_i = v_n a_i$, obtenemos

$$\sigma_i^{p^n} = (v_n a_i)\sigma_1^{p^n}, \quad (86)$$

de manera que a_i se vuelve $v_n a_i$. Además, $X^{\gamma_0-1} = (\gamma_0 - 1)X$ se vuelve$(\gamma_0^{p^n} - 1)X = v_n X^{\gamma_0-1}$. Por tanto, Y_0 se vuelve $v_n Y_0$, lo cual conduce al resultado deseado. □

Lema 4.6. Tomemos como cierta la Suposición. Entonces, $X = \mathrm{Gal}(L/K_\infty)$ es un Λ–módulo finitamente generado.

Demostración. Como $v_1 = [(1+T)^p - 1]/T \in (p, T)Y_0$, entonces

$$Y_0/(p,T)Y_0 \cong [Y_0/v_1Y_0]/[(p,T)Y_0/v_1Y_0] \quad (87)$$

es un cociente de $Y_0/v_1Y_0 = Y_0/Y_1 \subseteq X/Y_1 \cong X_1$, que es finito. Por el lema de Nakayama, Y_0 es finitamente generado, y como $X/Y_0 = X_0$ es finito, entonces X debe ser finitamente generado. □

Olvidamos ahora la Suposición, es decir, no suponemos que todos los primos ramificados en K_∞/K están totalmente ramificados.

Por el lema 2.7, existe un $e \geq 0$ tal que todos los primos que están ramificados en K_e están totalmente ramificados. Podemos aplicar el lema 4.6 a la extensión K_∞/K_e, de manera que $X = \mathrm{Gal}(L/K_\infty)$, que es el mismo para las extensiones K_∞/K_e y K_∞/K, es un Λ–módulo finitamente generado.

Utilizando la notación del lema 4.5, tenemos

$$v_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n-1}, \quad (88)$$
$$v_e = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^e-1}. \quad (89)$$

Esto nos permite definir

$$v_{n,e} = \frac{v_n}{v_e} = 1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \cdots + \gamma_0^{p^n-p^e}. \quad (90)$$

Como $\gamma_0^{p^e}$ genera $\mathrm{Gal}(K_\infty/K_e)$, en el lema 4.5 podemos reemplazar v_n por $v_{n,e}$, de manera que si Y_e corresponde al Y_0 del lema cuando la extensión considerada es K_∞/K_e, tenemos que

$X_n \cong X/Y_n$ para todo $n \geq e$, con $Y_n = v_{n,e}Y_e$.

Como X es un Λ–módulo finitamente generado, podemos aplicarle el Teorema de Clasificación de Λ–módulos. Equivalentemente, como $X/Y_e \cong X_e$ es finito, tenemos el pseudo–isomorfismo $Y_e \sim X$, por lo que podemos aplicar el teorema a Y_e y obtener el mismo resultado. Tenemos

$$Y_e \sim X \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j^{m_j}) \right), \tag{91}$$

con $r, s, t, k_i, m_j \in \mathbb{Z}$ y $f_j \in \Lambda$ distinguidos e irreductibles. Si escogemos $g_j = f_j^{m_j}$, que siguen siendo polinomios distinguidos, tenemos

$$Y_e \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(g_j) \right). \tag{92}$$

Proposición 4.7. Supongamos

$$E = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(g_j) \right), \tag{93}$$

con $r, s, t, k_i \in \mathbb{Z}$ y $g_j \in \Lambda$ distinguidos (no necesariamente irreductible). Sean $m = \sum_{i=1}^{s} k_i$ y $l = \sum_{j=1}^{t} \deg g_j$. Si $E/v_{n,e}E$ es finito para todo n, entonces $r = 0$ y existen $n_0, c \in \mathbb{Z}$ tales que $|E/v_{n,e}E| = p^{mp^n + ln + c}$ para todo $n > n_0$.

Demostración. A continuación, calcularemos $V/v_{n,e}V$ para cada término de la suma directa.

