Facultad de Matemáticas

Departamento de Álgebra

Teoría de Cuerpos de Clase

realizado por

Francisco García Cortés

Tutorizado por Antonio Rojas León

Sevilla, a 29 de junio de 2021

Abstract

Class field theory studies abelian extensions of a given field using only intrinsic data of the field itself. Moreover, it gives information about the Galois groups of these extensions along with some functorial properties. Currently, global class field theory is constructed from local class field theory. For this reason, it is customary to focus first on the local aspects of class field theory. In this way, the present project compiles full proofs of the core results of local class field theory following the method of Iwasawa [Iwa86] as presented by Yoshida [Yos08].

Instead of focusing on the analogies between elliptic curves and Lubin-Tate groups, this work stresses the algebraic aspects of the theory by visualizing the construction as a kind of "categorification" that gives rise to the comparison of uniformizing elements by algebraic means. Once the main results of local class field theory has been proved, these notable results are subsequently used to prove the Kronecker-Weber theorem following Šafarevič [Š51, Cas86].

Due to space limitation and for the sake of clarity, the scope of this project is limited to providing only the proofs of the main theorems without justifying every step of the construction of the relative Lubin-Tate groups. In addition to the technical results, a brief outline of the history of class field theory is included for the purpose of showing how trascendental this theory has been for the mathematical community. The relevant bibliography for this part is [Conb, Lem00, PS04, Tak94].

Resumen

La teoría de cuerpos de clase estudia las extensiones abelianas de un cuerpo dado usando únicamente información intrínseca del cuerpo. Además, da información sobre los grupos de Galois de dichas extensiones junto con algunas propiedades funtoriales. Hoy en día, la teoría de cuerpos de clase global se construye a partir de la teoría de cuerpos de clase local. Por esta razón, es usual concentrarse primero en los aspectos locales de la teoría de cuerpos de clase. De esta forma, el presente trabajo recoge pruebas completas de los resultados centrales de la teoría de cuerpos de clase local siguiendo el método de Iwasawa [Iwa86] tal y como lo expone Yoshida [Yos08].

En lugar de concentrarse en las analogías entre las curvas elípticas y los grupos de Lubin-Tate, este trabajo resalta los aspectos algebraicos de la teoría visualizando la construcción como cierta "categorificación" que permite la comparación de los parámetros de uniformización de una forma algebraica. Una vez los resultados principales de la teoría de cuerpos de clase local hayan sido demostrados, estos resultados profundos se usan posteriormente para probar el teorema de Kronecker-Weber siguiendo Šafarevič [Š51, Cas86].

Por la limitación de espacio y en beneficio de la claridad, el ámbito de este proyecto se limita a probar los resultados más importantes de la teoría de cuerpos de clase sin justificar todos los pasos de la construcción de los grupos de Lubin-Tate relativos. Además de los resultados técnicos, se añade un resumen de la historia de la teoría de cuerpos de clase con el objetivo de mostrar cómo de trascendente ha sido esta teoría para la comunidad matemática. La bibliografía relativa a esta parte es [Conb, Lem00, PS04, Tak94].

Motivación Histórica

Gauss, en 1801, publicó su obra *Disquisitiones Arithmeticae* la cual incluía las dos primeras demostraciones completas de la

Ley de Reciprocidad Cuadrática (Gauss, 1801). *Dados p, q dos números primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Este resultado era conocido parcialmente por algunos predecesores de Gauss como por ejemplo Euler y Lagrange. De hecho, Euler llegó a enunciar algunos resultados sobre residuos cúbicos que en cierto sentido eran enunciados embrionarios de lo que en el futuro se conocerían como leyes de reciprocidad superiores. Gauss, en dos de las ocho demostraciones que dio de la ley de reciprocidad cuadrática, utilizó las sumas que llevan su nombre (cuarta y sexta demostraciones) haciendo uso de las raíces de la unidad para extender el cuerpo de los números racionales. Gauss afirmó que esta forma de proceder daría lugar a nuevas leyes de reciprocidad. Kummer, quien quiso obtener esas nuevas leyes de reciprocidad, desarrolló la teoría algebraica de números introduciendo conceptos como los números ideales primos para poder reconstruir el teorema de factorización única en las extensiones ciclotómicas. Hilbert en el Congreso Internacional de Matemáticos de 1900 afirmó que la introducción de los números ideales primos de Kummer se hizo con vistas a resolver el último teorema de Fermat cuando en realidad hay evidencias de que aprovechó dicho concepto en el estudio de este último [Lem00].

Así mismo, otro de los temas tratados por Gauss fue el problema de la división de la circunferencia en partes iguales con regla y compás. Para ello, de nuevo utilizó las raíces de la unidad y estudió cuándo dichas raíces podían obtenerse haciendo únicamente uso de raíces cuadradas. Una vez más, sugirió que sus resultados se podían extender, en este caso, a la curva lemniscata de Bernouilli usando otras funciones trascendentales que recibirían el apellido de elípticas. Abel en 1828, desarrollando estas afirmaciones, encontró condiciones más generales sobre la resolubilidad de ecuaciones algebraicas llegando a la idea fundamental de que la resolubilidad de una ecuación algebraica se traduce en relaciones específicas de sus raíces. Durante el desarrollo de sus investigaciones se aproximó a la noción de ecuación abeliana que en terminología moderna se traduce en una extensión de Galois abeliana, extensiones que son el tema central de este trabajo.

Kronecker, analizando los trabajos de Gauss y Abel, dedujo cómo podía obtener extensiones abelianas de una extensión cuadrática imaginaria arbitraria haciendo uso de valores especiales de

ciertas funciones elípticas y modulares. Kronecker enunció en 1853 su famoso teorema sobre las extensiones abelianas de $\mathbb{Q}$, que hoy en día recibe el nombre de Kronecker-Weber y el propio Kronecker lo enunció en su carta a Dedekind de 1880 como sigue [PS04]:

> *" las raíces de cualquier ecuación abeliana con coeficientes racionales enteros pueden ser escritos como una función racional en la raíces de la unidad."*

En realidad, por entonces, Kronecker entendía por ecuación (extensión) abeliana lo que hoy entendemos por ecuación (extensión) cíclica. En cualquier caso, la demostración de Kronecker no estaba completa. Lo sorprendente fue que seguido a este teorema Kronecker hizo afirmaciones similares esta vez para el cuerpo de números racionales de Gauss $\mathbb{Q}(i)$. Kronecker entendía las raíces de la unidad como valores especiales de la función exponencial y con esta filosofía afirmó que las extensiones abelianas de $\mathbb{Q}(i)$ se podían obtener usando valores especiales de funciones elípticas y modulares. De hecho, como se ha mencionado antes, en la misma carta a Dedekind llegó a conjeturar que estos resultados serían ciertos para cualquier extensión cuadrática imaginaria, conjetura que se conoce como *el sueño de juventud de Kronecker (Jugendtraum)*.

Estos resultados se pueden interpretar como el nacimiento de la teoría de cuerpos de clase. En los años posteriores, Weber demostró con más detalle el resultado de Kronecker sobre las extensiones abelianas de $\mathbb{Q}$, obteniendo en 1886 la primera prueba, aceptada a pesar de ser errónea. Así mismo, Weber fue quien acuñó el término cuerpo de clase, aunque en esta primera etapa él se refería con este término a cierta extensión de una extensión cuadrática imaginaria verificando unas propiedades concretas. Weber estudió la ramificación de ideales primos e introdujo ciertas funciones L para obtener resultados análogos al teorema de Dirichlet sobre números primos en progresiones aritméticas.

Hilbert, basándose en el trabajo de sus predecesores, llevó la teoría de cuerpos de clase más lejos. De nuevo, una de las principales motivaciones de Hilbert era obtener leyes de reciprocidad en cuerpos de números. Así mismo, Hilbert dio la primera demostración correcta del teorema de Kronecker-Weber en 1896. Muchos de los elementos que aparecen en aquella demostración han perdurado hasta la demostración que aparece en este trabajo que data de 1951. Una propiedad esencial que uso Hilbert fue el hecho de que $\mathbb{Q}$ no admite extensiones no ramificadas no triviales y su demostración se basaba en un estudio detallado de ciertos grupos de ramificación que él introdujo. Comparar con 2.5.10.

Takagi, quien estudió un tiempo con Hilbert, extendió la demostración que dio Hilbert del teorema de Kronecker-Weber para probar el sueño de juventud de Kronecker para el cuerpo base $\mathbb{Q}(i)$. Cuando comenzó la Primera Guerra Mundial en 1914, Takagi, residente en Japón, perdió el contacto con Alemania donde se estaba desarrollando la teoría algebraica de números. En completa soledad desarrolló la teoría de cuerpos de clase hasta un estado casi definitivo. Él amplió el significado

del concepto "cuerpo de clase" al equivalente moderno. Sin embargo, sus teoremas ya no tenían el carácter explícito que tenía la teoría de cuerpos de clase tal y como la pensó Kronecker. De hecho, Takagi vio que existían ciertos isomorfismos entre objetos obtenidos a partir del cuerpo de números y grupos de Galois de las extensiones abelianas correspondientes, pero sólo pudo obtener estos isomorfismos en casos especiales. Además Takagi propuso en el Congreso Internacional de Matemáticos de 1920 el problema de comprender no sólo las extensiones abelianas sino las extensiones de Galois de los cuerpos de números.

Emil Artin se preguntó qué forma tendría que tener la teoría para poder describir las extensiones no abelianas. En sus investigaciones definió un nuevo tipo de funciones L asociadas a representaciones de grupos de Galois y comparándolas con las funciones L de Weber vio que a la teoría de cuerpos de clase de Takagi le faltaba un elemento esencial: el homomorfismo de Artin. El homomorfismo de Artin proveía a la teoría de Takagi de lo que ésta carecía, a saber, el homomorfismo de Artin permitía obtener de forma canónica los isomorfismos que Takagi sólo podía describir en casos muy concretos. Artin demostró la existencia de dicho homomorfismo en 1927 y hoy día se conoce como la *ley de reciprocidad de Artin*. El nombre que recibe el homomorfismo de Artin se justifica porque en años posteriores se demostró que todas las leyes de reciprocidad conocidas se podían deducir haciendo uso del homomorfismo de Artin. Aunque el homomorfismo de Artin devolvió algo de explicitud a la teoría, la descripción concreta de las extensiones abelianas no se había recuperado.

La teoría de cuerpos de clase global tenía problemas para tratar con los primos que ramifican. Hasse, inspirado por los trabajos de Hilbert, decidió estudiar la teoría en un contexto local para así poder tratar la presencia y/o ausencia de ramificación en pie de igualdad. Años antes Hilbert hizo esto último al obtener su reinterpretación de la ley de reciprocidad cuadrática en términos del símbolo que lleva su nombre. De este modo, Hasse dedujo los resultados de la teoría de cuerpos de clase local a partir de la teoría global y observó que los resultados locales no dependían de ningún tipo de información global. Estas investigaciones sugirieron que la teoría de cuerpos de clase local podría existir con independencia de la versión global. Los problemas para construir la teoría de cuerpos de clase local residían en la definición del homomorfismo de Artin local para las extensiones abelianas totalmente ramificadas. Hasse, Chevalley y E.Noether, entre otros, consiguieron la descripción del homomorfismo de Artin usando métodos de la teoría de álgebras cíclicas. Una vez más, como ocurrió con Takagi, la teoría no daba una descripción explícita de los cuerpos de clase sobre cuerpos locales.

Tras la Segunda Guerra Mundial, se reinterpretaron los trabajos de Hasse bajo la óptica de la cohomología y se consiguió distinguir lo que era cohomología de lo que correspondía a la teoría de cuerpos de clase. De esta forma, entre 1950 y 1952, la cohomología vio su aplicación en la teoría de

cuerpos de clase de la mano de Hochschild, Nakayama, Weil, Artin y Tate.

Años antes, Chevalley consiguió obtener la teoría de cuerpos de clase global a partir de la teoría de cuerpos de clase local usando los grupos de ideles introducidos por él mismo. Aunque originalmente este concepto no había sido diseñado para obtener los resultados globales de sus versiones locales, el propio Chevalley lo usó con este propósito en 1940 [Che40].

Para recuperar una descripción explícita de las extensiones abelianas de un cuerpo, al menos en el contexto local, hubo que esperar hasta 1965 cuando Lubin y Tate [LT65] usaron conceptos modernos de la geometría algebraica (grupos formales) para rescatar una descripción explícita de los cuerpos de clase. De hecho, mucho antes ya se conocía por qué Kronecker consiguió describir las extensiones abelianas de las extensiones cuadráticas imaginarias. La explicación la dio la teoría de multiplicación compleja por la que se sabe que la presencia de simetrías adicionales de ciertas curvas elípticas permiten obtener los valores especiales que Kronecker consideró. Basándose en esta analogía, Lubin y Tate aprovecharon el formalismo de los grupos formales para poder obtener ciertos puntos de torsión en clara analogía con el caso de las curvas elípticas. El presente trabajo se centra en esta teoría de Lubin-Tate como se comentó anteriormente, razón por la que el mismo podría recibir el nombre de Teoría de Cuerpos de Clase Explícita.

En la actualidad se conoce prácticamente todo sobre las extensiones abelianas de un cuerpo. Los resultados más actuales que se han obtenido en teoría de cuerpos de clase son ciertas leyes de reciprocidad explícitas o construcciones más explícitas en casos particulares. Sin embargo, la pregunta de Takagi sobre las extensiones no abelianas en el Congreso Internacional de Matemáticos de 1920 aún no ha recibido una respuesta satisfactoria. A este respecto, Robert Langlands en 1967 escribió una carta a Weil que contenía una serie de conjeturas (muy concretas) e ideas que revolucionarían la teoría algebraica de números. De esta forma se inició el programa de Langlands en el que se pretende demostrar todas las afirmaciones de Langlands además de obtener enunciados precisos. Las conjeturas de Langlands pueden entenderse como una vasta generalización de la teoría de cuerpos de clase al caso en que las extensiones no son necesariamente abelianas. La importancia de las conjeturas de Langlands es que unen áreas muy importantes de las matemáticas entre las que antes apenas había interconexiones aisladas. Ejemplos de estas áreas son la teoría de representaciones, la teoría de las formas automorfas y la teoría de números.

A grandes rasgos, los avances más recientes en el programa de Langlands se pueden enumerar como sigue:

> 1974 - Drinfeld construye los módulos elípticos (llamados así por la analogía con las curvas elípticas) y obtuvo resultados profundos sobre las extensiones de los cuerpos de funciones. Sus resultados se dicen que resuelven las conjeturas de Langlands para $\mathtt{GL}_2$. Drinfeld recibió la

medalla Fields en 1990 gracias a estos trabajos.

1995 - Andrew Wiles, junto a otros, demuestra la conjetura de Taniyama-Shimura-Weil, resultados que le permiten demostrar el último teorema de Fermat. La conjetura de Taniyama-Shimura-Weil se puede considerar como un caso particular de las conjeturas de Langlands.

2002 - Lafforgue recibe la medalla Fields tras demostrar las conjeturas de Langlands para $\mathtt{GL}_n$ en el caso de cuerpos de funciones basándose en los trabajos de Drinfeld.

2010 - Châu obtiene la medalla Fields por avances significativos en las conjeturas de Langlands.

2021 - Peter Scholze y Laurent Fargues han publicado un artículo del que se espera se obtengan avances importantes en las conjeturas de Langlands. Esta publicación ha creado gran expectación pues Scholze ganó la medalla Fields en 2018 y Fargues ha realizado contribuciones importantes en geometría aritmética y teoría de números.

Índice general

Capítulo 1

Preliminares

Vamos a repasar brevemente la teoría de Galois para extensiones algebraicas arbitrarias, la teoría de valoraciones incluyendo los cuerpos locales y la teoría de ramificación de éstos. Para un estudio considerablemente más detallado y con demostraciones del contenido que viene a continuación se puede consultar la memoria de la Beca de Colaboración [GC].

1.1. Teoría de Galois

Sea $L \supset k$ una extensión de Galois, es decir, algebraica, separable y normal. Definimos el grupo de Galois de la extensión por

$$G := \mathtt{Gal}(L|k) = \{\sigma \in \mathtt{Aut}(L) \ |\sigma_{|k} = \mathtt{id}_k\}.$$

Denotaremos por $\{L : k\}, \{G : 1\}$ los retículos de subextensiones intermedias, subgrupos respectivamente. Se define la *topología de Krull* del grupo G de modo que una base de entornos abiertos de un automorfismo σ viene dada por la familia de subconjuntos siguiente:

$$\{\sigma\mathtt{Gal}(L|F) \mid F \supset k \text{ extensión finita de Galois } F \in \{L : k\}\},$$

donde $\sigma\mathtt{Gal}(L|F)$ es la clase a izquierda de σ respecto a $\mathtt{Gal}(L|F)$ en G. El grupo G junto con la topología de Krull es un grupo topológico.

Observación 1.1.1. La intuición detrás de la topología de Krull es que dos elementos $\sigma, \tau \in G$ estarán próximos si y sólo si existe una subextensión de Galois finita F "grande" de modo que $\sigma_{|F} = \tau_{|F}$. ■

Esta topología posee las siguientes propiedades:

Proposición 1.1.2. ([Rib13], Proposition 1.6). G con la topología de Krull es un grupo topológico de Hausdorff, compacto y totalmente disconexo.

