Pontificia Universidad Católica de Valparaíso

Facultad de Ciencias

Instituto de Matemáticas

Teoría de Iwasawa

Trabajo final para obtener el grado de Magister en Matemáticas

Javiera Gallegos Zúñiga

Profesor Guía: *Florence Gillibert*

Valparaíso, Chile, 2017

Índice

Introducción

Fue en una conferencia de 1956, cuando Kenkichi Iwasawa presentó la demostración de un teorema, que corresponde al Teorema 2.4.1 de este trabajo, que inauguraba lo que hoy llamamos teoría de Iwasawa. La teoría de Iwasawa describe el crecimiento de la p-parte de Sylow del grupo de clase en un tipo de extensiones de cuerpos llamadas $\mathbb{Z}_p$-extensiones o extensiones p-ádicas.

El objetivo del primer capítulo de este trabajo es presentar resultados preliminares para el desarollo del capítulo principal. Comenzamos con definiciones y teoremas elementales de la teoría de Galois clásica. Abordamos la noción de grupos topológicos, grupos profinitos y definimos sobre grupos de Galois la topología de Krull. Todo esto para dar paso al teorema fundamental de la teoría de Galois de extensiones infinitas. Aplicamos este esencial resultado para desarrollar un ejemplo primordial para el resto del trabajo: encontrar una extensión de cuerpos cuyo grupo de Galois sea $(\mathbb{Z}_p, +)$, es decir, probamos la existencia de $\mathbb{Z}_p$-extensiones. También revisamos elementos sobre la teoría de ramificación y del cuerpo de clase.

Para finalizar, en el segundo capítulo comenzamos con anillo de grupo y series de potencias, para mostrar un isomorfismo entre el anillo de series de potencias sobre un anillo de enteros de una extensión finita de $\mathbb{Q}_p$ y el anillo de grupo profinito de Γ, con Γ un grupo topológico multiplicativo isomorfo al grupo $(\mathbb{Z}_p, +)$. Usando teoría de ramificación revisaremos algunos resultados sobre $\mathbb{Z}_p$-extensiones. También mostraremos un teorema

importantísimo que define la acción de Λ sobre $\mathbb{Z}_p$-extensiones con $\Lambda = \mathbb{Z}_p[[T]]$. Este teorema es conocido como el teorema de estructura de Λ-módulos. Para concluir enunciaremos el teorema de Iwasawa y desarrollamos la idea principal de su demostración.

El presente trabajo está basado en el capítulo *Teoría de Iwasawa de $\mathbb{Z}_p$-extensiones* del libro *Introduction to Cyclotomic Fields* de Lawrence Washington.

Capítulo 1

Extensiones de Galois infinitas

Un lugar donde la toplogía trae claridad a un tema algeraico es la teoría de Galois. Dicha teoría entrega relaciones entre grupos de automorfimos y cuerpos intermedios, siempre y cuando estemos trabajando en extensiones de cuerpos finitas. Sin embargo, si las extensiones en cuestión son infinitas las relaciones se rompen y es ahí donde la topología vuelve a entregar claridad.

Para comenzar introduciremos algunos conceptos y resultados elementales respecto a la teoría de Galois clásica, que para más detalles pueden ser encontrados en diversos textos sobre el tema.

1.1 Extensiones de Galois finitas

Definición 1. Sean E y F cuerpos. Decimos que E es una extensión de cuerpo de F y anotamos E/F si $F \subseteq E$. En particular, E es un F-espacio vectorial y su dimensión es llamada el grado de E sobre F y se anota $[E : F]$.

Definición 2. Decimos que E/F es una extensión de cuerpos algebraica si cada elemento

$\alpha \in E$ es algebraico sobre F, es decir, existe $f(X) \in F[X]$ no nulo tal que $f(\alpha) = 0$. Si $f(X)$ es mónico e irreducible sobre F, entonces decimos que $f(X)$ es el polinomio minimal de α sobre F.

Definición 3. Un cuerpo es algebraicamente cerrado si no tiene extensiones algebraicas salvo sí mismo. Una clausura algebraica de E es una extensión algebraica $\bar{E}$ que es algebraicamente cerrada.

Definición 4. Una extensión algebraica de cuerpos E/F es separable si el polinomio minimal sobre F de cada elemento de E es separable, es decir, si sus raíces en una clausura algebraica son distintas.

Definición 5. Una extensión algebraica de cuerpos E/F es normal si el polinomio minimal sobre F de cada elemento de E se escinde en E, es decir, se descompone en factores de grado 1.

Observación 1. *Sea E/F extensión algraica y $f \in F[X]$ irreducible de grado n, con $n = [E : F]$. Si f tiene una raíz en E entonces E/F es separable y normal si y sólo si f tiene n raíces distintas en E.*

Proposición 1.1.1: *Si E es el cuerpo de descomposición de un polinomio separable $f \in F[X]$, entonces el orden de $Gal(E/F)$ es $[E : F]$.*

Definición 6. Sea G un grupo de automorfismos de un cuerpo E, el conjunto

$$E^G = Inv(G) = \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \ \sigma \in G\}$$

es el cuerpo fijo de G respecto a E.

Definición 7. Sea F un cuerpo. Una extensión finita E/F es Galois si F es el cuerpo fijo del grupo $Aut(E/F)$. En tal caso, este grupo es llamado el grupo de Galois de E sobre F y es denotado $Gal(E/F)$.

Teorema 1.1.2: *Sea E/F una extensión de grado finito. Son equivalentes:*

1. *E es el cuerpo de descomposición de un polinomio separable $f \in F[X]$.*

2. *$F = E^G$ para algún grupo finito de automorfismos de E.*

3. *E es normal y separable sobre F.*

4. *E/F es de Galois.*

Observamos que el ítem 3 es frecuentemente usado como definición de extensión de Galois.

Corolario 1.1.3: *Sea $F \subseteq M \subseteq E$, si E/F es de Galois, entonces E/M es de Galois. Además, $Gal(E/M)$ es un subgrupo de $Gal(E/F)$.*

Teorema 1.1.4: *(Teorema fundamental de la teoría de Galois clásica) Sea E/F de Galois y $G = Gal(E/F)$. Entonces existe una biyección:*

$$\begin{array}{ccc} \{H \text{ subgrupos de } G\} & \longleftrightarrow & \{\text{cuerpos intermedios } F \subseteq M \subseteq E\} \\ H & \longmapsto & E^H \\ Gal(E/M) & \longleftarrow & M \end{array}$$

Más aún,

1. *la biyección revierte contenciones: $H_1 \supset H_2$ si y sólo si $E^{H_1} \subset E^{H_2}$;*

2. *índices iguales a grados: $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$;*

3. *H is normal in G si y sólo si E^H/F es normal (y por tanto Galois). En tal caso $Gal(E^H/F) \simeq G/H$.*

Ejemplo 1. *Consideremos el polinomio $f(X) = X^4 - 3 \in \mathbb{Q}[X]$. Por criterio de irreducibilidad de Eisenstein, el polinomio $f(X)$ es irreducible en $\mathbb{Q}$. Si denotamos $\alpha = \sqrt[4]{3} \in \mathbb{R}$, las raíces de $f(X)$ en $\mathbb{C}$ son $\alpha, -\alpha, \alpha i, -\alpha i$ y su cuerpo de descomposición es $E = \mathbb{Q}(\alpha, i)$. Analicemos el grupo de Galois de $E/\mathbb{Q}$ y la correspondencia entre sus subgrupo y los cuerpos intermedios de esta extensión.*

Observemos en primer lugar que la extensión $E/\mathbb{Q}$ *es de Galois puesto que* $f(X) \in \mathbb{Q}[X]$ *es irreducible y* E *es el cuerpo de descomposición de* f*. Ahora bien, como* $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ *y* $[\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)] = 2$ *entonces* $[E : \mathbb{Q}] = 8$ *y los 8 automorfismos de* E *están determinados por su acción sobre* i *y* α*. Así,* $Gal(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \cdots, \sigma_8\}$ *donde*

$$\begin{aligned}
\sigma_1(\alpha) &= \alpha, & \sigma_1(i) &= i \\
\sigma_2(\alpha) &= \alpha, & \sigma_2(i) &= -i \\
\sigma_3(\alpha) &= -\alpha, & \sigma_3(i) &= i \\
\sigma_4(\alpha) &= -\alpha, & \sigma_4(i) &= -i \\
\sigma_5(\alpha) &= \alpha i, & \sigma_5(i) &= i \\
\sigma_6(\alpha) &= \alpha i, & \sigma_6(i) &= -i \\
\sigma_7(\alpha) &= -\alpha i, & \sigma_7(i) &= i \\
\sigma_8(\alpha) &= -\alpha i, & \sigma_8(i) &= -i
\end{aligned}$$

La tabla de multiplicación de $Gal(E/\mathbb{Q})$ *es*

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_2	σ_2	σ_1	σ_4	σ_3	σ_8	σ_7	σ_6	σ_5
σ_3	σ_3	σ_4	σ_1	σ_2	σ_7	σ_8	σ_5	σ_6
σ_4	σ_4	σ_3	σ_2	σ_1	σ_6	σ_5	σ_8	σ_7
σ_5	σ_5	σ_6	σ_7	σ_8	σ_3	σ_4	σ_1	σ_2
σ_6	σ_6	σ_5	σ_8	σ_7	σ_2	σ_1	σ_4	σ_3
σ_7	σ_7	σ_8	σ_5	σ_6	σ_1	σ_2	σ_3	σ_4
σ_8	σ_8	σ_7	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

A partir de la tabla, deducimos que $Gal(E/\mathbb{Q}) = D_8$*,* $\sigma_2\sigma_5\sigma_2^{-1} = \sigma_5^{-1}$ *y* σ_2, σ_5 *son de orden* 2 *y* 4 *respectivamente.*

Los subgrupos de $Gal(E/\mathbb{Q})$ *son*

$$\langle\sigma_1\rangle = \{\sigma_1\},\ \langle\sigma_2\rangle = \{\sigma_1,\sigma_2\},\ \langle\sigma_3\rangle = \{\sigma_1,\sigma_3\},\ \langle\sigma_4\rangle = \{\sigma_1,\sigma_4\},$$
$$\langle\sigma_5\rangle = \{\sigma_1,\sigma_3,\sigma_5,\sigma_7\},\ \langle\sigma_6\rangle = \{\sigma_1,\sigma_6\},\ \langle\sigma_7\rangle = \{\sigma_1,\sigma_3,\sigma_5,\sigma_7\},$$
$$\langle\sigma_8\rangle = \{\sigma_1,\sigma_8\},\ \langle\sigma_2,\sigma_3\rangle = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\},\ \langle\sigma_3,\sigma_6\rangle = \{\sigma_1,\sigma_3,\sigma_6,\sigma_8\}$$

Usando que una base de E como $\mathbb{Q}$ espacio vectorial es $\{1,\alpha,\alpha^2,\alpha^3,i,\alpha i,\alpha^2 i,\alpha^3 i\}$, podemos encontrar los respetivos cuerpos fijos asociados a cada subgrupo de $Gal(E/\mathbb{Q})$ y así determinar los cuerpos intermedios de la extensión $E/\mathbb{Q}$, como se muesta a continuación:

$$\begin{array}{ccc}
\mathbb{Q} & \leftrightarrow & Gal(E/\mathbb{Q}) \\
\mathbb{Q}(\sqrt{3},i) & \leftrightarrow & \langle\sigma_3\rangle \\
\mathbb{Q}(\sqrt[4]{3}) & \leftrightarrow & \langle\sigma_2\rangle \\
\mathbb{Q}(\sqrt[4]{3},i) & \leftrightarrow & \langle\sigma_4\rangle \\
\mathbb{Q}(\sqrt[4]{3}+\sqrt[4]{3}i) & \leftrightarrow & \langle\sigma_6\rangle \\
\mathbb{Q}(\sqrt[4]{3}-\sqrt[4]{3}i) & \leftrightarrow & \langle\sigma_8\rangle \\
\mathbb{Q}(\sqrt{3}) & \leftrightarrow & \langle\sigma_2,\sigma_3\rangle \\
\mathbb{Q}(i) & \leftrightarrow & \langle\sigma_5\rangle = \langle\sigma_7\rangle \\
\mathbb{Q}(\sqrt{3}i) & \leftrightarrow & \langle\sigma_3,\sigma_6\rangle
\end{array}$$

Ejemplo 2. *Sea p un número primo, $\mathbb{F}_p$ cuerpo finito de cardinalidad y característica p y $\overline{\mathbb{F}_p}$ su clausura algebraica, entonces $\overline{\mathbb{F}_p}$ es infinito y $\overline{\mathbb{F}_p}/\mathbb{F}_p$ es una extensión de Galois (extensión normal y separable). Consideremos Γ el subgrupo de $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ generado por el automorfismo de Frobenius $a \mapsto a^p$. Dado k un entero positivo, entonces $\overline{\mathbb{F}_p}$ contiene un único subcuerpo de cardinalidad p^k, que corresponde al cuerpo de descomposición de $X^{p^k} - X$.*

Para n entero postivo, definamos E_n subcuerpo de $\overline{\mathbb{F}_p}$ de cardinalidad p^{2^n}. Como $2^n|2^{n+1}$, tenemos una cadena creciente de subcuerpos de $\overline{\mathbb{F}_p}$.

Sea $E = \bigcup_{n=1}^{\infty} E_n$, entonces $E \subsetneq \overline{\mathbb{F}_p}$ pues E no tiene un subcuerpo de cardinalidad p^3 y $\overline{\mathbb{F}_p}$ sí.

Por otro lado, $\overline{\mathbb{F}_p}/\mathbb{F}_p$ es Galois, entonces $\overline{\mathbb{F}_p}/E$ es Galois, esto significa que E es el cuerpo

fijo de $Gal(\overline{\mathbb{F}_p}/E)$ *y como* $E \subsetneq \overline{\mathbb{F}_p}$ *entonces* $Gal(\overline{\mathbb{F}_p}/E)$ *es no trivial. Observemos que si* $\sigma \in Gal(\overline{\mathbb{F}_p}/E)$ *distinto a* $Id_{\overline{\mathbb{F}_p}}$ *no puede existir un entero positivo* m *tal que* $\sigma(a) = a^{p^m}$ *para todo* $a \in \overline{\mathbb{F}_p}$*, porque de lo contrario cada elemento de* E*, que es infinito, sería un cero de* $X^{p^m} - X$*. Por lo tanto,* $Gal(\overline{\mathbb{F}_p}/E) \nsubseteq \Gamma$ *y así* $\Gamma \neq Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$*.*

Sabemos que $\mathbb{F}_p$ *es el cuerpo fijo de* Γ *y también lo es de* $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$*. De esta forma, a* Γ *subgrupo de* $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ *no le corresponde ningún cuerpo intermedio.*

En conclusión no es posible aplicar el Teorema de Galois clásico de forma directa en dimensión infinita. Sin embargo, para corregir esto incluimos una topología al grupo de Galois y obtenemos un resultado similar al clásico.

1.2 Grupos Topológicos y Grupos Profinitos

Definición 8. Un grupo topológico es un grupo G con una topología tal que la multiplicación e inversión

$$m_G: \begin{array}{ccc} G \times G & \to & G \\ (g,h) & \mapsto & gh \end{array} \quad \text{y} \quad n_G: \begin{array}{ccc} G & \to & G \\ g & \mapsto & g^{-1} \end{array}$$

son continuas. Un homomorfismo de grupos topológicos es un homomorfismo de grupos continuo y un isomorfismo es un isomorfismo de grupos homeomorfo.

Observación 2. *De la definición es claro que dado* $a \in G$*, la multiplicación a izquierda*

$$L_a: \begin{array}{ccc} G & \to & G \\ g & \mapsto & ag \end{array}$$

es continua. Es más, L_a *es un homeomorfismo con inversa* $L_{a^{-1}}$*. De forma similar, la multiplicacón a derecha, inversión y conjugación son homeomorfismos.*

Recordemos que si X un espacio topológico, una base de entornos para un punto $x \in X$ es un conjunto de entornos $\mathscr{M}$ tal que para todo U subconjunto abierto de X con $x \in U$ existe $M \in \mathscr{M}$ de manera que $x \in M \subseteq U$. Esta noción aplica también para grupos topológicos.

Proposición 1.2.1: *Sea $\phi : G \to H$ homomorfismo de grupos topológicos. Entonces ϕ es continuo si y sólo si ϕ es continuo en 1.*

Demostración. Si ϕ es continuo, entonces en particular es continua en 1. Por otra parte, sea $g \in G$ y V un entorno abierto de $\phi(g)$, entonces existe V' entorno abierto de 1_H tal que $\phi(g)V' \subseteq V$, por continuidad de la multiplicación a izquierda por $\phi(g)$ en 1_H. Como ϕ es continua en 1 también existe U' entorno abierto de 1_G tal que $\phi(U') \subseteq V'$.

Si consideramos $U = gU'$, U es u entorno abierto de g y así

$$\phi(U) = \phi(g)\phi(U') \subseteq \phi(g)V' \subseteq V$$

. De esta forma, ϕ es continua en todo $g \in G$. □

Proposición 1.2.2: *Sea $\{G_i\}_{i\in I}$ una familia de grupos topológicos, entonces $G = \prod_{i\in I} G_i$ es un grupo topológico con la topología producto.*

Demostración. Sean

$$m_G = \prod_{i\in I} m_{G_i} \quad \text{y} \quad n_G = \prod_{i\in I} n_{G_i}$$

donde m_{G_i} y n_{G_i} son la multiplicación e inversión en G_i para cada $i \in I$. Debemos probar que m_G y n_G son continuas. Para ello, sea $\pi_i : G \to G_i$ la proyección continua sobre el i-ésimo factor, entonces

$$\pi_i \circ m_G = m_i \circ (\pi_i \times \pi_i) \quad \text{y} \quad \pi_i \circ n_G = n_i \circ \pi_i \quad \text{para cada } i \in I$$

como $\pi_i \circ m_G$ y $\pi_i \circ n_G$ son compuestas de funciones continuas, entonces las respectivas proyecciones de m_G y $n_G$son continuas, y por tanto, m_G y n_G son continuas con la

topología producto. □

Proposición 1.2.3: *Sea G un grupo topológico y H subgrupo de G.*

1. *Si H abierto entonces H cerrado.*
2. *Si H cerrado de índice finito entonces H es abierto.*
3. *Supongamos que H es normal en G, entonces G/H es un espacio topológico discreto si y sólo si H es abierto.*

Demostración. En primer lugar notemos que $H^c = \bigcup_{g \notin H} gH$. A partir de esto:

1. Como H es abierto, todas las coclases $gH = L_g(H)$ son subconjuntos abiertos de G pues L_g es un homeomorfismo, como H^c es unión arbitraria de abiertos, entonces H^c es abierto. De esta forma, H es cerrado.
2. Como H es cerrado, todas las coclases $gH = L_g(H)$ son subconjuntos cerrados de G. Como el índice de H es finito, entonces hay finitas coclases. Luego H^c es unión finita de conjuntos cerrados, por tanto H^c es cerrado y así resulta ser H abierto.
3. Recordemos que $U \subseteq G/H$ es abierto si y sólo si su preimagen en G es abierto por definición de topología cociente. Ahora bien, G/H es un espacio topológico [7, Cap.1 Proposición 1.4] discreto si los singleton $\{gH\}$ con $g \in G$ son abiertos y como vimos antes, esto es equivalente a que H sea abierto.

□

Proposición 1.2.4: *Sea G un grupo topológico compacto y H un subgrupo de G abierto, entonces $(G : H)$ es finito.*

Demostración. Sabemos que gH coclase de G/H es un conjunto abierto de G y

$$G = \bigcup_{g \in R} gH$$

con R conjunto de representantes de las distintas coclases de G/H. El conjunto $\{gH : g \in R\}$ es un cubrimiento abierto de G, como G es compacto, este cubrimiento admite un subcubrimiento finito, por tanto, hay finitas coclases. Luego, $(G : H)$ es finito.

□

Ejemplo 3. *El grupo $GL_n(\mathbb{R})$ es un grupo topológico respecto a la multiplicación de matrices. En $GL_n(\mathbb{R})$ consideramos la topología generada por la métrica*

$$d(A, B) = \left(\sum_{i,j=1}^{n} |A_{ij} - B_{ij}|^2 \right)^{\frac{1}{2}}$$

para $A = (A_{ij}), B = (B_{ij}) \in GL_n(\mathbb{R})$. Las funciones $(A, B) \mapsto AB$ y $A \mapsto A^{-1}$ son continuas.

A continuación introduciremos la noción de Grupo Profinito que es un ejemplo de un grupo topológico que nos será de interés para las próximas secciones.

Definición 9. Un conjunto dirigido es un conjunto I con un orden parcial $\leq$ cumpliendo que para todo $i, j \in I$ exise $k \in I$ tal que $i \leq k$ y $j \leq k$.

Definición 10. Un sistema proyectivo $\{G_i, \phi_{ij}\}$ de grupos indexados por I conjunto dirigido consiste en una familia $\{G_i : i \in I\}$ de grupos y una familia $\{\phi_{ij} \in Hom(G_j, G_i) : i, j \in I, i \leq j\}$ de homomorfismos de grupos tal que:

i. $\phi_{ii} = Id_{G_i}$ para todo $i \in I$.

ii. $\phi_{ij} \circ \phi_{jk} = \phi_{ik}$ cuando $i \leq j \leq k$.

Definición 11. Dado un sistema proyetivo $\{G_i, \phi_{ij}\}$ de grupos indexados por I conjunto dirigido, formamos el producto cartesiano $\prod_{i\in I} G_i$ y consideramos el subgrupo

$$\varprojlim_{i\in I}(G_i, \phi_{ij}) = \{(x_i)_\epsilon \prod_{i\in I} G_i : \phi_{ij}(x_j) = x_i \quad \forall i, j \in I, i \leq j\}$$

llamado límite proyectivo. Si no hay ambigüedad respecto a los homomorfismos se denota $\varprojlim_{i\in I} G_i$. También a veces, si no hay confusión con el conjunto dirigido se denota simplemente $\varprojlim G_i$.

Definición 12. Un grupo profinito es un grupo topológico que es isomorfo (como grupo topológico) a un límite proyectivo de grupos finitos. Esta definición se puede formular también para anillos u objetos de otra categoría.

Ejemplo 4. *Definamos el orden parcial en* $\mathbb{N}$*:* $i \leq j$ *si y sólo si* $i \mid j$*. Sea* $G_i = \mathbb{Z}/i\mathbb{Z}$ *y para cada* $(i, j) \in \mathbb{N}^2$ *con* $i \leq j$ *sea*

$$\begin{array}{rccc} \phi_{ij}: & \mathbb{Z}/j\mathbb{Z} & \to & \mathbb{Z}/i\mathbb{Z} \\ & n \mod j & \mapsto & n \mod i \end{array}$$

entonces $\{\mathbb{Z}/i\mathbb{Z}, \phi_{ij}\}$ *es un sistema proyectivo y* $\varprojlim \mathbb{Z}/i\mathbb{Z} = \widehat{\mathbb{Z}}$ *por definición.*

Ejemplo 5. *Sea* p *un entero primo y* $\mathbb{F}_{p^i}$ *cuerpo finito de cardinalidad* p^i *con* $i \in \mathbb{N}$*. Bajo el mismo orden definido en el Ejemplo 4, consideremos* $G_i = Gal(\mathbb{F}_{p^i}/\mathbb{F}_p)$ *y*

$$\begin{array}{rccc} \varphi_{ij}: & Gal(\mathbb{F}_{p^j}/\mathbb{F}_p) & \to & Gal(\mathbb{F}_{p^i}/\mathbb{F}_p) \\ & \sigma & \mapsto & \sigma|_{\mathbb{F}_{p^i}} \end{array}$$

la familia $\{G_i, \varphi_{ij}\}$ *forma un sistema proyectivo. Además para cada* $i \in \mathbb{N}$*,* $Gal(\mathbb{F}_{p^i}/\mathbb{F}_p) \simeq_{f_i} \mathbb{Z}/i\mathbb{Z}$ *y los isomorfismos* f_i *son compatibles con los homomorfismos* ϕ_{ij}*, esto decir, el*

siguiente diagrama conmuta

$$\begin{array}{ccc} Gal(\mathbb{F}_{p^j}/\mathbb{F}_p) & \xrightarrow{\varphi_{ij}} & Gal(\mathbb{F}_{p^i}/\mathbb{F}_p) \\ {\scriptstyle f_j}\downarrow & & \downarrow{\scriptstyle f_i} \\ \mathbb{Z}/j\mathbb{Z} & \xrightarrow{\phi_{ij}} & \mathbb{Z}/i\mathbb{Z} \end{array}$$

Luego, tenemos un isomorofismo de límites proyectivos

$$\varprojlim Gal(\mathbb{F}_{p^i}/\mathbb{F}_p) \simeq \varprojlim \mathbb{Z}/i\mathbb{Z} = \hat{\mathbb{Z}}.$$

1.3 Topología de Krull sobre Grupos de Galois

Sea E/F una extensión algebraica, decimos por definición que E/F es de Galois si es normal y separable. Sobre el grupo $Gal(E/F)$ definiremos la topología de Krull que nos permitirá crear una correspondencia biyectiva entre las extensiones intermedias de E/F y los subgrupos cerrados de $Gal(E/F)$.

Definición 13. Sea $G = Gal(E/F)$ y $K \subseteq E$ una extensión intermedia finita sobre F. Sea $g \in G$, definimos $U_{g,F}$ conjunto que consta de los automorfismo $\sigma \in G$ que coinciden con g sobre F. Construímos una topología sobre G de manera que los $U_{g,F}$ formen una base de entornos abiertos de g.

Claramente estos conjuntos cubren todo G y si $\sigma \in U_{g_1,K_1} \cap U_{g_2,K_2}$ entonces $U_{g,K_1K_2} \subset U_{g_1,K_1} \cap U_{g_2,K_2}$, por lo tanto, los conjuntos $U_{g,K}$ forman una base para la topología que se define a partir de ellos. En particular,

$$U_{Id,K} = \{Gal(E/K) : K \subseteq E \text{ es una extensión finita y Galois sobre } F\}$$

es una base de entornos abiertos para $Id \in G$.

Definición 14. La topología sobre G generada por los conjuntos $U_{g,F}$ es llamada Topología de Krull.

Observación 3. *Para $S \subseteq E$ finito y G-estable (es decir, $\sigma(S) = S$, para todo $\sigma \in G$), sea $G(S) = \{\sigma \in G : \sigma(s) = s$, para todo $s \in S\}$. Entonces, $G(S)$ también forman una base de entornos abiertos para Id. Es más, basta considerar $K = F(S)$ y obtenemos que $U_{Id,K} = \{Gal(E/K) : K$ es una extensión finita y Galois sobre $F\} = G(S)$, además, cualquier $K \subseteq E$ extensión finita de F es de la forma $F(S)$ para algún $S \subseteq E$ finito.*

Observación 4. *Si $S \subseteq E$ es finito y G-estable entonces $G(S)$ es un subgrupo normal de G. En efecto, claramente $G(S)$ es un subgrupo de G. Ahora bien, sea $\sigma \in G$, $\tau \in G(S)$ y $s' \in S$ tal que $s' = \sigma^{-1}(s)$, entonces tenemos que*

$$\sigma\tau\sigma^{-1}(s) = \sigma\tau(s') = \sigma(s') = s$$

Por lo tanto, $\sigma\tau\sigma^{-1} \in G(S)$ y así, $G(S)$ es un subgrupo normal de G. A partir de esto, podemos concluir que también $U_{Id,K}$ con K una extensión intermedia de E/F Galois y finita sobre F es un subgrupo normal de G.