(1) Caso $V = \Lambda$. Por el lema 4.2, $\Lambda/v_{n,e}\Lambda$ es infinito. Como $E/v_{n,e}E$ es finito por hipótesis, entonces Λ no puede aparecer como sumando, por lo que $r = 0$.

(2) Caso $V = \Lambda/(p^k)$. En este caso, $V/v_{n,e}V \cong \Lambda/(p^k, v_{n,e})$. Si el cociente de dos polinomios distinguidos es un polinomio, entonces es distinguido o constante, por lo que $v_{n,e} = v_n/v_e$ es un polinomio distinguido. Por el algoritmo de la división en Λ dado por el corolario 3.5, todo elemento de $\Lambda/(p^k, v_{n,e})$ se representa de manera única por un polinomio módulo p^k, de grado menor que $\deg v_{n,e} = p^n - p^e$. Equivalentemente, tenemos

$$V/v_{n,e}V = \Lambda/(p^k, v_{n,e}) \cong \mathbb{Z}/(p^k) + \mathbb{Z}/(p^k)T + \cdots + \mathbb{Z}/(p^k)T^{\deg v_{n,e}}. \tag{94}$$

Por tanto, $|V/v_{n,e}V| = p^{k \deg v_{n,e}} = p^{k(p^n - p^e)} = p^{kp^n + c}$, con $c = p^{-kp^e}$.

(3) Caso $V = \Lambda/(g)$. Sea $d = \deg g$. Como g es distiguido, podemos escribir $g = T^d + pq$, con q un polinomio de grado menor que d. Tenemos $T^d \equiv pq \mod g$, de donde se tiene que

$$T^k \equiv p(\text{polinomio}) \mod g \tag{95}$$

para $k \geq d$. Si $p^n \geq d$, de lo anterior se deduce que

$$(1+T)^{p^n} = 1 + p(\text{polinomio}) + T^{p^n} \equiv 1 + p(\text{polinomio}) \mod g \tag{96}$$

Por tanto,

$$(1+T)^{p^{n+1}} \equiv 1 + p^2(\text{polinomio}) \mod g \tag{97}$$

Sea $P_n = (1+T)^{p^n} - 1$, que es un polinomio distiguido. De lo anterior se deduce que

$$\begin{aligned} P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 \\ &= ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1)((1+T)^{p^{n+1}} - 1) \\ &\equiv (1 + \cdots + 1 + (p^2)(\text{polinomio}))(P_{n+1}) \quad \text{mód } g \\ &\equiv p(1 + (p)(\text{polinomio}))P_{n+1} \quad \text{mód } g \end{aligned} \tag{98}$$

Como $1 + (p)(\text{polinomio}) \in \Lambda^\times$, entonces P_{n+2}/P_{n+1} actúa como $(p)(\text{unidad})$ sobre $V = \Lambda/(g)$ para $p^n \geq d$.

Supongamos $n_0 > e$, $p^{n_0} \geq d$, y $n \geq n_0$. Entonces,

$$\frac{v_{n+2,e}}{v_{n+1,e}} = \frac{v_{n+2}}{v_{n+1}} = \frac{P_{n+2}}{P_{n+1}}, \tag{99}$$

de donde se tiene que

$$v_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(v_{n+1,e}V) = pv_{n+1,e}V. \tag{100}$$

Por tanto,

$$|V/v_{n+2,e}V| = |V/pv_{n+1,e}V| = |V/pV||pV/pv_{n+1,e}V|, \tag{101}$$

para $n \geq n_0$. Como g y p son coprimos, la multiplicación por p es inyectiva, por lo que

$$|pV/pv_{n+1,e}V| = |V/v_{n+1,e}V|, \tag{102}$$

de manera que

$$|V/v_{n+2,e}V| = |V/pV||V/v_{n+1,e}V|. \tag{103}$$

Como $V/pV \cong \Lambda/(p,g) = \Lambda/(p,T^d)$, entonces $|V/pV| = |\Lambda/(p,T^d)| = p^d$, ya que

$$\Lambda/(p,T^d) \cong \mathbb{Z}/(p) + \mathbb{Z}/(p)T + \cdots + \mathbb{Z}/(p)T^d. \tag{104}$$