Gracias a estas propiedades sabemos que G es un grupo profinito. Visto como límite proyectivo, tenemos

$$G \simeq \varprojlim \mathtt{Gal}(F|k),$$

es decir, el límite proyectivo del sistema formado por los grupos de Galois de las subextensiones finitas de Galois de $L \supset k$ y los homomorfismos de restricción como aplicaciones. El **teorema fundamental de la teoría de Galois** es como sigue:

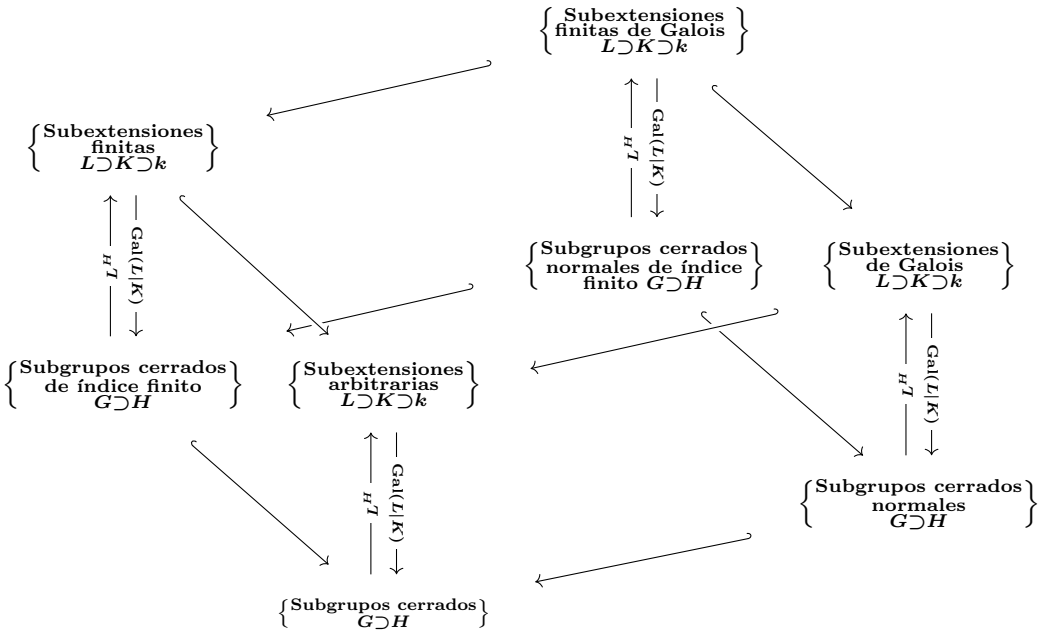
Teorema 1.1.3. ([Milb], Theorem 7.12). Sea $L \supset k$ una extensión de Galois con grupo de Galois G. Las aplicaciones

$$\begin{array}{ccc} \{G:1\} & \longrightarrow & \{L:k\} \\ H & \longmapsto & L^H \end{array} \quad \text{y} \quad \begin{array}{ccc} \{L:k\} & \longrightarrow & \{G:1\} \\ K & \longmapsto & \mathtt{Gal}(L|K) \end{array}$$

son biyecciones, una inversa de la otra, entre los retículos de subextensiones de $L \supset k$ y subgrupos cerrados de G. Además, se cumplen las siguientes propiedades:

1. La correspondencia invierte las inclusiones: $H_1 \supset H_2 \Leftrightarrow L^{H_1} \subset L^{H_2}$.
2. Un subgrupo cerrado H de G es abierto si y sólo si L^H tiene grado finito sobre k y en ese caso $(G:H) = [L^H : k]$.
3. Para todo $\sigma \in G$ tenemos que $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$, $\mathtt{Gal}(L|\sigma K) = \sigma \mathtt{Gal}(L|K)\sigma^{-1}$.
4. Un subgrupo cerrado H de G es normal si y sólo si L^H es una extensión de Galois sobre k y en ese caso $\mathtt{Gal}(L^H|k) \simeq G/H$.

Para resumir la teoría de Galois, tener en mente el siguiente esquema:



Observación 1.1.4. Si la extensión $L \supset k$ es finita, la topología de Krull es la topología discreta. De este modo, todos los subgrupos son cerrados y recuperamos el teorema fundamental de la teoría de Galois clásica. ■

Proposición 1.1.5. ([Lan02], Theorems 1.12,1.14, Chapter IV).

1. Sea $L \supset k$ una extensión de Galois, sea $K \supset k$ una extensión arbitraria y supongamos que L, K son subcuerpos de algún cuerpo. Entonces las extensiones $LK \supset K$ y $L \supset L \cap K$ son de Galois y la aplicación
$$\begin{array}{ccc} \mathtt{Gal}(KL|K) & \longrightarrow & \mathtt{Gal}(L|L\cap K), \\ \sigma & \longmapsto & \sigma_{|L}, \end{array}$$
es un isomorfismo de grupos topológicos.

2. Sean L_1, L_2 extensiones de Galois del cuerpo k con grupos de Galois G_1, G_2 respectivamente y supongamos que L_1, L_2 son subcuerpos de algún cuerpo. Entonces la extensión $L_1L_2 \supset k$ es de Galois. Denotamos por G al grupo de Galois de la extensión $L_1L_2 \supset k$. Se verifica que la siguiente aplicación es un homomorfismo continuo e inyectivo de grupos topológicos:
$$\begin{array}{ccc} G & \longrightarrow & G_1 \times G_2, \\ \sigma & \longmapsto & (\sigma_{|L_1}, \sigma_{|L_2}). \end{array}$$
Si $L_1 \cap L_2 = k$ entonces es un isomorfismo continuo.

Decimos que una extensión $L \supset k$ es *abeliana* si es de Galois con grupo de Galois abeliano. Gracias a 1.1.5, el compuesto de dos extensiones abelianas contenidas en un mismo cuerpo es de nuevo una extensión abeliana.

El siguiente ejemplo será relevante en lo que sigue:

Ejemplo 1.1.6. (Grupo de Galois de $\mathbb{F}_q^{\mathtt{sep}} \supset \mathbb{F}_q$ y Enteros Profinitos $\widehat{\mathbb{Z}}$).

Denotamos por $\mathbb{F}_q^{\mathtt{sep}}$ a una clausura separable del cuerpo finito con q elementos $\mathbb{F}_q$. En este caso, la clausura separable coincide con la clausura algebraica pues los cuerpos finitos son perfectos.

Es conocido que si $n|m$ entonces existe una $\mathbb{F}_q$-inmersión $\tau_{n,m}$ de $\mathbb{F}_{q^n}$ en $\mathbb{F}_{q^m}$ y además todas estas inmersiones se pueden tomar compatibles entre sí de modo que $\tau_{n,m} = \tau_{k,m} \circ \tau_{n,k}$ siempre que $n|k, k|m$. Haciendo el límite inyectivo de este sistema directo de $\mathbb{F}_q$-homomorfismos obtenemos una clausura separable de $\mathbb{F}_q$:
$$\mathbb{F}_q^{\mathtt{sep}} \simeq \varinjlim \mathbb{F}_{q^n}.$$
Si se prefiere, se puede pensar en el límite inyectivo anterior como la unión de todas las extensiones finitas de $\mathbb{F}_q$ una vez hemos asumido que todas están contenidas en una misma clausura algebraica

de $\mathbb{F}_q$. Para cada n tenemos el *automorfismo de Frobenius* $\mathtt{Frob}_{n,q} \in \mathtt{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ definido por $\mathtt{Frob}_{n,q}(x) = x^q$ para todo $x \in \mathbb{F}_{q^n}$. Cada automorfismo de Frobenius genera al correspondiente grupo de Galois y obtenemos que $\mathtt{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) = \langle \mathtt{Frob}_{n,q} \rangle \simeq \mathbb{Z}/\mathbb{Z}n$. Por tanto, el grupo de Galois de $\mathbb{F}_q^{\mathtt{sep}}$ sobre $\mathbb{F}_q$ es

$$\mathtt{Gal}(\mathbb{F}_q^{\mathtt{sep}}|\mathbb{F}_q) \simeq \varprojlim \mathtt{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \simeq \varprojlim \mathbb{Z}/\mathbb{Z}n.$$

El anillo $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/\mathbb{Z}n$ es el *anillo de los enteros profinitos*. Si consideramos las aplicaciones naturales $\mathbb{Z} \to \mathbb{Z}/\mathbb{Z}n$, en el límite obtenemos un homorfismo canónico inyectivo $\mathbb{Z} \to \widehat{\mathbb{Z}}$ y además $\mathbb{Z}$ es denso en $\widehat{\mathbb{Z}}$, entendiendo $\mathbb{Z}$ como subgrupo por medio de la identificación anterior. Por definición, $\widehat{\mathbb{Z}}$ es *la compleción profinita* de $\mathbb{Z}$. De hecho, si dotamos a $\mathbb{Z}$ con la topología que se obtiene de declarar que los subgrupos de índice finito forman un sistema fundamental de entornos, entonces $\widehat{\mathbb{Z}}$ es su compleción en el sentido topológico del término. Se comprueba que para todo $n \in \mathbb{Z}$ es $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}n \simeq \mathbb{Z}/\mathbb{Z}n$, y todos los subgrupos abiertos de $\widehat{\mathbb{Z}}$ son de la forma $\widehat{\mathbb{Z}}n$ con $n \in \mathbb{Z}$. Visto como grupo, $\widehat{\mathbb{Z}}$ es un ejemplo de un grupo procíclico y en particular es un grupo abeliano.

Volviendo al cálculo de $\mathtt{Gal}(\mathbb{F}_q^{\mathtt{sep}}|\mathbb{F}_q)$, concluimos que el automorfismo de Frobenius $\mathtt{Frob}_q = (\mathtt{Frob}_{n,q})_{n\in\mathbb{N}}$ es un generador topológico del grupo de Galois, esto es, $\mathtt{Gal}(\mathbb{F}_q^{\mathtt{sep}}|\mathbb{F}_q) = \overline{\langle \mathtt{Frob}_q \rangle}$. Es inmediato que $\mathtt{Frob}_q(x) = x^q$ para todo $x \in \mathbb{F}_q^{\mathtt{sep}}$.

■

1.2. Cuerpos Locales

Definición 1.2.1. (Valores Absolutos). *Dado un cuerpo k, la aplicación $|\cdot| : k \to \mathbb{R}$ se dice que es un* **valor absoluto de** *k si verifica las propiedades:*

1. $|x| \geq 0 \ \forall x \in k \ y \ |x| = 0 \Leftrightarrow x = 0$.

2. $|xy| = |x||y| \ \forall x, y \in k$.

3. $|x + y| \leq |x| + |y| \ \forall x, y \in k$. *(Desigualdad triangular).*

Si en lugar de **3.** *el valor absoluto verifica la condición más fuerte*

3′. $|x + y| \leq \mathtt{max}(|x|, |y|), \ \forall x, y \in k$,

decimos que el valor absoluto es no arquimediano.

Un ejemplo es el *valor absoluto trivial* definido por $|0| = 0$ y $|x| = 1, \forall x \neq 0$. Todo valor absoluto permite definir una *distancia* $\mathtt{d}(x, y) = |x - y|$ sobre k y podemos dotar a k con la estructura de un espacio métrico, en particular, podemos dar una topología de Hausdorff a k. Dados dos valores

absolutos $|\cdot|_1, |\cdot|_2$ sobre un cuerpo k, se dicen *equivalentes* si ambos inducen la misma topología en k. Se comprueba que dos valores absolutos son equivalentes si y sólo si existe un número real $s > 0$ tal que $|x|_1 = |x|_2^s$ para todo $x \in k$. Cada clase de equivalencia de valores absolutos sobre k se dirá que es un *lugar* de k.

Dado un valor absoluto no arquimediano de k, consideramos la aplicación $\nu : k \to \mathbb{R} \cup \{\infty\}$ definida por $\nu(x) := -\mathtt{log}|x|$ para $x \neq 0$ y $\nu(0) = \infty$. Esta aplicación verifica las siguientes propiedades:

1. $\nu(x) = \infty \Leftrightarrow x = 0$,

2. $\nu(xy) = \nu(x) + \nu(y)\ \forall x, y \in k$,

3. $\nu(x + y) \geq \mathtt{min}\{\nu(x), \nu(y)\}\ \forall x, y \in k$.

Una aplicación verificando las propiedades anteriores se dice que es una *valoración* de k. Dos valoraciones ν_1, ν_2 son *equivalentes* si existe un número real $s > 0$ tal que $\nu_1 = s \cdot \nu_2$. Dada una valoración ν de k, definimos el *anillo de valoración* de ν como

$$\mathcal{O}_k := \{x \in k \mid \nu(x) \geq 0\}.$$

El conjunto $\mathcal{O}_k$ sólo depende de la clase de equivalencia de ν y es un anillo de valoración. Su ideal maximal es $\mathfrak{p}_k = \{x \in k \mid \nu(x) > 0\}$. Se define el *cuerpo residual* de k en ν como $\overline{k} := \mathcal{O}_k/\mathfrak{p}_k$. A menudo denotamos la imagen de $x \in \mathcal{O}_k$ en $\overline{k}$ por $\overline{x}$.

Diremos que una valoración ν es *discreta* si $\nu(k^\times) \sim \mathbb{Z}$. Si ν es discreta, diremos que está *normalizada* si $\nu(k^\times) = \mathbb{Z}$. Es claro que siempre podemos normalizar una valoración discreta. Si ν es una valoración discreta normalizada, todo elemento $\pi \in \mathcal{O}_k$ tal que $\nu(\pi) = 1$ se llama *parámetro de uniformización de* ν. En este caso, π es un elemento primo de $\mathcal{O}_k$ y $\mathfrak{p}_k = \mathcal{O}_k\pi = (\pi)$. Cuando la valoración es discreta, el anillo de valoración $\mathcal{O}_k$ es un dominio de ideales principales, es decir, es un *anillo de valoración discreta*. En este caso se comprueba que el conjunto de todos los ideales de $\mathcal{O}_k$ coincide con el conjunto de las potencias $\{\mathfrak{p}_k^n \mid n \in \mathbb{N} \cup \{0\}\}$ de $\mathfrak{p}_k$.

Sea k un cuerpo con valor absoluto $|\cdot|$. Decimos que el cuerpo k es *completo respecto a* $|\cdot|$ si toda sucesión de Cauchy respecto a la topología inducida por $|\cdot|$ es convergente. Siempre podemos completar un cuerpo y obtener su *compleción*, que denotamos por $\hat{k}$. Claramente la compleción sólo depende de la clase de equivalencia de $|\cdot|$. El valor absoluto lo extendemos a $\hat{k}$ por continuidad y lo denotamos igual. Se comprueba que hay una *inmersión* de k en $\hat{k}$ y bajo esa inmersión k es un subconjunto denso de $\hat{k}$. Si el valor absoluto es no arquimediano, con valoración asociada ν, se comprueba fácilmente que su extensión continua a $\hat{k}$ de nuevo es no arquimediano, y $\nu(k^\times) = \nu(\hat{k}^\times)$, siendo la aplicación ν en el término del lado derecho la extensión de ν a $\hat{k}$ por continuidad. Denotamos

el anillo de valoración de ν en $\hat{k}$ por $\widehat{\mathcal{O}}_k$. Es inmediato que $\widehat{\mathcal{O}}_k$ coincide con la clausura topológica de $\mathcal{O}_k \subset k \subset \hat{k}$ y análogamente, $\hat{\mathfrak{p}}_k$ es la clausura topológica de $\mathfrak{p}_k$. Por esta razón, también se tiene que $\widehat{\mathcal{O}}_k/\hat{\mathfrak{p}}_k \simeq \mathcal{O}_k/\mathfrak{p}_k$ de modo que el cuerpo residual de $\hat{k}$ en ν coincide con $\overline{k}$.

En el caso en que la valoración ν es discreta, se tiene el siguiente isomorfismo continuo:

$$\widehat{\mathcal{O}}_k \simeq \varprojlim \mathcal{O}_k/\mathfrak{p}_k^n,$$

el límite proyectivo tomado sobre el sistema constituido por los morfismos naturales entre los anillos $\mathcal{O}_k/\mathfrak{p}_k^n$. El isomorfismo anterior también induce un isomorfismo al nivel de los grupos de unidades.

El siguiente resultado, conocido como **Lema de Hensel**, es esencial para la teoría de los cuerpos locales:

Teorema 1.2.2. ([Neu99], Hensel's Lemma, pg. 129). Si un polinomio primitivo $f \in \mathcal{O}_k[x]$ admite, módulo $\mathfrak{p}_k[x]$, la factorización $f(x) + \mathfrak{p}_k[x] = \overline{g}(x)\overline{h}(x)$ siendo $\overline{g}, \overline{h} \in \overline{k}[x]$ polinomios coprimos, entonces f admite una factorización $f = g \cdot h$ con $g, h \in \mathcal{O}_k[x]$ tales que $\mathtt{deg}(g) = \mathtt{deg}(\overline{g})$ y $g + \mathfrak{p}_k[x] = \overline{g},\ h + \mathfrak{p}_k[x] = \overline{h}$.

Ejemplo 1.2.3. (Valores Absolutos de $\mathbb{Q}$).

Aparte del valor absoluto trivial, otro valor absoluto de $\mathbb{Q}$ es la restricción del valor absoluto de $\mathbb{R}$, que denotamos por $|\cdot|_\infty$, y podemos expresarlo como $|a|_\infty = \mathtt{sgn}(a)a,\ \forall a \in \mathbb{Q}$. Sin embargo, para cada número primo p podemos definir una valoración de $\mathbb{Q}$ como sigue:

Dado $a \in \mathbb{Z}$, denotamos por $\mathtt{ord}_p(a)$ al mayor número natural de modo que $p^{\mathtt{ord}_p(a)}$ divide a a. Definimos la aplicación $\nu_p : \mathbb{Q} \to \mathbb{Z}$ de forma que $\nu_p(a/b) := \mathtt{ord}_p(a) - \mathtt{ord}_p(b)$. Es claro que ν_p es una valoración discreta normalizada de $\mathbb{Q}$. De hecho, el anillo de valoración de ν_p coincide con el anillo localizado $\mathbb{Z}_{(p)}$ de $\mathbb{Z}$ en el ideal primo (p). Claramente, los anillos $\mathbb{Z}_{(p)}$ son distintos para distintos números primos p y por ello las valoraciones construidas son no equivalentes, en particular, son todas distintas.

Si definimos las aplicaciones $|\cdot|_p$ como $|\cdot|_p = p^{-\nu_p(\cdot)}$, claramente son valores absolutos de $\mathbb{Q}$ distintos para números primos distintos. El siguiente teorema, debido a **Ostrowski**, nos dice que hemos encontrado todos los valores absolutos de $\mathbb{Q}$ salvo equivalencia:

Proposición 1.2.4. ([Art59], Páginas 21 y 37). Sea $|\cdot|$ un valor absoluto de $\mathbb{Q}$ no trivial.

1. Si $|\cdot|$ es arquimediano entonces es equivalente al valor absoluto usual, denotado $|\cdot|_\infty$.
2. Si $|\cdot|$ es no arquimediano entonces es equivalente a un valor absoluto $|\cdot|_p$ para un único primo p.