Observación 5. *Sea K una extensión intermedia de E/F Galois y finita sobre F, entonces $U_{Id,K}$ es de índice finito sobre G. Para ver esto, notemos que en primer lugar, $G/U_{Id,K}$ es un grupo, por Observación 5. Ahora bien, sea $S \subseteq E$ finito y G-estable tal que $K = F(S)$, entonces $U_{Id,K} = G(S)$. Definimos $G \to Sym(S)$ homomorfismo restricción a S, entonces $G(S)$ es el kernel de este homomorfismo y $G/G(S)$ es finito puesto que $Sym(S)$ es finito. De esta forma, $U_{Id,K}$ es de índice finito sobre G.*

Desde ahora denotaremos por $G = Gal(E/F)$ al grupo de Galois dotado de la topología de Krull.

Proposición 1.3.1: *El grupo G es Hausdorff, totalmente disconexo y compacto.*

Demostración. Sean $\sigma, \tau \in G$ distintos, entonces existe $a \in E$ tal que $\sigma(a) \neq \tau(a)$. Sea

$K = F(a)$. Observamos que $K \neq F$ ya que $a \notin F$. Consideremos los entornos abiertos $U_{\sigma,K}$ y $U_{\tau,K}$ de σ y τ respectivamente. Sean $\alpha \in U_{\sigma,K}$ y $\beta \in U_{\tau,K}$ entonces como $a \in K$ tenemos

$$\alpha(a) = \sigma(a) \neq \tau(a) = \beta(a)$$

es decir, $\alpha \neq \beta$ para todo $\alpha \in U_{\sigma,K}$ y $\beta \in U_{\tau,K}$. Luego, $U_{\sigma,K}$ y $U_{\tau,K}$ son disjuntos y por tanto, G es Hausdorff.

Para probar que G es totalmente disconexo, verificamos para la identidad, puesto que por traslación la propiedad se tiene para los otros elementos de G. Sea $\mathcal{C}$ una componente conexa que contenga a la identidad. Si $S \subseteq E$ y es G-estable, $Id \in G(S)$ y $G(S)$ es abierto, por tanto, $G(S)$ es cerrado. Luego, $\mathcal{C} \cap G(S)$ es un abierto y cerrado de $\mathcal{C}$. El conjunto $\mathcal{C}$ es conexo, entonces $\mathcal{C} \cap G(S) = \mathcal{C}$ o bien $\mathcal{C} \cap G(S) = \varnothing$, como $Id \in \mathcal{C} \cap G(S)$ tenemos que $\mathcal{C} \cap G(S) = \mathcal{C}$. De esta forma, $\mathcal{C} \subseteq G(S)$ para todo $S \subseteq E$ finito y G-estable, entonces

$$\mathcal{C} \subseteq \bigcap_{\substack{S \subseteq G \text{ finito} \\ G-\text{estable}}} G(S) = \{Id\}.$$

Así, $\mathcal{C}$ se reduce a un punto, y por tanto, G es totalmente disconexo.
Por otro lado, para la compacidad de G, por Observación 6 y Proposición 1.2.3 $G/G(S)$ es discreto y finito, por tanto, compacto. Luego, por teorema de Tychonoff

$$\prod_{\substack{S \subseteq G \text{ finito} \\ G-\text{estable}}} G/G(S)$$

es compacto. La idea es probar que G es cerrrado en este compacto y por tanto G es compacto. Para los detalles de este último argumento, ver [1, Cap. 7, Proposición 7.8]. □

1.4 Teorema fundamental de la teoría de Galois de extensiones infinitas

Proposición 1.4.1: *Sea E extensión de Galois de F y K extensión de F contenida en E. Entonces todo F-homomorfismo $K \to E$ se puede extender a un F-isomorfismo $E \to E$. De esta forma, si K/F es de Galois, la función*

$$\begin{array}{ccc} Gal(E/F) & \longrightarrow & Gal(K/F) \\ \sigma & \longmapsto & \sigma|_K \end{array}$$

es epiyectiva y continua.

Demostración. Ver [1, cap.7, Proposición 7.7] □

Proposición 1.4.2: *Sea E extensión de Galois de F.*

a) Sea M un subcuerpo de E que contiene a F, entonces E es Galois sobre M, $Gal(E/M)$ es cerrado en $Gal(E/F)$ y $E^{Gal(E/M)} = M$.

b) Para todo subgrupo H de $Gal(E/F)$, se tiene que $Gal(E/E^H)$ es la clausura topológica de H.

Demostración. Sea $G = Gal(E/F)$ entonces:

a) Sea $\alpha \in E$ y $f(X) \in M[X]$ su polinomio minimal sobre M. Sea $g(X)$ polinomio minimal de α sobre F. La extensión E/F es normal y separable, por lo que todas las raíces de $g(X)$ son distintas y pertenecen a E. Por otra parte, $g(X) \in M[X]$ entonces $f(X)$ divide $g(X)$ en $M[X]$. En otras palabras, las raíces de f son también raíces de g y por tanto, todas las raíces de f son distintas y pertenecen a E. Luego, E/M es Galois.

Para mostrar que $Gal(E/M)$ es cerrado en G observamos que

$$Gal(E/M) = \bigcap_{S \subseteq M \text{ finito}} G(S),$$

$G(S)$ es un subconjunto abierto de G, entonces es cerrado. Como la intersección arbitraria de cerrados es cerrada, se tiene el resultado.

Sea $\alpha \in E$, como E/M es una extensión algebraica, $F(\alpha)/M$ es una extensión finita y por tanto $E^{Gal(F(\alpha)/M)} = M$, entonces existe $\sigma \in Gal(F(\alpha)/M)$ tal que $\sigma(\alpha) \neq \alpha$. Ahora bien, usando el axioma de elección (Proposición 1.4.1) es posible extender $\sigma \in Gal(F(\alpha)/M)$ a $\tilde{\sigma} \in Gal(E/M)$ con $\tilde{\sigma}(\alpha) \neq \alpha$. A partir de esto, haciendo variar $\alpha \in E$ se concluye que $E^{Gal(E/M)} \subseteq M$. La otra inclusión es evidente.

b) Claramente $H \subseteq Gal(E/E^H)$. Como $Gal(E/E^H)$ es cerrado y $\bar{H}$ clausura topológica de H es el menor cerrado que contiene a H, se tiene que $\bar{H} \subseteq Gal(E/E^H)$.

Sea $\sigma \in G \setminus \bar{H}$. Queremos mostrar que $\sigma \notin Gal(E/E^H)$, es decir, $\sigma|_{E^H} \neq Id$. El subgrupo H es disjunto a algún abierto que contenga a σ. En otras palabras, utilizando la base de entornos mencionada en la Definición 13 existe K extensión finita y Galois de F contenida en E tal que

$$\sigma Gal(E/K) \cap H = \varnothing \tag{1.1}$$

porque $Gal(E/K)$ es parte de una base de entornos abiertos de la Id, entonces por traslación $\sigma Gal(E/K)$ es un entorno abierto de σ.

Sea $\phi : Gal(E/F) \to Gal(K/F)$ homomorfismo restricción, epiyectivo y de kernel $Gal(E/K)$ (Proposición 1.4.1). Notamos que si existe $\tau \in H$ tal que $\sigma|_K = \tau|_K$, $\sigma^{-1}\tau \in Gal(E/K)$ entonces $\tau \in \sigma Gal(E/K) \cap H$, lo que contradice (1.1). De modo que, $\sigma|_K \notin \phi(H)$, es decir, $\sigma|_K$ mueve elementos de $K^{\phi(H)}$. Como $K^{\phi(H)} \subseteq E^H$, concluímos que σ mueve un elemento de E^H y por tanto $\sigma \in G \setminus Gal(E/E^H)$.

Finalmente, por doble contención, hemos probado que $\bar{H} = Gal(E/E^H)$.

□

Teorema 1.4.3: *Sea E Galois sobre F con $G = Gal(E/F)$. Existe una biyección:*

$$\begin{array}{ccc} \{H \text{ subgrupos cerrados de } G\} & \longleftrightarrow & \{\text{cuerpos intermedios } F \subseteq M \subseteq E\} \\ H & \longmapsto & E^H \\ Gal(E/M) & \longleftarrow & M \end{array}$$

Más aún,

1. *la biyección revierte contenciones: $H_1 \supset H_2$ si y sólo si $E^{H_1} \subset E^{H_2}$;*
2. *sea H un subgrupo cerrado de G, entonces H es abierto si y sólo si E^H tiene grado finito sobre F. En tal caso, $(G : H) = [E^H : F]$;*
3. *sea H un subgrupo cerrado de G, entonces H is normal si y sólo si E^H/F es normal (y por tanto Galois). En tal caso, $Gal(E^H/F) \simeq G/H$.*

Demostración. Ver [1, cap. 7, Teorema 7.12] □

Proposición 1.4.4: *Sean K y L dos extensiones de F contenidas en algún subcuerpo común E. Si K/F es Galois, entonces KL/L y $K/K \cap L$ son Galois y*

$$\begin{array}{ccc} Gal(KL/L) & \to & Gal(K/K \cap L) \\ \sigma & \mapsto & \sigma|_K \end{array}$$

es un isomorfismo de grupos topológicos.

Demostración. Ver [1, cap. 7, Proposición 7.14] □

Para finalizar el capítulo notemos la conexión entre grupos profinitos y la teoría de Galois infinita.

Sea E/F una extensión de Galois infinita y consideremos una torre de subextensiones de E/F finitas y Galois sobre F

$$F \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq E$$

el teorema de Galois clásico nos brinda una epiyección canónica que consiste en el homomorfismo restricción

$$\phi_{ij} : Gal(M_j/F) \to Gal(M_i/F).$$

Más aún, si $i < k < j$ entonces $\phi_{ij} = \phi_{ik} \circ \phi_{kj}$, luego $\{Gal(M_i/F), \phi_{ij}\}$ forman un sistema proyectivo y su límite será $Gal(E/F)$. La topología de Krull definida antes, coincide con la topología restringida de la topología producto

$$\prod_{i\in\mathbb{N}} Gal(M_i/F)$$

donde $Gal(M_i/F)$ tiene la topología discreta y el grupo $Gal(M_i/F)$ se identifica con un cociente del grupo de Galois infinito $Gal(E/F)$.

Proposición 1.4.5: *Sea E/F una extensión de Galois. Los grupos de Galois de subextensiones de E/F finitas y Galois sobre F junto con los homomorfismos restricción $\phi_{ij} : Gal(M_j/F) \to Gal(M_i/F)$ forman un sistema proyectivo cuyo límite proyectivo es isomorfo a $Gal(E/F)$. En particular, $Gal(E/F)$ es un grupo profinito.*

Demostración. Ver [5, cap.1, Proposición 1.3.5] □

Ejemplo 6. *Ahora que tenemos las herramientas necesarias, analicemos $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. Sea Γ el subgrupo de $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ generado por el automorfismo de Frobenius, entonces como el cuerpo fijo de Γ es $\mathbb{F}_p$, $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \overline{\Gamma}$ clausura topológica de Γ. Descubramos la estrucutura de este conjunto.*

En primer lugar, notemos que $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \varprojlim_{i\in\mathbb{N}} Gal(\mathbb{F}_{p^i}/\mathbb{F}_p)$ como grupos topológicos. El isomorfismos se construye a partir de lo siguiente: para cada $i \in \mathbb{N}$ tenemos un homomor-

fismo

$$\begin{array}{ccc} Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) & \longrightarrow & Gal(\mathbb{F}_{p^i}/\mathbb{F}_p) \\ \sigma & \longmapsto & \sigma|_{\mathbb{F}_{p^i}} \end{array}$$

con esto, definimos

$$\begin{array}{rccc} \Phi: & Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) & \longrightarrow & \prod_{i\in\mathbb{N}} Gal(\mathbb{F}_{p^i}/\mathbb{F}_p) \\ & \sigma & \longmapsto & (\sigma|_{\mathbb{F}_{p^i}})_{i\in\mathbb{N}} \end{array}$$

Es posible probar que Im $\Phi = \varprojlim Gal(\mathbb{F}_{p^i}/\mathbb{F}_p)$ *como grupos topológicos, ver [1, Cap.7, Ejemplo 7.16]. Así, usando el Ejemplo 5, obtenemos que* $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$. *Más aún, usando un resultado clásico de Grupos Profinitos y corolario del Teorema Chino del resto, tenemos finalmente que*

$$Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \prod_{l \ primo} \mathbb{Z}_l,$$

donde $\mathbb{Z}_l$ *es el anillo de los enteros l-ádicos.*

1.5 El grupo $\mathbb{Z}_p$ como un grupo de Galois

Para $n \in \mathbb{N}$, sea $\zeta_n \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad y $\mu_n = \{{\zeta_n}^i : 0 \leq i < n\}$ el grupo de todas las raíces n-ésimas de la unidad. La extensión $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ es de Galois. En efecto, es separable y es normal porque es cuerpo de descomposición de $X^n - 1$. Denotemos $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Sea $\sigma \in G$ entonces $\sigma(\zeta_n) \in \mu_n$, así, existe $i \in \mathbb{Z}/n\mathbb{Z}$ bien determinado tal que $\sigma(\zeta_n) = {\zeta_n}^i$. Siendo aún mas precisos, i es una unidad en $\mathbb{Z}/n\mathbb{Z}$. Si no lo fuera, existiría $j \in \mathbb{Z}/n\mathbb{Z}$ no nulo tal que $ij \equiv 0 \pmod{n}$ y, por tanto $\sigma({\zeta_n}^j) = {\zeta_n}^{ij} = 1$, esto es imposible, ya que ${\zeta_n}^j \neq 1$. De esta forma, por cada $\sigma \in G$ existe un entero i, que denotaremos i_σ, con $(i, n) = 1$ tal que $\sigma(\zeta) = \zeta^{i_\sigma}$ para todo $\zeta \in \mu_n$.

Teorema 1.5.1: *El homomorfismo*

$$\begin{array}{rccc} \iota: & Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ & \sigma & \longmapsto & i_\sigma \ mód\ n \end{array}$$

es un isomorfismo de grupos.

Demostración. Ver [3, Cap.6, Teorema 3.1]. □

Observación 6. *El teorema anterior se puede extender para otros cuerpos K distintos de $\mathbb{Q}$. Si $X^n - 1$ es separable sobre K entonces $K(\zeta_n)/K$ es de Galois porque $K(\zeta_n)$ es cuerpo de descomposición de $X^n - 1$ sobre K. El homomorfismo*

$$\iota: \ Gal(K(\zeta_n)/K) \ \longrightarrow \ (\mathbb{Z}/n\mathbb{Z})^\times$$

es inyectivo, pero no necesariamente sobreyectivo. La sobreyectividad depende del cuerpo K. Por ejemplo, si $K = \mathbb{R}$ y $n \geq 3$ entonces $K(\mu_n)/K = \mathbb{C}/\mathbb{R}$ es una extensión cuadrática, el $\mathbb{R}$-automorfismo no trivial de $\mathbb{C}$ es la conjugación compleja, cuyo efecto sobre las raíces de la unidad en $\mathbb{C}$ es invertirlas: $\overline{\zeta} = \zeta^{-1}$. Por lo tanto, $Gal(K(\zeta_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ para $n \geq 3$ tiene imagen $\{\pm 1 \ mód\ n\}$ que es más pequeño que $(\mathbb{Z}/n\mathbb{Z})^\times$ para $n \neq 2, 3, 4, 6$.

Sea $p \in \mathbb{N}$ primo y $n \in \mathbb{N}$, definimos

$$\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 0} \mathbb{Q}(\zeta_{p^n}),$$

tras verificar que el siguiente diagrama conmuta para m dividendo n

$$\begin{array}{ccc} Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\iota_n} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \Big\downarrow \text{restricción} & & \Big\downarrow \text{proyección} \\ Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \xrightarrow{\iota_m} & (\mathbb{Z}/m\mathbb{Z})^\times \end{array}$$

y por teoría de Galois infinito se tiene que

$$Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \simeq \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

donde los homomorfismos ϕ_{nm} del sistema proyectivo son las restricciones mód p^n.

A su vez, $\varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p{}^\times$, ya que dado $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ con inverso $(b_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ entonces para todo $n \in \mathbb{N}$, $a_n b_n = 1$, es decir, para todo $n \in \mathbb{N}$, $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ es una unidad. Recíprocamente, sea $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ tal que para todo $n \in \mathbb{N}$, $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ entonces para todo $n \in \mathbb{N}$ existe $b_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ tal que $a_n b_n = 1$ y para todo $n, m \in \mathbb{Z}$ con $n \leq m$ se tiene que $b_n \equiv b_m$ mód p^n. Por tanto, $(b_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ es un inverso de $(a_n)_{n\in\mathbb{N}}$.

De ahí que

$$Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p{}^\times.$$

Por otra parte, si $a \in \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ y conozco sólo $(a_n)_{n\geq N}$ para algún $N \in \mathbb{N}$ puedo deducir a_n para $n < N$ a partir de la compatibilidad de los homomorfismos. De esta forma, si $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p{}^\times$ entonces para $n < N$

$$a_n = \left(\sum_{i=0}^{N} a_i p^i\right) \text{mód } p^n.$$

Por lo tanto, $\mathbb{Z}_p{}^\times = \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^\times = \varprojlim_{n\in\mathbb{N}} \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times = \varprojlim_{n\in\mathbb{N}} \left(\mathbb{Z}/p^{n+2}\mathbb{Z}\right)^\times$. Esto nos será útil para encontrar una descomposición de $\mathbb{Z}_p{}^\times$ en grupos cíclicos.

Sea p primo impar. El grupo $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ es cíclico de orden $\varphi(p^{n+1}) = p^n(p-1)$ (con φ función de Euler). Por teoría de grupos cíclicos sabemos $1+p \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ tiene orden p^n y que existe $\omega_n \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ de orden $p-1$, por tanto, podemos considerar $\mathcal{C}_{p^n} = (1+p)$

y $\mathcal{C}_{p-1} = (\omega_n)$ para obtener

$$\left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^{\times} = \mathcal{C}_{p^n} \times \mathcal{C}_{p-1} \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \tag{1.2}$$

Sea $p = 2$, por teoría de grupos sabemos que el elemento $5 \in (\mathbb{Z}/2^{n+2}\mathbb{Z})^{\times}$ tiene orden 2^n y $-1 \notin (5) \subseteq (\mathbb{Z}/2^{n+1}\mathbb{Z})^{\times}$ tiene orden 2. Como $(5) \cap (-1) = \{1\}$, entonces si consideramos $\mathcal{C}_{2^n} = (5)$ y $\mathcal{C}_2 = (-1)$ entonces

$$\left(\mathbb{Z}/2^{n+2}\mathbb{Z}\right)^{\times} = \mathcal{C}_{2^n} \times \mathcal{C}_2 \simeq \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \tag{1.3}$$

Ahora bien, si probamos que los isomorfismos en (1.2) y (1.3), que originan estas descomposiciones de $(\mathbb{Z}/p^{n+1}\mathbb{Z})^{\times}$ y $(\mathbb{Z}/2^{n+2}\mathbb{Z})^{\times}$, son compatibles con los homomorfismos ϕ_{nm} del límite proyectivo de $\mathbb{Z}_p^{\times}$ entonces es posible concluir que

$$\begin{aligned} p \neq 2: &\qquad \mathbb{Z}_p^{\times} = \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^{n+1}\mathbb{Z})^{\times} \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \\ p = 2: &\qquad \mathbb{Z}_2^{\times} = \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/2^{n+2}\mathbb{Z})^{\times} \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/2^n\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^* \simeq \mathbb{Z}_2 \times (\mathbb{Z}/2\mathbb{Z})^* \end{aligned} \tag{1.4}$$

Analizaremos esta compatibilidad solo en el caso $p \neq 2$ ya que para el caso $p = 2$ es similar. Para esto mostramos que el siguiente diagrama conmuta

$$\begin{array}{ccc} (\mathbb{Z}/p^{m+1}\mathbb{Z})^{\times} & \xleftarrow[\alpha_{m+1}]{} & \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \\ \downarrow{\scriptstyle \phi_{n+1,m+1}} & & \downarrow{\scriptstyle \phi_{nm}\times Id} \\ (\mathbb{Z}/p^{n+1}\mathbb{Z})^{\times} & \xleftarrow[\alpha_{n+1}]{} & \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \end{array}$$

donde ϕ_{nm} corresponde a la restricción mód p^n y α_{n+1} y α_{m+1} son unos isomorfismos. Notemos que no son los únicos, pero los escogemos de modo que el diagrama conmute. En particular, α_{n+1} corresponde a elegir un elemento $a = (a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p^{\times}$ tal que a_n sea de

orden p^n (por ejemplo $a = 1+p$) y $b = (b_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$ tal que b_n sea de orden $p-1$. Definimos $\alpha_{n+1}(u,v) = a_{n+1}^u b_{n+1}^v$.

Para mostrar que el diagrama conmuta mostraremos que existen $a_{m+1}, b_{m+1} \in (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$ de órdenes $p^m, p-1$ respectivamente y $a_{n+1}, b_{n+1} \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ de órdenes $p^n, p-1$ respectivamente tales que

$$\alpha_{m+1}((\bar{1},\bar{0})) = a_{m+1} \qquad \alpha_{n+1}((\bar{1},\bar{0})) = a_{n+1}$$
$$\alpha_{m+1}((\bar{0},\bar{1})) = b_{m+1} \qquad \alpha_{n+1}((\bar{0},\bar{1})) = b_{n+1}$$

Si el diagrama conmuta entonces $a_{m+1} \equiv a_{n+1}$ mód p^{n+1}. Luego, existe una sucesión $(a_n)_{n\geq 1}$ tal que para todo $m \geq n$, $a_m \equiv a_n$ mód p^n. La idea de la demostración es precisamente hacer lo inverso, demostrar que existe una tal sucesión y a partir de ella definir el isomorfismo α_{m+1} a partir de a_{m+1}: comienzo desde a_1 y hago alzamientos sucesivos.

Sea $a = 1 + p \in \mathbb{Z}_p^\times$ entonces contruímos una sucesión $(a_n)_{n\in\mathbb{N}}$ tal que $a_n = a$ mód p^n. Para $(b_n)_{n\in\mathbb{N}}$ comenzamos con $b_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ raíz simple de $X^{p-1}-1$ y generador del grupo $(\mathbb{Z}/p\mathbb{Z})^\times$. Por el lema de Hensel existe $b \in \mathbb{Z}_p^\times$ tal que $b \equiv b_1$ mód p y b raíz de $X^{p-1}-1$ en $\mathbb{Z}_p$. De esta forma,

$$(\bar{1},\bar{0}) \overset{\alpha_{n+1}}{\longmapsto} a_{n+1} \qquad (\bar{0},\bar{1}) \overset{\alpha_{n+1}}{\longmapsto} b_{n+1}$$

define el isomorfismo α_{n+1}.

Para $p = 2$, procedemos de forma análoga al caso $p \neq 2$ considerando $a = 5 \in \mathbb{Z}_2^\times$ y $b = -1$.

Otra demostración de esto se encuentra en [4, Cap.2, Proposición 8].

Lo anterior nos da una idea para obtener una extensión de cuerpos de Galois de modo que su grupo de Galois sea $\mathbb{Z}_p$, que es un factor de la descomposición en (1.4).

Con este fin, para $n \in \mathbb{N}$ sea $q_n = qp^n \in \mathbb{Z}$ con

$$q = \begin{cases} p, & \text{si } p \neq 2 \\ 4, & \text{si } p = 2 \end{cases}$$

Para $n \in \mathbb{N}$, sea ζ_n una raíz n- ésima primitiva de la unidad. Definimos $K_n = \mathbb{Q}(\zeta_{q_n})$ y $K_\infty = \bigcup_{n\geq 0} \mathbb{Q}(\zeta_{q_n})$. Observemos que $K_0 = \mathbb{Q}(\zeta_4)$ si $p = 2$ y $K_0 = \mathbb{Q}(\zeta)$ si $p \neq 2$.

El objetivo es mostrar que $Gal(K_\infty/K_0) \simeq \mathbb{Z}_p$. El primer paso es analizar el grupo de Galois $Gal(K_n/K_0)$ de subextensiones finitas de K_∞/K_0.

Si $p \neq 2$ entonces $q_n = p^{n+1}$. Sabemos que $Gal(K_n/\mathbb{Q}) \simeq (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \simeq \mathbb{Z}/p^n\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$ y por teoría de Galois clásica, si consideramos $\mathbb{Z}/p^n\mathbb{Z}$, se identifica con el subgrupo H de $Gal(K_n/\mathbb{Q})$ generado por $1+p$ y $K_n^H = K_0$. En efecto, como el orden de ζ_p es p, entonces ζ_p queda fijo por la acción de H, por tanto, $K_0 \subseteq K_n^H$. Además, usando un argumento de grados, tenemos que $[K_n^H : \mathbb{Q}] = [K_0 : \mathbb{Q}] = p - 1$ entones $K_0 = K_n^H$

Si $p = 2$ entonces $q_n = 2^{n+2}$ y sabemos que $Gal(K_n/\mathbb{Q}) \simeq (\mathbb{Z}/2^{n+2}\mathbb{Z})^\times \simeq \mathbb{Z}/2^n\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^\times$. De forma análoga al caso $p \neq 2$ si consideramos $H = \mathbb{Z}/2^n\mathbb{Z}$ entonces $K_n^H = K_0$.

De esta forma, para p entero primo, $Gal(K_n/K_0) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Ahora bien, para concluir es necesario usar límite proyectivo y por ende, debemos verificar la compatibilidad de los homomorfismos, esto es, verificar que el siguiente diagrama conmuta: si $m \geq n$

$$\begin{array}{ccc} Gal(K_m/K_0) & \xrightarrow{\phi_{nm}} & Gal(K_n/K_0) \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^m\mathbb{Z} & \xrightarrow{\psi_{nm}} & \mathbb{Z}/p^n\mathbb{Z} \end{array}$$

Sea $\sigma_{1+p,n} \in Gal(K_n/K_0)$ el automorfismo que eleva a la potencia $1+p$ las p^k-ésimas raíces de la unidad ($k \in \mathbb{N}$)e ntonces $Gal(K_n/K_0) = (\sigma_{1+p,n})$ porque $1+p$ y p^n son coprimos.

Luego, el diagrama anterior envía verticalmente $\sigma_{1+p,n} \mapsto 1(\text{mód } p^n)$ y horizontalmente $\sigma_{1+p,m} \mapsto \sigma_{1+p,n}$ que es restringir a K_n y $1(\text{mód } p^m) \mapsto 1(\text{mód } p^n)$. De lo que resulta que el diagrama claramente conmuta.

Finalmente, obtenemos que

$$Gal(K_\infty/K_0) \simeq \varprojlim Gal(K_n/K_0) \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

1.6 Teoría de Ramificación

Comenzaremos con algunas definiciones y resultados elementales de teoría de cuerpo de números.

Definición 15. Un dominio de Dedekind es un dominio de integridad R tal que

1. Todo ideal de R es finitamente generado.
2. Todo ideal primo no cero de R es un ideal maximal.
3. R es integralmente cerrado en su cuerpo de fracciones

$$K = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}.$$

Observación 7. *Un anillo satisfaciendo el primer ítem de la definición es llamado anillo Noetheriano. El último ítem significa que si $\alpha/\beta \in K$ es una raíz de algun polinomio mónico sobre R, entonces $\alpha/\beta \in R$, es decir, β divide α en R.*

Teorema 1.6.1: *Sea L un cuerpo de números y $\mathcal{O}_L$ su anillo de enteros algebraicos. Entonces $\mathcal{O}_L$ es un dominio de Dedekind.*

Demostración. Ver [8, Cap.3, Teorema 14]. □

Teorema 1.6.2: *Todo ideal en un anillo de Dedekind se escribe de manera única como producto de ideales primos.*

Demostración. Ver [8, Cap.3, Teorema16] □

Teorema 1.6.3: *Un dominio de Dedekind es un dominio de factorización única si y sólo si es un dominio de ideles principales.*

Demostración. Ver [8, Cap.3, Teorema 18] □

Definición 16. Sea B un anillo y $A \subseteq B$ un subanillo. Sea $\mathfrak{p} \subseteq A$ y $\mathfrak{b} \subseteq B$ ideales primos. Diremos que $\mathfrak{b}$ está sobre $\mathfrak{p}$ si $\mathfrak{b} \cap A = \mathfrak{p}$ o bien que $\mathfrak{p}$ está bajo $\mathfrak{b}$ y denotaremos esto por $\mathfrak{b}|\mathfrak{p}$.