Aplicando lo anterior, veremos por inducción sobre n que

$$|V/v_{n,e}V| = p^{d(n-n_0-1)}|V/v_{n_0+1,e}V|, \tag{105}$$

para $n \geq n_0 + 1$. En efecto, si $n = n_0 + 1$ el resultado es evidente. Supongámoslo cierto hasta $n+1$ y veamos que se cumple para $n+2$. Aplicando (103) tenemos $|V/v_{n+2,e}V| = p^d|V/v_{n+1,e}V|$, y aplicándo la hipótesis de inducción, tenemos

$$|V/v_{n+2,e}V| = p^d p^{d((n+1)-n_0-1)}|V/v_{n_0+1,e}V| = p^{d((n+2)-n_0-1)}|V/v_{n_0+1,e}V|, \tag{106}$$

por lo que (105) se cumple.

Como $E/v_{n,e}E$ es finito por hipótesis, $|V/v_{n,e}V|$ debe ser finito para todo n, por lo que de (105) tenemos que $|V/v_{n,e}V| = p^{dn+c}$ si $n \geq n_0 + 1$, con $c = p^{d(-n_0-1)}$.

Juntándo **(1)**, **(2)** y **(3)**, como $|E/v_{n,e}E|$ es el producto de todos los $|V/v_{n,e}V|$, tenemos $|E/v_{n,e}E| = p^{mp^n+ln+c}$ si $n > n_0$, con c una nueva constante obtenida como suma de las múltiples constantes anteriores. □

Lema 4.8. Sean Y y E dos Λ–módulos tales que $Y \sim E$ y que $Y/v_{n,e}Y$ es finito para todo $n \geq e$. Entonces, para ciertos $c, n_0 \in \mathbb{Z}$ tenemos que $|Y/v_{n,e}Y| = p^d|E/v_{n,e}E|$ para todo $n \geq n_0$.

Demostración. Tenemos el diagrama conmutativo siguiente, en que ϕ es la aplicación dada por $Y \sim E$, ϕ'_n es la restricción de ϕ a $v_{n,e}Y$, y ϕ''_n es tal que si $\bar{y} \in Y/v_{n,e}Y$, entonces $\phi''_n(\bar{y}) = \overline{\phi(y)} \in v_{n,e}E$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & v_{n,e}Y & \longrightarrow & Y & \longrightarrow & Y/v_{n,e}Y & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & v_{n,e}E & \longrightarrow & E & \longrightarrow & E/v_{n,e}E & \longrightarrow & 0 \end{array}$$

Veamos que la secuencia $0 \xrightarrow{\alpha_1} v_{n,e}Y \xrightarrow{\alpha_2} Y \xrightarrow{\alpha_3} Y/v_{n,e}Y \xrightarrow{\alpha_4} 0$ es exacta. Consideremos α_1, α_2 como las inclusiones naturales, y α_3, α_4 como las proyecciones naturales. Las condiciones $\operatorname{Im}\alpha_1 = \operatorname{Ker}\alpha_2$ y $\operatorname{Im}\alpha_3 = \operatorname{Ker}\alpha_4$ corresponden a la inyectividad y exhaustividad de las aplicaciones α_2 y α_3 respectivamente. La condición $\operatorname{Im}\alpha_2 = \operatorname{Ker}\alpha_3$ se satisface por la definición del cociente $Y/v_{n,e}Y$. Por tanto, la secuencia es exacta. De manera análoga se comprueba que la secuencia $0 \to v_{n,e}E \to E \to E/v_{n,e}E \to 0$ es exacta.