Por definición, la compleción de $\mathbb{Q}$ respecto al valor absoluto $|\cdot|_\infty$ es $\mathbb{R}$. Para el valor absoluto $|\cdot|_p$, la compleción es el *cuerpo de los números p-ádicos*, y lo denotamos por $\mathbb{Q}_p$. Su anillo de valoración es el anillo de los *enteros p-ádicos*, notado $\mathbb{Z}_p$. $\mathbb{Z}$ es un subanillo denso de $\mathbb{Z}_p$ y el ideal maximal de $\mathbb{Z}_p$ es $\mathbb{Z}_p p$. Gracias a lo comentado anteriormente, $\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}/\mathbb{Z}p^n$. Observar que el cuerpo residual de $\mathbb{Q}_p$ es el cuerpo finito con p elementos. Debido al teorema chino del resto, tenemos el siguiente isomorfismo

$$\widehat{\mathbb{Z}} \simeq \prod_{p \text{ primo}} \mathbb{Z}_p,$$

donde $\widehat{\mathbb{Z}}$ denota el anillo de los enteros profinitos introducido en 1.1.6. En particular, esto prueba que $\widehat{\mathbb{Z}}$ no es un dominio de integridad. La inmersión $\mathbb{Z} \to \widehat{\mathbb{Z}}$ se corresponde bajo este isomorfismo con el homomorfismo diagonal $\mathbb{Z} \to \prod_p \mathbb{Z}_p$. Esto nos da otra forma de ver que $\mathbb{Z}$ es denso en $\widehat{\mathbb{Z}}$.

■

Tenemos el siguiente resultado sobre extensiones de cuerpos completos:

Teorema 1.2.5. ([Neu99], Theorem 4.8, pg. 131). Sea k completo respecto al valor absoluto $|\cdot|_k$ y sea $L \supset k$ una extensión algebraica arbitraria. Entonces $|\cdot|_k$ puede ser extendido de manera única a un valor absoluto $|\cdot|_L$ de L. Cuando $n := [L:k] < \infty$ la extensión $|\cdot|_L$ viene dada por la fórmula $|x|_L = \sqrt[n]{|\mathtt{N}_{L|k}(x)|_k}$ $\forall x \in L$ y en este caso L es completo respecto a $|\cdot|_L$.

Si el valor absoluto $|\cdot|_k$ es no arquimediano con valoración asociada ν, la fórmula anterior toma la siguiente forma:

$$\omega(x) = \frac{1}{n}\nu(\mathtt{N}_{L|k}(x)), \ \forall x \in L.$$

En particular, cuando ν es discreta también lo será ω. Denotamos que ω extiende a ν por $\omega|\nu$. En general, decimos que una valoración ω extiende a otra ν si lo hacen salvo equivalencias, y lo notaremos también por $\omega|\nu$. Si la valoración ν hubiese estado normalizada, en general, la extensión ω no lo está.

Cuando ν es discreta, tenemos que $\nu(k^\times) \subset \omega(L^\times)$ y $\overline{k} \subset \overline{L}$. Definimos el *índice de ramificación* como $e = e(\omega|\nu) := (\omega(L^\times) : \nu(k^\times))$ y el *grado de inercia* como $f = f(\omega|\nu) := [\overline{L} : \overline{k}]$, pudiendo ser ambos infinitos. Cuando las valoraciones de L y k se sobrentienden como en este caso, escribimos $e = e(L|k)$ y $f = f(L|k)$. La siguiente proposición prueba que los números anteriores son finitos para el caso que nos interesa:

Proposición 1.2.6. ([Art59], Páginas 60 y 81). Cuando la valoración ν es discreta y la extensión $L \supset k$ es finita de grado n se tiene la igualdad $n = e(L|k)f(L|k)$. De hecho, el anillo de valoración $\mathcal{O}_L$ es un $\mathcal{O}_k$-módulo libre finitamente generado.

En las hipótesis de esta última proposición, el conjunto $\{w_i\pi_L^j \mid 0 \leq j \leq e-1,\ 1 \leq i \leq f\}$, donde los $w_i \in \mathcal{O}_L$ son tales que módulo $\mathfrak{p}_L$ forman una $\overline{k}$-base de $\overline{L}$, es una base integral de $\mathcal{O}_L$ como $\mathcal{O}_k$-módulo.

Supuesto que $\nu = \nu_k$ es discreta normalizada, si π_k es un parámetro de uniformización de k y π_L de L, tenemos que $\mathcal{O}_L\mathfrak{p}_k = \mathcal{O}_L\pi_k = \mathfrak{p}_L^e$. La relación entre la valoración normalizada de ω, denotada ν_L, y ν_k es la siguiente:

$$\nu_L(x) = \frac{1}{f(L|k)}\nu_k(\mathtt{N}_{L|k}(x)),\ \forall x \in L.$$

En general, tenemos el siguiente resultado sobre extensibilidad de valoraciones:

Proposición 1.2.7. ([Neu99], Proposition 8.3, pg. 164). Sea k un cuerpo con una valoración no arquimediana discreta ν. Sea $L \supset k$ una extensión finita separable. Entonces $L \otimes_k \hat{k}_\nu \simeq \prod_{w|v} \hat{L}_\omega$, donde el producto recorre el conjunto de todas las posibles extensiones de ν a L y $\hat{L}_\omega$ denota la compleción de L respecto de ω.

Como corolario obtenemos la identidad fundamental de la teoría de valoraciones:

Proposición 1.2.8. ([Neu99], Proposition 8.5, pg. 165). Si ν es discreta y $L \supset k$ es finita separable, entonces $[L : k] = \sum_{\omega|\nu} e(\omega|\nu)f(\omega|\nu)$.

Pasamos a la definición de cuerpo local:

Definición 1.2.9. (Cuerpos Locales). *Un cuerpo k con valor absoluto $|\cdot|$ se dice que es un cuerpo local si el valor absoluto $|\cdot|$ es no trivial y k con la topología inducida por $|\cdot|$ es un espacio topológico localmente compacto.*

Los cuerpos locales poseen las siguientes propiedades [Sut19]:

1. Todo cuerpo local k es completo.

2. Supongamos que el valor absoluto $|\cdot|$ viene inducido por una valoración discreta ν. Entonces k es un cuerpo local respecto a $|\cdot|$ si y sólo si k es completo respecto a $|\cdot|$ y su cuerpo residual $\overline{k}$ es finito.

3. Si el valor absoluto $|\cdot|$ es arquimediano, entonces k es isomorfo a $\mathbb{R}$ o $\mathbb{C}$. Si el valor absoluto $|\cdot|$ es no arquimediano entonces k es isomorfo a una extensión finita de $\mathbb{Q}_p$ para algún primo p o es isomorfo a una extensión finita de $\mathbb{F}_p((T))$ para algún primo p. En particular, si $|\cdot|$ es no arquimediano entonces $|\cdot|$ es un valor absoluto discreto.

En vista del apartado **3.**, hemos de comentar que en el presente trabajo estamos interesados en los cuerpos locales con valor absoluto no arquimediano. Principalmente nuestros resultados serán para

el caso de cuerpos locales no arquimedianos de característica 0, es decir, la extensiones finitas de $\mathbb{Q}_p$ aunque todos los resultados serán ciertos para los cuerpos locales no arquimedianos de característica no nula.

A partir de ahora k **siempre** denotará a un cuerpo local no arquimediano con valoración discreta normalizada ν_k y diremos simplemente que k es un cuerpo local. De forma general, siempre que escribamos ν_L nos estaremos refiriendo a la valoración normalizada de un cuerpo local L.

1.3. Ramificación

Sea $L \supset k$ una extensión finita del cuerpo local k. Diremos que la extensión $L \supset k$ es *no ramificada* si la extensión $\overline{L} \supset \overline{k}$ es separable y $e(L|k) = 1$, o equivalentemente gracias a 1.2.6, $f(L|k) = [L : k]$. La extensión $L \supset k$ se dirá *totalmente ramificada* si $\overline{L} = \overline{k}$, es decir, $f(L|k) = 1$. En general, una extensión algebraica $L \supset k$ se dice *no ramificada* si toda subextensión finita de k es no ramificada en el sentido anterior y $L \supset k$ se dirá *totalmente ramificada* si toda subextensión finita de k es totalmente ramificada. El siguiente resultado caracteriza las extensiones finitas no ramificadas:

Proposición 1.3.1. ([FV93], Proposition 3.2, Chapter II).

1. Sea $L \supset k$ una extensión finita no ramificada con $\overline{L} = \overline{k}(\overline{\alpha}), \alpha \in \mathcal{O}_L$, $f \in \mathcal{O}_k[x]$ el polinomio irreducible de α sobre k y $\overline{f}$ el polinomio f con coeficientes módulo el ideal primo $\mathfrak{p}_k$. Entonces $L = k(\alpha)$, L es separable sobre k, $\mathcal{O}_L = \mathcal{O}_k[\alpha]$ y $\overline{\alpha}$ es una raíz simple del polinomio $\overline{f}$.

2. Sea $f \in \mathcal{O}_k[x]$ un polinomio mónico tal que $\overline{f} = f + \mathfrak{p}[x] \in \overline{k}[x]$ es un polinomio mónico separable sobre $\overline{k}$. Sea α una raíz de f en alguna clausura algebraica de k y consideremos $L = k(\alpha)$. Entonces la extensión finita $L \supset k$ es no ramificada y $\overline{L} = \overline{k}(\overline{\alpha})$.

Esto nos dice que hay una biyección entre las extensiones finitas no ramificadas de k y las extensiones finitas separables de $\overline{k}$. Como corolario de 1.3.1 obtenemos que las extensiones finitas no ramificadas forman una familia distinguida de extensiones, es decir, se tienen las siguientes propiedades:

1. Dada una cadena de extensiones $L \supset K \supset k$, entonces las extensiones $L \supset K, K \supset k$ son finitas no ramificadas si y sólo si la extensión $L \supset k$ es finita no ramificada.

2. Si la extensión $L \supset k$ es una extensión finita no ramificada y $K \supset k$ es una extensión algebraica de modo que L, K están contenidos en algún cuerpo común, entonces $LK \supset K$ es una extensión finita no ramificada.

3. Dadas $L \supset k, K \supset k$ extensiones finitas no ramificadas contenidas en algún cuerpo (por ejemplo $k^{\mathtt{sep}}$), entonces la extensión $LK \supset k$ es finita no ramificada.

El siguiente resultado nos indica cómo interaccionan las extensiones de Galois con las extensiones no ramificadas:

Proposición 1.3.2. ([FV93], Proposition 3.3, Chapter II).

1. Sea $L \supset k$ una extensión no ramificada con $\overline{L} \supset \overline{k}$ una extensión de Galois. Entonces $L \supset k$ es una extensión de Galois.

2. Sea $L \supset k$ una extensión no ramificada de Galois. Entonces $\overline{L} \supset \overline{k}$ es de Galois. Además, los grupos $\mathtt{Gal}(L|k)$ y $\mathtt{Gal}(\overline{L}|\overline{k})$ son isomorfos vía el isomorfismo $\sigma \in \mathtt{Gal}(L|k) \mapsto \overline{\sigma} \in \mathtt{Gal}(\overline{L}|\overline{k})$ donde $\overline{\sigma}$ se define por medio de la identidad $\overline{\sigma}\ \overline{\alpha} = \overline{\sigma\alpha}\ \forall \alpha \in \mathcal{O}_L$.

Consideramos la unión de todas las extensiones finitas no ramificadas supuesto que todas están contenidas en una misma clausura algebraica de k y a esta unión la denotamos por $k^{\mathtt{ur}}$. Dicha extensión será no ramificada pues toda subextensión finita de $k^{\mathtt{ur}} \supset k$ es no ramificada. Decimos que $k^{\mathtt{ur}}$ es la *extensión no ramificada maximal de* k. La extensión de ν_k a $k^{\mathtt{ur}}$ la notaremos por $\nu_{\mathtt{ur}}$ y en general el cuerpo $k^{\mathtt{ur}}$ no es completo respecto a la misma. Se verifica que el índice de ramificación de la extensión $k^{\mathtt{ur}} \supset k$ es igual a 1. La extensión $k^{\mathtt{ur}} \supset k$ es de Galois y su cuerpo residual $\overline{k^{\mathtt{ur}}}$ coincide con la clausura separable $\overline{k}^{\mathtt{sep}}$ de $\overline{k}$. De hecho, $\mathtt{Gal}(k^{\mathtt{ur}}|k) \simeq \mathtt{Gal}(\overline{k}^{\mathtt{sep}}|\overline{k})$.

Si $\overline{k} = \mathbb{F}_q$ es el cuerpo finito con q elementos, sabemos que para cada $n \in \mathbb{N}$ existe, salvo isomorfismos, una única extensión finita de $\mathbb{F}_q$, a saber, $\mathbb{F}_{q^n}$. Deducimos que k tiene, salvo isomorfismos, una única extensión no ramificada de grado n que denotaremos por k_n. Como el cuerpo finito con q^n elementos es el conjunto de raíces del polinomio $X^{q^n} - X$ añadidas al cuerpo primo de característica $\mathtt{char}(\overline{k})$, gracias al **lema de Hensel** 1.2.2, tenemos que la extensión finita no ramificada de k de grado n es la extensión obtenida al adjuntar las raíces de la unidad μ_{q^n-1} a k. Tenemos que $k^{\mathtt{ur}} = \bigcup_{n\geq 0} k_n = k(\bigcup_{n\geq 0} \mu_{q^n-1})$.

Gracias al isomorfismo $\mathtt{Gal}(k^{\mathtt{ur}}|k) \simeq \mathtt{Gal}(\mathbb{F}_q^{\mathtt{sep}}|\mathbb{F}_q) = \overline{\langle \mathtt{Frob}_q \rangle}$, existe un único automorfismo $\varphi_k \in \mathtt{Gal}(k^{\mathtt{ur}}|k)$ de modo que $\overline{\varphi_k(x)} = \overline{x}^q$ para todo $x \in \mathcal{O}_{k^{\mathtt{ur}}}$. Decimos que φ_k es el *elemento de Frobenius de* k y es un generador topológico del grupo $\mathtt{Gal}(k^{\mathtt{ur}}|k)$.

Proposición 1.3.3. ([FV93], Proposition 3.4, Corollary 3.4, Chapter II). Sea $L \supset k$ una extensión algebraica separable de modo que la extensión de ν_k a L es discreta. Entonces $L^{ur} = L \cdot k^{ur}$ y $L_0 = L \cap k^{ur}$ es la subextensión no ramificada maximal de k que está contenida en L. Además, se tiene la igualdad $\overline{L} = \overline{L_0}$.

Si además la extensión $L \supset k$ es finita, las extensiones $L \supset L_0, L^{\mathtt{ur}} \supset k^{\mathtt{ur}}$ son totalmente ramificadas teniéndose la igualdad $[L : L_0] = [L^{\mathtt{ur}} : k^{\mathtt{ur}}]$. Por último, si φ_L es el elemento de Frobenius de L, es fácil comprobar la igualdad

$$(\varphi_L)_{|k^{\mathtt{ur}}} = \varphi_k^{f(L|k)}.$$

En [GC], Subsección 3.3.1 se puede encontrar una descripción prácticamente explícita del elemento de Frobenius de un cuerpo local y dicha descripción se prueba útil para la teoría de cuerpos de clase. Si la extensión $L \supset k$ es de Galois, $\mathtt{Gal}(L|L_0)$ se denota por $\mathtt{I}(L|k)$ y se llama *grupo de inercia* de la extensión $L \supset k$.

Por otro lado, dada una extensión de Galois $L \supset k$ (posiblemente infinita), consideramos el homomorfismo restricción $\mathtt{res} : \mathtt{Gal}(L|k) \to \mathtt{Gal}(L_0|k)$. El grupo $\mathtt{Gal}(L_0|k)$ está generado topológicamente por $(\varphi_k)_{|L_0}$. Definimos el *grupo de Weil de la extensión* $L \supset k$ como

$$\mathtt{W}(L|k) := \mathtt{res}^{-1}(\langle(\varphi_k)_{|L_0}\rangle) = \{\sigma \in \mathtt{Gal}(L|k) \mid \sigma_{|L_0} \in \langle(\varphi_k)_{|L_0}\rangle\}.$$

Se comprueba que el grupo de Weil es un subgrupo normal denso de $\mathtt{Gal}(L|k)$. Si la extensión $L \supset k$ es finita entonces $\mathtt{W}(L|k) = \mathtt{Gal}(L|k)$. Para las demostraciones, ver [GC], Subsección 4.3.1. Dado $\sigma \in \mathtt{W}(L|k)$, se define $\nu(\sigma)$ de forma que $\sigma_{|L_0} = (\varphi_k)_{|L_0}^{\nu(\sigma)}$.

Observación 1.3.4. El grupo de Weil suele dotarse de una topología que es más fina que la topología inducida de $\mathtt{Gal}(L|k)$. Para nuestros objetivos esta topología no importa. Se pueden encontrar más detalles en [Cona]. ■

Dado un polinomio mónico $g \in \mathcal{O}_k[X]$ de la forma $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, decimos que es un *polinomio de Eisenstein* si $a_i \in \mathfrak{p}_k \ \forall i,\ a_0 \notin \mathfrak{p}_k^2$. Para las extensiones totalmente ramificadas finitas tenemos la siguiente caracterización:

Proposición 1.3.5. ([FV93], Proposition 3.6, Chapter II).

1. Todo polinomio de Eisenstein g es irreducible. Si Π es una raíz de g, entonces $k(\Pi) \supset k$ es una extensión totalmente ramificada de grado n, y Π es un elemento primo en $k(\Pi)$ verificando ademas que $\mathcal{O}_{k(\Pi)} = \mathcal{O}_k[\Pi]$.

2. Sea $L \supset k$ una extensión separable totalmente ramificada de grado n, y sea π_L un elemento primo de L. Entonces π_L es una raíz de un polinomio de Eisenstein sobre k de grado n. En particular, la norma de π_L es un parámetro de uniformización de k.

Ahora nos centraremos en entender la ramificación en extensiones de Galois de un cuerpo k **general** (no necesariamente local). Estos resultados de carácter gobal se introducen con vistas a la demostración del teorema de Kronecker-Weber. Fijamos un cuerpo base k con una valoración discreta normalizada ν. Sea $L \supset k$ una extensión finita de Galois con grupo de Galois G. Se define la acción del grupo G sobre el conjunto de extensiones $\omega|\nu$ como $\omega^\sigma := \omega \circ \sigma$. Esta acción está bien definida y es transitiva. Fijada una extensión $\omega|\nu$, definimos su *grupo de descomposición* como

$$\mathtt{G}_\omega(L|k) = \{\sigma \in G \mid \omega \circ \sigma = \omega\}.$$

Se puede comprobar que el grupo de descomposición de ω está constituido por los automorfismos σ que son continuos respecto a ω.