Sean $E \subseteq L$ una extensión cuerpos de números y $\mathcal{O}_E \subseteq \mathcal{O}_L$ sus respectivos anillos de enteros algebraicos.

Teorema 1.6.4: *Todo ideal primo no nulo $\mathfrak{b}$ de $\mathcal{O}_L$ está sobre un único ideal primo no nulo $\mathfrak{p}$ de $\mathcal{O}_E$ y todo ideal primo no nulo $\mathfrak{p}$ de $\mathcal{O}_E$ está bajo al menos un ideal primo no nulo $\mathfrak{b}$ de $\mathcal{O}_L$.*

Demostración. Ver [8, Cap.3, Teorema 20]. □

A partir de los resultados anteriores, es posible notar que los ideales primos en $\mathcal{O}_L$ que están sobre un ideal dado $\mathfrak{p}$ en $\mathcal{O}_E$ son precisamente los que aparecen en la descomposición en ideales primos de $\mathfrak{p}\mathcal{O}_L$. Por lo tanto, hay finitos ideales primos sobre un ideal no nulo dado. Además la división de ideales corresponde a la inclusión.

Definición 17. El índice de ramificación de $\mathfrak{b}$ sobre $\mathfrak{p}$, denotado por $e(\mathfrak{b}|\mathfrak{p})$, es la potencia exacta de $\mathfrak{b}$ en la descomposición en ideales primos de $\mathfrak{p}\mathcal{O}_L$. Si $e(\mathfrak{b}|\mathfrak{p}) > 1$ para algún $\mathfrak{b}$ ideal primo no nulo de $\mathcal{O}_L$ decimos que $\mathfrak{p}$ se ramifica en $\mathcal{O}_L$ (o en L).

Veamos otro número importante asociado a los ideales primos $\mathfrak{b}$ y $\mathfrak{p}$. Sean $\mathbb{F}_{\mathfrak{b}} = \mathcal{O}_L/\mathfrak{b}$ y $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_E/\mathfrak{p}$, estos son cuerpos finitos y $\mathbb{F}_{\mathfrak{b}}$ es una extensión finita de $\mathbb{F}_{\mathfrak{p}}$.

Definición 18. Los cuerpos $\mathbb{F}_{\mathfrak{b}}$ y $\mathbb{F}_{\mathfrak{p}}$ son llamados cuerpos residuales asociados a los ideales $\mathfrak{b}$ y $\mathfrak{p}$ respectivamente y el grado $[\mathbb{F}_{\mathfrak{b}} : \mathbb{F}_{\mathfrak{p}}]$ es llamado grado de inercia de $\mathfrak{b}$ sobre $\mathfrak{p}$ y se denota $f(\mathfrak{b}|\mathfrak{p})$.

Proposición 1.6.5: *Los índices de ramificación y los grados de inercia son multiplicativos en torres, es decir, si $\mathfrak{p} \subseteq \mathfrak{b} \subseteq \mathfrak{q}$ son ideales primos no nulos de $\mathcal{O}_E \subseteq \mathcal{O}_L \subseteq \mathcal{O}_K$ respectivamente, entonces*

$$e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{b})e(\mathfrak{b}|\mathfrak{p})$$
$$f(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{b})f(\mathfrak{b}|\mathfrak{p}).$$

Ahora bien, analicemos los conceptos anteriores pero para extensiones de $\mathbb{Q}$ no necesariamente finitas.

Sea $k/\mathbb{Q}$ una extensión algebraica, no necesariamente finita. Sea $\mathcal{O}_k$ anillo de enteros algebraicos de k y $\mathcal{P}_k$ un ideal primo no cero de $\mathcal{O}_k$ entonces $\mathcal{P}_k \cap \mathbb{Z}$ es un ideal primo no cero de $\mathbb{Z}$. En efecto, es claro que $\mathcal{P}_k \cap \mathbb{Z}$ es un ideal primo, sea $\alpha \in \mathcal{P}_k$ no nulo y $p(X)$ el polinomio minimal de α sobre $\mathbb{Q}$, entonces $f(X) \in \mathbb{Z}[X]$ y

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \alpha_i \in \mathcal{P}_k \cap \mathbb{Z}$$

donde $n = \deg f$, α_i son los conjugados de α y $\alpha = \alpha_j$ para algún j.

Por lo tanto, $\mathcal{P}_k \cap \mathbb{Z} = p\mathbb{Z}$ para algún p primo. De esta forma,

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\mathcal{P}_k \cap \mathbb{Z} \simeq (\mathbb{Z} + \mathcal{P}_k)/\mathcal{P}_k \subseteq \mathcal{O}_k/\mathcal{P}_k$$

Notemos que $\mathcal{O}_k$ es integral sobre $\mathbb{Z}$ entonces $\mathcal{P}_k$ es maximal en $\mathcal{O}_k$ (Ver [9, Cap.1, Proposición 10]). De esto resulta que $\mathcal{O}_k/\mathcal{P}_k$ es un cuerpo. Denotamos por $\mathbb{F}_k = \mathcal{O}_k/\mathcal{P}_k$ y

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ a los cuerpos residuales asociados a $\mathcal{P}_k$ y (p) respecivamente.

Usando el mismo hecho, $\mathcal{O}_k/\mathcal{P}_k$ es una extensión algebraica de $\mathbb{Z}/p\mathbb{Z}$ porque todo elemento en $\mathcal{O}_k$, en particular, en $\mathcal{O}_k/\mathcal{P}_k$ es algebraico sobre $\mathbb{Z}$ y por tanto sobre $\mathbb{Z}/p\mathbb{Z}$.

Más aún, esta extensión es abeliana. En efecto, si consideramos una sucesión de cuerpos intermedios

$$\mathbb{Q} = L_0 \subseteq \cdots \subseteq L_n \subseteq \cdots \subseteq k$$

tal que $\bigcup_{n\geq 0} L_n = k$ y $L_n/\mathbb{Q}$ es finita y Galois sobre $\mathbb{Q}$ entonces tendremos una sucesión de cuerpos finitos

$$\mathbb{F} = \mathbb{F}_{L_0} \subseteq \cdots \subseteq \mathbb{F}_{L_n} \subseteq \cdots \subseteq \mathbb{F}_k$$

tal que $\bigcup_{n\geq 0} \mathbb{F}_{L_n} = \mathbb{F}_k$ y $\mathbb{F}_{L_n}/\mathbb{F}$ es finita y Galois sobre $\mathbb{F}$. Luego, por teoría de Galois infinita

$$Gal(\mathbb{F}_k/\mathbb{F}) \simeq \varprojlim Gal(\mathbb{F}_{L_n}/\mathbb{F})$$

Cada grupo $Gal(\mathbb{F}_{L_n}/\mathbb{F})$ es cíclico generado por el correspondiente automorfismo de Frobenius , por tanto es abeliano y el límite proyectivo de grupos abelianos es abeliano.

Sea K/k una extensión algebraica, no necesariamente finita. Sea $\mathcal{P}_K \subseteq \mathcal{O}_K$ un ideal primo no nulo y $\mathcal{P}_k = \mathcal{P}_K \cap \mathcal{O}_k \subseteq \mathcal{O}_k$ ideal primo no nulo. Entonces, por los mismos argumentos usados antes, $\mathbb{F}_K$ es una extensión de $\mathbb{F}_k$. Como $\mathbb{F}_K$ es uan extensión abeliana de $\mathbb{F}_p$, resulta que $\mathbb{F}_K/\mathbb{F}_k$ es abeliana porque $Gal(\mathbb{F}_K/\mathbb{F}_k)$ es un subgrupo de $Gal(\mathbb{F}_K/\mathbb{F}_p)$.

Por otra parte, sea $\mathcal{P}_k \subseteq \mathcal{O}_k$ ideal primo no nulo, entonces existe $\mathcal{P}_K \subseteq \mathcal{O}_K$ ideal primo no nulo tal que $\mathcal{P}_K|\mathcal{P}_k$ (Ver [9, Cap.1, Proposición 9]).

Observación 8. *Notemos que como $\mathbb{Q}$ es numerable entonces $\mathbb{Q}[X]$ es numerable. Sea $f(X) \in \mathbb{Q}[X]$ no constante, definimos $\mathscr{R}_f$ el conjunto de las raíces en $\overline{\mathbb{Q}}$ de $f(X)$, entonces*

$\mathscr{R}_f$ es finito y por tanto numerable. Luego

$$\overline{\mathbb{Q}} = \bigcup_{\substack{f\in\mathbb{Q}[X]\\ \deg(f)\geq 1}} \mathscr{R}_f$$

como $\mathbb{Q}[X]$ y $\mathscr{R}_f$ son numerables entonces $\overline{\mathbb{Q}}$ su clausura alebraica es numerable. De esta forma, $\overline{\mathbb{Q}} = \mathbb{Q}(\alpha_n : n \in \mathbb{N})$ donde $\{\alpha_n\}_{n\in\mathbb{N}}$ es una sucesión en $\overline{\mathbb{Q}}$ que contiene todos los números de $\overline{\mathbb{Q}}$. Como $\overline{\mathbb{Q}}/K/k/\mathbb{Q}$, esto nos entrega la existencia de sucesiones de cuerpos intermedios F_n como en el siguiente lema.

Lema 1.6.6: *Supongamos que K/k es una extensión de Galois. Sean $\mathcal{P}_K, \mathcal{P}'_K$ ideales primos de $\mathcal{O}_K$ tales que $\mathcal{P}_K \cap \mathcal{O}_k = \mathcal{P}'_K \cap \mathcal{O}_k$. Entonces existe $\sigma \in Gal(K/k)$ tal que $\sigma(\mathcal{P}_K) = \mathcal{P}'_K$.*

Demostración. Por [9, Cap.1, Proposición 11] el lema es válido para extensiones de Galois finitas. Ahora bien, la idea es usar este resultado para construir un tal σ. Sean

$$k = F_0 \subseteq \cdots \subseteq F_n \subseteq \cdots \subseteq K \tag{1.5}$$

una sucesión de cuerpos intermedios tal que $\bigcup_{n\geq 0} F_n = K$ y F_n/k es finita y Galois. Entonces por teoría de Galois infinito, $Gal(K/k) \simeq \varprojlim_{n\in\mathbb{N}} Gal(F_n/k)$.

Sea $\mathcal{P}_n = \mathcal{P}_K \cap \mathcal{O}_{F_n}$ y $\mathcal{P}'_n = \mathcal{P}'_K \cap \mathcal{O}_{F_n}$. Como F_n/k es finita, aplicando el lema en su versión finito, tenemos que existe $\tau_n \in Gal(F_n/k)$ tal que $\tau_n(\mathcal{P}_n) = \mathcal{P}'_n$.

Para $n \in \mathbb{N}$, sea $\sigma_n \in Gal(K/k)$ tal que $\sigma_n|_{F_n} = \tau_n$. Como $Gal(K/k)$ es compacto, la sucesión $\{\sigma_n\}_{n\geq 1}$ tiene un punto de acumulación en $Gal(K/k)$. Por tanto, existe una subsucesión convergente de $\{\sigma_n\}_{n\geq 1}$ que por comodidad llamaremos también $\{\sigma_n\}_{n\geq 1}$. Supongamos que $\{\sigma_n\}_{n\geq 1}$ converge a σ, entonces $\sigma^{-1}\sigma_n \underset{n\to\infty}{\longrightarrow} Id$. Luego, dado $m \in \mathbb{N}$ arbitrario, existe $n \geq m$ tal que $\sigma^{-1}\sigma_n \in Gal(K/F_m)$ entorno de la identidad.

Por consiguiente, para todo $m \in \mathbb{N}$ se tiene $\sigma^{-1}\sigma_n(\mathcal{P}_m) = \mathcal{P}_m$ porque $\mathcal{P}_m \subseteq F_m$, como

además $\mathcal{O}_{F_m} \subseteq \mathcal{O}_{F_n}$ entonces

$$\sigma(\mathcal{P}_m) = \sigma_n(\mathcal{P}_m) = \sigma_n(\mathcal{P}_K \cap \mathcal{O}_{F_m}) = \sigma_n(\mathcal{P}_n \cap \mathcal{O}_{F_m}) = \sigma_n(\mathcal{P}_n) \cap \sigma_n(\mathcal{O}_{F_m}) = \mathcal{P}'_n \cap \mathcal{O}_{F_m} = \mathcal{P}'_m$$

De esta forma, como

$$\mathcal{P}_K = \bigcup_{m\geq 1} \mathcal{P}_m \quad \text{y} \quad \mathcal{P}'_K = \bigcup_{m\geq 1} \mathcal{P}'_m$$

tenemos que

$$\sigma(\mathcal{P}_K) = \sigma\left(\bigcup_{m\geq 1} \mathcal{P}_m\right) = \bigcup_{m\geq 1} \sigma(\mathcal{P}_m) = \bigcup_{m\geq 1} \mathcal{P}'_m = \mathcal{P}'_K.$$

□

En cuerpos de números, es decir, extensiones finitas de $\mathbb{Q}$ sabemos que sus respectivos anillos de enteros son dominios de Dedekind, por tanto, hay factorización única de ideales a partir de ideales primos no nulos, así podemos definir índice de ramificación como cierto exponente en esta descomposición. Sin embargo, en el caso de extensiones infinitas de $\mathbb{Q}$ sus anillos de enteros no son necesariamente dominios de Dedekind, entonces es necesario definir el índice de ramificación de otra forma, pero que sea compatible con la definición en el caso finito. Para ello, usaremos el grupo de inercia. Analizaremos por separado el caso en que la extensión sea de Galois y el caso en que no lo es.

Sea K/k una extensión de Galois no necesariamente finita, $\mathcal{P}_K \subseteq \mathcal{O}_K$ ideal primo no nulo sobre $\mathcal{P}_k \subseteq \mathcal{O}_k$ ideal primo no nulo ($\mathcal{P}_K \cap \mathcal{O}_k = \mathcal{P}_k$).

Definición 19. Definimos el grupo de descomposición

$$D = D(\mathcal{P}_K|\mathcal{P}_k) = \{\sigma \in Gal(K/k) : \sigma(\mathcal{P}_K) = \mathcal{P}_K\}$$

Lema 1.6.7: *El grupo de descomposición D es un subgrupo cerrado de $Gal(K/k)$.*

Demostración. Claramente D es un subgrupo, ahora bien, con las notaciones anteriores,

sea

$$D_n = D_n(\mathcal{P}_n|\mathcal{P}_k) = \{\sigma \in Gal(K/k) : \sigma(\mathcal{P}_n) = \mathcal{P}_n\}$$

entonces para todo $n \in \mathbb{N}$, $D \subseteq D_n$ y como $\mathcal{P}_K = \bigcup_{n\geq 1} \mathcal{P}_n$ entonces $D = \bigcap_{n\geq 1} D_n$. En efecto, es claro que $D \subseteq \bigcap_{n\geq 1} D_n$. Recíprocamente, sea $\sigma \in \bigcap_{n\geq 1} D_n$ entonces $\sigma \in D_n$ para todo $n \geq 1$, es decir, $\sigma(\mathcal{P}_n) = \mathcal{P}_n$ para todo $n \geq 1$. Luego, por el mismo argumente usado para concluir en el lema anterior, $\sigma(\mathcal{P}_K) = \mathcal{P}_K$, por tanto, $\sigma \in D$.

Por otro lado, como para todo $\sigma \in Gal(K/F_n)$, $\sigma(\mathcal{P}_n) = \mathcal{P}_n$ tenemos que para todo $n \geq 1$, $Gal(K/F_n) \subseteq D_n$. El subgrupo $Gal(K/F_n)$ es un entorno abierto de Id, entonces dado $\sigma \in D_n$, $\sigma Gal(K/F_n)$ es un entorno abierto de σ y $\sigma Gal(K/F_n) \subseteq D_n$, por tanto, D_n es abierto. Luego, D_n es cerrado, de lo que resulta que D es cerrado. □

Definición 20. Definimos el grupo de inercia

$$I = I(\mathcal{P}_K|\mathcal{P}_k) = \{\sigma \in D : \sigma(\alpha) \equiv \alpha \text{ mód } \mathcal{P}_K \text{ para todo } \alpha \in \mathcal{O}_K\}$$

es decir, I consta de $\sigma \in D$ que son la identidad en el cuerpo residual $\mathbb{F}_K$.

Observación 9. *Recordemos que si L/F es una extensión de Galois finita de cuerpos de números, $\mathcal{P}_L$ y $\mathcal{P}_F$ ideales primos no nulos de $\mathcal{O}_L$ y $\mathcal{O}_F$ respectivamente tal que $\mathcal{P}_L$ está sobre $\mathcal{P}_F$, entonces por teoría de Galois de extensiones finitas*

$$e(\mathcal{P}_L|\mathcal{P}_F) = |I(\mathcal{P}_L|\mathcal{P}_F)|$$

Ver [9, Cap.1, Corolario 21.3].

Lema 1.6.8: *I es un subgrupo cerrado de $Gal(K/k)$.*

Demostración. Demostraremos que el complemente de I es abierto en $Gal(K/k)$. Para ello, si $\sigma \in Gal(K/k) \setminus I$, probaremos que existe F/k finita y Galois tal que $\sigma Gal(K/F) \subseteq Gal(K/k) \setminus I$.

Sea $\sigma \in D \setminus I$ entonces existe $\alpha \in \mathcal{O}_K$ tal que $\sigma(\alpha) \neq \alpha$ mód $\mathcal{P}_K$. Sea F la clausura normal de $k(\alpha)$ (es necesaria la clausura normal, porque a priori $k(\alpha)$ puede no contener todos los conjugados de α), entonces F/k es finita y Galois.

Sea $\tau \in Gal(K/F)$ entonces $\sigma\tau(\alpha) = \sigma(\alpha) \neq \alpha$ mód $\mathcal{P}_K$, por tanto, $\sigma\tau \in Gal(K/k) \setminus I$, lo que implica que $\sigma Gal(K/F) \subseteq Gal(K/k) \setminus I$. De esta forma, como $\sigma Gal(K/F)$ es un entorno abierto de σ, tenemos que $Gal(K/k) \setminus I$ es abierto.

Si $\sigma \notin D$ el resultado es claro porque D es cerrado en $Gal(K/k)$. □

Si L/E es una extensión de Galois de cuerpos de números y $\mathcal{P}_L$ es un ideal primo no nulo de $\mathcal{O}_L$ que esta sobre $\mathcal{P}_E$ ideal primo no nulo de $\mathcal{O}_E$ entonces tenemos la siguiente secuencia exacta

$$1 \to I(\mathcal{P}_L|\mathcal{P}_E) \xrightarrow{i} D(\mathcal{P}_L|\mathcal{P}_E) \xrightarrow{\pi} Gal(\mathbb{F}_L/\mathbb{F}_E) \to 1$$

donde i es el homomorfismo inclusión y π es el homomorfismo reducción módulo $\mathcal{P}_L$. Ver [9, Cap.1, Proposición 14]. Este resultado lo podemos extender a una extensión infinita de un cuerpo de números k.

Proposición 1.6.9: *Sea K/k una extensión de Galois no necesariamente finita, $\mathcal{P}_K$ ideal primo no nulo de $\mathcal{O}_K$ sobre $\mathcal{P}_k$ ideal primo no nulo de $\mathcal{O}_k$, entonces la secuencia*

$$1 \to I(\mathcal{P}_K|\mathcal{P}_k) \xrightarrow{i} D(\mathcal{P}_K|\mathcal{P}_k) \xrightarrow{\pi} Gal(\mathbb{F}_K/\mathbb{F}_k) \to 1$$

es exacta.

Demostración. Es claro que i es inyectiva porque es la inclusión. Como es natural, consideremos una sucesión de subcuerpos $\{F_n\}$ como en (2.9), $\mathcal{P}_n = \mathcal{P}_K \cap \mathcal{O}_{F_n}$ y $\mathbb{F}_n = \mathcal{O}_{F_n}/\mathcal{P}_n$ entonces el siguiente diagrama conmuta

$$\begin{array}{ccc} D(\mathcal{P}_K|\mathcal{P}_k) & \xrightarrow{\pi} & Gal(\mathbb{F}_K/\mathbb{F}_k) \\ \downarrow{\scriptstyle r_n} & & \downarrow{\scriptstyle \tilde{r}_n} \\ D(\mathcal{P}_n|\mathcal{P}_k) & \xrightarrow{\pi_n} & Gal(\mathbb{F}_n/\mathbb{F}_k) \end{array}$$

donde π, π_n son las respectivas proyecciones módulo $\mathcal{P}_K, \mathcal{P}_n$ y $\tilde{r}_n, r_n$ son las respectivas restricciones a $\mathbb{F}_n, F_n$.

El homomorfismo π_n es sobreyectivo por la versión finita de esta proposición. A continuación mostraremos que r_n es sobreyectiva, es decir, que dado $\sigma \in D(\mathcal{P}_n|\mathcal{P}_k)$ existe $\tilde{\sigma} \in Gal(K/k)$ tal que $\tilde{\sigma}(\mathcal{P}_K) = \mathcal{P}_K$ y $\tilde{\sigma}|_{F_n} = \sigma$.

Notemos que siempre podemos considerar $\rho \in Gal(K/k)$ tal que $\rho|_{F_n} = \sigma$ y tenemos que $\rho(\mathcal{P}_K) = \mathcal{P}'_K$ para algún $\mathcal{P}'_K$ ideal primo no nulo de $\mathcal{O}_K$. Tanto $\mathcal{P}_K$ como $\mathcal{P}'_K$ están sobre $\mathcal{P}_n$ porque

$$\mathcal{P}_n = \sigma(\mathcal{P}_n) = \rho(\mathcal{P}_n) = \rho(\mathcal{P}_K \cap F_n) = \mathcal{P}'_K \cap F_n = \mathcal{P}'_K \cap F_n$$

esto permite el uso del Lema 1.1.6 pero reemplazando k por F_n, entonces existe $\tau \in Gal(K/F_n)$ tal que $\tau(\mathcal{P}'_K) = \mathcal{P}_K$. Luego, si definimos $\tilde{\sigma} = \tau \circ \rho$ tenemos el resultado y con esto concluimos que $\pi_n \circ r_n$ es sobreyectiva.

Ahora bien, sea $\alpha \in Gal(\mathbb{F}_K/\mathbb{F}_k)$ y $\alpha_n = \alpha|_{\mathbb{F}_n}$, entonces tenemos una sucesión $\{\alpha_n\}_{n\geq 1}$ en $Gal(\mathbb{F}_K/\mathbb{F}_k)$. Sea $\sigma_n \in D(\mathcal{P}_K|\mathcal{P}_k)$ preimagen de α_n vía $\tilde{r}_n \circ \pi$, como $Gal(K/k)$ es compacto y $D(\mathcal{P}_K|\mathcal{P}_k)$ es cerrado, existe $\hat{\sigma} \in D(\mathcal{P}_K|\mathcal{P}_k)$ punto de acumulación de $\{\sigma_n\}_{n\geq 1}$. Luego, existe una subsucesión de $\{\sigma_n\}_{n\geq 1}$ que converge a $\hat{\sigma}$, por simplicidad notamos a esta subsucesión $\{\sigma_n\}_{n\geq 1}$.

De forma análoga a la demostración del Lema 1.1.6, dado $m \in \mathbb{N}$ existe $n \in \mathbb{N}$, $n \geq m$ suficientemente grande tal que $\hat{\sigma}^{-1}\sigma_n \in Gal(K/F_m) \cap D(\mathcal{P}_K|\mathcal{P}_k)$, es decir, $\hat{\sigma}|_{F_m} = \sigma_n|_{F_m}$. A partir de esto podemos concluir que $\pi_m(r_m(\hat{\sigma})) = \alpha_m$, como el diagrama es conmutativo, esto es equivalente a $\pi(\tilde{r}_n(\hat{\sigma})) = \alpha_m = \alpha|_{F_m}$ para todo m. Por lo tanto, $\hat{\sigma}$ es la preimagen

de cada restricción α_m, así, $\hat{\sigma}$ es la preimagen de α. □

Supongamos ahora que K/k es una extensión algebraica pero no necesariamente de Galois de k un cuerpo de números. Sea $\overline{\mathbb{Q}}$ clausura algebraica de $\mathbb{Q}$ entonces $\overline{\mathbb{Q}}/K$ y $\overline{\mathbb{Q}}/k$ son extensiones de Galois. Sean $\mathcal{P}_K$ y $\mathcal{P}_k$ como antes. Sea $\mathcal{P}_{\overline{\mathbb{Q}}} \subseteq \mathcal{O}_{\overline{\mathbb{Q}}}$ ideal primo no nulo sobre $\mathcal{P}_K$, entonces

$$I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k) \subseteq Gal(\overline{\mathbb{Q}}/k)$$
$$I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K) \subseteq Gal(\overline{\mathbb{Q}}/K) \subseteq Gal(\overline{\mathbb{Q}}/k)$$

Luego, $I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K) = I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k) \cap Gal(\overline{\mathbb{Q}}/K)$.

Definición 21. Definimos el índice de ramificación por la cardinalidad del siguiente cociente

$$e(\mathcal{P}_K|\mathcal{P}_k) = (I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k) : I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K))$$

el cual puede ser infinito.

Observación 10. *Esta definición no depende de la elección de $\mathcal{P}_{\overline{\mathbb{Q}}}$. De hecho, si $\mathcal{P}'_{\overline{\mathbb{Q}}}$ es otro ideal primo de $\mathcal{O}_{\overline{\mathbb{Q}}}$ sobre $\mathcal{P}_K$ entonces por una aplicación del Lema 1.1.6 existe $\sigma \in Gal(\overline{\mathbb{Q}}/K)$ tal que $\mathcal{P}'_{\overline{\mathbb{Q}}} = \sigma(\mathcal{P}_{\overline{\mathbb{Q}}})$. Luego,*

$$I(\mathcal{P}'_{\overline{\mathbb{Q}}}|\mathcal{P}_k) = \sigma I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k)\sigma^{-1}$$
$$I(\mathcal{P}'_{\overline{\mathbb{Q}}}|\mathcal{P}_K) = \sigma I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K)\sigma^{-1}$$

y por tanto

$$\begin{aligned} e(\mathcal{P}_K|\mathcal{P}_k) &= (I(\mathcal{P}'_{\overline{\mathbb{Q}}}|\mathcal{P}_k) : I(\mathcal{P}'_{\overline{\mathbb{Q}}}|\mathcal{P}_K)) \\ &= (\sigma I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k)\sigma^{-1} : \sigma I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K)\sigma^{-1}) \\ &= (I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k) : I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K)). \end{aligned}$$

Si K/k es Galois, este índice de ramificación puede ser definido de manera más sencilla, sin pasar por la elección de un ideal $\mathcal{P}_{\overline{\mathbb{Q}}}$ de $\overline{\mathbb{Q}}$. Esto debido a que tenemos un homomorfismo

natural, la restricción

$$Gal(\overline{\mathbb{Q}}/k) \longrightarrow Gal(K/k)$$

con kernel $Gal(\overline{\mathbb{Q}}/K)$. Esto induce un homomorfismo

$$I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k) \longrightarrow I(\mathcal{P}_K|\mathcal{P}_k)$$

que resulta ser sobreyectivo (demostración análoga a la demostración de la sobreyectividad de r_n en la Proposición 1.6.9) con kernel $I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K)$ porque $\mathcal{P}_{\overline{\mathbb{Q}}}$ es un ideal sobre $\mathcal{P}_K$. Para probar la sobreyectividad la idea es replicar en este contexto la demostración de la sobreyectividad de la Proposición 1.6.9.