Por el Lema de la Serpiente, hay una secuencia exacta

$$0 \to \operatorname{Ker}\phi'_n \to \operatorname{Ker}\phi \to \operatorname{Ker}\phi''_n \to \operatorname{Coker}\phi'_n \to \operatorname{Coker}\phi \to \operatorname{Coker}\phi''_n \to 0. \tag{107}$$

Todas las aplicaciones son naturales excepto la aplicación $\operatorname{Ker}\phi''_n \longrightarrow \operatorname{Coker}\phi'_n$. Dado un $x \in \operatorname{Ker}\phi''_n$, existe $y \in Y$ tal que su imagen es x en $Y/(v_{n,e})Y$. Como $\phi(y) \in E$ tiene imagen cero en $E/v_{n,e}E$ por la conmutatividad del diagrama, debemos tener $\phi(y) \in v_{n,e}E$. Además, $\phi(y) \mod \phi'_n(v_{n,e}Y)$ depende solo de x, de manera que la aplicación $\operatorname{Ker}\phi''_n \longrightarrow \operatorname{Coker}\phi'_n$ es la dada por $x \mapsto \phi(y)$.

Notemos que $\operatorname{Ker}\phi$ y $\operatorname{Coker}\phi$ son finitos porque $Y \sim E$. $\operatorname{Ker}\phi'_n$ es finito porque la aplicación $\operatorname{Ker}\phi'_n \to \operatorname{Ker}\phi$ es inyectiva, y $\operatorname{Coker}\phi''_n$ es finito porque la aplicación $\operatorname{Coker}\phi \to \operatorname{Coker}\phi''_n$ es exhaustiva. $\operatorname{Ker}\phi''_n$ es finito porque $Y/v_{n,e}Y$ es finito. Además, $\operatorname{Coker}\phi'_n$ es finito porque $\operatorname{Coker}\phi''_n$ es finito y $\operatorname{Coker}\phi'_n/\operatorname{Coker}\phi''_n$ se inyecta en $\operatorname{Coker}\phi$, que es finito.

Veremos que se cumplen las siguientes desigualdades:

(i) $|\operatorname{Ker}\phi'_n| \leq |\operatorname{Ker}\phi|$,

(ii) $|\operatorname{Coker}\phi'_n| \leq |\operatorname{Coker}\phi|$,

(iii) $|\operatorname{Coker}\phi''_n| \leq |\operatorname{Coker}\phi|$,

(iv) $|\operatorname{Ker}\phi''_n| \leq |\operatorname{Ker}\phi||\operatorname{Coker}\phi|$.

La desigualdad (i) se cumple porque la aplicación $\operatorname{Ker}\phi'_n \to \operatorname{Ker}\phi$ es inyectiva. La desigualdad (iii) se cumple porque la aplicación $\operatorname{Coker}\phi \to \operatorname{Coker}\phi''_n$ es exhaustiva. La desigualdad (ii) se cumple porque $\operatorname{Coker}\phi'_n \subseteq v_{n,e}\operatorname{Coker}\phi \subseteq \operatorname{Coker}\phi$.

Notemos que la aplicación natural $\operatorname{Ker}\phi/\operatorname{Ker}\Phi'_n \longrightarrow \operatorname{Ker}\phi''_n$ es inyectiva. Si consideramos la aplicación $\varphi : \operatorname{Ker}\phi''_n \longrightarrow \operatorname{Coker}\phi'_n$, claramente la aplicación $\operatorname{Ker}\phi''_n \longrightarrow \operatorname{Im}\varphi$ es exhaustiva. Tenemos así una secuencia exacta $0 \to \operatorname{Ker}\phi/\operatorname{Ker}\Phi'_n \to \operatorname{Ker}\phi''_n \to \operatorname{Im}\varphi \to 0$. Por el lema 1.19, tenemos

$$|\operatorname{Ker}\phi''_n| = |\operatorname{Ker}\phi/\operatorname{Ker}\Phi'_n||\operatorname{Im}\varphi|. \tag{108}$$

Como $|\operatorname{Ker}\phi/\operatorname{Ker}\Phi'_n| \leq |\operatorname{Ker}\phi|$ y $|\operatorname{Im}\varphi| \leq |\operatorname{Coker}\phi'_n|$, aplicando (ii) tenemos

$$|\operatorname{Ker}\phi''_n| \leq |\operatorname{Ker}\phi||\operatorname{Coker}\phi'_n| \leq |\operatorname{Ker}\phi||\operatorname{Coker}\phi|, \tag{109}$$

por lo que (iv) queda demostrado.