Notaremos por $\mathcal{O}_{L,\omega}, \mathfrak{p}_{L,\omega}, \overline{L}_\omega$ el anillo de valoración de ω, su ideal maximal y su cuerpo residual respectivamente. Análogamente, $\mathcal{O}_{k,\nu}, \mathfrak{p}_{k,\nu}, \overline{k}_\nu$ denotan los correspondientes objetos. Se puede demostrar que la extensión $\overline{L}_\omega \supset \overline{k}_\nu$ es de Galois. Por definición, para todo $\sigma \in \mathtt{G}_\omega(L|k)$ tenemos $\sigma(\mathcal{O}_{L,\omega}) = \mathcal{O}_{L,\omega}, \sigma(\mathfrak{p}_{L,\omega}) = \mathfrak{p}_{L,\omega}$. Definimos la aplicación $\mathtt{G}_\omega(L|k) \to \mathtt{Gal}(\overline{L}_\omega|\overline{k}_\nu)$ que a cada automorfismo σ le asigna la aplicación $\overline{\sigma}$ que hace $\overline{\sigma}(x + \mathfrak{p}_{L,\omega}) = \sigma x + \mathfrak{p}_{L,\omega}$. Esta aplicación está bien definida y es un homomorfismo de grupos sobreyectivo. El núcleo del homomorfismo anterior se llama *grupo de inercia de* ω y es igual a

$$\mathtt{I}_\omega(L|k) := \{\sigma \in \mathtt{G}_\omega(L|k) \mid \sigma x + \mathfrak{p}_{L,\omega} = x + \mathfrak{p}_{L,\omega} \ \forall x \in \mathcal{O}_{L,\omega}\}.$$

Los grupos de descomposición e inercia verifican las siguientes propiedades funtoriales [Rib01, Neu99]:

1. Dada una cadena de extensiones $L \supset K \supset k$, se tienen las igualdades: $\mathtt{G}_\omega(L|K) = \mathtt{G}_\omega(L|k) \cap \mathtt{Gal}(L|K)$, $\mathtt{I}_\omega(L|K) = \mathtt{I}_\omega(L|k) \cap \mathtt{Gal}(L|K)$. Así mismo, si μ es una valoración de K tal que $\mu|\nu$ verificándose además que $\omega|\mu$ y $K \supset k$ es de Galois, entonces se tienen los siguientes isomorfismos canónicos $\mathtt{G}_\mu(K|k) \simeq \mathtt{G}_\omega(L|k)/\mathtt{G}_\omega(L|K)$, $\mathtt{I}_\mu(K|k) \simeq \mathtt{I}_\omega(L|k)/\mathtt{I}_\omega(L|K)$.

2. Si denotamos por $\hat{L}_\omega, \hat{k}_\nu$ la compleción de L, k respecto a ω, ν respectivamente, se tienen isomorfismos canónicos $\mathtt{G}_\omega(L|k) \simeq \mathtt{Gal}(\hat{L}_\omega|\hat{k}_\nu)$, $\mathtt{I}_\omega(L|k) \simeq \mathtt{I}(\hat{L}_\omega|\hat{k}_\nu)$, obtenidos mediante extensión continua a las compleciones.

3 Dado $\tau \in G$, entonces $\mathtt{G}_{\omega\circ\tau}(L|k) = \tau^{-1}\mathtt{G}_\omega(L|k)\tau$, $\mathtt{I}_{\omega\circ\tau}(L|k) = \tau^{-1}\mathtt{I}_\omega(L|k)\tau$. En particular, cuando la extensión $L \supset k$ es abeliana los grupos de descomposición e inercia sólo dependen de la valoración ν.

El cuerpo fijo de $\mathtt{G}_\omega(L|k)$, denotado Z_ω, se llama *cuerpo de descomposición de ω sobre k*. El cuerpo fijo de $\mathtt{I}_\omega(L|k)$, denotado T_ω, se llama *cuerpo de inercia de ω sobre k*. La extensión $T_\omega \supset Z_\omega$ es de Galois y tenemos el isomorfismo canónico $\mathtt{Gal}(T_\omega|Z_\omega) \simeq \mathtt{G}_\omega(L|k)/\mathtt{I}_\omega(L|k) \simeq \mathtt{Gal}(\overline{L}_\omega|\overline{k}_\nu)$. Algunas propiedades de estos cuerpos son las siguientes [Neu99]:

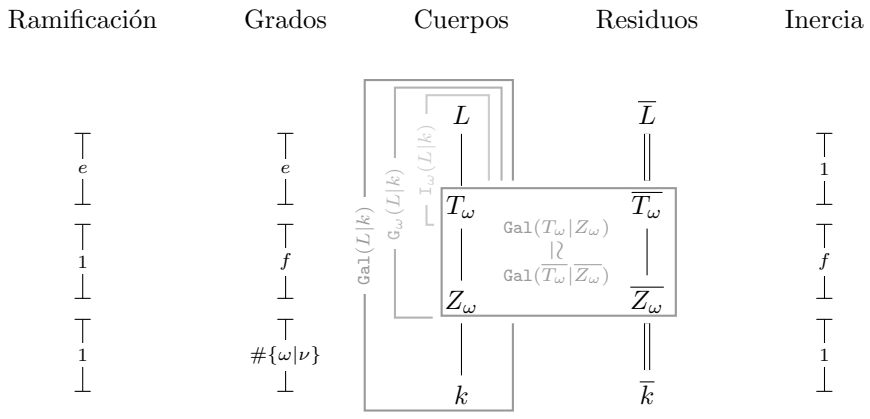
1. La restricción de ω a Z_ω, denotada ω_Z, se extiende de manera única a L. Además, ω_Z tiene el mismo cuerpo residual y el mismo grupo de valores que ν.

2. La extensión $T_\omega \supset Z_\omega$ es la extensión maximal no ramificada de $L \supset Z_\omega$. De este modo, la extensión de ω_Z a T_ω, denotada ω_T, no ramifica y $f(\omega_T|\omega_Z) = f(\omega|\nu)$. Por último, ω_T ramifica completamente en L y se cumple que $e(\omega|\omega_T) = e(\omega|\nu)$.

3. Tenemos la siguiente fórmula: $[L : k] = (G : G_\omega)e(\omega|\nu)f(\omega|\nu)$, siendo $(G : G_\omega)$ el número de posibles extensiones $\omega|\nu$.

4. Si el grupo de descomposición $\mathtt{G}_\omega(L|k)$ es normal en G, por ejemplo cuando G es abeliano, entonces $\mathtt{G}_\omega(L|k)$ sólo depende de ν y podemos denotarlo por $\mathtt{G}_\nu(L|k)$. En este caso, para toda extensión $\omega|\nu$ se verifica que $e(\omega_Z|\nu) = 1, f(\omega_Z|\nu) = 1$, es decir, ν factoriza completamente en Z_ω para todo $\omega|\nu$.

Todo lo anterior lo resumimos en el siguiente esquema:



Capítulo 2

Teoría de Cuerpos de Clase Local

2.1. Objetivos y Organigrama

La teoría de cuerpos de clase se ocupa del estudio de las extensiones abelianas de un cuerpo local o global k en términos de la aritmética del cuerpo en sí mismo. En palabras de *Claude Chevalley* [Che40]: *"L'objet de la théorie du corps de classes est de montrer comment les extensions abéliennes d'un corps de nombres algébriques k peuvent être déterminées par des éléments tirés de la connaissance de K lui-même; ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possède en soi les éléments de son propre dépassement."*

La aritmética del cuerpo se codifica de forma distinta según el cuerpo k sea global o local. En el caso local, que es el que nos interesa, dicha información vendrá codificada por el grupo de unidades $k^\times$ y cierta familia de subgrupos. Los enunciados principales de la teoría de cuerpos de clase local son los siguientes:

Homomorfismo de Artin.

1. Para todo cuerpo local k, *existe* un *único* homomorfismo $\mathtt{Art}_k : k^\times \to \mathtt{Gal}(k^{\mathtt{ab}}|k)$, caracterizado por las siguientes dos propiedades:
   - **a.** Si π es un parámetro de uniformización de k, entonces $\mathtt{Art}_k(\pi)_{|k^{\mathtt{ur}}} = \varphi^{-1}$, siendo φ el elemento de Frobenius de k.
   - **b.** Si $k' \supset k$ es una extensión abeliana finita, entonces $\mathtt{Art}_k\left(\mathtt{N}_{k'|k}(k'^\times)\right)_{|k'} = \mathtt{id}$.

   Además, este homomorfismo es *inyectivo* y su imagen es el conjunto
   $$\mathtt{W}_k^{\mathtt{ab}} := \mathtt{W}(k^{\mathtt{ab}}|k) = \left\{\sigma \in \mathtt{Gal}(k^{\mathtt{ab}}|k) \ : \ \sigma_{|k^{\mathtt{ur}}} \in \varphi_k^{\mathbb{Z}}\right\}.$$

2. Si $k' \supset k$ es una extensión separable finita, entonces $\mathtt{Art}_{k'}(x)_{|k^{\mathtt{ab}}} = \mathtt{Art}_k(\mathtt{N}_{k'|k}(x))$ para todo $x \in k'^\times$, y $\mathtt{Art}_k$ induce un isomorfismo
   $$k^\times/\mathtt{N}_{k'|k}(k'^\times) \xrightarrow{\simeq} \mathtt{Gal}\left((k' \cap k^{\mathtt{ab}})|k\right).$$

Teorema de existencia:

> Para todo subgrupo abierto de índice finito $H \subset k^\times$ existe una única extensión abeliana finita $k' \supset k$ tal que $\mathtt{N}_{k'|k}(k'^\times) = H$.

Observar que estos dos resultados juntos nos permiten clasificar todas las extensiones abelianas del cuerpo local k, pues gracias al homomorfismo de Artin vemos que toda extensión abeliana da lugar a un subgrupo abierto de índice finito de $k^\times$. Recíprocamente, por el toerema de existencia sabemos que todos los subgrupos abiertos de índice finito proceden de alguna extensión abeliana finita.

Nuestro objetivo es demostrar estos resultados y dar los detalles necesarios para alcanzar una comprensión profunda de sus demostraciones. El enfoque será el de la teoría de Lubin-Tate, teoría en la que se construyen explícitamente extensiones abelianas del cuerpo k a partir de polinomios asociados a los parámetros de uniformización de k. En el proceso, conseguiremos visualizar el conjunto de los parámetros de uniformización como cierta categoría y la noción de morfismo que introduzcamos nos servirá para comparar las extensiones abelianas construidas. Veremos que dichas extensiones sólo dependen de la clase de isomorfía. Además, veremos cómo estas clases de isomorfía evolucionan conforme el cuerpo sobre el que llevamos a cabo la construcción va cambiando a lo largo del conjunto de las extensiones finitas no ramificadas de k. Eventualmente, el número de clases de isomorfía se reducirá a una única clase y de esta forma podremos definir una extensión abeliana canónica $k^{\mathtt{LT}}$ de la que tendremos un buen conocimiento. Usando dicha extensión, probaremos los teoremas de la teoría de cuerpos de clase local cambiando $k^{\mathtt{ab}}$ por $k^{\mathtt{LT}}$. Concluida esta tarea, sólo quedará probar que dicha extensión coincide con la extensión abeliana maximal de k, es decir $k^{\mathtt{LT}} = k^{\mathtt{ab}}$, resultado que se conoce como el teorema de Kronecker-Weber local.

Algo destacable de nuestra forma de proceder es que conseguiremos probar todos los resultados sin la necesidad de admitir la existencia del homomorfismo de Artin. En la bibliografía estándar, la teoría de Lubin-Tate suele verse como una herramienta para obtener una descripción detallada del homomorfismo de Artin pero no se usa esta teoría para demostrar la existencia del mismo. Por lo general, la existencia se prueba por otros métodos como puede ser la cohomología de grupos y posteriormente se comparan los homomorfismos construidos usando Lubin-Tate con el homomorfismo de Artin para concluir que ambos coinciden. Esto último es una simplificación considerable de la teoría pues es mucho más fácil comparar objetos que demostrar la existencia y construir un objeto poseyendo unas propiedades concretas. Nosotros demostraremos la existencia del homomorfismo de Artin usando únicamente las construcciones de Lubin-Tate. De hecho, esto explica que se generalicen ligeramente las definiciones ya que necesitaremos un poco de flexibilidad.

Como en el capítulo anterior, esta es la versión resumida de la memoria del proyecto de colaboración [GC] que contiene demostraciones detalladas de los resultados que siguen.

2.2. Grupos Formales y Grupos de Lubin-Tate

Leyes de Grupo Formal

Sea A un anillo conmutativo con unidad no trivial, consideramos su anillo de series de potencias $A[[X]]$. Este anillo contiene el ideal $(X) \subset A[[X]]$ formado por todos los elementos con término constante igual a 0. Es sencillo comprobar que (X) junto con la composición es un monoide, donde la serie de potencias X juega el papel de elemento neutro. Además, los elementos invertibles de este monoide son aquellas series de potencias $f = aX + \cdots \in (X)$ tales que $a \in A^\times$. De hecho, si tomamos una serie de potencias $F \in A[[X_1, \ldots, X_n]]$ de varias variables de modo que su término independiente es nulo, podemos definir las composiciones siguentes:

$$f \circ F := f(F(X_1, \ldots, X_n)),\ F \circ f := F(f(X_1), \ldots, f(X_n)) \in A[[X_1, \ldots, X_n]].$$

Por otro lado, dadas dos series de potencias $F, G \in A[[X_1, \ldots, X_n]]$ y cualquier entero $d \geq 0$ escribiremos $F \equiv G \pmod{\texttt{deg}d}$ para indicar que $F - G$ no tiene términos de grado total menor que d. Esto es equivalente a decir que $F - G \in (X_1, \ldots, X_n)^d \subset A[[X_1, \ldots, X_n]]$.

Definición 2.2.1. (Ley de Grupo Formal). *Una ley formal de grupo sobre A es una serie de potencias de dos variables $F(X, Y) \in A[[X, Y]]$ verificando las condiciones siguientes:*

1. $F(X, Y) \equiv X + Y \pmod{\texttt{deg}2}$.
2. $F(F(X, Y), Z) = F(X, F(Y, Z))$.
3. $F(X, Y) = F(Y, X)$.

Lema 2.2.2. ([GC], Lema 5.2.2, Capítulo 5). Sea F una ley de grupo formal sobre A. Se tienen las siguientes propiedades:

1. $F(X, 0) = X$ y $F(0, Y) = Y$. En particular, $F(X, Y) = X + Y + \sum_{i,j>1} a_{ij} X^i Y^j$ para ciertos $a_{ij} \in A$.
2. Existe una única serie de potencias $i_F \in (X) \subset A[[X]]$ de modo que $F(X, i_F(X)) = 0$, igualdad en el anillo $A[[X]]$.

Ejemplo 2.2.3. (Grupo Aditivo Formal $\mathbb{G}_a$ y Grupo Multiplicativo Formal $\mathbb{G}_m$). Se define la *ley de grupo formal aditiva* por $\mathbb{G}_a := X + Y \in A[[X, Y]]$. La *ley de grupo formal multiplicativa* se define como $\mathbb{G}_m := X + Y + XY = (1 + X)(1 + Y) - 1 \in A[[X, Y]]$. Claramente $i_{\mathbb{G}_a}(X) = -X$ y $i_{\mathbb{G}_m}(X) = (1 + X)^{-1} - 1 = \sum_{n\geq 1}(-1)^n X^n$. ■

Observación 2.2.4. (Grupos asociados a una Ley de Grupo Formal). Si en el ideal $(X) \subset A[[X]]$ definimos la suma de elementos f, g por la fórmula $f +_F g := F(f(X), g(X))$, entonces el conjunto (X) se convierte en un grupo abeliano con la serie idénticamente nula 0 como elemento neutro y el inverso de f es $i_F \circ f$. Vemos que cada ley de grupo formal F da lugar a una ley de grupo "clásica" sobre el ideal (X).

Así mismo, si $A = \mathcal{O}_k$ es el anillo de valoración de un cuerpo local k y F es una ley de grupo formal sobre $\mathcal{O}_k$, podemos dotar al ideal maximal $\mathfrak{p}_k$ con una ley de grupo distinta de la aditividad de $\mathcal{O}_k$. En efecto, definimos $\alpha +_F \beta := F(\alpha, \beta)$ para $\alpha, \beta \in \mathfrak{p}_k$. La suma está bien definida pues el término general de la serie $F(\alpha, \beta)$ converge a cero y esto es suficiente para obtener la convergencia de la serie en el contexto no arquimediano. De hecho, se tiene que $(\mathfrak{p}_k, +_{\mathbb{G}_a}) = (\mathfrak{p}_k, +)$. Se comprueba que la aplicación $(\mathfrak{p}_k, +_{\mathbb{G}_m}) \to (1 + \mathfrak{p}_k, \cdot) = U_k^{(1)}$ dada por $a \mapsto 1 + a$ es un isomorfismo de grupos. En general, para toda extensión finita K de k podemos definir sobre $\mathfrak{p}_K$ la suma como antes y obtenemos que la inclusión $(\mathfrak{p}_k, +_F) \hookrightarrow (\mathfrak{p}_K, +_F)$ es un homomorfismo de grupos. Teniendo en cuenta que $\mathfrak{p}_{k^{\text{sep}}} = \cup_{k\subset K\subset k^{\text{sep}}} \mathfrak{p}_K$, con K recorriendo las subextensiones finitas, vemos que podemos también definir una ley de grupo sobre $\mathfrak{p}_{k^{\text{sep}}}$. ■

Definición 2.2.5. (Homomorfismo). *Sean F, G leyes de grupo formal sobre A. Una serie de potencias $f(X) \in (X) \subset A[[X]]$ se dice que es un homomorfismo de F en G y escribiremos $f : F \to G$ si verifica que $f \circ F = G \circ f$, es decir, $f(F(X, Y)) = G(f(X), f(Y))$. Dos homomorfismos se componen mediante la composición de series de potencias. Si existe el inverso para la composición f^{-1} de f, esta serie de potencias define $f^{-1} : G \to F$. En este caso diremos que f es un isomorfismo.*

Proposición 2.2.6. ([GC],Proposición 5.2.4, Capítulo 5). Sean F, G leyes de grupo formal sobre A. El conjunto $\mathtt{Hom}_A(F, G)$ de todos los homomorfismos de F a G es un grupo abeliano con la suma $+_G$. Además, el conjunto $\mathtt{End}_A(F) := \mathtt{Hom}_A(F, F)$ es un anillo con $+_F$ como suma y la composición $\circ$ como producto.