Así,

$$I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_k)/I(\mathcal{P}_{\overline{\mathbb{Q}}}|\mathcal{P}_K) \simeq I(\mathcal{P}_K|\mathcal{P}_k)$$

y entonces

$$e(\mathcal{P}_K|\mathcal{P}_k) = |I(\mathcal{P}_K|\mathcal{P}_k)|$$

que puede ser infinito. Notemos que por la Observación 9, para extensiones de Galois finitas o infinitas, el índice de ramificación de dos ideales primos nulos coincide con la cardinalidad del sus respectivos grupos de inercia.

A continuación introduciremos la noción de primo arquimedeano, con la finalidad de extender lo visto hasta ahora, para este nuevo objeto. Para ello, comenzaremos con la definición y resultados relevantes sobre valor absoluto o valuación (multiplicativa).

Definición 22. Un valor absoluto o valuación (multiplicativa) sobre un cuerpo K es una funcion $|\cdot| : K \to \mathbb{R}$ que cumple :

(a) $|x| > 0$ excepto que $|0| = 0$.

(b) $|xy| = |x||y|$.

(c) $|x+y| \leq |x| + |y|$ (desigualdad triangular).

si además satisface que $|x+y| \leq \max\{|x|, |y|\}$ se dice que el valor absoluto es no arquimediano.

Ejemplo 7. *Para todo cuerpo de números K e incrustación $\sigma : K \hookrightarrow \mathbb{C}$ podemos definir un valor absoluto en K por $|a| = |\sigma(a)|$ utilizando el módulo de un número complejo.*

Ejemplo 8. *Sea $ord : K^\times \to \mathbb{Z} \subseteq \mathbb{R}$ una valuación (aditiva) discreta (en el sentido de que su imagen es un subconjunto discreto de $\mathbb{R}$) y sea $\rho \in \mathbb{R}$, con $\rho > 1$, entonces*

$$|a| = \rho^{-ord(a)}, \quad a \neq 0, \quad |0| = 0 \tag{1.6}$$

es un valor absoluto no arquimediano sobre K. Por ejemplo, si p un número primo, entonces definimos el valor absoluto p-ádico $|\cdot|_p$ sobre $\mathbb{Q}$:

$$|a|_p = \rho^{-ord_p(a)}.$$

Usualmente normalizamos esto tomando $\rho = p$, entonces

$$|a|_p = p^{-ord_p(a)}$$

donde $ord_p(a) = r$ si $a = a_0 p^r$ con $ord_p(a_0) = 0$.

Observación 11. *La función $ord(\cdot)$ es una valuación (aditiva) que satisface*

(a) $ord(xy) = ord(x) + ord(y)$

(b) $ord(x+y) \geq \min\{ord(x), ord(y)\}$

este último ítem es análogo a la propiedad no arquimediana de una valuación multiplicativa o valor absoluto.

Además, tomando logaritmo en (1.6) en base ρ tenemos que $\log_\rho |a| = -ord(a)$*, es decir,* $ord(a) = -\log_\rho |a|$*. Esto nos sugiere una forma de pasar de una valuación multiplicativa no arquimediana a una aditiva. Para ello, si* $|\cdot|$ *es un valor absoluto (no trivial) no arquimediano, basta definir* $v(x) = -\log|x|$*,* $x \neq 0$ *(log en base* ρ *para cualquier real* $\rho > 1$*), entonces* v *satisface* $(a), (b)$ *(Ver [10, Cap.7, Proposición 7.5]).*

Todo valor absoluto $|\cdot|$ define una métrica sobre K dada por $d(x, y) = |x - y|$. Esta métrica es ultramétrica si y sólo si el valor absoluto es no arquimediano.

Teorema 1.6.10: *Sea* $|\cdot|$ *un valor absoluto no trivial sobre* $\mathbb{Q}$*.*

(a) Si $|\cdot|$ *es arquimediano, entonces* $|\cdot|$ *es equivalente a* $|\cdot|_\infty$ *(valor absoluto usual).*

(b) Si $|\cdot|$ *es no arquimediano, entonces* $|\cdot|$ *es equivalente a* $|\cdot|_p$ *para exactamente un* p *primo.*

Demostración. Ver [10, Cap.7, Teorema 7.12] □

Recordemos que dos valores absolutos o valuaciones (multiplicativas) son equivalentes si sus métricas inducen la misma topología sobre K. Esto nos motiva a definir

Definición 23. Una clase de equivalencia v de valores absolutos o valuaciones (multiplicativas) de K es un primo o lugar de K.

Si v consiste de valores absolutos arquimedianos, entonces v es un primo infinito (o arquimediano). En caso contrario, v es un primo finito (o no arquimediano).

En el caso que K sea un cuerpo de números, primos como se ha definido es una generalización de la noción de ideales primos. Para comprender esto, primero necesitamos la siguiente definición:

Definición 24. Sea K un cuerpo de números, $\mathcal{O}_K$ su anillo de enteros. Dado $I \subseteq \mathcal{O}_K$ ideal no nulo definimos la norma de un ideal por

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

Observación 12. *Esta norma es siempre finita. Ver [11, Cap.3, Proposición 1]*

Teorema 1.6.11: *Sea K un cuerpo de números. Existe exactamente un primo de K*

(a) por cada ideal primo $\mathfrak{p}$;

(b) por cada incrustación real ϕ;

(c) por cada par de incrustaciones complejas conjugadas $(\psi, \bar{\psi})$.

Demostración. Ver [10, Cap.7, Teorema 7.14] □

Los valores absolutos que asociamos en cada caso son:

(a) $|a|_{\mathfrak{p}} =: N(\mathfrak{p})^{-ord_{\mathfrak{p}}(a)}$, donde $ord_{\mathfrak{p}}(a)$ corresponde a la máxima potencia de $\mathfrak{p}$ dividiendo al ideal generado por a;

(b) $|a|_{\phi} =: |\phi(a)|$;

(c) $|a|_{\psi,\bar{\psi}} =: |\psi(a)| = |\overline{\psi}(a)|$.

Si v corresponda a un primo infinito, lo llamamos real o complejo según sea el caso.

Un resultado importantísimo que es necesario mencionar es el siguiente:

Teorema 1.6.12: *Sea K un cuerpo completo con respecto a una valuación (multiplicativa) o valor absoluto $|\cdot|$ y sea L una extensión finita de K, entonces existe una única extensión de $|\cdot|$ a L.*

Demostración. Ver [12, Cap. 1, Teorema 5.1] □

Observación 13. *El cuerpo $\mathbb{Q}_p$ es completo con el valor absoluto p-ádico, por tanto hay una única forma de extender $|\cdot|_p$ a un valor absoluto sobre K, extensión finita de $\mathbb{Q}_p$. Sin embargo, $\mathbb{Q}$ no es completo con este valor absoluto, es por eso que dado K una extensión finita de $\mathbb{Q}$ hay varias formas de extender $|\cdot|_p$ a K.*

Ahora bien, si $K \subseteq L$ cuerpos de números y w, v son primos de L, K respectivamente tal que $|\cdot|_w$ restricto a K es equivalente $|\cdot|_v$, decimos que w divide v o que w está sobre v y lo denotamos $w|v$. Para primos finitos, se puede mostrar que esto significa lo usual, que $\mathfrak{p}_w \cap \mathcal{O}_K = \mathfrak{p}_v$, para primos infinitos esto significa que w corresponde a una incrustación $\sigma : L \to \mathbb{C}$ que extiende la incrustación correspondiente a v (o su complejo conjugado).

Ahora que tenemos clara la definición de primo o lugar de un cuerpo, nos interesa poder definir para ellos el grupo de inercia. Sabemos que un primo arquimediano de k es una incrustación real $\phi : k \to \mathbb{R}$ o un par de incrustaciones complejas conjugadas $(\psi, \bar{\psi})$ con $\bar{\psi} \neq \psi$ y $\psi : k \to \mathbb{C}$. Como $\mathbb{C}$ es algebraicamente cerrado, toda incrustación ϕ o ψ puede ser extendida a una incrustación $\overline{\mathbb{Q}} \to \mathbb{C}$ (usando el Lema de Zorn), en particular, las podemos extender a K. Si K/k es Galois y ϕ_1, ϕ_2 son dos extensiones de ϕ, entonces $\phi_2^{-1}\phi_1 \in Gal(K/k)$, por lo tanto, $\phi_1 = \phi_2\sigma$ para algún $\sigma \in Gal(K/k)$. Si $(\psi_1, \bar{\psi}_1), (\psi_2, \bar{\psi}_2)$ extienden ϕ, entonces $\psi_1 = \psi_2\sigma$, por lo tanto, $(\psi_1, \bar{\psi}_1) = (\psi_2, \bar{\psi}_2)\sigma$ para algún $\sigma \in Gal(K/k)$. Análogo ocurre con la extensión de un primo infinito complejo. De esta forma, podemos cocluir que $Gal(K/k)$ actúa transitivamente sobre las extensiones de un primo infinito dado.

Si K/k es Galois, w es un primo infinito de K que está sobre v es un primo infinito de k, definimos

$$I(w|v) = D(w|v) = \{\sigma \in Gal(K/k) : w\sigma = v\}.$$

Notemos que en general $I(w|v)$ es trivial, salvo cuando v es un primo infinito real, $w = (\psi, \bar{\psi})$ es complejo y $\sigma \neq Id$ es la conjugación compleja, la cual permuta ψ y $\bar{\psi}$ y tiene

orden 2. Por lo tanto

$$|I(w|v)| = 1, 2.$$

De esta forma, podemos definir índice de ramificación para primos infinitos de igual forma que para primos finitos, usando la cardinalidad del respectivo grupo de inercia.

1.7 Teoría del Cuerpo de clase

Definición 25. Sea R un dominio de Dedekind y K su cuerpo de fracciones. Un ideal fraccionario de R es un R-súbmodulo $\mathfrak{a}$ no nulo de K tal que $d\mathfrak{a} \subseteq R$ para algún $d \in R$ no nulo, es decir, es un es un R-súbmodulo cuyos elementos tienen un común denominador.

Nos referiremos a los ideales usuales de R como ideales enteros.

Teorema 1.7.1: *Sea R un dominio de Dedekind. El conjunto $J(R)$ de ideales fraccionarios es un grupo con la multiplicación de ideales y con R actuando como elemento identidad. Es más, es un grupo abeliano libre sobre el conjunto de los ideales primos no nulos de R.*

Demostración. Ver [10, Cap.3, Teorema 3.20] □

Definición 26. Definimos el grupo de clase de ideales (o grupo de clase) $Cl(R)$ de R como el cociente $Cl(R) = J(R)/P(R)$ donde $P(R)$ es el subgrupo de $J(R)$ de ideales principales. El número de clase de R es el orden de $Cl(R)$.

Observación 14. *En el caso que R sea el anillo de enteros $\mathcal{O}_K$ de un cuerpo de números K, nos referiremos a $Cl(\mathcal{O}_K)$ como el grupo de clase de ideales de K y a su orden h_K como el número de clase de K.*

Teorema 1.7.2: *Sea K un cuerpo de números y $\mathcal{O}_K$ su anillo de enteros. Entonces $Cl(\mathcal{O}_K)$ es finito.*

Demostración. Ver [10, Cap.4, Teorema 4.4] □

Observación 15. *En conclusión, si bien un anillo de Dedekind R no tiene porque tener factorización única, sí la tiene a nivel de ideales. Sabemos que un dominio de Dedekind es un dominio de factorización única si y sólo si es un dominio de ideales principales, así, el grupo de clase $Cl(R)$ lo que mide es que tan lejos estan los ideales principales de ser todos los ideales o en definitiva que tan lejos está R de tener factorización única.*

Definición 27. Sea L/K una extensión de cuerpos de números y $\mathcal{O}_L, \mathcal{O}_K$ sus respectivos anillos de enteros. Para $\mathcal{P}_L$ un ideal primo no nulo de $\mathcal{O}_L$ sobre $\mathcal{P}_K$ un ideal primo no nulo de $\mathcal{O}_K$ y $\alpha \in L$, definimos el homomorfismo norma

$$\begin{array}{rccc} N_{L/K}: & Cl(\mathcal{O}_L) & \longrightarrow & Cl(\mathcal{O}_K) \\ & \mathcal{P}_L & \longmapsto & {\mathcal{P}_K}^{f(\mathcal{P}_L|\mathcal{P}_K)} \\ & \alpha\mathcal{O}_L & \longmapsto & N_{L/K}(\alpha)\mathcal{O}_K \end{array}$$

Observación 16. *En un principio, como $J(\mathcal{O}_L)$ (resp. $J(\mathcal{O}_K)$) es un grupo abeliano libre generado por el conjunto de ideales primos no nulos $\mathcal{P}_L$ de $\mathcal{O}_L$ (resp. $\mathcal{P}_K$ de $\mathcal{O}_K$) es suficiente definir $N(\mathcal{P}_L)$. Sin embargo, por [13, Cap 1, Proposición 14], si $\alpha \in L$ entonces $N(\alpha\mathcal{O}_L) = N_{L/K}(\alpha)\mathcal{O}_K$.*

Ahora bien, sea L/K una extensión de Galois finita de cuerpos de números, $\mathcal{P}_L \subseteq \mathcal{O}_L$ ideal primo no nulo sobre $\mathcal{P}_K \subseteq \mathcal{O}_K$ ideal primo no nulo. Sabemos que por Proposición 1.6.9 la secuencia

$$1 \to I(\mathcal{P}_L|\mathcal{P}_K) \xrightarrow{i} D(\mathcal{P}_L|\mathcal{P}_K) \xrightarrow{\pi} Gal(\mathbb{F}_L/\mathbb{F}_K) \to 1$$

es exacta. El grupo $Gal(\mathbb{F}_L/\mathbb{F}_K)$ es cíclico de orden $[\mathbb{F}_L : \mathbb{F}_K]$ generado por el automorfismo de Frobenius $Frob : x \mapsto x^{\#\mathbb{F}_K}$ entonces para $Frob \in Gal(\mathbb{F}_L/\mathbb{F}_K)$ existe una preimagen en $D(\mathcal{P}_L|\mathcal{P}_K)$, pero no necesariamente una: si $\rho \in \pi^{-1}(Frob)$ entonces $\rho I(\mathcal{P}_L|\mathcal{P}_K) = \pi^{-1}(Frob)$.

Definición 28. Una preimagen del automorfismo de Frobenius, $\omega \in D(\mathcal{P}_L|\mathcal{P}_K)$, es llamada

una sustitución de Frobenius.

Notemos que si $\mathcal{P}_L$ es un ideal primo sobre $\mathcal{P}_K$ y $\mathcal{P}_K$ no se ramifica en L (o $\mathcal{P}_L$ es no ramificado) entonces $I(\mathcal{P}_L|\mathcal{P}_K) = \{1\}$ y por tanto hay una única sustitución de Frobenius para $\mathcal{P}_L$. Así, a cada ideal $\mathcal{P}_L$ sobre un ideal primo no nulo dado puedo asociar una sustitución de Frobenius $\omega_{\mathcal{P}_L}$ que depende de la elección de $\mathcal{P}_L$.

Proposición 1.7.3: *Sea L/K una extensión de Galois finita. Sean $\mathcal{P}_L, \mathcal{P}_K$ ideales primos no nulos de $\mathcal{O}_L$ y $\mathcal{O}_K$ respectivamente. Supongamos que $\mathcal{P}_L$ está sobre $\mathcal{P}_K$ y que $\mathcal{P}_K$ es no ramificado en L. La sustitución de Frobenius $\omega_{\mathcal{P}_L}$ es el único $\omega \in Gal(L/K)$ tal que para todo $x \in \mathcal{O}_L$ se tiene que*

$$\omega(x) \equiv x^{\#\mathbb{F}_K} \text{ mód } \mathcal{P}_L$$

Demostración. Claramente $\omega_{\mathcal{P}_L}$ satisface esta propiedad, por ende, solo es necesario probar la unicidad. Supongamos que $\omega \in Gal(L/K)$ la satisface. Para cualquier $x \in \mathcal{P}_L$ tenemos que $\omega(x) \equiv x^{\#\mathbb{F}_K} \equiv 0$ mód $\mathcal{P}_L$, entonces $\omega(x) \in \mathcal{P}_L$. Luego, $\omega(\mathcal{P}_L) = \mathcal{P}_L$ y por tanto $\omega \in D(\mathcal{P}_L|\mathcal{P}_K)$. El isomorfismo $D(\mathcal{P}_L|\mathcal{P}_K) \xrightarrow{\pi} Gal(\mathbb{F}_L/\mathbb{F}_K)$ envía ambos ω y $\omega_{\mathcal{P}_L}$ en el automorfismo de Frobenius $x \mapsto x^{\#\mathbb{F}_K}$. Así, concluimos que $\omega = \omega_{\mathcal{P}_L}$. □

Proposición 1.7.4: *Sea L/K una extensión de Galois finita. Sean $\mathcal{P}_L, \mathcal{P}'_L, \mathcal{P}_K$ ideales primos no nulos de $\mathcal{O}_L$ y $\mathcal{O}_K$ respectivamente. Supongamos que $\mathcal{P}_L$ y $\mathcal{P}'_L$ están sobre $\mathcal{P}_K$ y que $\mathcal{P}_K$ es no ramificado en L. Entonces si ω es la sustitución de Frobenius asociada a $\mathcal{P}_L$, existe $\sigma \in Gal(L/K)$ tal que $\sigma\omega\sigma^{-1}$ es la sustitución de Frobenius asociada a $\mathcal{P}'_L$.*

Demostración. Por Lema 1.1.6, $Gal(L/K)$ actúa transitivamente sobre los ideales primos $\mathcal{P}_L$ que están sobre $\mathcal{P}_K$, entonces existe $\sigma \in Gal(L/K)$ tal que $\sigma(\mathcal{P}_L) = \mathcal{P}'_L$. Luego,

$$\sigma\omega\sigma^{-1}(\mathcal{P}'_L) = \mathcal{P}'_L$$

por lo tanto, $\sigma\omega\sigma^{-1} \in D(\mathcal{P}'_L|\mathcal{P}_K)$ y si ω es una sustitución para $\mathcal{P}_L$, entonces $\sigma\omega\sigma^{-1}$ es una sustitución para $\mathcal{P}'_L$ por Proposición 1.7.3. □

Esta Proposición nos indica que las distintas sustituciones de Frobenius asociadas a distintos ideales primos de $\mathcal{O}_L$ sobre un mismo ideal primo de $\mathcal{O}_K$ son conjugadas por un elemento de $Gal(L/K)$.

Definición 29. Sea L/K una extensión de Galois finita, $\mathcal{P}_L$ un ideal primo sobre $\mathcal{P}_K$ no ramificado en L. La clase de Frobenius de $\mathcal{P}_K$, denotada por $Frob_{\mathcal{P}_K}$, consiste de los conjugados de la sustitución de Frobenius $\omega_{\mathcal{P}_L}$.

Si añadimos la hipótesis de que L/K sea abeliana, las clases de conjugación constan de un elemento, en tal caso $Frob_{\mathcal{P}_K} = \{\omega_{\mathcal{P}_L} : \mathcal{P}_L|\mathcal{P}_K\}$ es un único elemento que llamaremos $\omega_{\mathcal{P}_K}$.

Hay otra notación comunmente usada para denotar las sustituciones de Frobenius que incluye la extensión de cuerpo en su notación.

Definición 30. Para cada primo $\mathcal{P}_L$ no ramificado de L definimos el símbolo de Artin

$$\left(\frac{L/K}{\mathcal{P}_L}\right) := \omega_{\mathcal{P}_L}.$$

Si L/K es abeliana entonces escribimos

$$\left(\frac{L/K}{\mathcal{P}_K}\right) := \omega_{\mathcal{P}_K} := \omega_{\mathcal{P}_L}.$$

A partir de esto podemos ver el símbolo de Artin como una función entre los primos $\mathcal{P}_K$ no ramificados y las sustituciones de Frobenius $\omega_{\mathcal{P}_K} \in Gal(L/K)$. Nos gustaría extender esta función a un homomorfismo multiplicativo del grupo de ideales $J(\mathcal{O}_K)$ en $Gal(L/K)$, pero los primos ramificados $\mathcal{P}_L|\mathcal{P}_K$ causan problemas: el homomorfismo $\pi : D(\mathcal{P}_L|\mathcal{P}_K) \to Gal(\mathbb{F}_L/\mathbb{F}_K)$ no es una biyección cuando $\mathcal{P}_K$ es ramificado.

Para cualquier subconjunto de ideales primos S de $\mathcal{O}_K$, sea $J(\mathcal{O}_K)^S$ el subgrupo de $J(\mathcal{O}_K)$ generado por todos los primos de $\mathcal{O}_K$ que no están en S. El grupo $J(\mathcal{O}_K)^S$ es abeliano

libre de base los primos de $\mathcal{O}_K$ que no están en S. En particular, sea S el conjunto de todos los primos de $\mathcal{O}_K$ que se ramifican en L, entonces podemos definir el siguiente homomorfismo:

$$\begin{array}{rccc} \omega_{(\cdot)}: & J(\mathcal{O}_K)^S & \longrightarrow & Gal(L/K) \\ & \mathcal{P}_i & \longmapsto & \omega_{\mathcal{P}_i} \\ & \prod_{i=1}^m \mathcal{P}_i^{e_i} & \longmapsto & \prod_{i=1}^m \omega_{\mathcal{P}_i}^{e_i} \end{array}$$

llamado el mapa de Artin. Un resultado importante de la teoría del cuerpo de clase es que el mapa de Artin es sobreyectivo, por eso es conocido como la reciprocidad de Artin.

Observemos que si L/K es una extensión abeliana no ramificada en ningún lugar finito entonces no es necesario hacer uso de S, así tenemos un epimomorfismo

$$\begin{array}{rccc} \omega_{(\cdot)}: & J(\mathcal{O}_K) & \longrightarrow & Gal(L/K) \\ & \mathcal{P}_i & \longmapsto & \omega_{\mathcal{P}_i} \\ & \prod_{i=1}^m \mathcal{P}_i^{e_i} & \longmapsto & \prod_{i=1}^m \omega_{\mathcal{P}_i}^{e_i} \end{array}$$

Definición 31. Sea K un cuerpo de números, L/K es el cuerpo de clase de Hilbert de K si satisface:

(a) L/K es Galois;

(b) L/K no se ramifica en ningún primo, finito o infinito

(c) Para todo cuerpo M, tal que M/K es Galois abeliana no ramificada entonces $M \subseteq L$. Es decir, L es la máxima extensión Galois abeliana no ramificada de K.

Observación 17. *El mapa de Artin correspondiente a la extensión L/K, con L el cuerpo de clase de Hilbert de K, nos entrega el siguiente isomorfismo*

$$Cl(\mathcal{O}_K) \simeq Gal(L/K).$$

es decir, los ideales principales constituyen el kernel del mapa de Artin.

Capítulo 2

Teoría de Iwasawa de $\mathbb{Z}_p$-extensiones

En el presente capítulo, probaremos algunos resultados sobre $\mathbb{Z}_p$-extensiones. Luego, determinaremos la estructura de módulos sobre el anillo $\Lambda = \mathbb{Z}_p[[T]]$ obteniendo un notable teorema de estructura para Λ-módulos. Para terminar, enunciaremos el teorema de Iwasawa que describe el comportamiento de la p-parte del número de clase en una $\mathbb{Z}_p$-extensión, explicaremos la idea de la demostración y desarrollaremos en detalle el argumento fundamental de esta idea.

En este capítulo usaremos resultados de la teoría de ramificación y del cuerpo de clase desarrollados en el capítulo anterior.

2.1 Anillos de grupo y Series de potencia

Fijemos p un número primo. Sea $\mathcal{O}$ el anillo de enteros algebraicos de una extensión finita de $\mathbb{Q}_p$ y Γ grupo topológico multiplicativo isomorfo a $(\mathbb{Z}_p, +)$ y fijemos γ generador topológico de Γ, es decir, $\Gamma = \overline{\langle\gamma\rangle}$. Notemos que tal isomorfismo en particular puede relacionar $0, 1 \in \mathbb{Z}_p$ con $1, \gamma \in \Gamma$.

Sabemos que los subgrupos cerrados de $\mathbb{Z}_p$ son de la forma $p^n\mathbb{Z}_p$, por lo tanto los subgrupos cerrados de Γ son de la forma Γ^{p^n}. Definimos $\Gamma_n = \Gamma/\Gamma^{p^n}$, entonces $\Gamma_n \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$ es cíclico de orden p^n generado por γ_n, coclase de γ.

Definición 32. Sea R un anillo con identidad $1 \neq 0$ y sea G un grupo. Definimos el conjunto

$$R[G] = \left\{ \sum_{g\in G} r_g g \ : \ r_g \in R, \ r_g = 0 \text{ excepto una cantidad finita.} \right\}$$

y definimos las operaciones

- Suma:
$$\sum_{g\in G} r_g g + \sum_{g\in G} s_g g = \sum_{g\in G} (r_g + s_g) g.$$
- Producto:
$$\left(\sum_{g\in G} r_g g \right) \left(\sum_{h\in G} s_h h \right) = \sum_{g,h\in G} (r_g s_h) gh.$$

El conjunto $R[G]$ con estas operaciones es un anillo y se llama anillo de grupo. En el caso particular que $G = \{g_1, g_2, \ldots, g_n\}$ entonces

$$R[G] = \{ r_1 g_1 + r_2 g_2 + \cdots + r_n g_n \ : \ r_i \in R, \ \forall i \in \{1, \ldots, n\} \}.$$

y es posible mostrar que todo elemento de $R[G]$ admite una escritura única de la forma $r_1 g_1 + r_2 g_2 + \cdots + r_n g_n$.

Observación 18. *El anillo $R[G]$ es conmutativo si y sólo si G es un grupo conmutativo.*

Consideremos el anillo de grupo $\mathcal{O}[\Gamma_n]$, entonces $\mathcal{O}[\Gamma_n] = \mathcal{O}[\gamma_n]$ es generado como $\mathcal{O}$-álgebra por γ_n y consiste en las sumas formales

$$r_0 + r_1\gamma_n + r_2\gamma_n^2 + \cdots + r_{p^n-1}\gamma_n^{p^n-1}$$

con $r_0, r_1, r_2, \ldots, r_{p^n-1} \in \mathcal{O}$. A partir de esto, podemos definir el isomorfismo

$$\mathcal{O}[Y]/(Y^{p^n} - 1) \simeq \mathcal{O}[\Gamma_n]$$

definido por

$$\sum_{i=0}^{p^n-1} r_i \overline{Y}^i \mapsto \sum_{i=0}^{p^n-1} r_i \gamma_n^i$$

Primero es bien definido ya que $1, \bar{Y}, \ldots, \bar{Y}^{p^n-1}$ forman una base de $\mathcal{O}[Y]/(Y^{p^n} - 1)$ como $\mathcal{O}$–módulo. Es claramente sobreyectivo pues la preimagen de γ es $\overline{Y}$. También es inyectivo, $\{1, \overline{Y}, \overline{Y}^2, \ldots, \overline{Y}^{p^n-1}\}$ y $\{1, \gamma_n, \gamma_n^2, \ldots, \gamma_n^{p^n-1}\}$ forman una base de $\mathcal{O}[Y]/(Y^{p^n} - 1)$ y $\mathcal{O}[\Gamma_n]$ respectivamente como $\mathcal{O}$–módulos. Y es un homomorfsmo de $\mathcal{O}$-álgebras ya que es factorización del homomorfismo evaluación $Y \mapsto \gamma_n$.