Supongamos ahora que $m \geq n \geq 0$. Veremos que se cumplen las desigualdades siguientes:

(a) $|\operatorname{Ker}\phi'_n| \geq |\operatorname{Ker}\phi'_m|$,

(b) $|\operatorname{Coker}\phi'_n| \geq |\operatorname{Coker}\phi'_m|$,

(c) $|\operatorname{Coker}\phi''_n| \leq |\operatorname{Coker}\phi''_m|$.

Observando que $v_{m,e} = (v_{m,e}/v_{n,e})v_{n,e}$, vemos que $v_{m,e}Y \subseteq v_{n,e}Y$, por lo que tenemos $\operatorname{Ker}\phi'_m \subseteq \operatorname{Ker}\phi'_n$, de manera que $|\operatorname{Ker}\phi'_m| \leq |\operatorname{Ker}\phi'_n|$, por lo que (a) queda demostrado.

Sea $v_{m,e}y \in v_{m,e}E$, y sea $z \in v_{n,e}E$ un representante de $v_{n,e}y$ en $\operatorname{Coker}\phi'_n$. Entonces, $v_{n,e}y - z = \phi(v_{n,e}x)$ para algún $x \in Y$. Si multiplicamos por $v_{m,e}/v_{n,e}$, obtenemos

$$v_{m,e}y - \frac{v_{m,e}}{v_{n,e}}z = \frac{v_{m,e}}{v_{n,e}}\phi(v_{n,e}x) = \phi(v_{m,e}x) = \phi'_m(v_{m,e}x). \tag{110}$$

Por tanto, $v_{m,e}/v_{n,e}$ multiplicado por representantes de $\operatorname{Coker}\phi'_n$ da representantes de $\operatorname{Coker}\phi'_m$, por lo que $\operatorname{Coker}\phi'_m \subseteq \operatorname{Coker}\phi'_n$, que demuestra (b).

Como $v_{m,e}E \subseteq v_{n,e}E$, entonces $E/v_{n,e}E \subseteq E/v_{m,e}E$, de donde $\operatorname{Coker}\phi''_n \subseteq \operatorname{Coker}\phi''_m$, que demuestra (c).

Veamos a continuación que los órdenes de $\operatorname{Ker}\phi'_n$, $\operatorname{Coker}\phi'_n$, $\operatorname{Coker}\phi''_n$ y $\operatorname{Ker}\phi''_n$ son constantes si $n \geq n_0$, para algun n_0. Como $\operatorname{Ker}\phi$ es finito por ser ϕ pseudo–isomorfismo, que $|\operatorname{Ker}\phi'_n|$ es constante si $n \geq n_0$ se deduce de (i) y (a). Como $\operatorname{Coker}\phi$ es finito por ser ϕ pseudo–isomorfismo, que $|\operatorname{Coker}\phi'_n|$ es constante si $n \geq n_0$ se deduce de (ii) y (b), y que $|\operatorname{Coker}\phi'_n|$ es constante si $n \geq n_0$ se deduce de (iii) y (c). Además, aplicando el lema 1.19 a (107), tenemos

$$|\operatorname{Ker}\phi'_n||\operatorname{Ker}\phi''_n||\operatorname{Coker}\phi| = |\operatorname{Ker}\phi||\operatorname{Coker}\phi'_n||\operatorname{Coker}\phi''_n|, \tag{111}$$

de donde se deduce que $|\operatorname{Ker}\phi''_n|$ debe ser constante para $n \geq n_0$.