Grupos de Lubin-Tate Relativos

Denotamos por k al cuerpo local, su valoración normalizada por ν_k, su anillo de valoración por $\mathcal{O}_k$, su ideal maximal por $\mathfrak{p}_k$ y su cuerpo residual $\overline{k} = \mathcal{O}_k/\mathfrak{p}_k \simeq \mathbb{F}_q$ con q una potencia de un primo p. Sea $L \supset k$ una extensión no ramificada completa de k. Para nosotros, esto significa que L es una

extensión no ramificada finita de k o es la compleción de la extensión no ramificada maximal de k, que denotamos por $\hat{k}^{\mathtt{ur}}$. Por ser una extensión no ramificada, sabemos que $\mathfrak{p}_L = \mathcal{O}_L\mathfrak{p}_k$. Denotaremos por φ al elemento de Frobenius de k, y su extensión a L (por continuidad si es necesario) la denotaremos igual. Dado $\alpha \in L$ y $n \in \mathbb{Z}$ escribiremos $\alpha^{\varphi^n} := \varphi^n(\alpha)$. Dada una serie de potencias F sobre $\mathcal{O}_L$, definimos F^{φ^n} como la serie obtenida a partir de F aplicando φ^n a cada coeficiente de F. Las siguientes propiedades son inmediatas:

1. $(F+G)^{\varphi^n} = F^{\varphi^n} + G^{\varphi^n}$,
2. $F(H_1,\dots,H_n)^{\varphi^n} = F^{\varphi^n}(H_1^{\varphi^n},\dots,H_N^{\varphi^n})$,
3. Si F es una ley de grupo formal sobre $\mathcal{O}_L$ entonces F^{φ^n} también lo es.

Definición 2.2.7. *Dado $u \in \mathcal{O}_L^\times$ definimos el conjunto $\Theta_u^L := \{\theta \in \mathcal{O}_L \ : \ \theta^\varphi = u\theta\}$. Así mismo se define $\Theta_u^{L,\times} := \Theta_u^L \cap \mathcal{O}_L^\times$.*

Observación 2.2.8. Θ_u^L es un grupo aditivo pues dados $\theta,\theta' \in \Theta_u^L$ tenemos que $(\theta+\theta')^\varphi = \theta^\varphi + \theta'^\varphi = u\theta + u\theta'$. Además, dados $u,v \in \mathcal{O}_L^\times$, si tomamos $\theta \in \Theta_u^L, \theta' \in \Theta_v^L$ entonces $\theta\theta' \in \Theta_{uv}^L$. Por último, observar que $\mathcal{O}_k \subset \Theta_1^L$. ■

Definición 2.2.9. (Serie de Frobenius). *Sea π un parámetro de uniformización de L. Diremos que una serie de potencias $f \in \mathcal{O}_L[[X]]$ es una serie de potencias de Frobenius para π si verifica las siguientes condiciones:*

1. $f(X) \equiv \pi X \pmod{\mathtt{deg}2}$,
2. $f(X) \equiv X^q \pmod{\mathcal{O}_L[[X]]\mathfrak{p}_L}$.

Ejemplo 2.2.10. Dado $\pi \in L$ siempre podemos considerar la serie de potencias de Frobenius $f = \pi X + X^q$. Si $L = k = \mathbb{Q}_p$, podemos tomar $\pi = p$ como parámetro de uniformización y en este caso hay otra serie de Frobenius natural definida por $f_p = (1+X)^p - 1 = pX + \binom{p}{2}X^2 + \cdots + pX^{p-1} + X^p$. ■

Lema 2.2.11. ([Yos08], Lemma 3.4). Sean π,π' parámetros de uniformización de L y sean $f,f' \in \mathcal{O}_L[[X]]$ series de potencias de Frobenius para π y π' respectivamente. Supongamos que tenemos $\theta_1,\dots,\theta_n \in \Theta_{\pi/\pi'}^L$. Entonces existe una única serie de potencias $F \in \mathcal{O}_L[[X_1,\dots,X_n]]$ verificando las siguientes condiciones:

$$F \equiv \theta_1 X_1 + \cdots + \theta_n X_n \pmod{\mathtt{deg}2}, \qquad f' \circ F = F^\varphi \circ f.$$

Gracias a este resultado podemos asociar una ley de grupo formal a cada serie de potencias de Frobenius asociada a un parámetro de uniformización. También nos permitirá interpretar los grupos Θ_u^L como conjuntos de homomorfismos entre leyes de grupo formal. Concretamente, se verifica la

Proposición 2.2.12. ([Yos08], Proposition 3.5). Sean $f, f' \in \mathcal{O}_L[[X]]$ series de potencias de Frobenius asociadas a parámetros de uniformización π, π' respectivamente.

1. Existe una única ley de grupo formal F_f sobre $\mathcal{O}_L$ tal que $f \in \mathtt{Hom}_{\mathcal{O}_L}(F_f, F_f^{\varphi})$. Diremos que F_f es el *grupo de Lubin-Tate* asociado a f.

2. Existe una única aplicación inyectiva $[\cdot]_{f,f'} : \Theta^L_{\pi/\pi'} \to (X) \subset \mathcal{O}_L[[X]]$ tal que:

$$[\theta]_{f,f'}(X) \equiv \theta X \pmod{\mathtt{deg}2}, \qquad f' \circ [\theta]_{f,f'} = [\theta]^{\varphi}_{f,f'} \circ f.$$

   Además tiene las siguientes propiedades: $[\theta]_{f,f'} +_{F_{f'}} [\theta']_{f,f'} = [\theta + \theta']_{f,f'}$ $\forall \theta, \theta' \in \Theta^L_{\pi/\pi'}$ y $[\theta']_{f',f''} \circ [\theta]_{f,f'} = [\theta\theta']_{f,f''}$ $\forall \theta \in \Theta^L_{\pi/\pi'}, \theta' \in \Theta^L_{\pi'/\pi''}$ con π'' otro parámetro de uniformización de L y f'' una de serie de Frobenius asociada.

3. Tenemos que $[\theta]_{f,f'} \in \mathtt{Hom}_{\mathcal{O}_L}(F_f, F_{f'})$ para todo $\theta \in \Theta^L_{\pi/\pi'}$.

Corolario 2.2.13. 1. La aplicación $[\cdot]_f := [\cdot]_{f,f} : \mathcal{O}_k \to \mathtt{End}_{\mathcal{O}_L}(F_f)$ es un homomorfismo de anillos inyectivo. Por esta razón diremos que $(F_f, [\cdot]_f)$ es un *$\mathcal{O}_k$-módulo formal*.

2. Si $\theta \in \Theta^{L,\times}_{\pi/\pi'}$ entonces $[\theta]_{f,f'}$ es un isomorfismo y $[\theta]^{-1}_{f,f'} = [\theta^{-1}]_{f',f}$.

Ejemplo 2.2.14. ($\mathbb{G}_m$ como Grupo de Lubin-Tate asociado a f_p). Gracias a las igualdades $\mathbb{G}_m(f_p(X), f_p(Y)) = (1+X)^p(1+Y)^p - 1 = f_p(\mathbb{G}_m(X,Y))$ vemos que f_p es un endomorfismo de $\mathbb{G}_m$ y gracias a la unicidad de 2.2.12.1 tenemos que $F_{f_p} = \mathbb{G}_m$. Es fácil comprobar que dado $a \in \mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p}$ tenemos que $[a]_f = (1+X)^a - 1$, donde $(1+X)^a = \sum_{m \geq 0} \binom{a}{m} X^m$ siendo $\binom{a}{m} = \frac{a(a-1)\cdots(a-m+1)}{m(m-1)\cdots 1}$ con $a \in \mathbb{Z}_p$. La definición de los coeficientes binomiales sólo usa las operaciones (continuas) del grupo topológico de manera que podemos extender la definición por continuidad. Para demostrar que $[a]_f = (1+X)^a - 1$ se comprueba para $a \in \mathbb{Z}$ y automáticamente por continuidad se tiene para $a \in \mathbb{Z}_p$ de modo que basta invocar la unicidad. ■

Observación 2.2.15. Notar que $\mathcal{O}_k^{\times} \subset \mathcal{O}_k \subset \Theta_1^L$ y por tanto, dado un parámetro de uniformización π de L y dos series de potencias de Frobenius $f, f' \in \mathcal{O}_L[[X]]$ para π, sabemos que F_f y $F_{f'}$ son leyes de grupo formal isomorfas. Por tanto, salvo isomorfismo, a cada parámetro de uniformización le estamos asociando una única ley de grupo formal. Así mismo, observar que los grupos Θ_u^L pueden tener un comportamiento muy dispar, por ejemplo, $\Theta_u^k = \emptyset$ si $u \in \mathcal{O}_k^{\times} \setminus \{1\}$ y para $u = 1$ tenemos $\mathcal{O}_k \subset \Theta_1^k$. Nos interesará conocer estos grupos. ■

Observación 2.2.16. **1.** Tenemos que $\pi \in \Theta^L_{\pi^\varphi/\pi}$ y $[\pi]_{f,f^\varphi} : F_f \to F_f^\varphi$ coincide con f, siendo f una serie de potencias de Frobenius de π.

2. Se tiene que $F_f^\varphi = F_{f^\varphi}$ y $[\theta]^\varphi_{f,f'} = [\theta^\varphi]_{f^\varphi,f'^\varphi}$.

3. Definimos $f_m := f^{\varphi^{m-1}} \circ \cdots \circ f^\varphi \circ f \in \mathcal{O}_k[[X]]$ para $m \geq 1$ y establecemos $f_0(X) := X$. Gracias a las propiedades anteriores tenemos que $f_m = [\pi_m]_{f,f^{\varphi^m}}$, con $\pi_m \in \mathcal{O}_L$ definido por $\pi_m := \prod_{t=0}^{m-1} \pi^{\varphi^t}$, $\pi_0 = 1$. La idea subyacente a esta definición es obtener algo similar a una norma "truncada" de π respecto al Frobenius de k, razón por la que no se define f_m como la composición m-veces de f consigo misma. Por ejemplo, cuando $L = k_n$ es la extensión finita no ramificada de k de grado n, es $\pi_n = \mathtt{N}_{k_n|k}(\pi)$ pues $\mathtt{Gal}(k_n|k) = \langle \varphi_{|k_n} \rangle \simeq \mathbb{Z}/\mathbb{Z}n$.

■

2.3. Extensiones de Lubin-Tate y Aplicaciones de Artin

Extensiones de Lubin-Tate

Como antes, consideramos una extensión no ramificada completa $L \supset k$.

Definición 2.3.1. (Polinomio de Frobenius, Extensiones y Módulos de Lubin-Tate). *Sea $f \in \mathcal{O}_L[X]$ un polinomio mónico que además es una serie de Frobenius para un parámetro de uniformización π de L, que llamaremos polinomio de Frobenius para π. Para $m \geq 1$ denotamos por L_f^m al cuerpo de descomposición de $f_m \in \mathcal{O}_L[X]$ sobre L, y definimos $\mu_{f,m} := \{\alpha \in L_f^m \ : \ f_m(\alpha) = 0\}$, $\mu^\times_{f,m} := \mu_{f,m} \setminus \mu_{f,m-1}$. (Ver 2.3.3)*

Ejemplo 2.3.2. Cuando $L = k = \mathbb{Q}_p$, el polinomio $f_p := (1-X)^p - 1 \in \mathcal{O}_k[X]$ y tenemos que $(f_p)_m = (1+X)^{p^m} - 1$. En este caso $\mu_{f_p,m} = \{\alpha \in \mathbb{Q}_p^{\mathtt{sep}} | (1+\alpha)^{p^m} = 1\}$. Obviamente, el conjunto $\mu_{f_p,m}$ bajo el isomorfismo $a \mapsto 1 + a$ se corresponde con el conjunto de las raíces de la unidad p^m-ésimas, que denotamos por μ_{p^m}. Además, $[p]_{f_p} = f_p$ de modo que los elementos de $\mu_{f_p,m}$ son los puntos de p^m-torsión. Esta idea es la que da pie a la analogía entre curvas elípticas y leyes de grupo formal y que motiva, en cierto sentido, la introducción de los últimos. ■

Observación 2.3.3. Al suponer que el polinomio f es mónico y es una serie de potencias de Frobenius para π estamos obligados a que sea $\mathtt{deg}(f) = q$. De hecho, tenemos que $f(X) = \pi X + \cdots + X^q$, con los coeficientes de las potencias $n \neq q$ elementos del ideal $\mathfrak{p}_L$. En particular, cada uno de estos polinomios divididos por X es $\mathfrak{p}_L$-Eisenstein, luego irreducible y separable sobre L. El más sencillo de los polinomios de Frobenius es $\pi X + X^q$. También observar que $f_m = f^{\varphi^{m-1}} \circ f_{m-1}$ y como $X|f$ llegamos a que $f_{m-1}|f_m$. El coeficiente de grado 0 de f_m/f_{m-1} es $\pi^{\varphi^{m-1}}$.

En general, los polinomios f_m son separables sobre L. Podemos suponer que estamos trabajando en característica 0 y que nuestros cuerpos son extensiones del cuerpo $\mathbb{Q}_p$ de modo que no tenemos que preocuparnos por la separabilidad. Para el caso en que la característsitca del cuerpo es no nula, una demostración de la separabilidad de f_m se puede encontrar en [Yos08], Appendix II. ■

Lema 2.3.4. ([Yos08], Lemma 4.3). Sea $m \geq 1$ y $f \in \mathcal{O}_L[X]$ un polinomio de Frobenius para cierto π parámetro de uniformización de L. Se verifican los siguientes enunciados:

1. La extensión $L_f^m \supset L$ es separable y $\mu_{f,m} \subset \mathfrak{p}_{L_f^m}$. En particular, podemos sustituir los elementos de $\mu_{f,m}$ en series de potencias sobre $\mathcal{O}_L$ pues en ese caso el término general de la serie converge a 0 y esto es suficiente para obtener la convergencia de una serie en el contexto no arquimediano.

2. Dado $x \in k^\times$ con $\nu_k(x) = m$ y $\alpha \in \mathfrak{p}_{L^{\text{sep}}}$:

$$\alpha \in \mu_{f,m} \Leftrightarrow [x]_f(\alpha) = 0 \Leftrightarrow [a]_f(\alpha) = 0 \ (\forall\ a \in \mathfrak{p}_L^m).$$

Proposición 2.3.5. ([Yos08], Proposition 4.4). Sea $m \geq 1, \pi$ un parámetro de uniformización de L y $f \in \mathcal{O}_L[X]$ un polinomio de Frobenius para π.

1. El conjunto $\mu_{f,m}$ es un $\mathcal{O}_k$-módulo con suma $+_{F_f}$ y acción de $\mathcal{O}_k$ vía $[\cdot]_f$. Para cada $\alpha \in \mu_{f,m}^\times$ tenemos el siguiente isomorfismo de $\mathcal{O}_k$-módulos:

$$\begin{array}{ccc} \mathcal{O}_k/\mathfrak{p}_k^m & \longrightarrow & \mu_{f,m}, \\ a + \mathfrak{p}_k^m & \longmapsto & [a]_f(\alpha). \end{array}$$

2. Si $\alpha \in \mu_{f,m}^\times$ entonces $L_f^m = L(\alpha)$, $\mathtt{N}_{L_f^m|L}(-\alpha) = \pi^{\varphi^{m-1}}$ y α es un parámetro de uniformización de L_f^m. La extensión $L_f^m \supset L$ es una extensión de Galois totalmente ramificada de grado $|\mu_{f,m}^\times| = q^{m-1}(q-1)$.

3. Tenemos isomorfismos canónicos de grupos abelianos:

$$\begin{array}{rccc} \rho_{f,m}: & \mathtt{Gal}(L_f^m|L) & \longrightarrow & (\mathcal{O}_k/\mathfrak{p}_k^m)^\times, \\ & \sigma : \alpha \mapsto [u]_f(\alpha) & \longmapsto & u + \mathfrak{p}^m. \end{array}$$

Ejemplo 2.3.6. Como $\mu_{f_p,m} \simeq \mu_{p^m}$ y $\mu_{p^m} \sim \mathbb{Z}/\mathbb{Z}p^m$, dependiendo este último isomorfismo de la raíz primitiva p^m-ésima de la unidad elegida, vemos que el isomorfismo $\mu_{f_p,m} \sim \mathbb{Z}_p/\mathbb{Z}_p p^m \simeq \mathbb{Z}/\mathbb{Z}p^m$ depende de la raíz $\alpha \in \mu_{f_p,m}^\times$ elegida que se corresponde con la anterior elección de la raíz primitiva p^m-ésima de la unidad. Bajo el isomorfismo $(\mathbb{Z}_p p, +_{\mathbb{G}_m}) \overset{a\mapsto 1+a}{\longrightarrow} 1 + \mathbb{Z}_p p$ la acción

de $\mathbb{Z}_p$ se corresponde con la acción clásica de $\mathbb{Z}_p$ sobre $1+\mathbb{Z}_p p$ definida por exponenciación. En este caso, el cuerpo $(\mathbb{Q}_p)_{f_p}^m = \mathbb{Q}_p(\mu_{p^m})$, extensión totalmente ramificada de $\mathbb{Q}_p$. El isomorfismo $\mathtt{Gal}((\mathbb{Q}_p)_{f_p}^m|\mathbb{Q}_p) = \mathtt{Gal}(\mathbb{Q}_p(\mu_{p^m})|\mathbb{Q}_p) \to (\mathbb{Z}_p/\mathbb{Z}_p p^m)^\times \simeq (\mathbb{Z}/\mathbb{Z}p^m)^\times$ coincide con el isomorfismo usual de las extensiones ciclotómicas. ■

Observación 2.3.7. Podemos describir con más detalle la acción de $\mathcal{O}_k$ sobre $\mu_{f,m}$. En concreto, dado $\alpha \in \mu_{f,m}^\times$, *¿qué elementos* $a \in \mathcal{O}_k$ *verifican que* $[a]_f(\alpha) \in \mu_{f,t}^\times$*?* Gracias a 2.3.4.2 sabemos que $[a]_f(\alpha) \in \mu_{f,t}^\times$ si y sólo si para todo $x \in \mathfrak{p}_L^t$ es $[xa]_f(\alpha) = [x]_f([a]_f(\alpha)) = 0$ y existe $x_0 \in \mathfrak{p}_L^{t-1} \setminus \mathfrak{p}_L^t$ tal que $[x_0 a]_f(\alpha) = [x_0]_f([a]_f(\alpha)) \neq 0$. En este caso $ax_0 \notin \mathfrak{p}_L^m$, de modo que

$$m > \nu_L(ax_0) = \nu_L(a) + \nu_L(x_0) = \nu_k(a) + t - 1.$$

Por tanto, $\nu_k(a) < m-t+1$, es decir, $0 \leq \nu_k(a) \leq m-t$. Ahora bien, los conjuntos $\mu_{f,k}^\times$, $k = 0, \ldots, m$ son disjuntos de modo que debe ser $\nu_k(a) = m - t$. ■

Homomorfismo de Artin

Extendemos la definición de $\pi_j \in L^\times$ para valores negativos de $j \in \mathbb{Z}$. Con $j > 0$ definimos $\pi_{-j} := (\pi_j^{-1})^{\varphi^{-j}}$. De hecho, gracias a esta definición, tenemos que para todo $j \in \mathbb{Z}$ será $\pi_j = (\pi_{-j}^{-1})^{\varphi^j}$. La relación $\pi_{j+j'} = \pi_{j'+j}$ se cumple para todo $j, j' \in \mathbb{Z}$. Es claro que $\nu_L(\pi_j) = j$ para todo $j \in \mathbb{Z}$. Se verifica que $\pi_{j+j'} = {\pi_{j'}}^{\varphi^j} \pi_j$.