A su vez, tenemos un isomorfismo $\mathcal{O}[Y]/(Y^{p^n} - 1) \simeq \mathcal{O}[T]/((1+T)^{p^n} - 1)$ mediante la correspondencia $\overline{Y} \mapsto \overline{T+1}$. Luego,

$$\mathcal{O}[\Gamma_n] \simeq \mathcal{O}[T]/((1+T)^{p^n} - 1). \tag{2.1}$$

Por otro lado, para $m \geq n \geq 0$, como p^n divide p^m, existe un homomorfismo natural $\Gamma_m \to \Gamma_n$ que induce un homomorfismo de $\mathcal{O}$-álgebras

$$\begin{array}{rccc} \phi_{m,n}: & \mathcal{O}[\Gamma_m] & \to & \mathcal{O}[\Gamma_n] \\ & \gamma_m & \mapsto & \gamma_n \\ & a \in \mathcal{O} & \mapsto & a \in \mathcal{O} \end{array}$$

Como $m \geq n \geq 0$, $(1+T)^{p^n} - 1$ divide $(1+T)^{p^m} - 1$ y por ende, $((1+T)^{p^m} - 1) \subseteq ((1+T)^{p^n} - 1)$, Luego, a partir de (2.1) usando los homomorfismos $\phi_{m,n}$ podemos definir homomorfismos $\tilde{\phi}_{m,n}$ entre los anillos de polinomios. Estos homomorfismos forman dos sistemas proyec-

tivos isomorfos de $\mathcal{O}$-álgebras debido a que el siguiente diagrama conmuta

$$\begin{array}{ccc} \mathcal{O}[\Gamma_m] & \xrightarrow{\sim} & \mathcal{O}[T]/((1+T)^{p^m}-1) \\ \downarrow & & \downarrow \\ \mathcal{O}[\Gamma_n] & \xrightarrow{\sim} & \mathcal{O}[T]/((1+T)^{p^n}-1) \end{array}$$

De esta forma,

$$\mathcal{O}[[\Gamma]] = \varprojlim_{n\in\mathbb{N}} \mathcal{O}[\Gamma_n] \simeq \varprojlim_{n\in\mathbb{N}} \mathcal{O}[T]/((1+T)^{p^n}-1) \tag{2.2}$$

como $\mathcal{O}$-álgebras. Observamos que si $\alpha \in \mathcal{O}[\Gamma]$, tenemos una sucesión $\alpha_n = \alpha \mod \Gamma^{p^n}$ y si $\beta \in \mathcal{O}[T]$ es tal que para todo $n \in \mathbb{N}$, $\beta = \alpha \mod \Gamma^{p^n}$ entonces $\beta = \alpha$. Así podemos definir de manera natural una incrustación $\mathcal{O}[\Gamma] \hookrightarrow \mathcal{O}[[\Gamma]]$ de $\mathcal{O}$-álgebras.

Para fijar notaciones, sea $\mathcal{O}^\times$ grupo de las unidades de $\mathcal{O}$, sea π uniformizante de $\mathcal{O}$ y $\mathscr{P} = \langle \pi \rangle$ el único ideal máximal de $\mathcal{O}$ (ideal de las no unidades).

Definición 33. Sea $x \in \mathcal{O}$, entonces existen únicos $u \in \mathcal{O}^\times$ y $n \in \mathbb{N}$ tal que $x = \pi^n u$, a partir de esto, definimos sobre $\mathcal{O}$ la valuación (aditiva) v asociada a π como $v(x) = n$ y el valor absoluto

$$|x| = \begin{cases} p^{-v(x)}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Ahora que tenemos todas las notaciones podemos mencionar el objetivo de la sección: Mostrar que $\mathcal{O}[[\Gamma]]$ y $\mathcal{O}[[T]]$ son isomorfos como $\mathcal{O}$-álgebras.

Proposición 2.1.1: *Sean $f, g \in \mathcal{O}[[T]]$ y supongamos que $f = \sum_{i\geq 0} a_i T^i$, con $a_i \in \mathscr{P}$ para $0 \leq i \leq n-1$, pero $a_n \in \mathcal{O}^\times$. Entonces existen únicos $q \in \mathcal{O}[[T]]$ y $r \in \mathcal{O}[T]$ polinomio de grado a lo más $n-1$ tal que*

$$g = qf + r$$

Demostración. Para probar la existencia, consideremos el operador

$$\begin{array}{rccc} \tau = \tau_n : & \mathcal{O}[[T]] & \longrightarrow & \mathcal{O}[[T]] \\ & \sum_{i=0}^{\infty} b_i T^i & \longmapsto & \sum_{i=n}^{\infty} b_i T^{i-n} \end{array}$$

τ cumple las siguientes propiedades:

i) es lineal sobre $\mathcal{O}$:

ii) $\tau(T^n h(T)) = h(T)$ para todo $h(T) \in \mathcal{O}[[T]]$;

iii) $\tau(h(T)) = 0$ si y sólo si $h(T) \in \mathcal{O}[T]$ con $\deg h \leq n-1$

En efecto, la linealidad de τ se desprende de la linealidad de la sumatoria.
Sea $h(T) = \sum_{i=0}^{\infty} b_i T^i \in \mathcal{O}[[T]]$ entonces

$$\tau(T^n h(T)) = \tau\left(\sum_{i=0}^{n-1} 0T^i + \sum_{i=0}^{\infty} b_i T^{i+n}\right) = \sum_{i=0}^{\infty} b_i T^i = h(T).$$

Por otro lado,

$$\tau(h(T)) = 0 \Leftrightarrow b_i = 0 \ \forall i \geq n \Leftrightarrow h(T) \in \mathcal{O}[T] \text{ y } \deg h \leq n-1.$$

Como π divide a_i en $\mathcal{O}$ para $0 \leq i \leq n-1$, si consideramos $P(T) = b_0 + b_1 T + \cdots b_{n-1} T^{n-1}$ de modo que $a_i = \pi b_i$ para $0 \leq i \leq n-1$ y $U(T) = a_n + a_{n+1} T + \cdots = \tau(f(T))$ podemos escribir

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

El elemento $U(T) \in \mathcal{O}[[T]]$ es una unidad porque su término constante a_n pertenece a $\mathcal{O}^\times$. Sea

$$\begin{array}{rccc} \mu : & \mathcal{O}[[T]] & \longrightarrow & \mathcal{O}[[T]] \\ & h(T) & \longmapsto & \frac{P(T)}{U(T)} h(T) \end{array}$$

entonces definimos

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

donde la potencia j quiere decir componer las funciones j veces.

Para aclarar la definición de los sumandos, explicitemos los primeros:

$$\begin{aligned}
j = 0 &\rightarrow \tau(g(T)) \\
j = 1 &\rightarrow -\pi\tau\left(\tfrac{P}{U}\tau(g(T))\right) \\
j = 2 &\rightarrow \pi^2\tau\left(\tfrac{P}{U}\tau\left(\tfrac{P}{U}\tau(g(T))\right)\right) \\
j = 3 &\rightarrow -\pi^3\tau\left(\tfrac{P}{U}\tau\left(\tfrac{P}{U}\tau\left(\tfrac{P}{U}\tau(g(T))\right)\right)\right)
\end{aligned}$$

Para analizar la convergencia de $q(T)$ usamos la convergencia coeficiente a coeficiente. Para ello, consideremos $h_j(T) = (-1)^j(\tau \circ \mu)^j(\tau(g(T))) \in \mathcal{O}[[T]]$, entonces

$$U(T)q(T) = \sum_{j=0}^{\infty} \pi^j h_j(T).$$

Definimos su convergencia:

$$\lim_{N\to\infty} \sum_{j=0}^{N} \pi^j h_j(T) \text{ existe si y sólo si para todo } n \in \mathbb{N},\ \sum_{j=0}^{\infty} \pi^j c_n(h_j(T)) \text{ converge en } \mathcal{O}.$$

donde $c_n(h_j(T))$ es el n-ésimo coeficiente de $h_j(T)$. Si el límite es $\alpha_n \in \mathcal{O}$, denotamos

$$\lim_{N\to\infty} \sum_{j=0}^{N} \pi^j h_j(T) = \sum_{j=0}^{\infty} \alpha_n T^n.$$

Para probar la convergencia de una serie en $\mathcal{O}$, como es completo, basta probar que la sucesión de su término general es de Cauchy. La valuación $v(\pi^j) \overset{j\to\infty}{\longrightarrow} \infty$, por tanto,

$v(\pi^i c_n(h_i(T)) - \pi^j c_n(h_j(T))) \overset{i,j\to\infty}{\longrightarrow} \infty$. Así, dado $\varepsilon > 0$ existe n_0 tal que

$$|\pi^i c_n(h_i(T)) - \pi^j c_n(h_j(T))| < \varepsilon \quad \text{para } i, j \geq n_0.$$

De esta forma, $\lim_{N\to\infty} \sum_{j=0}^{N} \pi^j h_j(T)$ existe y es por esto que $U(T)q(T) \in \mathcal{O}[[T]]$. Además, $U(T) \in \mathcal{O}[[T]]$ entonces

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} \pi^j h_j(T) \in \mathcal{O}[[T]].$$

Luego, $qf = \pi qP + T^n qU$ y aplicando a esta igualdad el operador τ tenemos que

$$\tau(qf) = \pi\tau(qP) + \tau(T^n qU) = \pi\tau(qP) + qU \tag{2.3}$$

Ahora bien,

$$\pi\tau(qP) = \pi\left(\tau \circ \mu\right) \circ \left(\sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \mu\right)^j \left(\tau(g)\right) \right) = \sum_{j=0}^{\infty} (-1)^j \pi^{j+1} \left(\tau \circ \mu\right)^{j+1} \left(\tau(g)\right)$$

arreglamos la suma, multiplicando por -1 y agregando un cero conveniente $\tau(g) - \tau(g)$ para obtener

$$-\pi\tau(qP) = -\tau(g + \sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \mu\right)^j \left(\tau(g)\right) = -\tau(g) + qU$$

lo que se reduce a $\pi\tau(qP) = \tau(g) - qU$. Usando esto en (2.3) tenemos que $\tau(qf) = \tau(g)$. Como τ es un operador lineal, lo anterior es equivalente a $\tau(g - qf) = 0$ y por propiedad de τ, $g - qf = r$ con $r(T) \in \mathcal{O}[T]$ y $\deg(r(T)) \leq n - 1$. Por lo tanto, $g = qf + r$ con $q \in \mathcal{O}[[T]]$ y $r \in \mathcal{O}[T]$ de grado menor que n.

Finalmente, para la unicidad de esta escritura, supongamos que existen $q_1, q_2 \in \mathcal{O}[[T]]$ y

$r_1, r_2 \in \mathcal{O}[T]$ como en el enunciado, tal que

$$g = q_1 f + r_1 = q_2 f + r_2$$

esto ocurre si y sólo si $(q_1 - q_2)f + (r_1 - r_2) = 0$. Sea $Q = q_1 - q_2$ y $R = r_1 - r_2$ y veamos que $Q = R = 0$.

Si $Q, R \neq 0$, podemos asumir que π no divide a Q o bien π no divide a R, pues de lo contrario, eliminamos el factor π. Si $\tilde{f} = \sum_{i=n}^{\infty} a_i T^i$, haciendo reducción módulo π tenemos que

$$Q\tilde{f} + R \equiv 0 \ (\text{mód } \pi),$$

con $\deg Q\tilde{f} \geq n$ y $\deg R \leq n-1$. Luego, π divide R y $Q\tilde{f}$. Como π no divide $\tilde{f}$ entonces π divide Q, lo que es una contradicción. De esta forma, $Q = R = 0$, así $g_1 = g_2$ y $r_1 = r_2$. □

Definición 34. El polinomio $P(T) \in \mathcal{O}[T]$ es llamado distinguido si $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ con $a_i \in \mathscr{P}$ para $0 \leq i \leq n-1$. (Notemos que si π^2 no divide a_0 entonces $P(T)$ es un polinomio de Eisentein).

Observación 19. *Por la Proposición 2.1.1 tenemos un algoritmo de la división para polinomios distinguidos: si $f(T) \in \mathcal{O}[[T]]$ y $P(T)$ es un polinomio distinguido, entonces existen únicos $q(T) \in \mathcal{O}[[T]]$ y $r(T) \in \mathcal{O}[T]$ con $\deg(r) < \deg(P)$ tal que*

$$f(T) = q(T)P(T) + r(T)$$

donde por conveniencia $\deg(0) = -\infty$.

Teorema 2.1.2: *Sea*

$$f(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathcal{O}[[T]],$$

y supongamos que para algún n tenemos que $a_i \in \mathcal{P}$ para $0 \leq i \leq n-1$, pero $a_n \in \mathcal{O}^\times$.

Entonces f tiene una escritura única de la forma

$$f(T) = P(T)U(T),$$

donde $U(T) \in \mathcal{O}[[T]]$ es una unidad y $P(T)$ es un polinomio distinguido de grado n.
En general, si $f(T) \in \mathcal{O}[[T]]$ es no cero, entonces tiene una escritura única de la forma

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

con P y U son como anteriormente y μ es un entero no negativo.

Demostración. Por Proposición 2.1.1, dado T^n y $f(T)$ existen únicos $q \in \mathcal{O}[[T]]$ y $r \in \mathcal{O}[T]$ con $\deg r \leq n-1$ tal que

$$T^n = q(T)f(T) + r(T). \tag{2.4}$$

Luego,

$$T^n \equiv (q(T)f(T) + r(T))(\text{mód } \pi)$$

como $q(T)f(T) \equiv q(T)(a_n T^n + \text{términos de grado mayor grado})(\text{mód } \pi)$ y $\deg r \leq n-1$, $r(T) \equiv 0 \ (\text{mód } \pi)$. Por tanto, $P(T) = T^n - r(T)$ es un polinomio distinguido de grado n. Sea q_0 el término constante de $q(T)$, entonces $1 \equiv q_0 a_n \ (\text{mód } \pi)$, así, $q_0 \in \mathcal{O}$ es una unidad y por consiguiente, $q(T)$ es una unidad en $\mathcal{O}[[T]]$. Si consideramos $U(T) = 1/q(T)$, usando (2.4) tenemos que

$$f(T) = \frac{1}{q(T)}(T^n - r(T)) = P(T)U(T).$$

La unicidad de esta escritura viene dada por la unicidad de la Proposición 2.1.1.
Para generalizar, basta factorizar los coeficientes de f por una potencia lo más grande posible de π y obtener n como en el enunciado. □

Corolario 2.1.3: *Sea $f(T) \in \mathcal{O}[[T]]$ no cero, entonces $\{x \in \mathbb{C}_p : |x| < 1 \wedge f(x) = 0\}$ es un*

conjunto finito.

Demostración. Sea $f(T) = \pi^{\mu}P(T)U(T)$ y $x \in \{x \in \mathbb{C}_p : |x| < 1 \wedge f(x) = 0\}$. Obsevar que todo $f(T) \in \mathcal{O}[[T]]$, sus coeficientes a_i cumplen $|a_i| \leq 1$. Entonces si $|x| < 1$, $f(x)$ converge, puesto que el término general de $U(T)$ tiende a 0 cuando i tiende a infinito y este argumento es suficiente para concluir porque $\mathbb{C}_p$ es no arquimediano.

Ahora bien, como $U(T)$ es una unidad, existe $U^{-1}(T) \in \mathcal{O}[[T]]$ tal que $U(T)U^{-1}(T) = 1$. Esta última es una igualdad de series formales, de la que se deduce una igualdad de funciones, por tanto, $U(x) \neq 0$, lo que quiere decir que $U(x)$ no se anula para $x \in \mathbb{C}_p$ con $|x| < 1$. Luego, $P(x) = 0$. Como $P(T)$ es un polinomio distinguido, $P(x) = 0$ tiene finitas soluciones. □

Observación 20. *Recordamos que $\mathbb{C}_p = \hat{\overline{\mathbb{Q}}}_p$ (donde $\hat{}$ designa la completación como espacio métrico) es completo y algebraicamente cerrado (Ver [6, cap. 3, Teorema 13]). De hecho, la definición y propiedades de $\mathbb{C}_p$ no son necesarias para demostrar el Corolario, ya que sólo necesitamos considerar los ceros en $\overline{\mathbb{Q}}_p$.*

Lema 2.1.4: *Sea $P(T) \in \mathcal{O}[T]$ un polinomio distinguido y $g(T) \in \mathcal{O}[T]$ arbitrario. Si $g(T)/P(T) \in \mathcal{O}[[T]]$ entonces $g(T)/P(T) \in \mathcal{O}[T]$.*

Demostración. Supongamos que $g(T) = f(T)P(T)$ para algún $f \in \mathcal{O}[[T]]$. Sea $x \in \mathbb{C}_p$ tal que $P(x) = 0$, entonces $|x| \leq 1$ ya que x es entero sobre $\mathcal{O}$ y como P es distinguido se tiene que $|x| < 1$. Por lo tanto, $f(x)$ converge y como $P(x) = 0$, se tiene que $g(x) = 0$, es decir, x es también un cero de g. Dividiendo g por $T - x$ en $\mathcal{O}[T]$ y repitiendo este proceso con cada cero de P (considerando su multiplicidad), obtenemos que cada cero de P es un cero de g. Este procedimiento es finito, porque el grado de P es finito. De esta forma, P divide a g en $\mathcal{O}[T]$. □

Para finalizar, el objetivo de esta sección:

Teorema 2.1.5: $\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]]$ *como* $\mathcal{O}$*-álgebras, el isomorfismo viene dado por* $\gamma \mapsto 1+T$.

Demostración. Por (2.2), es suficiente probar que

$$\mathcal{O}[[T]] \simeq \varprojlim \mathcal{O}[T]/((1+T)^{p^n}-1).$$

Sea $P_n(T) = (1+T)^{p^n}-1$, entonces $P_n(T)$ es un polinomio de grado p^n, mónico, cuyos coeficientes no principales son divisibles por p, por tanto, son divisibles por π. Luego, $P_n(T)$ es un polinomio distinguido de grado p^n.

Por otra parte, (π, T) es un ideal máximal de $\mathcal{O}[[T]]$. En efecto, basta considerar el homomorfismo

$$\begin{array}{ccc} \mathcal{O}[[T]] & \longrightarrow & \mathcal{O}/(\pi) \\ g & \longmapsto & g(0) \end{array}$$

cuyo kernel es (π, T) y así obtener que $\mathcal{O}[[T]]/(\pi, T) \simeq \mathcal{O}/(\pi)$. Como (π) es un ideal máximal de $\mathcal{O}$, entonces lo anterior nos permite afirmar que $\mathcal{O}[[T]]/(\pi, T)$ es un cuerpo y por ende, (π, T) es un ideal máximal de $\mathcal{O}[[T]]$. Este ideal, en particular contiene a (p, T) puesto que π divide p.

Por inducción probemos que $P_n(T) \in (p, T)^{n+1}$.
Claramente $P_0(T) = T \in (p, T)$. Por otra parte, sea $u = (1+T)^{p^n}$ entonces

$$\frac{P_{n+1}(T)}{P_n(T)} = \frac{(1+T)^{p^{n+1}}-1}{(1+T)^{p^n}-1} = \frac{u^p-1}{u-1} = 1 + u + \cdots + u^{p-1}$$

como tenemos p sumandos, y cada uno de ellos aporta con un 1, entonces lo anterior se reduce a

$$\frac{P_{n+1}(T)}{P_n(T)} = p + \text{serie formal sin término constante en } \mathcal{O}[[T]] \in (p, T).$$

Ahora bien, supongamos que para n entero positivo, $P_n(T) \in (p,T)^{n+1}$, entonces

$$P_{n+1}(T) = \frac{P_{n+1}}{P_n} P_n \in (p,T)^{n+2}$$

dado que $\frac{P_{n+1}}{P_n} \in (p,T)$ y $P_n \in (p,T)^{n+1}$.

Dado $f(T) \in \mathcal{O}[[T]]$, por Proposición 2.1.1, existen únicos $q_n(T) \in \mathcal{O}[[T]]$ y $f_n(T) \in \mathcal{O}[T]$ con $\deg f_n < p^n$ tal que $f(T) = q_n(T)P_n(T) + f_n(T)$. Usando esto, para cada $n \in \mathbb{N}$, existe un homomorfismo de $\mathcal{O}-$álgebras sobreyectivo

$$\begin{array}{rccc} \psi_n : & \mathcal{O}[[T]] & \longrightarrow & \mathcal{O}[T]/(P_n(T)) \\ & f(T) & \longmapsto & f_n(T)(\text{mód } P_n(T)) \end{array}$$

la verificación de que ψ_n es un homomorfismo es sencilla para la suma, sin embargo, para el producto debemos tener cuidado. Sean $f(T), g(T) \in \mathcal{O}[[T]]$ entonces exiten únicos $q_n(T), \tilde{q}_n(T) \in \mathcal{O}[[T]]$, $f_n(T), \tilde{f}_n(T) \in \mathcal{O}[T]$ con $\deg f_n, \deg \tilde{f}_n < p^n$ tal que

$$\begin{aligned} f(T) &= q_n(T)P_n(T) + f_n(T) \\ g(T) &= \tilde{q}_n(T)P_n(T) + \tilde{f}_n(T) \end{aligned}$$

entonces $f(T)g(T) = f_n(T)\tilde{f}_n(T)(\text{mód}P_n)$.

Por otra parte, también existen únicos $a_n(T) \in \mathcal{O}[[T]]$ y $b_n(T) \in \mathcal{O}[T]$ con $\deg b_n < p^n$ tal que $f(T)g(T) = a_n(T)P_n(T) + b_n(T)$. Si bien, por un asunto de grados $b_n \neq f_n(T)\tilde{f}_n(T)$, estos son congruentes módulo $P_n(T)$.

Si $m \geq n \geq 0$, podemos definir el siguiente sistema proyectivo $\{\mathcal{O}[T]/(P_n(T)), \phi_{nm}\}$

$$\begin{array}{rccc} \phi_{nm} : & \mathcal{O}[T]/(P_m(T)) & \longrightarrow & \mathcal{O}[T]/(P_n(T)) \\ & g(T)(\text{mód } P_m(T)) & \longmapsto & g(T)(\text{mód } P_n(T)) \end{array}$$

Observemos que $f(T) = q_m(T)P_m(T) + f_m(T)$ con $\deg f_n < \deg f_m < p^m$. Luego, tenemos

la relación

$$f_m(T) - f_n(T) = \left(q_n(T) + \frac{P_m(T)}{P_n(T)} q_m(T)\right) P_n(T),$$

donde $P_n(T)$ divide $P_m(T)$. Como el polinomio $P_n(T)$ es distinguido y divide al polinomio $f_m(T) - f_n(T)$ en $\mathcal{O}[[T]]$, por Lema 2.1.4, esta división es en $\mathcal{O}[T]$. Luego, $f_m(T) - f_n(T) \equiv 0 \pmod{P_n(T)}$, es decir, $f_m(T) \equiv f_n(T) \pmod{P_n(T)}$ como polinomios. A partir de esto, concluimos que el siguiente diagrama

$$\begin{array}{ccc} \mathcal{O}[[T]] & \xrightarrow{\psi_n} & \mathcal{O}[T]/(P_n(T)) \\ {\scriptstyle \psi_m}\downarrow & \nearrow_{\phi_{nm}} & \\ \mathcal{O}[T]/(P_m(T)) & & \end{array}$$

conmuta lo que finalmente nos permite definir el homomorfismo

$$\begin{array}{rccc} \Phi: & \mathcal{O}[[T]] & \longrightarrow & \varprojlim_{n\in\mathbb{N}} \mathcal{O}[T]/(P_n(T)) \\ & f(T) & \longmapsto & (f_n(T))_{n\geq 0}. \end{array}$$

donde $f_n(T) = \psi_n(f(T))$. Veamos que es un isomorfismo.

Sea $f(T) \in \mathcal{O}[T]$ tal que $f_n(T) = 0$ para todo $n \in \mathbb{N}$, entonces $P_n(T)$ divide $f(T)$ para todo $n \in \mathbb{N}$, es decir,

$$f(T) \in \bigcap_{n\in\mathbb{N}} (P_n(T)).$$

Ahora bien, como $P_n(T) \in (p, T)^{n+1}$ tenemos que

$$\bigcap_{n\in\mathbb{N}} (P_n(T)) \subseteq \bigcap_{n\in\mathbb{N}} (p, T)^{n+1}.$$

Si $h(T) \in (p, T)^{n+1}$ para todo $n \in \mathbb{N}$, dado $i \in \mathbb{N}$ fijo, el coeficiente i-ésimo de $h(T)$ es divisible por p^{n-i} para todo $n > i$, entonces este coeficiente es nulo. Y esto ocurre para

todo $i \in \mathbb{N}$. Por esta razón, $h(T) = 0$ y

$$\bigcap_{n\in\mathbb{N}} (p,T)^{n+1} = \{0\}.$$

Luego, Φ es inyectiva.

Para la sobreyectividad, sea $(f_n)_{n\geq 0} \in \varprojlim_{n\in\mathbb{N}} \mathcal{O}[T]/(P_n(T))$. Para $m \geq n \geq 0$, sabemos que

$$f_m(T) \equiv f_n(T) (\text{mód } P_n(T)), \tag{2.5}$$

como $(P_n(T)) \subseteq (p,T)^{n+1}$ entonces

$$f_m(T) \equiv f_n(T) (\text{mód } (p,T)^{n+1}),$$

además, $(p,T)^{n+1} = (p^{n+1}, p^n T, \cdots, p^{n-k+1}T^k, \cdots, pT^n, T^{n+1})$, por tanto, hay una relación entre los coeficientes de f_m y f_n:

$$c_k(f_m) \equiv c_k(f_n) (\text{mód } p^{n-k+1}),$$

Fijemos $k \geq 0$. Para todo $n_0 \in \mathbb{N}$ tal que para todo $m \geq n \geq N$, $|c_k(f_n) - c_k(f_m)| < p^{n_0}$, es decir, $\{c_k(f_n)\}_{n\in\mathbb{N}} \subseteq \mathcal{O}$ es una sucesión de Cauchy. El anillo $\mathcal{O}$ es completo, entonces $\{c_k(f_n)\}_{n\in\mathbb{N}}$ converge en $\mathcal{O}$. Nótesee $a_k = \lim_{n\to\infty} c_k(f_n)$, definimos

$$f(T) = \sum_{k=0}^{\infty} a_k T^k$$

esto es, $f(T) = \lim_{n\to\infty} f_n(T)$. Probemos que $\Phi(f) = (f_n)_{n\in\mathbb{N}}$.

Si $m \geq n \geq 0$, por (2.5) existe $q_{m,n}(T) \in \mathcal{O}[T]$ tal que $f_m(T) - f_n(T) = q_{m,n}(T)P_n(T)$, es decir,

$$q_{m,n}(T) = \frac{f_m(T) - f_n(T)}{P_n(T)},$$

si hacemos tender m a infinito, tenemos que

$$\lim_{m\to\infty} q_{m,n}(T) = \frac{f(T) - f_n(T)}{P_n(T)}$$

con $\lim_{m\to\infty} q_{m,n}(T) \in \mathcal{O}[[T]]$. Observando que la noción de límite coeficiente por coeficiente es compatible con las operaciones binarias suma, resta, multiplicación y división.