Si consideramos la aplicación $\phi''_n : Y/v_{n,e}Y \longrightarrow E/v_{n,e}E$, tenemos la secuencia exacta $\operatorname{Ker}\phi''_n \to Y/v_{n,e}Y \to E/v_{n,e}E \to \operatorname{Coker}\phi''_n$. Por el lema 1.19, tenemos

$$|\operatorname{Ker}\phi''_n||E/v_{n,e}E| = |Y/v_{n,e}Y||\operatorname{Coker}\phi''_n|. \tag{112}$$

Si $n \geq n_0$, $|\operatorname{Ker}\phi''_n|$ y $|\operatorname{Coker}\phi''_n|$ son constantes, por lo que tenemos

$$|Y/v_{n,e}Y| = \frac{|\operatorname{Ker}\phi''_n|}{|\operatorname{Coker}\phi''_n|}|E/v_{n,e}E| = p^d|E/v_{n,e}E|, \tag{113}$$

para cierto d, tal y como queríamos demostrar. □

Como $Y_e \sim X$ y $X/v_{n,e}Y_e \cong X_n$ es finito, entonces $Y_e/v_{n,e}Y_e \sim X/v_{n,e}Y_e$ es finito. De (92) tenemos que $Y_e \sim E$, con E dado por (93). Aplicando la proposición 4.7, tenemos

$$|E/v_{n,e}E| = p^{mp^n+ln+c}, \tag{114}$$

para todo $n > n_0$.

Por el teorema 1.51, tenemos que $X_n = \mathrm{Gal}(L_n/K_n)$ es isomorfo a la p–parte de $\mathrm{Cl}(K_n)$. Como p^{e_n} es la potencia exacta de p que divide $|\mathrm{Cl}(K_n)|$, tenemos $p^{e_n} = |X_n|$.

Aplicando que $X_n \cong X/v_{n,e}Y_e$ y que X/Y_e es finito, tenemos

$$|X_n| = |X/Y_e||Y_e/v_{n,e}Y_e|, \tag{115}$$

y como $X/Y_e \cong X_e$, entonces $|X/Y_e| = p^{c'}$ para cierto c'. Aplicando ahora (114) y el lema 4.8, tenemos

$$p^n = p^{c'+c}|E/v_{n,e}E| = p^{mp^n+ln+c+c'+d} \tag{116}$$

para todo $n > n_0$. Si escogemos $\lambda = m$, $\mu = l$ y $\nu = c + c' + d$, entonces

$$e_n = \lambda n + \mu p^n + \nu, \tag{117}$$

para todo $n > n_0$, tal y como queríamos ver.

4.2. μ–invariantes.

Uno de los principales resultados sobre μ–invariantes es el dado por el teorema siguiente.

Teorema 4.9 (Teorema de Ferrero–Washington). Sea K una extensión abeliana de $\mathbb{Q}$ y K_∞/K su $\mathbb{Z}_p$–extensión ciclotómica. Entonces, $\mu = 0$.

Demostración. Véase el capítulo 7 de [14]. □

Notemos que el teorema anterior solo es válido para extensiones ciclotómicas. De hecho, Iwasawa construyó ejemplos explícitos de extensiones no ciclotómicas para las cuales $\mu > 0$. No obstante, Iwasawa conjeturó que el teorema anterior puede extenserse a cualquier extensión de $\mathbb{Q}$, no necesariamente abeliana.

Conjetura 4.10 (Conjetura de Iwasawa). Sea K un cuerpo de números y K_∞/K su $\mathbb{Z}_p$–extensión ciclotómica. Entonces, $\mu = 0$.

De hecho, Iwasawa realizó la conjetura anterior con anterioridad a que Ferrero y Washington demostraran su teorema.

4.3. λ–invariantes.

A continuación, enunciaremos un resultado recopilatorio sobre el λ–invariante en ciertas $\mathbb{Z}_2$–extensiones ciclotómicas de un cuerpo real cuadrático.