Lema 2.3.8. ([Yos08], Lemma 4.5). Sean π, π' parámetros de uniformización de L. Si $\theta \in \Theta_{\pi'/\pi}^L$, entonces $\theta^{\varphi^j}/\theta = \pi_j'/\pi_j$ para todo $j \in \mathbb{Z}$. Además, $\pi_j \in \Theta_{\pi^{\varphi^j}/\pi}^L$.

Lema 2.3.9. ([Yos08], Lemma 4.6). Sean $f, f' \in \mathcal{O}_L[X]$ polinomios de Frobenius para parámetros de uniformización π, π' de L. Si $\theta \in \Theta_{\pi'/\pi}^{L,\times}$ entonces para todo $m \geq 1$ tenemos que $[\theta]_{f,f'} : \mu_{f,m} \to \mu_{f',m}$ es un isomorfismo de $\mathcal{O}_k$-módulos y $L_f^m = L_{f'}^m$.

Si $L \supset k$ es una extensión finita, al ser $L_f^m \supset L$ una extensión totalmente ramificada y $L \supset k$ una extensión no ramificada sabemos que la subextensión no ramificada maximal de k dentro de L_f^m es L.

Proposición 2.3.10. ([Yos08], Proposition 4.7). Consideremos $m \geq 1$ y $f \in \mathcal{O}_L[X]$ un polinomio de Frobenius para un parámetro de uniformización π de L. Se verifican los siguientes enunciados:

1. Todo $\sigma \in \langle \varphi_{|L} \rangle \subset \mathtt{Aut}_k(L)$ admite exactamente $[L_f^m : L]$ extensiones a L_f^m. Además, fijado

$\alpha \in \mu_{f,m}^{\times}$, la siguiente aplicación es una biyección:

$$\begin{array}{rcl} k^{\times}/(1+\mathfrak{p}_k^m) & \longrightarrow & \coprod_{j\in\mathbb{Z}} \mu_{f^{\varphi^j},m}^{\times}, \\ x(1+\mathfrak{p}_k^m) \ : \ \nu_k(x) = -j & \longmapsto & [x\pi_j]_{f,f^{\varphi^j}}(\alpha). \end{array}$$

2. Sea $L = \hat{k}^{\mathtt{ur}}$ la compleción de la extensión no ramificada maximal de k. Los homomorfismos $\rho_{f,m}$ de 2.3.5.3 podemos extenderlos a los siguientes isomorfismos:

$$\begin{array}{rccl} \rho_{f,m}: & \mathtt{W}((\hat{k}^{\mathtt{ur}})_f^m|k) & \longrightarrow & k^{\times}/(1+\mathfrak{p}_k^m), \\ & \sigma \ : \ \sigma_{|\hat{k}^{\mathtt{ur}}}=\varphi^j \ \wedge & & \\ & \sigma(\alpha)=[x\pi_j]_{f,f^{\varphi^j}}(\alpha) \quad \forall \alpha\in\mu_{f,m} & \longmapsto & x(1+\mathfrak{p}_k^m). \end{array}$$

Si definimos $(\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}} := \cup_{m\geq 1}(\hat{k}^{\mathtt{ur}})_f^m$, haciendo el límite proyectivo obtenemos el isomorfismo $\rho_f : \mathtt{W}((\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}}|k) \to k^{\times}$.

Nota: Los grupos de Weil que aparecen en el segundo apartado son respecto a la extensión continua del elemento de Frobenius a $\hat{k}^{\mathtt{ur}}$. Todas las definiciones son análogas a las vistas en los preliminares. Ver 2.3.13 para comprobar que no hay demasiado por lo que preocuparse.

Denotamos por $\hat{\mathcal{O}}_{k^{\mathtt{ur}}}$ al anillo de valoración de la compleción $\hat{k}^{\mathtt{ur}}$:

Lema 2.3.11. ([Yos08], Proposition 4.8). El homomorfismo $\psi : \hat{\mathcal{O}}_{k^{\mathtt{ur}}}^{\times} \to \hat{\mathcal{O}}_{k^{\mathtt{ur}}}^{\times}$ que hace $\theta \mapsto \theta^{\varphi}/\theta$ es sobreyectivo. En particular, para todo par de parámetros de uniformización π, π' de $\hat{k}^{\mathtt{ur}}$ tenemos que $\Theta_{\pi'/\pi}^{\hat{k}^{\mathtt{ur}},\times} \neq \emptyset$.

Gracias a este último lema deducimos que las extensiones construidas y los homomorfismos son independientes de f :

Corolario 2.3.12. ([Yos08], Corollary 4.9). Las extensiones $(\hat{k}^{\mathtt{ur}})_f^m$ y los homomorfismos $\rho_{f,m}$ de 2.3.10.2 no dependen de f. En particular, $(\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}}, \rho_f$ tampoco dependen de f.

El siguiente es un lema de carácter técnico que nos permitirá eliminar la compleción de los resultados anteriores:

Lema 2.3.13. ([GC], Lema 5.3.9, Capítulo 5). Consideremos la cadena de extensiones $E \supset F \supset k$, y denotemos por $\widehat{F}, \widehat{E}$ las respectivas compleciones. Se verifican las siguientes propiedades:

1. Si $E \supset F$ es una extensión finita entonces $E\widehat{F} = \widehat{E}$.

2. Si $E \supset F$ es finita de Galois, entonces también lo es $\widehat{E} \supset \widehat{F}$ y la siguiente aplicación es un isomorfismo de grupos:
$$\begin{array}{ccc} \mathtt{Gal}(\widehat{E}|\widehat{F}) & \longrightarrow & \mathtt{Gal}(E|F), \\ \sigma & \longmapsto & \sigma_{|E}. \end{array}$$

3. Si la extensión $E \supset F$ es separable, entonces $E \cap \widehat{F} = F$.

Usando este último lema podemos hacer la siguiente definición:

Definición 2.3.14. *Supongamos que $L \supset k$ es una extensión finita no ramificada. Sea $f \in \mathcal{O}_L[X]$ un polinomio de Frobenius asociado a un parámetro de uniformización π de L. Definimos $k_f^m := k^{\mathtt{ur}} L_f^m$. Por definición, k_f^m no depende de L. Sabemos que la extensión $k_f^m \supset k$ es de Galois. Así mismo, la compleción de k_f^m es $\hat{k}^{\mathtt{ur}} L_f^m = (\hat{k}^{\mathtt{ur}})_f^m$ y $k_f^m = (\hat{k}_f^m) \cap k^{\mathtt{sep}}$, luego k_f^m también es independiente de f. Definiendo $k_f^{\mathtt{LT}} := \cup_{m \geq 1} k_f^m = (\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}} \cap k^{\mathtt{sep}}$, sabemos que $\mathtt{W}(k_f^{\mathtt{LT}}|k) \simeq \mathtt{W}((\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}}|k)$. Diremos que toda extensión finita de k contenida en $k_f^{\mathtt{LT}}$ es una subextensión finita de Lubin-Tate. Al inverso de $\rho_f : \mathtt{W}(k_f^{\mathtt{LT}}|k) \to k^\times$ lo llamamos Homomorfismo de Artin y lo denotaremos por $\mathtt{Art}_k : k^\times \to \mathtt{W}(k_f^{\mathtt{LT}}|k)$. Es claro que $\nu \circ \mathtt{Art}_k = -\nu_k$.*

A pesar de la independencia respecto a f de las extensiones y homomorfismos anteriores, usualmente nos convendrá mantener el subíndice f para ganar claridad en las demostraciones.

Resumen de la Teoría de Lubin-Tate

Ya podemos entender el esquema general de la demostración usando la teoría de Lubin-Tate. Nuestro objetivo es obtener la teoría de cuerpos de clase para la extensión abeliana maximal $k^{\mathtt{ab}}$. En lugar de obtener los teoremas para $k^{\mathtt{ab}}$ nosotros los vamos a demostrar para la *extensión maximal de Lubin-Tate de k*, que hemos denotado por $k^{\mathtt{LT}}$. Posteriormente, demostraremos que en realidad $k^{\mathtt{LT}} = k^{\mathtt{ab}}$ pero este resultado no será necesario a la hora de demostrar que podemos hacer teoría de cuerpos de clase con $k^{\mathtt{LT}}$.

Es importante entender cómo hemos obtenido la extensión $k^{\mathtt{LT}}$ a partir de k. Para ello, dada una extensión no ramificada completa $L \supset k$, por medio de las leyes de grupo formal, hemos conseguido obtener una noción de morfismo entre los elementos de $\nu_L^{-1}(1)$, proceso que se asemeja a "categorificar" dicho conjunto. En realidad, los morfismos son entre las series de potencias de Frobenius f asociadas a los parámetros de uniformización, aunque sabemos que dos series de potencias de Frobenius para un mismo parámetro de uniformización son isomorfas (lo que nos permite abusar del lenguaje y hablar sencillamente de parámetros de uniformización). Para ser precisos, antes hacemos una primera simplificación de la teoría: **No** estudiamos toda la categoría de las series de potencias de Frobenius y los homomorfismos entre las leyes de grupo formal asociadas, sino que nos centramos

en los morfismos que proceden de los grupos abelianos Θ_u^L. Reducidos los conjuntos de morfismos, el siguiente paso ha sido restringirnos a los polinomios de Frobenius f de modo que hemos podido considerar las raíces de éstos y obtener los llamados módulos de Lubin-Tate $\mu_{f,m}$.

El último paso ha sido adjuntar estas raíces al cuerpo base L y obtener las extensiones de Lubin-Tate L_f^m, con un control total de sus grupos de Galois sobre L si $L \supset k$ es finita y sabiendo que, en general, respecto al elemento de Frobenius tienen un buen comportamiento (número de posibles extensiones). Como los morfismos que proceden de los grupos abelianos $\Theta_u^{L,\times} \subset \Theta_u^L$ inducen isomorfismos entre los módulos de Lubin-Tate y además son series de potencias, concluimos que las extensiones de Frobenius son un invariante de la clase de isomorfía de f (2.3.9)

Para concluir nuestro estudio, hemos visto que cuando llegamos a la mayor extensión no ramificada completa $L \supset k$ posible, a saber $L = \hat{k}^{\mathtt{ur}}$, todos los polinomios de Frobenius f son isomorfos y obtenemos cuerpos de Lubin-Tate sobre $\hat{k}^{\mathtt{ur}}$ independientes de f. De esta forma, intersecando estas extensiones con $k^{\mathtt{sep}}$ conseguimos obtener una extensión algebraica separable (es decir, eliminamos la compleción) que es nuestro cuerpo candidato sobre el que probar los resultados de la teoría de cuerpos de clase.

Observación 2.3.15. Si hubiéramos incluido en nuestro estudio todas las series de Frobenius en general, el lema de Preparación de Weierstrass nos habría servido para ver que podemos considerar el caso de polinomios sin perder módulos de Lubin-Tate ya que nos garantiza que los ceros de cualquiera de dichas series serían ceros de algún polinomio de Frobenius.

Por otro lado, nosotros no hemos prestado demasiada atención a los grupos de homomorfismos entre las leyes de grupo formal de Lubin-Tate. Para estudiar estos grupos con más detalle habría hecho falta tener información de la clasificación de las leyes de grupo formal usando invariantes como la altura de un grupo formal. En nuestro caso no es necesario ese nivel de conocimiento, nos basta con saber que eventualmente todas las leyes de grupo son isomorfas y saber cuándo esos isomorfismos se dan sobre una extensión finita no ramificada como hacemos en 2.4.2. Dicho esto, hay que admitir que esta información no se debe omitir si se quieren obtener resultados más fuertes y susceptibles de tener una generalización. ■

2.4. Grupos de Galois, Grupos de Normas y Cambio de Base

Grupos de Galois

Denotaremos por k_n a la extensión finita no ramificada de k de grado n.

Lema 2.4.1. ([Yos08], Lemma 5.2).

1. Con $n \geq 1$, el cuerpo fijo de φ^n en $\hat{k}^{\mathtt{ur}}$ es k_n.

2. La norma $\mathtt{N}_{k_n|k}$ es sobreyectiva sobre el conjunto $\nu_k^{-1}(\mathbb{Z}n) \subset k^\times$.

Proposición 2.4.2. ([Yos08], Proposition 5.1). Sean π, π' parámetros de uniformización de k_n y $\theta \in \Theta^{\hat{k}^{\mathtt{ur}},\times}_{\pi'/\pi}$. Entonces $\theta \in \Theta^{k_n,\times}_{\pi'/\pi}$ si y sólo si $\mathtt{N}_{k_n|k}(\pi) = \mathtt{N}_{k_n|k}(\pi')$.

Observación 2.4.3. Gracias a este resultado vemos que, dado $x \in k^\times$ con $\nu_k(x) = n > 0$, si consideramos la extensión $k_n \supset k$, las extensiones $(k_n)^m_f$ sólo dependen de los conjuntos (no vacíos por 2.4.1.2) $\{\pi \in k_n \mid \nu_{k_n}(\pi) = 1 \text{ y } \mathtt{N}_{k_n|k}(\pi) = x\}$, pues para un mismo parámetro de uniformización considerar distintos polinomios de Frobenius da lugar a leyes de grupo formal isomorfas y gracias a 2.4.2, si tomamos distintos parámetros de uniformización con la misma norma sobre k entonces existe un isomorfismo entre las leyes de grupo formal asociadas a cualesquiera que sean polinomios de Frobenius asociados. ■

El siguiente resultado ya nos acerca a la teoría de cuerpos de clase:

Proposición 2.4.4. ([Yos08], Proposition 5.4). Sea $x \in k^\times$ con $\nu_k(x) = n > 0$, $\pi \in k_n$ parámetro de uniformización con $\mathtt{N}_{k_n|k}(\pi) = x$ y $f \in \mathcal{O}_{k_n}[X]$ un polinomio de Frobenius asociado a π. El elemento $\sigma := \mathtt{Art}_k\left(\mathtt{N}_{k_n|k}(\pi)\right) \in \mathtt{W}(k_f^{\mathtt{LT}}|k)$ se caracteriza por las siguientes condiciones:

$$\nu(\sigma) = -\nu_k(x) = -n, \ \sigma_{|(k_n)^m_f} = \mathtt{id} \ \forall m \geq 1.$$

Además, para todo $m \geq 1$, el homomorfismo de Artin induce un isomorfismo

$$\frac{k^\times}{(1+\mathfrak{p}_k^m) \times \langle x \rangle} \longrightarrow \mathtt{Gal}((k_n)^m_f|k).$$

Operador Norma de Coleman y Grupos de Normas

Operador Norma de Coleman

Ya hemos visto que el homomorfismo de Artin está íntimamente relacionado con el conocimiento de los subgrupos de normas de $k^\times$. Para poder estudiar con detalle la norma de extensiones totalmente ramificadas como las que hemos construido, necesitamos el operador norma de Coleman. Informalmente, podemos decir que el operador norma es una representación de la norma como serie de potencias.

Fijemos de nuevo el contexto: $k_n \supset k$ extensión finita no ramificada de grado n, π parámetro de uniformización de k_n, $f \in \mathcal{O}_{k_n}[X]$ polinomio de Frobenius para π. Para la construcción de dicho operador hace falta el siguiente lema sobre series de potencias:

Lema 2.4.5. ([Yos08], Lemma 5.5.iii). Sea $g \in \mathcal{O}_{k_n}[[X]]$. Si $g(X +_{F_f} \alpha) = g(X)$ para todo $\alpha \in \mu_{f,1}$, entonces $g = h \circ f$ para una única serie $h \in \mathcal{O}_{k_n}[[X]]$.

Dada $g \in \mathcal{O}_{k_n}[[X]]$, tenemos que los coeficientes del producto $\prod_{\alpha\in\mu_{f,1}} g(X +_{F_f} \alpha)$ son polinomios con coeficientes en $\mathcal{O}_{k_n}$ en las funciones simétricas de $\mu_{f,1}$, de modo que de nuevo vuelven a estar en $\mathcal{O}_{k_n}$ como se comprueba al aplicar todos los elementos de $\mathtt{Gal}((k_n)_f^1|k_n)$ a dichos coeficientes. Notar que dicho producto verifica las condiciones de 2.4.5 y por ello existe un único $\mathtt{N}_f(g) \in \mathcal{O}_L[[X]]$ verificando:

$$(\mathtt{N}_f(g) \circ f)(X) = \prod_{\alpha\in\mu_{f,1}} g(X +_{F_f} \alpha).$$

Por construcción, tenemos que $\mathtt{N}_f(g_1g_2) = \mathtt{N}_f(g_1)\mathtt{N}_f(g_2)$. Por otro lado, definimos $\mathtt{N}_f^0(g) := g$ y

$$\mathtt{N}_f^m(g) := \left(\mathtt{N}_f^{m-1}\left(\mathtt{N}_f(g)^{\varphi^{-1}}\right)\right)^{\varphi}, \quad m \geq 1.$$

Estas iteraciones se comprenden mejor gracias a la igualdad $\mathtt{N}_f^m = \mathtt{N}_{f^{\varphi^{m-1}}} \circ \cdots \circ \mathtt{N}_{f^\varphi} \circ \mathtt{N}_f$. (Ver [GC] para la demostración).

El operador norma tiene las siguientes propiedades:

Lema 2.4.6. ([Yos08], Lemmas 5.7,5.8).

1. Para todo $m \geq 1$ tenemos que $(\mathtt{N}_f^m(g) \circ f_m)(X) = \prod_{\alpha\in\mu_{f,m}} g(X +_{F_f} \alpha)$.
2. $\mathtt{N}_f(g) \equiv g^\varphi \pmod{\mathfrak{p}_L}$. En particular, $\mathtt{N}_f\left(\mathcal{O}_L[[X]]^\times\right) \subset \mathcal{O}_L[[X]]^\times$.
3. Para todo $m \geq 1$, si $g \equiv 1 \pmod{\mathfrak{p}_L^m}$ entonces $\mathtt{N}_f(g) \equiv 1 \pmod{\mathfrak{p}_L^m}$.
4. Si $g \in \mathcal{O}_L[[X]]^\times$ y $m \geq 1$ entonces $\mathtt{N}_f^m(g)/\mathtt{N}_f^{m-1}(g)^\varphi \equiv 1 \pmod{\mathfrak{p}_L^m}$.