De esta forma, para cada $n \in \mathbb{N}$

$$f(T) = P_n(T)\left(\lim_{m\to\infty} q_{m,n}(T)\right) + f_n(T)$$

y por definición esto es $\psi_n(f) = f_n$. Por lo tanto, $\Phi(f) = (f_n)_{n\in\mathbb{N}}$. □

2.2 $\mathbb{Z}_p$- extensiones

Definición 35. Una $\mathbb{Z}_p$-extensión de un cuerpo de número K es una extensión K_∞/K tal que $Gal(K_\infty/K) \simeq (\mathbb{Z}_p, +)$

Todo cuerpo de número tiene al menos una $\mathbb{Z}_p$-extensión. Basta considerar K_∞ un subcuerpo apropiado de $K(\zeta_{p^\infty})$ según sea el caso, haciendo una construcción análoga a la hecha en el capítulo 1: adjuntando raíces de la unidad para construir una secuencia de cuerpos

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_{n\geq 0} K_n$$

tal que $Gal(K_n/K)) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Proposición 2.2.1: *Sea K_∞/K una $\mathbb{Z}_p$-extensión. Entonces para cada $n \geq 0$, existe un único subcuerpo K_n de grado p^n sobre K y K_n, K_∞ son los únicos cuerpos entre K y K_∞.*

Demostración. Por teorema de Galois para extensiones infinitas, los cuerpos intermedios

de K_∞/K se corresponden biyectivamente con los subgrupos cerrados de $\mathbb{Z}_p$. Sabemos que existe un único subgrupo cerrado de $\mathbb{Z}_p$ con índice p^n y este es $H = p^n\mathbb{Z}_p$. Entonces por teorema de Galois, si consideramos $K_n = K^H$ tenemos que

$$[K_n : K] = (\mathbb{Z}_p : H) = p^n.$$

De la unicidad del subgrupo H se desprende que K_n es el único subcuerpo propio entre K y K_∞. □

Proposición 2.2.2: *Sea K_∞/K una $\mathbb{Z}_p$-extensión y sea l un primo (posiblemente arquimediano) de K que no está sobre p. Entonces K_∞/K no se ramifica en l. En otras palabras, las $\mathbb{Z}_p$-extensiones no se ramifican fuera de p.*

Demostración. Sea $I \subseteq Gal(K_\infty/K) \simeq \mathbb{Z}_p$ grupo de inercia. Sabemos por Lema 1.6.8 que I es cerrado, entonces tenemos dos opciones $I = 0$ o bien $I = p^n\mathbb{Z}_p$ para algún $n \in \mathbb{N}$.

Si $I = 0$ entonces el índice de ramificación es 1, porque este es el orden del grupo de inercia, por tanto, la extensión K_∞/K no ramifica.

Si $I = p^n\mathbb{Z}_p$ tenemos que $|I|$ es infinito, entonces l es un primo finito, porque para primos infinitos $|I| = 1, 2$. Ahora bien, por la Proposición 2.2.1, podemos considerar una sucesión de subcuerpos K_n de K_∞/K tal que K_n/K es Galois y de grado p^n sobre K,

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_{n\geq 0} K_n.$$

Sea l_∞ primo de $\mathcal{O}_{K_\infty}$ tal que $l_\infty \cap \mathcal{O}_K = l$. Para cada $n \geq 1$, sea l_n un primo finito de K_n tal que $l_n = l_\infty \cap \mathcal{O}_{K_n}$ y $\mathcal{O}_{K_n} \cap l_{n-1} = l_n$ ($l_0 = l$). A cada primo l_n asociamos una valuación v_{l_n}: dado $\alpha \in K_n$ consideramos el ideal (α) de $\mathcal{O}_{K_n}$, como este anillo es de Dedekind, definimos $v_{l_n}(\alpha) = a$ siendo a el exponente de l_n en la factorización de (α). A partir de

esto, definimos la siguiente valuación sobre K_n:

$$v_n(\alpha) = \frac{v_{l_n}(\alpha)}{e(l_n|l)},$$

observamos que la corrección en el denominador es para que $v_n(l) = 1$ y de esta forma, v_n extiende la valuación l-ádica.

La valuación v_{n+1} extiende a v_n. En efecto, como $e(l_{n+1}|l) = e(l_{n+1}|l_n)e(l_n|l)$, para $\alpha \in K_n$ tenemos que

$$v_{n+1}(\alpha) = \frac{v_{l_{n+1}}(\alpha)}{e(l_{n+1}|l)} = \frac{v_{l_n}(\alpha)e(l_{n+1}|l_n)}{e(l_{n+1}|l)} = \frac{v_{l_n}(\alpha)}{e(l_n|l)} = v_n(\alpha).$$

Sea $\widehat{K}_n$ la completación de K_n por v_n y $\widehat{K}_\infty = \bigcup_{n\geq 0} \widehat{K}_n$. Observamos que $\widehat{K}_n \hookrightarrow \widehat{K}_{n+1}$ porque v_{n+1} extiende a v_n y $K_n \hookrightarrow K_{n+1}$.

La extensión $\widehat{K}_\infty/\widehat{K}$ es Galois porque para todo $n \in \mathbb{N}$, $\widehat{K}_n/\widehat{K}$ es Galois. Ahora

$$\begin{array}{ccc} Gal(\widehat{K}_n/\widehat{K}) & \xrightarrow{\sim} & D(l_n/l) \\ \sigma & \longmapsto & \sigma|_{K_n} \\ \tilde{\sigma} & \longmapsto & \sigma \end{array}$$

donde $\tilde{\sigma}$ es la extensión de σ usando la continuidad de σ para la topología l_n-ádica para así extender σ a la completación $\widehat{K}_n$ de K_n (Ver [10, Cap.8, Proposición 8.10]). Como el siguiente diagrama conmuta

$$\begin{array}{ccc} Gal(\widehat{K}_\infty/\widehat{K}) & \longrightarrow & D(l_\infty/l) \\ \downarrow & & \downarrow \\ Gal(\widehat{K}_n/\widehat{K}) & \longrightarrow & D(l_n/l) \end{array}$$

y deducimos que $Gal(\widehat{K}_\infty/\widehat{K}) \simeq D(l_\infty/l)$. Entonces, de forma natural $I \hookrightarrow Gal(\widehat{K}_\infty/\widehat{K})$.

El cuerpo $\widehat{K}$ es una extensión finita de $\mathbb{Q}_{\tilde{l}}$ con $\tilde{l}$ entero distinto de p y $l|\tilde{l}$. Además $\widehat{K}_\infty/\widehat{K}$

es una extensión abeliana porque se identifica con un subgrupo (de descomposición) de $Gal(K_\infty/K)$ que es abeliana, por lo que $\widehat{K}_\infty \subseteq \widehat{K}^{ab}$ con $\widehat{K}^{ab}$ máxima extensión abeliana de $\widehat{K}$. Sea U las unidades enteras de $\widehat{K}$, usando [2, Apéndice, Teorema 10] tenemos un un epimorfismo continuo

$$U \twoheadrightarrow I \simeq p^n\mathbb{Z}_p.$$

Por otra parte,

$$U \simeq \mathbb{Z}_{\tilde{l}}^a \times (\text{grupo finito}) \quad \text{para algún } a \in \mathbb{Z} \tag{2.6}$$

Observemos que para el caso $K = \mathbb{Q}$ revisamos esto en el capítulo 1, donde concluimos que

$$\mathbb{Z}_{\tilde{l}}^\times \simeq \mathbb{Z}_{\tilde{l}} \times \mathbb{Z}/(\tilde{l}-1)\mathbb{Z}, \quad \text{si } \tilde{l} \neq 2$$
$$\mathbb{Z}_2^\times \simeq \mathbb{Z}_2 \times (\mathbb{Z}/2\mathbb{Z})^*, \quad \text{si } \tilde{l} = 2.$$

Continuando con la demostración, como $p^n\mathbb{Z}_p$ no tiene torsión de (2.6) se deduce una compuesta de epimorfismos continuos

$$\mathbb{Z}_{\tilde{l}}^a \twoheadrightarrow p^n\mathbb{Z}_p \twoheadrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p,$$

el grupo $p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$ tiene cardinalidad p, si denotamos por H el kernel de esta compuesta continua, tenemos que H es un subgrupo cerrado de $\mathbb{Z}_{\tilde{l}}^a$ de índice p. Pero esto no es posible, porque en tal caso, H es un subgrupo cerrado de índice finito, entonces es sería un subgrupo abierto de $\mathbb{Z}_{\tilde{l}}^a$ que contiene a la identidad. Luego, existe un entorno de la identidad contenido en H. Para un m entero adecuado, sea $V = \tilde{l}^m\mathbb{Z}_{\tilde{l}} \times \cdots \times \tilde{l}^m\mathbb{Z}_{\tilde{l}}$ tal entorno. Como $\mathbb{Z}_{\tilde{l}}^a/V \simeq (\mathbb{Z}_{\tilde{l}}/\tilde{l}^m\mathbb{Z}_{\tilde{l}})$ entonces V es de índice $\tilde{l}^{ma}$ y $\mathbb{Z}_{\tilde{l}}^a/V$ es un subgrupo de $\mathbb{Z}_{\tilde{l}}^a/H$, lo que implica que $\tilde{l}$ divide p.

De esta forma, $I = 0$ y se concluye que l es no ramificado en K_∞/K. □

Lema 2.2.3: *Sea K_∞/K una $\mathbb{Z}_p$-extensión. Al menos un primo se ramifica en esta*

extensión, y existe $n \geq 0$ tal que todo primo que se ramifica en K_∞/K_n es totalmente ramificado.

Demostración. Recordemos que como K es un cuerpo de números, entonces su cuerpo de clase es finito, y por tanto, la máxima extensión abeliana no ramificada de K es finita. Como K_∞ es una extensión abeliana infinita de K, entonces al menos un primo se debe ramificar en K_∞/K. Por la Proposición 2.2.2, como hay finitos primos de K sobre p, entonces finitos primos se ramifican en K_∞/K. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ estos primos y $I_1, \ldots, I_s$ sus respectivos grupos de inercia $I(\tilde{\mathfrak{p}}_j|\mathfrak{p}_j)$ para $\tilde{\mathfrak{p}}_j$ un primo de K_∞ sobre $\mathfrak{p}_j$. Para $j \in \{1, \ldots, s\}$, $I_j \hookrightarrow \mathbb{Z}_p$ cerrado, entonces

$$I = \bigcap_{j=1}^{s} I_j \simeq p^n\mathbb{Z}_p$$

para algún $n \in \mathbb{N}$. Sea L cuerpo fijo de I, por correspondencia de Galois infinito y teniendo en cuenta que I es cerrado, tenemos que $Gal(K_\infty/L) = \bar{I} = I \simeq p^n\mathbb{Z}_p$. Además,

$$Gal(L/K) \simeq Gal(K_\infty/K)/Gal(K_\infty/L) \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$$

luego, $[L : K] = p^n$ y por Proposición 2.2.1, $L = K_n$.

Por otra parte, Por Proposición 2.2.2 sabemos que los primos que se ramifican en K_∞/K deben estar sobre p y estos primos son de la forma $\tilde{\mathfrak{p}}_j \cap \mathcal{O}_{K_n}$.

Observemos que tenemos un epimorfismo de restricción

$$Gal(K_\infty/K) \twoheadrightarrow Gal(K_\infty/K_n)$$

que actúa sobre los grupos de inercia como sigue: para todo $j \in \{1, \ldots, s\}$

$$I(\tilde{\mathfrak{p}}_j|\mathfrak{p}_j) \mapsto I(\tilde{\mathfrak{p}}_j|\tilde{\mathfrak{p}}_j \cap \mathcal{O}_{K_n})$$

Finalmente, $Gal(K_\infty/K_n) \subseteq Gal(K_\infty/K)$ y entonces

$$I(\tilde{\mathfrak{p}}_j|\tilde{\mathfrak{p}}_j \cap \mathcal{O}_{K_n}) = I(\tilde{\mathfrak{p}}_j|\mathfrak{p}_j) \cap Gal(K_\infty/K_n),$$

y de esta forma,

$$\begin{aligned} I(\tilde{\mathfrak{p}}_j|\tilde{\mathfrak{p}}_j \cap \mathcal{O}_{K_n}) &= I(\tilde{\mathfrak{p}}_j|\mathfrak{p}_j) \cap Gal(K_\infty/K_n) \\ &= I(\tilde{\mathfrak{p}}_j|\mathfrak{p}_j) \cap I \\ &= I \\ &= Gal(K_\infty/K_n) \end{aligned}$$

es decir, cada primo en K_n que se ramifica sobre K_∞ es totalmente ramificado. □

2.3 La estructura de Λ-módulos

Sea $\Lambda = \mathbb{Z}_p[[T]]$. En esta sección usaremos los resultados desarrollados en la primera sección de este capítulo, considerando $\mathcal{O} = \mathbb{Z}_p$.

Definición 36. Sean M y M' dos Λ-módulos. Se dice que M es pseudo-isomorfo a M', denotado por $M \sim M'$, si existe un homomorfismo $M \to M'$ con kernel y cokernel finito. En otras palabras, si existe un secuencia exacta de Λ-módulos

$$0 \to A \to M \to M' \to B \to 0$$

con A, B Λ-módulos finitos.

Observación 21. *Notemos que "ser pseudo-isomorfos" no es una relación de equivalencia, porque no es simétrica.*

1) Claramente es reflexiva, basta considerar el homomorfismo identidad que tiene kernel y cokernel trivial.

2) Sea $M \overset{\phi}{\sim} M'$ y $M' \overset{\psi}{\sim} M''$. Mostremos que es transitiva, es decir, que $\psi \circ \phi$ es un pseudo-

isomorfismo. Sabemos que $\ker(\phi), \ker(\psi)$ *son finitos. Sean* $x_1, \ldots, x_l$ *un antecedente para cada elemento de* $\ker(\psi) \cap \phi(M)$ *vía* ϕ *(*$1 \leq l \leq |\ker(\psi)$*), entonces*

$$\ker(\psi \circ \phi) \simeq \phi^{-1}(\ker(\psi)) = \bigcup_{i=1}^{l} \ker(\psi) x_i$$

es finito. Para el cokernel de $\psi \circ \phi$ *observemos que por el tercer teorema del isomorfismo*

$$M''/\psi(M') = \left(M''/\psi(\phi(M))\right) / \left(\psi(M')/\psi(\phi(M))\right)$$

como $M''/\psi(M')$ *es finito, para concluir basta probar que* $\psi(M')/\psi(\phi(M))$ *es finito y por un asunto de cardinalidades tendremos que* $M''/\psi(\phi(M))$ *es finito. Para ello, si* π *es la proyección entonces*

$$\pi \circ \psi : M' \longrightarrow \psi(M')/\psi(\phi(M))$$

es sobreyectivo. Como $\phi(M) \subseteq \ker(\pi \circ \psi)$*, se tiene que*

$$|\psi(M')/\psi(\phi(M))| \leq |M'/\phi(M)| < \infty.$$

Por lo tanto, $M \overset{\psi\circ\phi}{\sim} M''$.

Para notar que la simetría falla necesitamos algunos resultados extras. Dejaremos esto pendiente para luego analizarlo.

El objetivo de esta sección es probar el siguiente resultado, conocido como teorema de estructura para Λ-módulos.

Teorema 2.3.1: *Sea* M *un* Λ*-módulo finitamente generado. Entonces existe un psedo-isomorfismo*

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

donde r, s, t, n_i, m_j *son enteros no negativos y cada* $f_j(T)$ *es un polinomio distinguido e irreducible.*

Con este fin, comenzaremos enunciando y demostrando algunos resultados previos.

Definición 37. Un anillo R es DFU si:

1. R es un dominio de integridad.
2. Todo elemento irreducible $r \in R$ genera un ideal principal primo.
3. Todo elemento de R no nulo puede ser escrito como producto finito de elementos irreducibles por una unidad.

Teorema 2.3.2: *Λ es un DFU, cuyos elementos irreducibles son p y los polinomios distinguidos irreducibles.*

Demostración. Por Teorema 2.1.2, dado $f(T) \in \Lambda$ no nulo, existe μ entero no negativo, $P(T) \in \mathbb{Z}_p[T]$ polinomio distinguido y $U(T) \in \Lambda^\times$ tal que

$$f(T) = p^\mu P(T)U(T).$$

Observamos que si bien $P(T)$ no es necesariamente un polinomio irreducible, como $\mathbb{Z}_p$ es un DFU, entonces $\mathbb{Z}_p[T]$ es un DFU y por tanto, $P(T)$ se factoriza en polinomios mónicos irreducibles en $\mathbb{Z}_p$. Ahora bien, faltaría verificar que esta factorización es en polinomios distinguidos irreducibles. En efecto, sea

$$P(T) = P_1(T)\cdots P_s(T) \tag{2.7}$$

donde $P_i(T) \in \mathbb{Z}_p[T]$ irreducible para todo $i \in \{1, \ldots, s\}$. Si $n = \deg(P)$, reduciendo (2.7) módulo p tenemos que

$$T^n = P_1(T)\cdots P_s(T)(\text{mód } p)$$

luego, $P_1(T), \ldots, P_s(T)$ módulo p son potencias de T y los grados de estas potencias suman n. Por tanto,

$$P_i(T) = b_{i_0} + b_{i_1}T + \cdots + b_{i_l}T^{i_l}$$

con $b_{i_0}, \dots b_{i_{l-1}} \in p\mathbb{Z}_p$ y $b_{i_l} \in \mathbb{Z}_p^\times$. Para concluir basta considerar $\tilde{P}_i(T) = b_{i_l}^{-1} P_i(T)$ para todo $i \in \{1, \dots, s\}$ y obtenemos que $P(T)$ es producto de polinomios $\tilde{P}_i(T)$ distinguidos e irreducibles.

De esta forma, p y los polinomios distinguidos irreducibles sobre $\mathbb{Z}_p[T]$ factorizan todo elemento no nulo de Λ. Para finalizar, veamos que los ideales generados por estos elementos son primos en Λ.

Para p consideremos el epimorfismo reducción módulo p coeficiente a coeficiente

$$\Lambda \longrightarrow (\mathbb{Z}_p/p\mathbb{Z}_p)\,[[T]] \tag{2.8}$$

cuyo kernel es el ideal (p) de Λ. Como $(\mathbb{Z}_p/p\mathbb{Z}_p)\,[[T]] \simeq (\mathbb{Z}/p\mathbb{Z})\,[[T]]$ y este último es un dominio de integridad porque $\mathbb{Z}/p\mathbb{Z}$ lo es, entonces $\Lambda/(p)$ es un dominio de integridad y por tanto (p) es un ideal primo de Λ.

Para $P(T) \in \mathbb{Z}_p[[T]]$ polinomio distinguido e irreducible de grado n, construyamos el siguiente homomorfismo: $P(T) \in \Lambda$ satisface las hipótesis de la Proposición 2.1.1, entonces dado $f(T) \in \Lambda$ existen únicos $q(T) \in \Lambda$ y $r(T) \in \mathbb{Z}_p[T]$ con $\deg(r) < n$ tal que $f(T) = q(T)P(T) + r(T)$. Esta escritura única nos permite definir el siguiente homomorfismo

$$\begin{array}{ccc} \Lambda & \longrightarrow & \mathbb{Z}_p[T]/(P(T)) \\ f(T) & \longmapsto & r(T) \end{array} \tag{2.9}$$

el kernel de este homomorfismo es $(P(T))$ y claramente es epiyectivo, luego, $\Lambda/(P(T)) \simeq \mathbb{Z}_p[T]/(P(T))$. Como $P(T)$ es irreducible $\mathbb{Z}_p[T]$, luego $\mathbb{Z}_p[T]/(P(T))$ es un dominio de integridad y por tanto, $\Lambda/(P(T))$ también, de esto concluimos que $(P(T))$ es un ideal primo de Λ y que $P(T)$ es un irreducible sobre Λ.

Además, estos son los únicos elementos irreducibles en Λ. Para analizar esto, sea $f(T) \in \Lambda$ irreducible. En general, por Teorema 2.1.2, sabemos que $f(T) = p^\mu P(T) U(T)$, como

estamos suponiendo que $f(T)$ es irreducible entonces tenemos dos opciones $f(T) = pU(T)$ o bien $f(T) = P(T)U(T)$. En cualquiera de los casos, $f(T)$ es asociado a p o a un polinimio distinguido. □

Observación 22. *Las unidades de Λ son las series de potencia con término constante en $\mathbb{Z}_p^\times$, es decir, no divisible por p.*

Lema 2.3.3: *Supongamos que $f, g \in \Lambda$ son primos relativos. Entonces el ideal (f, g) es de índice finito en Λ.*

Demostración. Como Λ es un DFU, en un comienzo

$$f(T) = p^{\mu_f} P_f(T) U_f(T) \quad \text{y} \quad g(T) = p^{\mu_g} P_g(T) U_g(T)$$

con $\mu_f, \mu_g \geq 0$, $P_f(T), P_g(T) \in \Lambda$ polinomios distinguidos y $U_f(T), U_g(T) \in \Lambda^\times$. Pero f y g son coprimos, entonces $P_f(T)$ y $P_g(T)$ no tienen factores en común y sin pérdida de generalidad podemos suponer que $f(T)$ no es divisible por p y que $f(T) = P_f(T)$ y $g(T) = p^{\mu_g} P_g(T)$ porque

$$(f, g) = (P_f U_f, p^{\mu_g} P_g U_g) = (P_f, p^{\mu_g} P_g),$$

en particular, $f(T)$ y $g(T)$ son polinomios. Sea $h \in (f, g)$ polinomio de grado mínimo. En un principio, $h(T) = p^\mu P(T) U(T)$ como en el Teorema 2.1.2, entonces $h(T)/P(T) \in \Lambda$ y por Lema 2.1.4, $h(T)/P(T) = p^\mu U(T) \in \mathbb{Z}_p[T]$. Por la minimalidad del grado de h, como $U^{-1}(T)h(T) \in (f, g)$ se tiene que $\deg(U) = 1$ y $U \in \Lambda^\times$, entonces $U(T) \in \mathbb{Z}_p^\times$. A partir de esto, multiplicando por $U(T)^{-1}$ que es una constante, podemos suponer, sin perder la generalidad, que $h(T) = p^s P(T)$, donde s es un entero no negativo y $P(T) = 1$ o bien $P(T)$ un polinomio distinguido.

Si $P \neq 1$, como f y g son coprimos, podemos suponer que P no divide f, entonces por

Proposición 2.1.1

$$f(T) = q(T)P(T) + r(T)$$

donde $q(T) \in \Lambda$, $r(T) \in \mathbb{Z}_p[T]$ con $\deg(r) < \deg(P) = \deg(h)$. Multiplicando por p^s obtenemos

$$p^s f(T) = h(T)q(T) + p^s r(T)$$

donde $p^s r(T) \in (f, g)$ y $\deg(p^s r) = \deg(r) < \deg(h)$, lo que contradice la minimalidad de h. De esta forma, $P = 1$ y $h = p^s$.

Por otro lado, $(f, h) = (f, p^s) \subseteq (f, g)$ porque $p^s \in (f, g)$ y por el algoritmo de la división que nos brinda la Proposición 2.1.1, como f es un polinomio distinguido tenemos que

$$\mathbb{Z}_p[[T]]/(f, p^s) = \{\overline{\alpha(T)} : \alpha(T) = a_0 + a_1 T + \cdots + a_k T^k \in \mathbb{Z}_p[T]\}$$

En consecuencia, (f, p^s) es de índice finito y como $(f, p^s) \subseteq (f, g)$, resulta que (f, g) es de índice finito. □

Lema 2.3.4: *Supongamos que $f, g \in \Lambda$ son primos relativos. Entonces*

1. *el homomorfismo natural*

$$\Psi : \Lambda/(fg) \to \Lambda/(f) \times \Lambda/(g)$$

   es inyectivo con cokernel finito. Por lo tanto, Ψ es un pseudo-isomorfismo.

2. *existe un homomorfismo inyectivo*

$$\Phi : \Lambda/(f) \times \Lambda/(g) \to \Lambda/(fg)$$

   con cokernel finito. Por lo tanto, Φ es un pseudo-isomorfismo.

Demostración. Recordemos que el cokernel de un homomorfismo de módulos $\psi : A \to B$ es el cociente $B/\psi(A)$ y mide que tan "cercano" de ser epiyectivo es el homomorfismo.

1. Sea $\alpha \in \Lambda/(fg)$ tal que $\Psi(\alpha) = (0 \mod f, 0 \mod g)$, entonces α es divisible por f y g. Como f y g son coprimos entonces α es divisble por fg, por tanto $\alpha \equiv 0 \mod fg$, es decir, el homomorfismo es inyectivo.

   Para probar que el cokernel es finito, usamos que por el Lema 2.3.3 $\Lambda/(f,g) = \{\bar{r}_1, \ldots, \bar{r}_n\}$ para algunos $r_1, \ldots, r_n \in \Lambda$ y para algún $n \in \mathbb{N}$. Sean $a, b \in \Lambda$, entonces existe $i \in \{1, \ldots, n\}$ tal que $b - a \equiv r_i$ mód (f,g), es decir, $b - a - r_i \in (f,g)$. Luego existen $A, B \in \Lambda$ tal que $b - a - r_i = fA + gB$. Sea

   $$c = a + fA = b - r_i - gB$$

   entonces $c \equiv a$ mód f y $c \equiv b - r_i$ mód g. Esto nos dice que c mód(fg) es un antecedente de $(a$ mód $f, b - r_i$ mód $g)$.

   Desta forma, para todo $a, b \in \Lambda$ existe $i \in \{1, \ldots, n\}$ tal que

   $$(a \text{ mód } f, b - r_i \text{ mód } g) \in \Psi(\Lambda/(fg))$$

   es decir, tal que

   $$(a \text{ mód } f, b \text{ mód } g) \equiv (0 \text{ mód } f, r_i \text{ mód } g) \text{ mód } \Psi(\Lambda/(fg))$$

   Por lo tanto, el cokernel es finito, representado por

   $$\{(0 \text{ mód } f, r_i \text{ mód } g) \text{ mód } \Psi(\Lambda/(fg)) : 1 \leq i \leq n\}$$

   En resumen, si $b - a \in (f,g)$ entonces $(a$ mód f, b mód $g) \in \Psi(\Lambda/(fg))$ y lo interesante es que también tenemos la otra implicancia: si $(a$ mód f, b mód $g) \in \Psi(\Lambda/(fg))$

entonces

$$\begin{cases} a \equiv c \text{ mód } f \\ b \equiv c \text{ mód } g \end{cases} \implies \begin{cases} a = c + a'f, & a' \in \Lambda \\ b = c + b'g, & b' \in \Lambda \end{cases}$$

luego, $b - a \in (f, g)$. Esto nos permite caracterizar la imagen de Ψ:

$$(a \text{ mód } f, b \text{ mód } g) \in \Psi(\Lambda/(fg)) \iff b - a \in (f, g).$$

2. Sea $N = \Lambda/(f) \times \Lambda/(g)$. Usando el ítem anterior $\Lambda/(fg) \simeq M \subseteq N$, con $M = \Psi(\Lambda/(fg))$ de índice finito en N. Sea $P(T) \in \Lambda$ polinomio distinguido coprimo con fg, entonces $\Psi(P)$ es no nulo en M.

   Sea $(x, y) \in N$. Como N/M es finito, algunas de las siguientes potencias módulo M deben coincidir, esto es

   $$P^i(x, y) \equiv P^j(x, y) \text{ mód } M \quad \text{para algún } i < j.$$

   Luego, $P^i(1 - P^{j-i})(x, y) \equiv 0$ mód M. Notemos que como P es un polinimio distinguido, su término constante es divisible por p, y entonces el término constante de P^{j-i} también lo es, así el término constante de $1 - P^{j-i}$ no es divisible por p y por tanto, $1 - P^{j-i} \in \Lambda^\times$. De esta forma, $P^i(x, y) \equiv 0$ mód M, es decir, $P^i(x, y) \in M$.