Teorema 4.11. Sea $K = \mathbb{Q}(\sqrt{m})$ o $K = \mathbb{Q}(\sqrt{2m})$, y supongamos que m es uno de los siguientes:

1. $m = 2$,
2. $m = p$, con $p \equiv 5 \mod 8$,
3. $m = p$, con $p \equiv 3 \mod 4$,
4. $m = pq$, con $p \equiv 3, q \equiv 7 \mod 8$,
5. $m = p$, con $p \equiv 1 \mod 8$ y $2^{(p-1)/4} \not\equiv (-1)^{(p-1)/8} \mod p$,

6. $m = pq$, con $p \equiv q \equiv 3 \mod 8$,
7. $m = pq$, con $p \equiv 3, q \equiv 5 \mod 8$,
8. $m = pq$, con $p \equiv 5, q \equiv 7 \mod 8$,
9. $m = pq$, con $p \equiv q \equiv 5 \mod 8$,
10. $m = pq$, con $p \equiv 3, q \equiv 1 \mod 8$, $(p/q) = -1$ y $2^{(q-1)/4} \equiv -1 \mod q$,
11. $m = pq$, con $p \equiv 7 \mod 8$, $q \equiv 9 \mod 16$ y $(p/q) = -1$,
12. $m = pq$, con $p \equiv 7, q \equiv 1 \mod 16$, $(p/q) = -1$, y $2^{(q-1)/4} \equiv -1 \mod q$,

con p y q números primos diferentes y $(*/*)$ el símbolo de Legendre[9]. Entonces, el λ–invariante de la $\mathbb{Z}_2$–extensión ciclotómica de K es $\lambda_K = 0$.

Demostración. Véanse [9], [2] y [8]. □

El resultado siguiente determina una condición bajo la cual el λ–invariante de la $\mathbb{Z}_p$–extensión ciclotómica de un cuerpo de números se anula.

Teorema 4.12. Sea K un cuerpo de números. Si solo un primo de K divide p, y p no divide al número de clases de K, entonces el λ–invariante de la $\mathbb{Z}_p$ extensión ciclotómica de K es $\lambda_K = 0$.

Demostración. Véase [1]. □

[9]Si q es un entero y p un primo impar, el **símbolo de Legendre** (q/p) se define como $(q/p) = 0$ si p divide a q, $(q/p) = 1$ si q es residuo cuadrático módulo p, y $(q/p) = -1$ en cualquier otro caso.

5. Referencias

[1] D. S. Dummit, D. Ford, H. Kisilevsky, J. W. Sands, *Computation of Iwasawa Lambda Invariants for Imaginary Quadratic Fields.*. Journal of number theory 37, 1991.

[2] T. Fukuda, K. Komatsu, *On the Iwasawa λ–invariant of the Cyclotomic $\mathbb{Z}_2$-Extension of a Real Quadratic Field.* Tokyo J. Math 28, 2005.

[3] Serge Lang, *Cyclotomic fields I and II.* Springer-Verlag, 1990.

[4] Dino Lorenzini, *An Invitation to Arithmetic Geometry.* American Mathematical Society, 1996.

[5] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra.*

[6] Jürgen Neukirch, *Algebraic number theory.* Springer-Verlag, 2000.

[7] J. Neukirch, A. Schmidt, K. Wingberg *Cohomology of Number Fields.* Springer-Verlag, 1999.

[8] Y. Nishino, *On the Iwasawa Invariants of the Cyclotomic $\mathbb{Z}_2$-Extension of Certain Real Quadratic Fields.* Tokyo J. Math 29, 2006.

[9] M. Ozaki, H. Taya, *On the Iwasawa λ_2–invariants of certain family of real quadratic fields.* Manuscripta Math 94, 1997.

[10] L. Salce, *Structtura dei p-gruppi abeliani.* Quaderni dell'Unione Matematica Italiana 18, Pitagora Editrice, UMI, Bologna, 1980.

[11] J. C. Schettler, *The Change in Lambda Invariants for Cyclic p–Extensions of $\mathbb{Z}_p$–Fields.*. University of Arizona, 2012.

[12] Artur Travesa, *Teoria de Nombres.* Apunts del curs 1991/92, Universitat de Barcelona. Addison-Wesley, 1969.

[13] Jone Uria, *Correspondència bijectiva de Galois en extensions no finites.* UAB, 2012.

[14] Lawrence C. Washington, *Introduction to cyclotomic fields.* Springer-Verlag, 1982.

[15] C. A. Weibel, *An introduction to homological algebra.* Cambridge University Press, 1994.