Grupos de Normas

La introducción del operador norma se hace para poder demostrar la

Proposición 2.4.7. Sea $x \in k^\times$ con $\nu_k(x) = n > 0$. Sea $\pi \in k_n$ con $\mathtt{N}_{k_n|k}(\pi) = x$ y $f \in \mathcal{O}_{k_n}[X]$ un polinomio de Frobenius de π. Entonces, $\mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\times}) = (1 + \mathfrak{p}_k^m) \times \langle \mathtt{N}_{k_n|k}(\pi)\rangle$ para todo $m \geq 1$.

Demostración. Sea $\alpha \in \mu_{f,m}^\times$. En virtud de 2.3.5.2 sabemos que α es un parámetro de uniformización de $(k_n)_f^m$ verificando $(k_n)_f^m = k_n(\alpha)$. Por ser parámetro de uniformización tenemos $k_n(\alpha)^\times =$

$\mathcal{O}_{k_n(\alpha)}^{\times} \times \langle -\alpha \rangle$. Además, también por 2.3.5.2, sabemos que

$$\mathtt{N}_{k_n(\alpha)|k}(-\alpha) = \mathtt{N}_{k_n|k}(\mathtt{N}_{k_n(\alpha)|k_n}(-\alpha)) = \mathtt{N}_{k_n|k}(\pi^{\varphi^{m-1}}) = x.$$

Deducimos que es suficiente demostrar $\mathtt{N}_{k_n(\alpha)|k}(\mathcal{O}_{k_n(\alpha)}^{\times}) = 1 + \mathfrak{p}_k^m$.

$\mathtt{N}_{k_n(\alpha)|k}(\mathcal{O}_{k_n(\alpha)}^{\times}) \subset 1 + \mathfrak{p}_k^m$: Gracias a 1.3.5 tenemos que $\mathcal{O}_{k_n(\alpha)} = \mathcal{O}_{k_n}[\alpha]$ de modo que todo elemento $u \in \mathcal{O}_{k_n(\alpha)}^{\times}$ podemos escribirlo como $u = g(\alpha)$ para cierto polinomio $g \in \mathcal{O}_{k_n}[X]$. Como u es una unidad, $g(0) \neq 0$ pues en caso contrario α dividiría a u y $u \in \mathfrak{p}_{k_n(\alpha)}$. Deducimos que g, visto como elemento de $\mathcal{O}_{k_n(\alpha)}[[X]]$, es una unidad, i.e., $g \in \mathcal{O}_{k_n(\alpha)}[[X]]^{\times}$. Para $i \geq 0$ definimos $u_i := \mathtt{N}_f^i(g)(0)$. Gracias a 2.4.7.1 tenemos las expresiones $u_i = \prod_{\alpha \in \mu_{f,i}} g(\alpha)$, de modo que

$$\begin{aligned}\mathtt{N}_{k_n(\alpha)|k_n}(u) &= \prod_{\sigma \in \mathtt{Gal}(k_n(\alpha)|k_n)} \sigma(g(\alpha)) = \prod_{\sigma \in \mathtt{Gal}(k_n(\alpha)|k_n)} g(\sigma\alpha) \\ &= \prod_{\beta \in \mu_{f,m}^{\times}} g(\beta) = u_m/u_{m-1}.\end{aligned}$$

Gracias a 2.4.7.4 $u_m/u_{m-1}^{\varphi} \in 1 + \mathfrak{p}_{k_n}^m$. Concluimos que

$$\begin{aligned}\mathtt{N}_{k_n(\alpha)|k}(u) &= \mathtt{N}_{k_n|k}\left(\mathtt{N}_{k_n(\alpha)|k_n}(u)\right) = \mathtt{N}_{k_n|k}(u_m/u_{m-1}) \\ &= \mathtt{N}_{k_n|k}(u_m)\mathtt{N}_{k_n|k}(u_{m-1})^{-1} = \mathtt{N}_{k_n|k}(u_m)\mathtt{N}_{k_n|k}(u_{m-1}^{\varphi})^{-1} \\ &= \mathtt{N}_{k_n|k}(u_m/u_{m-1}^{\varphi}) \in \mathtt{N}_{k_n|k}(1 + \mathfrak{p}_{k_n}^m) \subset 1 + \mathfrak{p}_k^m.\end{aligned}$$

$\mathtt{N}_{k_n(\alpha)|k}(\mathcal{O}_{k_n(\alpha)}^{\times}) \supset 1 + \mathfrak{p}_k^m$: Gracias a 2.4.4 tenemos el isomorfismo

$$\begin{aligned}\frac{k^{\times}}{(1 + \mathfrak{p}_k^m) \times \langle \mathtt{N}_{k_n|k}(\pi) \rangle} &\longrightarrow \mathtt{Gal}((k_n)_f^m|k), \\ a\left((1 + \mathfrak{p}_k^m) \times \langle \mathtt{N}_{k_n|k}(\pi) \rangle\right) &\longmapsto \mathtt{Art}_k(a)_{|(k_n)_f^m}.\end{aligned}$$

Es decir, $(k_n)_f^m$ es el cuerpo fijo del subgrupo $\mathtt{Art}_k\left((1 + \mathfrak{p}_k^m) \times \langle \mathtt{N}_{k_n|k}(\pi) \rangle\right)$. Si $x'/x \in 1 + \mathfrak{p}_k^m$ para algún $x' \in k$ entonces $(1 + \mathfrak{p}_k^m) \times \langle x \rangle = (1 + \mathfrak{p}_k^m) \times \langle x' \rangle$ de modo que $(k_n)_f^m = (k_n)_{f'}^m$ con f' polinomio de Frobenius asociado a π' con $\mathtt{N}_{k_n|k}(\pi') = x'$. En particular, x' es la norma de algún elemento de $(k_n)_f^m$. Concluimos con la inclusión buscada pues para todo $u \in 1 + \mathfrak{p}_k^m$ es $(ux)/x \in 1 + \mathfrak{p}_k^m$ de modo que $u = (ux)/x \in \mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\times})$ y llegamos a la inclusión $1 + \mathfrak{p}_k^m \subset \mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\times})$, es decir, $1 + \mathfrak{p}_k^m \subset \mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\times}) \cap \mathcal{O}_k^{\times} = \mathtt{N}_{(k_n)_f^m|k}(\mathcal{O}_{(k_n)_f^m}^{\times})$.

□

Proposición 2.4.8. ([Yos08], Corollary 5.12). Sea $x \in k^\times$ con $\nu_k(x) = n > 0$. Si $E \supset k_n$ es una extensión totalmente ramificada que contiene a $\cup_m (k_n)_f^m$, entonces

$$\bigcap_{\substack{k \subset F \subset E \\ k \subset F \text{ finita}}} \mathtt{N}_{F|k}(F^\times) = \langle x \rangle.$$

La demostración de 2.4.8 usa los siguientes resultados "topológicos":

Lema 2.4.9. ([Iwa86], Lemma 3.5). Sea K un cuerpo completo respecto una valoración discreta normalizada ν_K. Para toda extensión finita $L \supset K$ el subgrupo $\mathtt{N}_{L|K}(L^\times)$ es cerrado en $K^\times$.

Lema 2.4.10. ([GC], Lema 5.4.8, Capítulo 5). Sea K un cuerpo completo respecto a una valoración discreta normalizada ν_k y $E \supset K$ una extensión algebraica totalmente ramificada. Se verifica:

$$\nu_K^{-1}(1) \cap \bigcap_{\substack{K \subset F \subset E \\ K \subset F \text{ finita}}} \mathtt{N}_{F|K}(F^\times) \neq \emptyset.$$

Este último lema, aunque pueda parecer que no es de carácter topológico, usamos en su demostración la propiedad de intersección finita de los espacios topológicos compactos.

2.4.1. Cambio de Base y Teoría de Cuerpos de Clase

El conocimiento que tenemos de los subgrupos de normas para la extensiones $(k_n)_f^m \supset k$ lo usaremos como balizas para estudiar en general todas las extensiones de Lubin-Tate finitas, esto es, subextensiones finitas de $k \subset k^{\mathtt{LT}}$. Antes de continuar, veamos que $k^{\mathtt{LT}} \supset k$ es una extensión abeliana. Sabemos que la extensión es de Galois por los resultados probados anteriormente. Para ver que es abeliana, consideramos la siguiente aplicación:

$$\begin{array}{rccc} \mathcal{C}: & \mathtt{Gal}(k^{\mathtt{LT}}|k) \times \mathtt{Gal}(k^{\mathtt{LT}}|k) & \longrightarrow & \mathtt{Gal}(k^{\mathtt{LT}}|k), \\ & (\sigma, \tau) & \longmapsto & [\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}. \end{array}$$

Esta aplicación es continua pues en su definición únicamente intervienen las operaciones de grupo de $\mathtt{Gal}(k^{\mathtt{LT}}|k)$, que son continuas pues es un grupo topológico. Ahora bien, sabemos que $\mathtt{W}(k^{\mathtt{LT}}|k)$ es un subgrupo denso de $\mathtt{Gal}(k^{\mathtt{LT}}|k)$, de modo que $\mathtt{W}(k^{\mathtt{LT}}|k) \times \mathtt{W}(k^{\mathtt{LT}}|k)$ también es un subgrupo denso de $\mathtt{Gal}(k^{\mathtt{LT}}|k) \times \mathtt{Gal}(k^{\mathtt{LT}}|k)$. Además, el grupo de Weil $\mathtt{W}(k^{\mathtt{LT}}|k)$ es abeliano pues es isomorfo a $k^\times$ via el homomorfismo de Artin $\mathtt{Art}_k$, de modo que $\mathcal{C}_{|\mathtt{W}(k^{\mathtt{LT}}|k) \times \mathtt{W}(k^{\mathtt{LT}}|k)} = \mathtt{id}$. Como el conjunto

$\{\mathtt{id}\} \subset \mathtt{Gal}(k^{\mathtt{LT}}|k)$ es cerrado (por ejemplo, gracias a la disconexión total) sabemos que $\mathcal{C}^{-1}(\{\mathtt{id}\})$ es un cerrado que contiene al conjunto denso $\mathtt{W}(k^{\mathtt{LT}}|k) \times \mathtt{W}(k^{\mathtt{LT}}|k)$, concluimos que $\mathcal{C}^{-1}(\{\mathtt{id}\})$ coincide con todo el espacio y $\mathtt{Gal}(k^{\mathtt{LT}}|k)$ es un grupo abeliano.

En particular, para toda subextensión $k \subset F \subset k^{\mathtt{LT}}$ será $k \subset F$ una extensión de Galois.

Proposición 2.4.11. ([Yos08], Proposition 5.4). Dado $\sigma \in \mathtt{W}(k^{\mathtt{sep}}|k)$ con $-\nu(\sigma) = n > 0$ consideramos su cuerpo fijo en $k^{\mathtt{sep}}$ denotado por $(k^{\mathtt{sep}})^{\sigma}$. Entonces

$$\bigcap_{\substack{k \subset F \subset (k^{\mathtt{sep}})^{\sigma} \\ k \subset F \text{ finita}}} \mathtt{N}_{F|k}(F^{\times}) = \langle \mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}}) \rangle.$$

El **teorema del cambio de base** es el resultado esencial para poder obtener la teoría de cuerpos de clase sobre $k^{\mathtt{LT}}$. Lo demostramos con detalle (comparar la siguiente prueba con la correspondiente prueba de [Yos08]):

Teorema 2.4.12. (Teorema del Cambio de Base). Sea $k' \supset k$ una extensión finita separable. Se verifica:

1. $k^{\mathtt{LT}} \subset k'^{\mathtt{LT}}$,
2. Para todo $x' \in k'^{\times}$ tenemos $\mathtt{Art}_{k'}(x')_{|k^{LT}} = \mathtt{Art}_k(\mathtt{N}_{k'|k}(x'))$. Equivalentemente, el siguiente diagrama conmuta:

$$\begin{array}{ccc} k'^{\times} & \xrightarrow{\mathtt{Art}_{k'}} & \mathtt{Gal}(k'^{\mathtt{LT}}|k') \\ {\scriptstyle \mathtt{N}_{k'|k}}\downarrow & & \downarrow{\scriptstyle \mathtt{res}} \\ k^{\times} & \xrightarrow{\mathtt{Art}_k} & \mathtt{Gal}(k^{\mathtt{LT}}|k). \end{array}$$

Demostración. Sea $x' \in \mathfrak{p}_{k'}$ un elemento no nulo. Consideremos $\mathtt{Art}_{k'}(x') \in \mathtt{W}(k'^{\mathtt{LT}}|k')$ y sea $\sigma \in \mathtt{Gal}(k^{\mathtt{sep}}|k')$ una extensión arbitraria de $\mathtt{Art}_{k'}(x')$ a $k^{\mathtt{sep}} = k'^{\mathtt{sep}}$, que es posible gracias a que la extensión $k^{\mathtt{sep}} \supset k$ es de Galois. Claramente $\sigma \in \mathtt{W}(k^{\mathtt{sep}}|k')$. Como $k'^{\mathtt{ur}} = k^{\mathtt{ur}}k'$, tenemos

$$\sigma_{|k^{\mathtt{ur}}} = (\sigma_{|k'^{\mathtt{ur}}})_{|k^{\mathtt{ur}}} = (\varphi_{k'}^{-\nu_{k'}(x')})_{|k^{\mathtt{ur}}} = \varphi_k^{-\nu_{k'}(x')f(k'|k)}$$

siendo $\varphi_k, \varphi_{k'}$ el elemento de Frobenius de k, k' respectivamente y $f(k'|k)$ el grado residual de $k' \supset k$.

Deducimos que $\sigma \in \mathtt{W}(k^{\mathtt{sep}}|k)$, en particular, $\sigma_{|k^{\mathtt{LT}}} \in \mathtt{W}(k^{\mathtt{LT}}|k)$. Por otro lado tenemos:

$$\begin{aligned}\langle \mathtt{N}_{k'|k}(x')\rangle = \mathtt{N}_{k'|k}(\langle x'\rangle) &= \mathtt{N}_{k'|k}(\langle \mathtt{Art}_{k'}^{-1}(\sigma_{|k'^{\mathtt{LT}}})\rangle)\\ &\overset{2.4.11}{=} \mathtt{N}_{k'|k}\left(\bigcap_{\substack{k'\subset F'\subset (k^{\mathtt{sep}})^{\sigma}\\ k'\subset F' \text{ finita}}} \mathtt{N}_{F'|k'}(F'^{\times})\right)\\ &\subset \bigcap_{\substack{k\subset F\subset (k^{\mathtt{sep}})^{\sigma}\\ k\subset F \text{ finita}}} \mathtt{N}_{F|k}(F^{\times}) \overset{2.4.11}{=} \langle \mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}})\rangle.\end{aligned}$$

Para obtener la igualdad, observar que en el grupo cíclico $\langle \mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}})\rangle$ hay un único elemento con valoración igual a $\nu_k(\mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}})) = -\nu(\sigma_{|k^{\mathtt{LT}}}) \neq 0$, luego es suficiente probar que en el grupo cíclico $\langle \mathtt{N}_{k'|k}(x')\rangle$ también hay un elemento con dicha valoración. Las siguientes igualdades bastan para obtener la igualdad entre los grupos cíclicos:

$$-\nu(\sigma_{|k^{\mathtt{LT}}}) \overset{*}{=} f(k'|k)\cdot \nu_{k'}(x') = \nu_k(\mathtt{N}_{k'|k}(x')),$$

donde $*$ se tiene gracias a la igualdad $\sigma_{|k^{\mathtt{ur}}} = \varphi_k^{-f(k'|k)\nu_{k'}(x')}$. Observar que para nuestro razonamiento es esencial la hipótesis $\nu_{k'}(x') \neq 0$ y sólo en este caso nuestras conclusiones tienen validez.

Más aún, debido a la igualdad de los grupos cíclicos y a la igualdad de las valoraciones de los generadores, concluimos que $\mathtt{N}_{k'|k}(x') = \mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}})$, i.e., $\sigma_{|k^{\mathtt{LT}}} = \mathtt{Art}_k(\mathtt{N}_{k'|k}(x'))$. Deducimos que para todo $\sigma \in \mathtt{W}(k^{\mathtt{sep}}|k')$ extensión de $\mathtt{Art}_{k'}(x')$ es $\sigma_{|k^{\mathtt{LT}}} = (\mathtt{Art}_k \circ \mathtt{N}_{k'|k} \circ \mathtt{Art}_{k'}^{-1})(\sigma_{|k'^{\mathtt{LT}}})$.

En particular, para todo $\tau \in \mathtt{Gal}(k^{\mathtt{sep}}|k'^{\mathtt{LT}}) \subset \mathtt{W}(k^{\mathtt{sep}}|k')$, será $\sigma\tau$ una extensión a $k^{\mathtt{sep}}$ de $\mathtt{Art}_{k'}(x')$ y tenemos $(\sigma\tau)_{|k^{\mathtt{LT}}} = \mathtt{Art}_k(\mathtt{N}_{k'|k}(x')) = \sigma_{|k^{\mathtt{LT}}}$, es decir, $\tau_{|k^{\mathtt{LT}}} = \mathtt{id}$. Por tanto $k^{\mathtt{LT}} \subset (k^{\mathtt{sep}})^{\mathtt{Gal}(k^{\mathtt{sep}}|k'^{\mathtt{LT}})} = k'^{\mathtt{LT}}$. Podemos restringir $\sigma_{|k'^{\mathtt{LT}}}$ al subcuerpo $k^{\mathtt{LT}}$ y deducir la igualdad $\mathtt{Art}_{k'}(x')_{|k^{\mathtt{LT}}} = \mathtt{Art}_k(\mathtt{N}_{k'|k}(x'))$ para todo $x' \in \mathfrak{p}_{k'} \setminus \{0\}$. Por último, como los elementos no nulos de $\mathfrak{p}_{k'}$ generan al grupo de unidades $k'^{\times}$, haber probado la conmutatividad del diagrama sobre dichos elementos es suficiente para concluir que el diagrama es conmutativo sobre todo $k'^{\times}$.

□

Gracias al teorema del cambio de base, el resultado central de la teoría de cuerpos de clase local sobre $k^{\mathtt{LT}}$ no es más que un corolario:

Corolario 2.4.13. (Teoría de Cuerpos de Clase para $k^{\mathtt{LT}}$).