   Ahora bien, sean $(x_1, y_1), \ldots, (x_n, y_n)$ un sistema de representantes de N/M, entonces para todo $(x, y) \in N$ existe $j \in \{1, \ldots, n\}$ tal que $(x, y) - (x_j, y_j) \in M$. Luego,

   $$P^i(x, y) = P^i(x_j, y_j) + P^i m$$

   como M es un sub-Λ-módulo, $P^i m \in M$, entonces $P^i(x, y) \in M$ si $P^i(x_j, y_j)$. Usando esto definimos

   $$k = \max\{i \in \mathbb{N} : P^i(x_j, y_j) \in M \text{ para todo } j \in \{1, \ldots, n\}\}$$

entonces $P^k(x,y) \in M$ para todo $(x,y) \in N$, es decir, $p^k N \subseteq M$. A partir de esto, podemos definir

$$\Phi : N \xhookrightarrow{\cdot P^k} M \xrightarrow{\sim} \Lambda/(fg)$$

para que esta composición sea inyectiva, basta verificar que el homomorfismo $\cdot P^k$ es inyectivo. Para simplificar notaciones para $a \in \Lambda$ denotamos por $[a]$ la clase de a en su respectivo cociente módulo f y módulo g.

Sea $([x],[y]) \in N$ tal que $P^k([x],[y]) = ([0],[0])$ entonces

$$P^k x \equiv 0 \text{ mód } f \quad \text{y} \quad P^k y \equiv 0 \text{ mód } g$$

es decir, f divide $P^k x$ y g divide $P^k y$, como P y fg son coprimos, P es coprimo con f y P es coprimo con g, entonces f divide x y g divide y, por tanto, $([x],[y]) = ([0],[0])$ y de esto resulta que el homomorfismo $\cdot P^k$ es inyectivo.

Para el cokernel, notemos que

$$(\Lambda/(fg))/([P^k]) \simeq \Lambda/(P^k, fg).$$

Como P^k y fg son coprimos, porque P y fg son coprimos, usando el Lema 2.3.3, obtenemos que $(\Lambda/(fg))/(P^k, fg)$ es finito. Por último, $(P^k \text{ mód } f, P^k \text{ mód } g) = P^k(1 \text{ mód } f, 1 \text{ mód } g)$ pertenece a la imagen del homomorfismo $\cdot P^k$ y usando el isomorfismo $M \xrightarrow{\sim} \Lambda/(fg)$ obtenemos que $(P^k, fg) \subseteq \Phi(N)$. Así, resulta que $(\Lambda/(fg))/\Phi(N)$ es finito.

□

Proposición 2.3.5: *Los ideales primos de Λ son 0, $(p,T), (p)$ y los ideales $(P(T))$ donde $P(T)$ es un polinomio distinguido irreducible. El ideal (p,T) es el único ideal maximal.*

Demostración. Como Λ es un dominio de integridad el ideal (0) es primo. En el Teorema

2.3.2 probamos que $(p), (P(T))$ con $P(T)$ un polinomio distinguido irreducible son ideales primos. Para (p, T) consideremos el siguiente homomorfismo

$$\begin{array}{ccc} \Lambda & \longrightarrow & \mathbb{Z}_p/p\mathbb{Z}_p \\ f(T) & \longmapsto & f(0) \text{ mód } p \end{array}$$

el kernel de este homomorfismo es precisamente (p, T), por lo tanto,

$$\Lambda/(p, T) \simeq \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$$

como p es un entero primo, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo y así, (p, T) es un ideal maximal de Λ.

Para finalizar, veamos que (p, T) es el único ideal maximal. Para ello, probaremos que todo ideal primo está contenido en (p, T). Esto es suficiente porque todo ideal maximal es primero un ideal primo, entonces probaremos que todo postulante a ideal maximal, no lo es, porque esta contenido en (p, T).

Sea $\mathscr{P}$ ideal primo de Λ no nulo y $h \in \mathscr{P}$ de grado minimal. Por el mismo argumento usado en la demostración del Lema 2.3.3, $h = p^s H$ con $H = 1$ o bien H distinguido. Como $\mathscr{P}$ es primo, entonces $p^s \in \mathscr{P}$ o $H \in \mathscr{P}$, lo que es equivalente a $p \in \mathscr{P}$ o $H \in \mathscr{P}$.

Si $H \neq 1$ entonces H debe ser irreducible por la minimalidad en el grado de h y el hecho que $\mathscr{P}$ es primo. Si $H = 1$ entonces $h = p^s$. En ambos casos $(f) \subseteq \mathscr{P}$ donde $f = p$ o f es distinguido irreducible.

Si $(f) = \mathscr{P}$ entonces $\mathscr{P} = (p)$ o $\mathscr{P} = (f)$ con f polinomio distinguido irreducible. En ambos casos, $\mathscr{P} \subseteq (p, T)$ y finaliza la demostración.

Ahora bien, si $(f) \neq \mathscr{P}$, entonces existe $g \in \mathscr{P}$ tal que $g \notin (f)$, es decir, existe $g \in \mathscr{P}$ tal que f no divide g. Como f es irreducible, esto último nos dice que f y g son coprimos. Luego, por el Lema 2.3.3, $\Lambda/(f, g)$ es finito y puesto que $(f, g) \subseteq \mathscr{P}$, $\Lambda/\mathscr{P}$ es finito.

Como $\Lambda/\mathscr{P}$ es finito enonces algunas potencias de p y de T deben coincidir módulo $\mathscr{P}$, esto es

$$p^n \equiv p^m \text{ mód } \mathscr{P} \quad \text{y} \quad T^i \equiv T^j \text{ mód } \mathscr{P}$$

para algunos enteros positivos i, j, n, m con $i < j$ y $n < m$. Esto es equivalente a

$$p^n(1 - p^{m-n}) \equiv 0 \text{ mód } \mathscr{P} \quad \text{y} \quad T^i(1 - T^{j-i}) \equiv 0 \text{ mód } \mathscr{P}$$

como $1 - p^{m-n}, 1 - T^{j-i} \in \Lambda^\times$ entonces

$$p^n \equiv 0 \text{ mód } \mathscr{P} \quad \text{y} \quad T^i \equiv 0 \text{ mód } \mathscr{P}$$

De esta forma, $p^n, T^i \in \mathscr{P}$, más aún, $p, T \in \mathscr{P}$ porque $\mathscr{P}$ es primo. En consecuencia, $(p, T) \subseteq \mathscr{P}$, pero (p, T) es maximal y $\mathscr{P} \neq \Lambda$, entonces $\mathscr{P} = (p, T)$, lo que completa la demostración. □

Lema 2.3.6: *Sea $f \in \Lambda^\times$ entonces $\Lambda/(f)$ es infinito.*

Demostración. Si $f = 0$ entonces $\Lambda/(f) = \Lambda$ que es infinito. Supongamos que $f \neq 0$, entonces

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

con μ entero no negativo, $P(T) \in \Lambda$ polinomio distinguido y $U(T) \in \Lambda^\times$. Como $(f) \subseteq (p)$ o bien $(f) \subseteq (P)$ con $P(T)$ distinguido, entonces, $\Lambda/(p)$ y $\Lambda/(P)$ son de cardinalidad menor que $\Lambda/(f)$, por eso sin pérdida de generalidad, podemos reducirnos al caso $f(T) = p$ o $f(T) = P(T)$ con $P(T)$ distinguido.

Si $f(T) = p$, por (2.8)

$$\Lambda/(p) \simeq (\mathbb{Z}/p\mathbb{Z})[[T]]$$

que es infinito porque en particular $(\mathbb{Z}/p\mathbb{Z})[T] \hookrightarrow (\mathbb{Z}/p\mathbb{Z})[[T]]$.

Si $f(T) = P(T)$, por (2.9)

$$\Lambda/(P(T)) \simeq \mathbb{Z}_p[T]/(P(T))$$

que también es infinito porque $\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p[T]/(P(T))$. □

Observación 23. *Ahora tenemos las herramientas para demostrar que la relación de pseu-isomorfismo no es simétrica. Para ello consideremos el siguiente ejemplo:* Λ *y su ideal* (p,T) *son de forma natural* Λ*-módulos y en ellos la relación "ser pseudo-isomorfos" no es simétrica. En efecto,* $(p,T) \sim \Lambda$ *porque el homomorfismo inclusión es tal que su kernel es trivial y su cokernel* $\Lambda/(p,T)$ *es finito por Lema 2.3.3. Sin embargo, si* $\phi : \Lambda \to (p,T)$ *es un homomorfismo y* $f = \phi(1)$ *entonces* $\phi(\Lambda) = (f) \subseteq (p,T)$*. Por Lema 3.2.6,* $\Lambda/(f)$ *es infinito, como*

$$(\Lambda/(f))/((p,T)/(f)) = \Lambda/(p,T)$$

es finito entonces $(p,T)/(f)$ *es infinito.*

Lema 2.3.7: Λ *es un anillo noetheriano.*

Demostración. Sea I un ideal de Λ. Notemos que $I = (I \cap \mathbb{Z}_p[T])$, entonces como $\mathbb{Z}_p$ es un anillo noetheriano por teorema de la base de Hilbert [3, cap. 4, Teorema 4.1], $\mathbb{Z}_p[T]$ es un anillo noetheriano. Luego, $I \cap \mathbb{Z}_p[T]$ es generado por un número finito de polinomios y estos polinomios generan I. □

Ahora probaremos el Teorema 2.3.1: *Sea* M *un* Λ*-módulo finitamente generado. Entonces existe un pseudo-isomorfismo*

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

donde r, s, t, n_i, m_j *son enteros no negativos y cada* $f_j(T)$ *es un polinomio distinguido e irreducible.*

Demostración. Para probar este resultado, usaremos operaciones filas y columnas sobre matrices con coeficientes en Λ. Además de los usuales empleadas en módulos finitamente generados, introduciremos otras 3 que preservan pseudo-isomorfismos.

Para comenzar, sea M un Λ-módulo finitamente generado y $u_1, \ldots, u_m$ un sistema de generadores con varias relaciones de la forma

$$\lambda_1 u_1 + \cdots + \lambda_n u_n = 0$$

con $\lambda_1, \ldots, \lambda_n \in \Lambda$. Cada relación está únicamente determinada por el vector $(\lambda_1, \ldots, \lambda_n) \in \Lambda^n$ llamado vector relación y estos forman un sub-Λ-módulo $\mathcal{R}$ de Λ^n llamado módulo de relaciones. Observamos que $\mathcal{R}$ es el kernel del homomorfismo natural

$$\begin{array}{ccc} \Lambda^n & \longrightarrow & M \\ (\lambda_1, \ldots, \lambda_n) & \longmapsto & \sum_{i=1}^n \lambda_i u_i \end{array}$$

de manera que $M \simeq \Lambda^n/\mathcal{R}$.

Como Λ es noetheriano entonces Λ^n es noetheriano, luego el sub-Λ-módulo de relaciones es finitamente generado. Por esta razón, podemos representar M por una matriz $R \in M_{m\times n}(\Lambda)$ cuyas filas son los m vectores relación que generan $\mathcal{R}$.

Las primeras operaciones de filas y columnas que revisaremos son las usuales, cuya consecuencia es un cambio en los generadores el orden del sistema de generadores de M. Estas operaciones producen Λ-módulos isomorfos a M y por tanto, pseudo-isomorfos a M.

Operación A: Permutar filas o columnas.

Operación B: Sumar un múltiplo de una fila (columna) a otra fila (columna).

Operación C: Multiplicar una fila o columna por un elemento de $\Lambda^\times$.

A continuación definiremos tres operaciones adicionales y probaremos que definen un módulo pseudo-isomorfo a M.

Operación 1: Si R contiene una fila $(\lambda_1, p\lambda_2, \ldots, p\lambda_n)$ tal que p no divide λ_1, entonces podemos cambiar R por la matriz R'.

$$R = \begin{pmatrix} \lambda_1 & p\lambda_2 & \cdots \\ \alpha_1 & \alpha_2 & \cdots \\ \beta_1 & \beta_2 & \cdots \\ \vdots & \vdots & \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p\alpha_1 & \alpha_2 & \cdots \\ p\beta_1 & \beta_2 & \cdots \\ \vdots & \vdots & \vdots \end{pmatrix} = R'$$

En otras palabras, $M \simeq \Lambda^n/\mathcal{R} \sim \Lambda^n/\mathcal{R}' \simeq M'$ donde $\mathcal{R}$ es el sub-Λ-módulo de relaciones generado por los vectores relación en R y $\mathcal{R}'$ es el sub-Λ-módulo de relaciones generado por los vectores relación en R'.

Observamos que si $\lambda_2 = \cdots = \lambda_n = 0$, lo anterior puede ser repetido de tal forma que podamos multiplicar $\alpha_1, \beta_1, \ldots$ por una potencia arbitraria de p.

Demostración. Por hipótesis, en M tenemos la relación

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

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

$$\begin{aligned} pV + (-u_1) &= 0 \\ \lambda_1 V + (\lambda_2 u_2 + \cdots + \lambda_n u_n) &= 0 \end{aligned} \tag{2.10}$$

Para probar que $M \sim M'$, sea v la clase de V módulo las relaciones (2.10) y consideremos

el homomorfismo (compuesta de la inclusión y proyección)

$$\begin{array}{rccccc} \phi: & M & \hookrightarrow & \Lambda V \oplus M & \longrightarrow & M' \\ & m & \longmapsto & 0v + m & \longmapsto & ov + m \end{array}$$

Sea $m \in \ker(\phi)$, entonces $\phi(m) = 0 \in M'$ lo que significa que $m \in (pV - u_1, \lambda_1 v + \lambda_2 u_2 + \cdots + \lambda_n u_n)$, es decir, existe $a, b \in \Lambda$ tal que

$$m = a(pV - u_1) + b(\lambda_1 V + \lambda_2 u_2 + \cdots + \lambda_n u_n)$$

Igualando según corresponda tenemos para la primera componente $apV = -b\lambda_1 V$, es decir, $ap = -b\lambda_1$ de lo que resulta que p divide $b\lambda_1$, pero por hipótesis, p no divide λ_1 entonces p divide b. Así concluimos que λ_1 divide a. Usando esto, para la segunda componente tenemos

$$\begin{aligned} m &= -au_1 + b(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= -\tfrac{a}{\lambda_1}\lambda_1 u_1 - \tfrac{a}{\lambda_1} p(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= -\tfrac{a}{\lambda_1}\left(\lambda_1 u_1 + p(\lambda_2 u_2 + \cdots + \lambda_n u_n)\right) \\ &= 0 \end{aligned}$$

Por lo tanto, ϕ es inyectiva y por ende, de kernel finito.

Para el cokernel, sea

$$\begin{array}{rccc} \pi: & \Lambda & \longrightarrow & M'/\phi(M) \\ & \lambda & \longmapsto & \lambda v \end{array}$$

claramente es epiyectivo porque $M'/\phi(M) \simeq \Lambda v$, luego, $\Lambda/\ker(\phi) \simeq M'/\phi(M)$. Ahora bien, notemos que por (2.10)

$$\begin{aligned} &pv = u_1 = \phi(u_1) \in \phi(M) \\ &\lambda_1 v = -(\lambda_2 u_2 + \cdots + \lambda_n u_n) = \phi(-(\lambda_2 u_2 + \cdots + \lambda_n u_n)) \in \phi(M) \end{aligned}$$

entonces $p, \lambda_1 \in \ker(\pi)$ y por tanto, $(p, \lambda_1) \subseteq \ker(\pi)$. Como p, λ_1 son coprimos, $\Lambda/(p, \lambda_1)$

es finito por el Lema 2.3.3, por lo que $\Lambda/\ker(\phi)$ es finito y en consecuencia $M'/\phi(M)$ es finito. De esta forma, $M \sim M'$.

El Λ-módulo M' tiene como generadores a $V, u_2, \ldots, u_n$ con todas las relaciones de R más las relaciones (2.10). Como $u_1 = pV$ cualquier relación $\gamma_1 u_1 + \cdots + \gamma_n u_n = 0$ puede ser reemplaza por $p\gamma_1 v + \cdots + \gamma_n u_n = 0$. A partir de esto, la matriz toma la forma

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

cuya última fila corresponde a la segunda relación en (2.10). Restando a la fila 1 p veces la fila $n+1$, luego intercambiando la fila 1 con la fila $n+1$ y eliminando la última fila nula, obtenemos la matriz R' como en el enunciado. □

Operación 2: Si todos los elementos de la primera columna de R son divisibles por p^k y si existe una fila $(p^k\lambda_1, \ldots, p^k\lambda_n)$ con p no dividiendo λ_1, entonces se obtiene un factor de un módulo M' pseudo-isomorfo a M. El otro factor es pseudo-isomorfo a $\Lambda/(p^k)$. Así, podemos cambiar R por la matriz R' que es igual a R salvo que $(p^k\lambda_1, \ldots, p^k\lambda_n)$ es reemplazado por $(\lambda_1, \ldots, \lambda_n)$.

$$R = \begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \\ p^k\beta_1 & \beta_2 & \cdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \\ p^k\beta_1 & \beta_2 & \cdots \end{pmatrix} = R'$$

Demostración. Sea $M' = \Lambda V \oplus M$ con $V \in M$ un generador adicional satisfaciendo las siguientes relaciones

$$\begin{aligned} -p^k V + p^k u_1 &= 0 \\ \lambda_1 V + (\lambda_2 u_2 + \cdots + \lambda_n u_n) &= 0 \end{aligned} \tag{2.11}$$

Si v es la clase de V módulo las relaciones (2.11), entonces de forma análoga a lo hecho en la operación 1 se muestra que $M \sim M'$ vía el homomorfismo

$$\begin{array}{rccc} \phi: & M & \longrightarrow & M' \\ & m & \longmapsto & 0v + m \end{array}$$

que tiene kernel trivial, resultado que se concluye porque p no divide λ_1. Para el cokernel definimos el epimorfismo

$$\begin{array}{rccc} \pi: & \Lambda & \longrightarrow & M'/\phi(M) \\ & \lambda & \longmapsto & \lambda v \end{array}$$

que cumple con que $(p^k, \lambda_1) \subseteq \ker(\pi)$ y como p^k y λ_1 son coprimos, entonces $\Lambda/(p^k, \lambda_1)$ es finito y por tanto $\Lambda/\ker(\pi) \simeq M'/\phi(M)$ es finito.

Ahora bien, sea M'' el sub-Λ-módulo de M' generado por $V, u_2, \ldots, u_n$. La matriz de relación de M'' es la siguiente:

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

En primer lugar, notemos que si en esta matriz restamos a la fila 2 p^k veces la fila 1, intercambiamos la fila 1 y la fila 2 y eliminamos la fila nula obtenemos la matriz R' del enunciado.

A continuación veamos que $M' = M'' \oplus (u_1 - V)\Lambda$. Es claro que $M' = M'' + (u_1 - V)\Lambda$, porque $M'' + (u_1 - V)\Lambda$ es generado por $V, u_2, \ldots, u_n, u_1 - V$. Por otro lado, sea $m \in M'' \cap (u_1 - V)\Lambda$ entonces existen $\gamma_1, \ldots, \gamma_n, a \in \Lambda$ tal que

$$m = \gamma_1 V + \gamma_2 u_2 + \cdots + \gamma_n u_n = a(u_1 - V)$$

esto es equivalente

$$(\gamma_1 + a)V - a u_1 + \gamma_2 u_2 + \cdots + \gamma_n u_n = 0$$

lo que significa que $(\gamma_1 + a, -a, \gamma_2, \ldots, \gamma_n)$ pertenece al módulo de relaciones de M' que es generado por las relaciones de R y las dos relaciones de (2.11), es decir,

$$(0, p^k\lambda_1, p^k\lambda_2, \ldots, p^k\lambda_n), (0, p^k\alpha_1, \alpha_2, \ldots, \alpha_n), \ldots, (-p^k, p^k, 0, \ldots, 0), (\lambda_1, 0, \lambda_2, \ldots, \lambda_n).$$

Tras hacer una combinación Λ-lineal, obtenemos que p^k divide a y por la primera relación de (2.11)

$$m = a(u_1 - V) = 0.$$

Por último, mostramos que $\Lambda V \simeq \Lambda/(p^k)$. Para esto, consideremos el homomorfismo

$$\begin{array}{rccc} \psi: & \Lambda & \longrightarrow & \Lambda(u_1 - V) \\ & \lambda & \longmapsto & \lambda(u_1 - V) \end{array}$$

Claramente, $(p^k) \subseteq \ker(\psi)$ porque $p^k(u_1 - V) = 0$. Sea $\lambda \in \ker(\psi)$ entonces $\lambda u_1 - \lambda V = 0$. Esto implica que $(-\lambda, \lambda, 0, \ldots, 0)$ pertenece al módulo de relaciones de M' y por la descripción dada antes, $(-\lambda, \lambda, 0, \ldots, 0)$ es múltiplo de $(-p^k, p^k, 0, \ldots, 0)$. Luego, p^k divide λ y por tanto $\lambda \in (p^k)$. De esta forma, $\ker(\psi) = (p^k)$, y $\Lambda/(p^k) \simeq \Lambda(u_1 - v)$.

En resumen,

$$M' = M'' \oplus \Lambda/(p^k),$$

como $M \sim M'$ basta descomponer M'' como suma directa, tal como en el enunciado del Teorema 2.3.1 para obtener una tal descomposición de M. Por lo tanto, es suficiente trabajar con M'' y R'. □

Operación 3: Si R contiene una fila $(p^k\lambda_1, \ldots, p^k\lambda_n)$ y existe $\lambda \in \Lambda$ tal que p no divide λ y $(\lambda\lambda_1, \ldots, \lambda\lambda_n)$ es también una relación (no necesariamente explícita en R), entonces podemos cambiar R por R' donde R' es igual a R, excepto que $(p^k\lambda_1, \ldots, p^k\lambda_n)$ es reemplazada por $(\lambda_1, \ldots, \lambda_n)$.

Demostración. Sea $M' = M/(\lambda_1 u_1 + \cdots + \lambda_n u_n)\Lambda$ y la proyección

$$\pi : M \longrightarrow M'$$

El cokernel de π es trivial, por tanto finito. Recordemos que tenemos las siguientes relaciones

$$\begin{aligned} p^k\lambda_1 u_1 + \cdots + p^k\lambda_n u_n &= 0 \\ \lambda\lambda_1 u_1 + \cdots + \lambda\lambda_n u_n &= 0 \end{aligned} \tag{2.12}$$

Para el kernel consideremos el epimorfismo

$$\begin{aligned} \phi : \ \Lambda &\longrightarrow \Lambda(\lambda_1 u_1 + \cdots + \lambda_n u_n) \\ \gamma &\longmapsto \gamma(\lambda_1 u_1 + \cdots + \lambda_n u_n) \end{aligned}$$

Notemos que por (2.12), $\phi(\lambda) = \phi(p^k) = 0$, entonces $\lambda, p^k \in \ker(\phi)$ y así $(\lambda, p^k) \subseteq \ker(\phi)$. Como p^k y λ son coprimos, $\Lambda/(p^k, \lambda)$ es finito y por tanto, $\Lambda/\ker(\phi)$ es finito. Además, $\Lambda/\ker(\phi) \simeq (\lambda_1 u_1 + \cdots + \lambda_n u_n)\Lambda$. De esta forma, $\ker(\pi)$ es finito y resulta que $M \sim M'$.

Ahora bien, en el contexto de las matrices relación, por la definición de M', se agregó otra relación al módulo de relaciones de M

$$\lambda_1 u_1 + \cdots + \lambda_n u_n = 0$$

Por consiguiente, la matriz asociada a M' es R con esta relación adicional.

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ \\ \lambda_1 & \lambda_2 & \cdots \end{pmatrix}$$

Sobre esta matriz, basta realizar restar a la fila 1 p^k veces la fila $n+1$, intercambiar la fila 1 con la fila $n+1$ y eliminar la fila nula para obtener la matriz R' del enunciado. □

Observación 24. *Las operaciones 1,2,3 se pueden definir con cualquier columna en lugar de la primera columna.*

Esto completa la demostración de las operaciones que definen módulos pseudo-isomorfos a M y que además preservan el tamaño de la matriz. Comenzaremos con la demostración del teorema:

Sea $f \in \Lambda$ no nulo, entonces $f(T) = p^{\mu}P(T)U(T)$ con μ entero no negativo, $P(T)$ polinomio distinguido y $U(T) \in \Lambda^{\times}$. Definimos el grado de Weierstrass de f como sigue

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

Dada una matriz $R \in M_{mn}(\Lambda)$, definimos

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

donde (a'_{ij}) se mueve sobre todas las matrices relaciones obtenidas de R vía una sucesión finita de operaciones admisibles que deja fijas las primeras $(k-1)$ filas.

Si la matriz R tiene la forma

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

con λ_{kk} polinomio distinguido y

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

entonces decimos que R es una $(r-1)$ forma normal.

Lema: *Sea $r \leq \min\{n,m\}$. Si la submatriz B es no nula entonces a partir de R se puede obtener R' una forma r normal que conserva los primeros $(r-1)$ elementos diagonales usando operaciones admisibles.*

Demostración. La idea es aumentar a r el tamaño del bloque diagonal D_{r-1}, conservando sus características. Para ello realizaremos operaciones admisibles sobre R. Notemos que p no divide λ_{kk} para $1 \leq k \leq r-1$ porque son polinomios distinguidos.

Sobre la primera fila de R aplicamos la operación 1 y obtenemos que p divide la primera columna de A. Tras cambiar filas y columnas, repetimos la operación 1, hasta conseguir que p divida A. Todo este procedimiento, no altera las primeras $(r-1)$ filas. Reiteramos lo anterior, hasta encontrar un $N \in \mathbb{N}$ tal que p^N divida A, pero que p^N no divida B, este tal N existe porque B es no nula

Sea $\mu \in \mathbb{N}$ la máxima potencia de p que divide B, entonces existen i,j con $r-1 \leq i,j \leq m$ tal que $\lambda_{ij} = p^{\mu}P_{ij}(T)U_{ij}(T)$ con $P_{ij}(T)$ polinomio distinguido y $U_{ij}(T) \in \Lambda^{\times}$, con λ_{ij} coeficiente de B. Supongamos además que de haber otros coeficiente de la matriz B satisfaciendo esto, si comparamos los grados de los polinomios distiguidos en sus descomposiciones, eligimos λ_{ij} tal que $P_{ij}(T)$ es el de menor grado.

Por comodidad, tras un cambio de fila y columna, trasladamos λ_{ij} a la posición (r,r) dentro de la matriz. De esta forma, para simplificar la potencia p^{μ} de B, realizamos el intercambio de la columna 1 y r para luego emplear la operación 2. Así, p no divide B porque su coeficiente λ_{rr} no es divisible por p. Observamos que todas las operaciones realizadas mantienen intactas las primeras $(r-1)$ filas.

Tras lo anterior, la entrada λ_{rr} de B satisface

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

En efecto, como p no divide λ_{rr}, entonces $\deg_w(\lambda_{rr}) < \infty$ y por su construcción,

$$\deg_w(\lambda_{rr}) = \deg(P_{rr}) \leq \deg(P_{kl}) \quad \text{para } k, l \geq r.$$

Luego, como las primeras $(r-1)$ filas se han mantenido intactas tenemos que

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

Sea $\lambda_{rr} = P(T)U(T)$. Luego de multiplicar la j-ésima columna por $U^{-1}(T) \in \Lambda^\times$ podemos suponer que $\lambda_{rr} = P(T)$. Hasta aquí hemos logrado generar un nuevo elemento diagonal, para la posición (r,r) sin alterar los elementos de D_{r-1} y que también es un polinomio distinguido de buen grado de Weierstrass. Para terminar, falta anular las entradas de F_r distintas a (r,r), es decir,

$$\lambda_{rj} = 0 \ \text{ para } j \neq r \iff \begin{cases} \lambda_{rj} = 0, & j < r \ \ (\text{coeficientes en } A) \\ \lambda_{rj} = 0 & j > r \ \ (\text{coeficientes en } B) \end{cases}$$

Por algoritmo de la división, como λ_{rr} es un polinomio distinguido, para $j \neq r$ tenemos que

$$\lambda_{rj} = q_{rj}\lambda_{rr} + \rho_{rj} \quad \text{con } \deg(\rho_{rj}) < \deg(\lambda_{rr})$$

sobre la matriz restamos a la columna j, q_{rj} veces la columna r para para $j \neq r$ y obtenemos que r-ésima fila es reemplazada en cada entrada por su resto módulo λ_{rr}: ρ_{rj}. Así, podemos suponer que

$$\deg(\lambda_{rj}) < \deg(\lambda_{rr}) \quad \text{para } j \neq r \tag{2.13}$$

De forma análoga, podemos realizar el mismo proceso pero con las filas F_j para $j < r$:

$$\lambda_{rj} = \tilde{q}_{rj}\lambda_{jj} + \tilde{\rho}_{rj} \quad \text{con } \deg(\tilde{\rho}_{rj}) < \deg(\lambda_{jj})$$

luego, hacemos la operación $F_{jr}(-\tilde{q}_{rj})$ y es por esto que podemos suponer

$$\deg(\lambda_{rj}) < \deg(\lambda_{jj}) \quad \text{para } j < r \tag{2.14}$$

Una vez más, notamos que como en $\lambda_{ir} = 0$ para $1 \leq i < r$, las operaciones realizadas no alteran las primeras $(r-1)$ filas.

Recordemos que por lo realizado anteriormente, p^N divide A pero p no divide B.

Comenzamos analizando los λ_{rj} con $j > r$: A partir de (2.13), como $\deg_w(\lambda_{rr})$ es minimal en B tenemos que p divide λ_{rj} para $j > r$.

Observemos que dado $P(T) \in \Lambda[T]$, si p no divide P entonces $\deg_w(P) \leq \deg(P)$.

Supongamos que $\lambda_{rj} \neq 0$ para algún j. Usamos la operación 1 las veces que sea necesario (tras un cambio de columnas y filas) para eliminar las potencias de p de cualquier λ_{rj}, con $j > r$ no nulo, es decir, λ_{rj} es de valuación p-ádica minimal. Después de hacer esto, usando la operación A devolvemos los coeficientes a su anterior posición. Como antes, estas operaciones no alteran las primeras $(r-1)$ filas. Así, podemos suponer que p no divide λ_{rj}. Luego, como $\lambda_{rj} = P(T)U(T)$ con $U(T) \in \Lambda^\times$ polinomio tenemos que

$$\deg_w(\lambda_{rj}) \leq \deg(\lambda_{rj}) < \deg(\lambda_{rr}) = \deg_w(\lambda_{rr})$$

lo que es una contradicción. Por lo tanto, $\lambda_{rj} = 0$ para $j > r$.

Supongamos que $\lambda_{rj} \neq 0$ para algún $j < r$ de valuación p-ádica minimal. Como antes, usamos la operación 1 para obtener que p no divide λ_{rj}, notemos que podemos hacerlo ya que $\lambda_{rl} = 0$ para $l \geq r$. Entonces

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

como $\deg_w(\lambda_{jj}) = \deg^{(j)} R$, lo anterior contradice la definición de $\deg^{(j)} R$. Por lo tanto, $\lambda_{rj} = 0$ para $j < r$. Lo que finaliza la demostración del lema. □

Continuando con la demostración del teorema, comenzamos con una matriz R asociada a un Λ-módulo M y $r = 1$. El lema anterior es parte del proceso de inducción "$(r-1) \Rightarrow r$". Luego, es posible tras operaciones admisibles, a partir de R obtener una matriz de la forma

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

donde λ_{ii} es un polinomio distinguido para $1 \leq i \leq r$ y $\deg(\lambda_{jj}) = \deg^{(j)} R$ para $j \leq r$. Como antes, usando el algoritmo de la división podemos suponer que λ_{ij} es un polinomio y $\deg(\lambda_{ij}) < \deg(\lambda_{jj})$ para $i \neq j$ (dividiendo λ_{ij} en λ_{jj} y tras la correspondiente operación quedarnos con el resto).

Supongamos que $\lambda_{ij} \neq 0$ para $i \neq j$, es decir, estamos suponiendo que $A \neq 0$. Como $\deg_w(\lambda_{jj})$ es minimal, si p no divide λ_{ij} entonces

$$\deg_w(\lambda_{ij}) \leq \deg(\lambda_{ij}) < \deg(\lambda_{jj}) = \deg_w(\lambda_{jj})$$

lo que es una contradicción. Por lo tanto, p divide λ_{ij}. De esta forma, tenemos el siguiente vector relación (no nulo) en R

$$(\lambda_{i1}, \ldots, \lambda_{ir}, 0, \ldots, 0)$$

que es divisible por p. Sea $\lambda = \lambda_{11} \cdots \lambda_{rr}$, entonces p no divide λ porque p no divide λ_{ii}

para cada $1 \leq i \leq r$. Además, $\lambda_{ii}u_i = 0$, de esto resulta que

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

es también un vector relación. Si la fila $(\lambda_{i1}, \ldots, \lambda_{ir}) \neq (0, \ldots, 0)$ aplicando la operación 3 podemos suponer que p no divide λ_{ij} para algún j y entonces

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

Esto es una contradicción. Así concluimos que $A = 0$.

Lo anterior, volviendo al contexto de Λ-módulos, nos muestra que

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

Observamos que a pesar de que λ_{ii} son polinomios distinguidos no son necesariamente irreducibles. En caso que alguno no lo fuera, sabemos que es factor de polinomios distinguidos irreducibles, entonces usamos el Lema 2.3.4 para concluir.

Por otro lado, recordemos que en la operación 2, eliminamos los factores de la forma $\Lambda/(p^k)$, agregando estos, obtenemos finalmente el resultado del enunciado. □

2.4 Teorema de Iwasawa

Teorema 2.4.1: *Sea K_∞/K una $\mathbb{Z}_p$-extensión. Sea p^{e_n} la potencia exacta de p dividiendo al número de clase de K_n. Entonce existen enteros $\lambda \geq 0, \mu \geq 0$, y ν, todos independientes de n y un entero n_0 tal que*

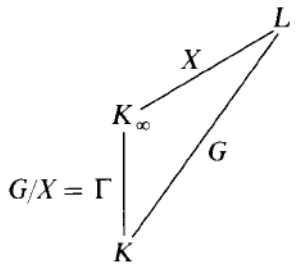
$$e_n = \lambda n + \mu p^n + \nu \qquad \textit{para todo } n \geq n_0.$$

El esquema de la demostración de este teorema es el siguiente:

Sea $\Gamma = Gal(K_\infty/K) \simeq \mathbb{Z}_p$. Como antes, consideremos $\{K_n\}_{n\geq 0}$ una sucesión de subcuerpos de K_∞/K tal que K_n/K es Galois y grado p^n sobre K

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_{n\geq 0} K_n.$$

Sea L_n la máxima p-extensión abeliana no ramificada de K_n entonces $X_n = Gal(L_n/K_n) \simeq A_n$ p-subgrupo de Sylow del grupo de clase de K_n. Sea $L = \bigcup_{n\geq 0} L_n$ entonces L/K es Galois, denotamos $G = Gal(L/K)$. Tenemos el siguiente diagrama



La idea de la demostración es definir sobre X una estructura de Γ-módulo y luego extenderla a una estructura de Λ-módulo. Esto se hace mostrando que X es finitamente generado y de Λ-torsión, entonces existe un homomorfismo de Λ-módulos

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

con kernel y cokernel Λ-módulos de orden finito, $n_i, m_j \geq 0$ y $f_j(T)$ polinomios irreducibles mónicos de $\mathbb{Z}_p[T]$. El siguiente paso es analizar lo que ocurre en el n-ésimo nivel de estos módulos y luego transferir este resultado a X.

Con las notaciones precedentes demostraremos el objetivo de este capítulo: Definir sobre X una estructura de Λ-módulo.

El cuerpo L_n es la máxima p-extensión abeliana no ramificada de K_n entonces $L_n \subseteq \tilde{L}_n$ con $\tilde{L}_n$ cuerpo de clase de Hilbert de K_n. Notemos que en principio, podría haber más de una elección para L_n si consideramos que esta p-extensión no ramificada es de grado maximal. Sin embargo, como $Gal(\tilde{L}_n/K_n) \simeq Cl(\mathcal{O}_{K_n})$, por el teorema de estructura de grupos abelianos y finitos, $Cl(\mathcal{O}_{K_n}) \simeq A_n \oplus H_n$ para algún subgrupo H_n de $Cl(\mathcal{O}_{K_n})$ y con A_n el único p-subgrupo de Sylow de $Cl(\mathcal{O}_{K_n})$ y entonces $Gal(L_n/K_n)$ se corresponde con un p-subgrupo de Sylow de $Cl(\mathcal{O}_{K_n})$, especificamente L_n es el subcuerpo de $\tilde{L}_n$ fijado por H_n. Así, la unicidad de L_n se desprende de la unicidad de este p-subgrupo. Definimos $X_n = Gal(L_n/K_n) \simeq A_n$ p-subgrupo de Sylow de $Cl(\mathcal{O}_{K_n})$.

Observemos que $L_n \subseteq L_{n+1}$ para todo $n \geq 0$. Para ello, en primer lugar veamos que si M/K_n es una p-extensión abeliana no ramificada entonces $M \subseteq L_n$. En efecto, M/K_n es Galois porque $Gal(\tilde{L}/M)$ es un subgrupo normal de $Gal(\tilde{L}_n/K_n)$ abeliano. De esta forma, si $|Gal(M/K_n)| = p^N$ para algún $N \in \mathbb{N}$ y $\sigma \in H_n$ entonces tenemos que para todo $m \in M$, $\sigma^{p^N}(m) = \sigma|_M^{p^N}(m) = m$. Sea a el orden de σ entonces a es coprimo con p^N y por tanto existe $b \in \mathbb{Z}$ tal que $p^N b \equiv 1$ mód a. Luego, $(\sigma^{p^N})^b(m) = m$ lo que implica que $\sigma(m) = m$ y asıse obtiene que $M \subseteq \tilde{L}_n^{H_n} = L_n$.

Por otra parte, mostremos que $L_n \subseteq L_{n+1}$. Para esto consideremos el cuerpo $K_{n+1}L_n$. La extensión $K_{n+1}L_n/K_{n+1}$ es de Galois porque L_n/K_n es Galois.

Además, $Gal(L_nK_{n+1}/K_{n+1}) \hookrightarrow Gal(L_n/K_n)$ asi que $K_{n+1}L_n/K_{n+1}$ es una p-extensión abeliana. Analicemos la ramificación de esta extensión en primos finitos e infinitos. Sea $\mathscr{P}$ un ideal primo no nulo de L_nK_{n+1} y $\mathcal{P}$ un ideal primo no nulo de K_{n+1} tal que $\mathscr{P}|\mathcal{P}$ entonces $I(\mathscr{P}|\mathcal{P}) \hookrightarrow I(\mathscr{P} \cap L_n|\mathcal{P} \cap K_n)$, de ahí que $K_{n+1}L_n/K_{n+1}$ es no ramificada para primos finitos. Para los primos infinitos, sea $\varphi : K_{n+1} \hookrightarrow \mathbb{R}$ incrustación y supongamos que se ramifica, entonces existe $\tilde{\varphi} : L_nK_{n+1} \hookrightarrow \mathbb{C}$ no real tal que $\tilde{\varphi}|_{K_{n+1}} = \varphi$. Por consiguiente, $\tilde{\varphi}|_{K_n}$ es real y $\tilde{\varphi}|_{L_n}$ es complejo, lo que significa que L_n/K_n se ramifica en un primo infinito. En consecuencia, $K_{n+1}L_n/K_{n+1}$ es no ramificada y por esta razón $K_{n+1}L_n \subseteq L_{n+1}$ lo que nos permite concluir que $L_n \subseteq L_{n+1}$.

Como $L_n \subseteq L_{n+1}$ entonces L es un cuerpo. Además, L/K_∞ es Galois porque L_n/K_n es Galois para todo $n \geq 0$. Denotamos $X = Gal(L/K_\infty)$.

Ahora bien, cada L_n es Galois sobre K. Para notar esto, sea $\overline{\mathbb{Q}}$ clausura algebraica de $\mathbb{Q}$ y $\sigma \in Gal(\overline{\mathbb{Q}}/K)$, entonces como K_n/K es Galois, $K_n = \sigma(K_n) \subseteq \sigma(L_n)$ y $[\sigma(L_n) : K_n] = [L_n : K_n]$ porque las extensiones son isomorfas. Ambas son p-extensiones y tienen la misma ramificación. Sea $\tau \in Gal(\overline{\mathbb{Q}}/K_n)$, como $Gal(\overline{\mathbb{Q}}/K_n)$ es un subgrupo normal de $Gal(\overline{\mathbb{Q}}/K)$ existe $\tau' \in Gal(\overline{\mathbb{Q}}/K_n)$ tal que $\sigma\tau'\sigma^{-1}(\sigma(L)) = \tau(\sigma(L))$ y $\tau'(L) = L$ porque L/K_n es de Galois. Luego, $\tau(\sigma(L)) = \sigma(L)$ para todo $\tau \in Gal(\overline{\mathbb{Q}}/K_n)$, entonces $\sigma(L)/K_n$ es Galois. Así, por la maximalidad de L_n se tiene que $\sigma(L_n) \subset L_n$, de lo que se concluye que L_n/K es Galois.

De esta forma, por teoría de Galois infinito, tenemos que L/K es Galois y $G = Gal(L/K)$.

Probaremos que X es un Γ-módulo. Para ello, comencemos suponiendo que todos los primos que son ramificados en K_∞/K son totalmente ramificados.

Por Lema 2.2.3, podemos reemplazar K por K_m para algún $m \geq 0$. La construcción de este K_m es la siguiente: Sea $I(K_\infty/K)$ grupo de inercia de K_∞/K, como es un subgrupo cerrado de $\mathbb{Z}_p$ entonces existe $m \in \mathbb{N}$ tal que $I(K_\infty/K) \simeq p^m\mathbb{Z}_p$, como hemos visto el cuerpo fijo asociado a este subgrupo es precisamente K_m. Entonces $Gal(K_\infty/K_m) = I(K_\infty/K)$ y se deduce que $Gal(K_\infty/K_m) = I(K_\infty/K_m)$. Por lo tanto, K_∞/K_m es totalmente ramificada.

Notemos que es posible obtener $n \geq 0$ lo bastante pequeño tal que K_n/K sea no ramificada, entonces K_n/K_{n-1} es no ramificada. Ajustando índices, K_{n+1}/K_n es no ramificada, es abeliana y de grado p. Por la maximalidad de L_n, tenemos que $K_{n+1} \subseteq L_n$. También por Lema 2.2.3 a partir de cierto rango, n_0, K_∞/K_{n_0} es totalmente ramificada en todo primo que ramifica en K_∞/K_{n_0}, entonces para $n \geq n_0$ suficientemente grande, K_{n+1}/K_n es totalmente ramificada. Como $L_n \cap K_{n+1}$ es una subextensión de K_{n+1}/K_n entonces $L_n \cap K_{n+1}$ sobre K_n es ramificada en todo primo que ramifica en K_∞/K_{n_0} (hay al menos uno) porque de no serlo, K_{n+1}/K_n no tendría el mayor índice de ramificación posible.

Nuevamente, usando el hecho de que L_n/K_n es no ramificada tenemos que

$$L_n \cap K_{n+1} = K_n \tag{2.15}$$

Para enfatizar en este punto, K_{n+1}/K_n puede ser no ramificada si $n+1 < n_0$, sin embargo, como las extensiones intermedias de una extensión totalmente ramificada son también totalmente ramificadas, entonces K_{n+1}/K_n es totalmente ramificada.

Usando (2.15) y teoria de Galois finito tenemos que

$$X_n = Gal(L_n/K_n) \simeq Gal(L_nK_{n+1}/K_{n+1}).$$

Luego,

$$Gal((L_nK_{n+1}/K_{n+1}) = Gal(L_{n+1}/K_{n+1})/Gal(L_{n+1}/L_nK_{n+1}) = X_{n+1}/Gal(L_{n+1}/L_nK_{n+1})$$

y por lo tanto, X_n es un cociente de X_{n+1}. Así tenemos un epimomorfismo

$$\phi_{n+1} : X_{n+1} \to X_n$$

que consiste en la restricción a L_n y que origina un sistema proyectivo.

Por otro lado, con los mismos argumentos usados para concluir (2.15) podemos obtener

$$K_N \cap L_n = K_n \quad \text{para } N > n$$

así pues $K_\infty \cap L_n = K_n$ y por Proposición 1.4.4 tenemos que

$$X_n \simeq Gal(L_nK_\infty/K_\infty).$$

Entonces

$$\varprojlim_{n\geq m} X_n = \varprojlim_{n\geq m} Gal(L_n/K_n) \simeq \varprojlim_{n\geq m} Gal(L_nK_\infty/K_\infty)$$

este isomorfismo viene dado por

$$\begin{array}{ccc} Gal(L_n/K_n) & \longrightarrow & Gal(L_nK_\infty/K_\infty) \\ \sigma_n & \longmapsto & \tilde{\sigma}_n \end{array}$$

donde σ_n se extiende a L_nK_∞ enviando por ejemplo $\alpha \in L_n$ a uno de sus conjugados. Esta descripción es suficiente porque σ_n fija punto a punto a K_∞. Respecto a la compatibilidad de los homomorfismos, esta se deduce del hecho $\sigma_{n+1}|_{L_n} = \sigma_n$ y $\tilde{\sigma}_{n+1}|_{L_nK_\infty} = \tilde{\sigma}_n|_{L_nK_\infty}$. También

$$\varprojlim_{n\geq m} Gal(L_nK_\infty/K_\infty) = Gal((\bigcup_{n\in\mathbb{N}} L_nK_\infty)/K_\infty)$$

como $Gal((\bigcup_{n\in\mathbb{N}} L_nK_\infty)/K_\infty) = Gal((\bigcup_{n\in\mathbb{N}} L_n)/K_\infty)$ porque $K_\infty \subseteq \bigcup_{n\in\mathbb{N}} L_n$, obtenemos que

$$\varprojlim_{n\geq m} X_n \simeq Gal(L/K_\infty) = X.$$

El objetivo ahora es demostrar que Γ actúa sobre X. La primera etapa es demostrar que Γ_n actúa sobre X_n.

La acción a verificar es

$$\begin{array}{ccccc} \Gamma_n & \times & X_n & \longrightarrow & X_n \\ (\gamma & , & \sigma) & \longmapsto & \sigma^\gamma = \tilde{\gamma}\sigma\tilde{\gamma}^{-1} \end{array} \tag{2.16}$$

donde $\tilde{\gamma} \in Gal(L_n/K)$ es un extensión de γ, es decir, $\tilde{\gamma}|_{K_n} = \gamma$.

Recordemos que $X_n = Gal(L_n/K_n)$ y $\Gamma_n = \Gamma/\Gamma^{p^n} \simeq Gal(K_n/K)$ por correspondencia de Galois infinito.

Sea $\tilde{\gamma} \in Gal(L_n/K)$ tal que $\tilde{\gamma}|_{K_n} = \gamma$. Como K_n/K es Galois entonces $Gal(L_n/K_n)$ es un subgrupo normal de $Gal(L_n/K)$, así si $\sigma \in Gal(L_n/K_n)$ se tiene que para $\tilde{\gamma} \in Gal(L_n/K)$, $\tilde{\gamma}\sigma\tilde{\gamma}^{-1}$. Por lo tanto, $\sigma^\gamma \in X_n$.

El siguiente paso es probar que (2.16) no depende de la elección de $\tilde{\gamma}$. Para ello, sea $\hat{\gamma} \in Gal(L_n/K)$ otra extensión de γ entonces $\tilde{\gamma}^{-1}\hat{\gamma} \in Gal(L_n/K_n)$. Luego,

$$\hat{\gamma}\sigma\hat{\gamma}^{-1} = \tilde{\gamma}(\tilde{\gamma}^{-1}\hat{\gamma})\sigma(\tilde{\gamma}^{-1}\hat{\gamma})^{-1}\tilde{\gamma}^{-1}$$

como $Gal(L_n/K_n)$ es abeliano, $(\tilde{\gamma}^{-1}\hat{\gamma})\sigma(\tilde{\gamma}^{-1}\hat{\gamma})^{-1} = \sigma$ por lo que $\hat{\gamma}\sigma\hat{\gamma}^{-1} = \tilde{\gamma}\sigma\tilde{\gamma}^{-1}$.

Para probar que (2.16) es una acción basta usar que su definición no depende de la elección de $\tilde{\gamma}$. De esta forma, (2.16) es efectivamente una acción. Lo interesante es que induce una acción de $\mathbb{Z}_p[\Gamma_n]$ sobre X_n. En efecto, sea p^{t_n} la cardinalidad X_n, como es un grupo abeliano entonces X_n es un $\mathbb{Z}$-módulo. Además es anulado por p^{t_n} por lo que X_n es un $\mathbb{Z}/p^{t_n}\mathbb{Z}$-módulo y por tanto es un $\mathbb{Z}_p/p^{t_n}\mathbb{Z}_p$-módulo. De esta forma, X_n es un $\mathbb{Z}_p$-módulo cuya acción se define como sigue: Sea $x \in X_n$ y $\alpha \in \mathbb{Z}_p$ entonces

$$x^{\alpha} = x^{\alpha \text{ mód } p^{t_n}}.$$

donde $x^t = \underbrace{x \circ \cdots \circ x}_{t \text{ veces}}$.

Por otra parte, Γ_n actúa sobre el $\mathbb{Z}_p$-módulo por funciones $\mathbb{Z}_p$-lineales, entonces X_n es un $\mathbb{Z}_p[\Gamma_n]$-módulo y su acción es la siguiente: sea γ_n generador de Γ_n, $x \in X_n$ y $\alpha_0, \ldots, \alpha_{p^n-1} \in \mathbb{Z}_p$. Si $a = \alpha_0 + \alpha_1\gamma_n + \cdots + \alpha_{p^n-1}\gamma_n^{p^n-1} \in \mathbb{Z}_p[\Gamma_n]$ entonces

$$x^a = \prod_{i=0}^{p^n-1} (x^{\alpha_i})^{\gamma_n^i}.$$

Para finalizar, definimos una acción de $\mathbb{Z}_p[[\Gamma]]$ sobre X usando que $\mathbb{Z}_p[[\Gamma]] = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[\Gamma_n]$ y $X = \varprojlim_{n\in\mathbb{N}} X_n$. Esta acción es componente a componenete, en otras palabras, si $a = (a_n)_{n\in\mathbb{N}}$

y $x = (x_n)_{n\in\mathbb{N}}$ entonces

$$\begin{array}{ccccc} \mathbb{Z}_p[[\Gamma]] & \times & X & \longrightarrow & X \\ (\ a & , & x\ ) & \longmapsto & x^a = (x_n^{a_n})_{n\in\mathbb{N}} \end{array} \tag{2.17}$$

Para verificar que (2.17) es efectivamente una acción es necesario asegurar la compatibilidad de los homomorfismos ϕ_n con las acciones de $\mathbb{Z}_p[\Gamma_{n+1}]$ y $\mathbb{Z}_p[\Gamma_n]$, es decir que dado $a = (a_n)_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[\Gamma_n]$ y $x = (x_n)_{n\in\mathbb{N}} \in X = \varprojlim_{n\in\mathbb{N}} X_n$

$$\phi_n(x_n^{a_n}) = x_{n-1}^{a_{n-1}}.$$

Para esto, diferenciamos dos casos: la acción de $\mathbb{Z}_p$ y la acción de Γ_n.
Sea $x = (x_n)_{n\in\mathbb{N}} \in X$, $\alpha \in \mathbb{Z}_p$ y $\gamma_n \in \Gamma_n$. Los respectivos homomorfismos de los sistemas proyectivos involucrados son

$$\phi_n : X_n \to X_{n-1} \quad \text{y} \quad \psi_n : \Gamma_n \to \Gamma_{n-1}.$$

El objetivo es probar los siguientes ítems:

1) $x^\alpha \in X$:

Esto es equivalente a mostrar que para todo $x_n \in X_n$ y para todo $\alpha \in \mathbb{Z}_p$ se tiene que $\phi_n(x_n^\alpha) = x_{n-1}^\alpha$.

Notar que $x_n^\alpha = x_n^{\alpha \text{ mód } p^{t_n}} = x_n^{\alpha \text{ mód } p^{s_n}}$ con p^{s_n} el orden de x_n y $s_n \geq s_{n-1}$. Luego,

$$\phi_n(x_n^\alpha) = \phi_n(x_n^{\alpha \text{ mód } p^{s_n}}) = \phi_n(x_n)^{\alpha \text{ mód } p^{s_n}} = x_{n-1}^{\alpha \text{ mód } p^{s_n}} = x_{n-1}^\alpha.$$

2) $x^{\gamma_n} \in X$:

Esto es equivalente a mostrar que para todo $x_n \in X_n$ y para todo $\gamma_n \in \Gamma_n$ se tiene que

$\phi_n(x_n^{\gamma_n}) = x_{n-1}^{\gamma_{n-1}}$

Sea $\tilde{\gamma}_n \in Gal(L_n/K_n)$ una extensión de γ_n. Notemos que podemos considerar que $\tilde{\gamma}_n|_{L_{n-1}} = \gamma_{n-1}$ donde $\psi_n(\gamma_n) = \gamma_{n-1}$, por lo que $\tilde{\gamma_n}|_{L_{n-1}} = \tilde{\gamma}_{n-1} \in Gal(L_{n-1}/K_{n-1})$ extensión de γ_{n-1}. Entonces

$$\phi_n(x_n^{\gamma_n}) = x_n^{\gamma_n}|_{L_{n-1}} = (\tilde{\gamma}_n x_n \tilde{\gamma}_n^{-1})|_{L_{n-1}} = \tilde{\gamma}_n|_{L_{n-1}} x_{n-1} \tilde{\gamma}_n^{-1}|_{L_{n-1}} = \tilde{\gamma}_{n-1} x_{n-1} \tilde{\gamma}_{n-1}^{-1} = x_{n-1}^{\gamma_{n-1}}.$$

Por último, por Teorema 2.1.5, concluimos finalmente que X es un Λ-módulo.

Bibliografía

[1] James S. Milne, (2017). *Course Note: Fields and Galois Theory.*

[2] Lawrence C. Washington, (1982). *Introduction to Cyclotomic Fields.*

[3] Serge Lang, (2002). *Algebra.*

[4] Jean-Pierre Serre, (1970). *A Course in Arithmetic.*

[5] Tamás Szamuely, (2009). *Galois groups and fundamental groups.*

[6] Neal Koblitz, (1996). *p-adic Numbers, p-adic Analysis, and Zeta-Functions.*

[7] Dinakar Ramakrishnan, Robert J. Valenza, (1998). *Fourier Analysis on Number Fields.*

[8] Daniel A. Marcus, (1977). *Number Fields.*

[9] Serge Lang,(1986). *Algebraic Number Theory*

[10] James S. Milne, (2017). *Algebraic Number Theory.*

[11] Pierre Samuel, (1970). *Algebraic Theory of Numbers.*

[12] Bernard Dwork, Giovanni Gerotto, Francis J. Sullivan, (1994). *Introduction to G-functions.*

[13] Jean-Pierre Serre, (1980). *Local fields.*