1. Existe un único homomorfismo $\mathtt{Art}_k : k^{\times} \to \mathtt{Gal}(k^{\mathtt{LT}}|k)$ verificando:

   a. Si π es un parámetro de uniformización de k entonces $\mathtt{Art}_k(\pi)_{|k^{\mathtt{ur}}} = \varphi^{-1}$,

b. Si $k \subset k'$ es una extensión de Lubin-Tate finita, entonces $\mathtt{Art}_{k'}(\mathtt{N}_{k'|k}(k'^{\times}))_{|k'} = \mathtt{id}$.

Además, $\mathtt{Art}_k$ es un isomorfismo sobre su imagen que coincide con el grupo de Weil $\mathtt{W}(k^{\mathtt{LT}}|k)$.

2. Si $k' \supset k$ es una extensión finita separable entonces $k^{\mathtt{LT}} \subset k'^{\mathtt{LT}}$ y $\mathtt{Art}_{k'}(x')_{|k^{\mathtt{LT}}} = \mathtt{Art}_k(\mathtt{N}_{k'|k}(x'))$ para todo $x' \in k'^{\times}$. Además, el homomorfismo de Artin $\mathtt{Art}_k$ induce un isomorfismo

$$\begin{array}{rccc} \mathtt{Art}_{k'|k}: & k^{\times}/\mathtt{N}_{k'|k}(k'^{\times}) & \longrightarrow & \mathtt{Gal}((k' \cap k^{LT})|k), \\ & x\mathtt{N}_{k'|k}(k'^{\times}) & \longmapsto & \mathtt{Art}_k(x)_{|(k' \cap k^{\mathtt{LT}})}. \end{array}$$

Demostración. 1. Claramente $\mathtt{Art}_k$ verifica (a) pues lo hemos construido de modo que $\nu \circ \mathtt{Art}_k = -\nu_k$. Así mismo, sabemos que $\mathtt{Art}_k$ verifica (b) gracias a 2.4.12. Recíprocamente, sea $\mathcal{F}$ un homomorfismo verificando (a) y (b). Sea π un parámetro de uniformización de k y $f \in \mathcal{O}_k[X]$ un polinomio de Frobenius para π, gracias a 2.3.5.2 sabemos que los cuerpos de Lubin-Tate asociados verifican que $(k_1)_f^m = k(\alpha)$ con $\alpha \in \mu_{f,m}^{\times}$ y $\mathtt{N}_{(k_1)_f^m|k}(-\alpha) = \pi^{\varphi^{m-1}} = \pi$. Como $\mathcal{F}$ verifica (b) entonces $\mathcal{F}(\pi)_{|(k_1)_f^m} = \mathcal{F}(\mathtt{N}_{k'|k}(-\alpha))_{|(k_1)_f^m} = \mathtt{id}$ para todo $m \geq 1$ y $\alpha \in \mu_{f,m}^{\times}$. Deducimos que $\mathcal{F}(\pi)_{|\cup_m (k_1)_f^m} = \mathtt{id}$. Así mismo, $\mathcal{F}$ verifica (a) de modo que $\mathcal{F}(\pi)_{|k^{ur}} = \varphi^{-1}$. Como $k_f^{\mathtt{LT}} = k^{\mathtt{ur}} \cdot \cup_m (k_1)_f^m = \cup_m k_f^m$, usando el isomorfismo de la teoría de Galois $\mathtt{Gal}(k_f^{\mathtt{LT}}|k) \longrightarrow \mathtt{Gal}(k^{\mathtt{ur}}|k) \times \mathtt{Gal}(\cup_m (k_1)_f^m|k)$ (es isomorfismo pues $k^{\mathtt{ur}} \cap \cup_m (k_1)_f^m = k_1 = k$) (ver 1.1.5.2) deducimos que $\mathcal{F}(\pi)$ está caracterizado por las condiciones $\mathcal{F}(\pi)_{k^{\mathtt{ur}}} = \varphi^{-1}, \mathcal{F}(\pi)_{|\cup_m (k_1)_f^m} = \mathtt{id}$ y como $\mathtt{Art}_k(\pi)$ verifica esas mismas condiciones tenemos que $\mathcal{F}(\pi) = \mathtt{Art}_k(\pi)$ para todo $\pi \in \nu_k^{-1}(1)$. Puesto que los parámetros de uniformización generan a $k^{\times}$ obtenemos la igualdad $\mathcal{F} = \mathtt{Art}_k$.

De nuevo, la última afirmación se tiene por construcción.

2. La primera parte es el contenido del teorema del cambio de base 2.4.12. Veamos que $\mathtt{Art}_k$ induce un isomorfismo como en el enunciado. Observar que la extensión $k' \cap k^{\mathtt{LT}} \supset k$ es de Galois pues $k^{\mathtt{LT}} \supset k$ es una extensión abeliana, de modo que tiene sentido considerar su grupo de Galois. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} k'^{\times} & \xrightarrow{\mathtt{Art}_{k'}} & \mathtt{W}(k'^{\mathtt{LT}}|k') \\ {\scriptstyle \mathtt{N}_{k'|k}}\downarrow & & \downarrow{\scriptstyle \mathtt{res}} \\ k^{\times} & \xrightarrow{\mathtt{Art}_k} & \mathtt{W}(k^{\mathtt{LT}}|k). \end{array}$$

Denotamos la imagen de la restricción $\mathtt{res}$ por $\mathtt{W}(k'^{\mathtt{LT}}|k')_{|k^{\mathtt{LT}}}$. Gracias a que el diagrama conmuta

tenemos que la siguiente aplicación está bien definida y es un isomorfismo:

$$\begin{array}{ccc} k^\times/\mathtt{N}_{k'|k}(k'^\times) & \longrightarrow & \mathtt{W}(k^{\mathtt{LT}}|k)/\mathtt{W}(k'^{\mathtt{LT}}|k')_{|k^{\mathtt{LT}}}, \\ x\mathtt{N}_{k'|k}(k'^\times) & \longmapsto & \mathtt{Art}_k(x) \pmod{\mathtt{W}(k'^{\mathtt{LT}}|k')_{|k^{\mathtt{LT}}}}. \end{array}$$

Para obtener el isomorfismo del enunciado es suficiente probar que $\mathtt{W}(k^{\mathtt{LT}}|k)/\mathtt{W}(k'^{\mathtt{LT}}|k')_{|k^{\mathtt{LT}}}$ es isomorfo a $\mathtt{Gal}((k' \cap k^{\mathtt{LT}})|k)$. Vamos a verlo haciendo algunas observaciones de naturaleza topológica:

i. **El homomorfismo restricción $\mathtt{W}(k^{\mathtt{LT}}|k) \to \mathtt{Gal}((k' \cap k^{\mathtt{LT}})|k)$ es sobreyectivo.** Se debe a la densidad de $\mathtt{W}(k^{\mathtt{LT}}|k)$ en $\mathtt{Gal}(k^{\mathtt{LT}}|k)$ y a que la extensión $k' \cap k^{\mathtt{LT}} \supset k$ es finita y de Galois.

ii. **La imagen del homomorfismo restricción $\mathtt{Gal}(k'^{\mathtt{ur}}|k') \to \mathtt{Gal}(k^{\mathtt{ur}}|k)$ es la clausura del conjunto $\left\langle \varphi_k^{f(k'|k)} \right\rangle$.** Para verlo, notar que $\mathtt{Gal}(k'^{\mathtt{ur}}|k') \to \mathtt{Gal}(k^{\mathtt{ur}}|k)$ es una aplicación continua y además cerrada por ser una aplicación entre espacios de Hausdorff compactos (grupos profinitos). Así mismo, sabemos que $(\varphi_{k'})_{|k^{\mathtt{ur}}} = \varphi_k^{f(k'|k)}$ y esto es suficiente para concluir la igualdad razonando como sigue:

$$\begin{aligned} \left\langle \varphi_k^{f(k'|k)} \right\rangle &= \langle (\varphi_{k'})_{|k^{\mathtt{ur}}} \rangle \subset \mathtt{Gal}(k'^{\mathtt{ur}}|k')_{|k^{\mathtt{ur}}} \\ &= \left(\overline{\langle \varphi_{k'} \rangle} \right)_{|k^{\mathtt{ur}}} \overset{\text{continuidad}}{\subset} \overline{\left\langle \varphi_k^{f(k'|k)} \right\rangle}, \end{aligned}$$

de modo que $\mathtt{Gal}(k'^{\mathtt{ur}}|k)_{|k^{\mathtt{ur}}}$ es un cerrado que contiene a $\left\langle \varphi_k^{f(k'|k)} \right\rangle$ y a su clausura, se concluye que debe coincidir con dicha clausura.

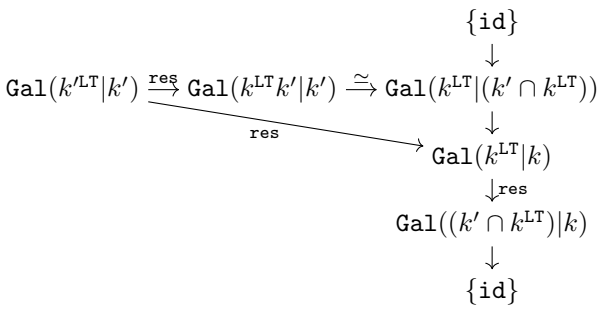
iii. **La preimagen de $\mathtt{W}(k^{\mathtt{LT}}|k)$ por el homomorfismo restricción $\mathtt{Gal}(k'^{\mathtt{LT}}|k') \to \mathtt{Gal}(k^{\mathtt{LT}}|k)$ es $\mathtt{W}(k'^{\mathtt{LT}}|k')$.** Demostraremos la parte no trivial del enunciado, es decir, $\mathtt{res}^{-1}(\mathtt{W}(k^{\mathtt{LT}}|k) \subset \mathtt{W}(k'^{\mathtt{LT}}|k')$. En efecto, si $\sigma \in \mathtt{Gal}(k'^{\mathtt{LT}}|k')$ es tal que $\sigma_{|k^{\mathtt{LT}}} \in \mathtt{W}(k^{\mathtt{LT}}|k)$ entonces $\sigma_{|k^{\mathtt{ur}}} = (\sigma_{|k^{\mathtt{LT}}})_{|k^{\mathtt{ur}}} \in \langle \varphi_k \rangle$. Tenemos $(\sigma_{|k'^{\mathtt{ur}}})_{|k^{\mathtt{ur}}} = \sigma_{|k^{\mathtt{ur}}} = (\sigma_{|k^{\mathtt{LT}}})_{|k^{\mathtt{ur}}} \in \langle \varphi_k \rangle$. Además, $\sigma_{|k'^{\mathtt{ur}}} \in \mathtt{Gal}(k'^{\mathtt{ur}}|k')$, de forma que

$$(\sigma_{|k'^{\mathtt{ur}}})_{|k^{\mathtt{ur}}} \in \mathtt{Gal}(k'^{\mathtt{ur}}|k')_{|k^{\mathtt{ur}}} \cap \langle \varphi_k \rangle = \overline{\left\langle \varphi_k^{f(k'|k)} \right\rangle} \cap \langle \varphi_k \rangle = \langle \varphi_k^{f(k'|k)} \rangle = \langle (\varphi_{k'})_{|k^{\mathtt{ur}}} \rangle.$$

Deducimos que $\sigma_{|k'^{\mathtt{ur}}} \in \langle \varphi_{k'} \rangle$, es decir, $\sigma \in \mathtt{W}(k'^{\mathtt{LT}}|k')$.

iv. **El núcleo del homomorfismo restricción $\mathtt{W}(k^{\mathtt{LT}}|k) \to \mathtt{Gal}((k' \cap k^{\mathtt{LT}})|k)$ coincide con $\mathtt{W}(k'^{\mathtt{LT}}|k')_{|k^{\mathtt{LT}}}$.** Claramente $\mathtt{W}(k'^{\mathtt{LT}}|k')_{|k^{\mathtt{LT}}}$ está incluido en el núcleo de este homomorfismo.

Para la otra inclusión comenzamos con el siguiente diagrama:



donde la columna de la derecha es una sucesión exacta de grupos abelianos y la fila superior se consigue gracias a la teoría de Galois. Supongamos que tenemos $\sigma \in \mathtt{Gal}(k^{\mathtt{LT}}|k)$ tal que $\sigma \in \mathtt{W}(k^{\mathtt{LT}}|k)$ y $\sigma_{|(k'\cap k^{\mathtt{LT}})} = \mathtt{id}$. Usando la exactitud de la columna deducimos que $\sigma \in \mathtt{Gal}(k^{\mathtt{LT}}|(k' \cap k^{\mathtt{LT}}))$. Usando el isomorfismo de la fila obtenemos que existe un único $\tau \in \mathtt{Gal}(k^{\mathtt{LT}}k'|k')$ tal que $\tau_{|k^{\mathtt{LT}}} = \sigma$. Como la extensión $k'^{\mathtt{LT}} \supset k'$ es de Galois vemos que podemos extender τ a un automorfismo $\tilde{\tau} \in \mathtt{Gal}(k'^{\mathtt{LT}}|k')$ verificándose $\tilde{\tau}_{|(k^{\mathtt{LT}}k')} = \tau$. En particular, $\tilde{\tau}_{|k^{\mathtt{LT}}} = \sigma$. Será suficiente probar que $\tilde{\tau} \in \mathtt{W}(k'^{\mathtt{LT}}|k')$, pero esto es inmediato gracias a (iii.) pues $\tilde{\tau}_{|k^{\mathtt{LT}}} = \sigma \in \mathtt{W}(k^{\mathtt{LT}}|k)$ de modo que $\tilde{\tau} \in \mathtt{W}(k'^{\mathtt{LT}}|k')$.

Aplicando el primer teorema de isomorfía y las observaciones anteriores verificamos la afirmación del enunciado.

□

Nuestro siguiente objetivo es demostrar el teorema de existencia para las extensiones de Lubin-Tate finitas. Los siguientes resultados de la teoría de cuerpos de clase local que nos simplificarán la tarea:

Corolario 2.4.14. ([Iwa86], Proposition 7.2,7.3).

1. **Teorema de Limitación:** Sea $k' \supset k$ una extensión separable finita arbitraria. Entonces

$$\mathtt{N}_{k'|k}(k'^{\times}) = \mathtt{N}_{(k'\cap k^{\mathtt{LT}})|k}((k' \cap k^{\mathtt{LT}})^{\times}), \qquad (k^{\times} : \mathtt{N}_{k'|k}(k'^{\times})) \leq [k' : k]$$

   teniénd,ose la igualdad si y sólo si $k' \supset k$ es una extensión de Lubin-Tate, i.e., $k' \subset k^{\mathtt{LT}}$.

2. Sea $k' \supset k$ una extensión finita separable y $k'' \supset k$ una extensión de Lubin-Tate finita. Entonces,

$$\mathtt{N}_{k'|k}(k'^{\times}) \subset \mathtt{N}_{k''|k}(k''^{\times}) \iff k'' \subset k'.$$

3. Sean $k \subset k' \subset k'' \subset k^{\mathtt{LT}}$ extensiones de Lubin-Tate finitas. El siguiente diagrama conmuta

$$\begin{array}{ccc} k^\times/\mathtt{N}_{k''|k}(k''^\times) & \xrightarrow{\mathtt{Art}_{k''|k}} & \mathtt{Gal}(k''|k) \\ \downarrow & & \downarrow{\scriptstyle \mathtt{res}} \\ k^\times/\mathtt{N}_{k'|k}(k'^\times) & \xrightarrow{\mathtt{Art}_{k'|k}} & \mathtt{Gal}(k'|k) \end{array}$$

siendo el homomorfismo vertical de la izquierda el inducido por la inclusión $\mathtt{N}_{k''|k}(k''^\times) \subset \mathtt{N}_{k'|k}(k'^\times)$. En particular, $\mathtt{Art}_{k''|k}$ induce un isomorfismo $\mathtt{N}_{k'|k}(k'^\times)/\mathtt{N}_{k''|k}(k''^\times) \to \mathtt{Gal}(k''|k')$.

Teorema 2.4.15. (Teorema de Existencia para $k^{\mathtt{LT}}$). Sea $H \subset k^\times$ un subgrupo cerrado de índice finito. Entonces existe una única extensión finita de Lubin-Tate $k' \supset k$ tal que $H = \mathtt{N}_{k'|k}(k'^\times)$.

Demostración. Sea $n = (k^\times : H) < \infty$ el índice de H en $k^\times$. Para todo parámetro de uniformización π de k tenemos que $\pi^n \in H$. $H \cap \mathcal{O}_k^\times$ es un subgrupo cerrado de $\mathcal{O}_k^\times$ con índice $(\mathcal{O}_k^\times : H \cap \mathcal{O}_k^\times) \leq n < \infty$. Ahora bien, $\mathcal{O}_k^\times$ es un grupo topológico compacto (de hecho profinito) de modo que todo subgrupo cerrado de índice finito es abierto y llegamos a que existe $m \geq 0$ tal que $1 + \mathfrak{p}_k^m \subset H \cap \mathcal{O}_k^\times \subset H$. Obtenemos que $(1 + \mathfrak{p}_k^m) \times \langle \pi^n \rangle \subset H$. Por 2.4.7 (con $x = \pi^n$) sabemos que $(1 + \mathfrak{p}_k^m) \times \langle \pi^n \rangle = \mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\,\times})$ para algún polinomio de Frobenius $f \in \mathcal{O}_{k_n}[X]$ asociado a π. Gracias a 2.4.13.2 tenemos el isomorfismo $\mathtt{Art}_{(k_n)_f^m|k} : k^\times/\mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\,\times}) \to \mathtt{Gal}((k_n)_f^m|k)$. Sea k' la subextensión de $k \subset (k_n)_f^m$ asociada al grupo $H/\mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\,\times})$ de modo que el homomorfismo $\mathtt{Art}_{(k_n)_f^m|k}$ induce un isomorfismo $H/\mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\,\times}) \to \mathtt{Gal}((k_n)_f^m|k')$. Sin embargo, usando 2.4.14.3, tenemos un isomorfismo $\mathtt{N}_{k'|k}(k'^\times)/\mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\,\times}) \xrightarrow{\sim} \mathtt{Gal}((k_n)_f^m|k')$, también inducido por $\mathtt{Art}_{(k_n)_f^m|k}$. Concluimos que $H = \mathtt{N}_{k'|k}(k'^\times)$. La unicidad se tiene gracias a 2.4.14.2.

□

Si combinamos 2.4.9 con 2.4.14.1 vemos que el grupo de normas de cualquier extensión separable finita $k' \supset k$ es un subgrupo cerrado de índice finito de $k^\times$. El recíproco nos lo da el teorema de existencia 2.4.15. Además se sabe que, en general, un subgrupo cerrado de índice finito de un grupo topológico es abierto. También tenemos que todo subgrupo abierto de un grupo topológico es cerrado, luego para los subgrupos de índice finito ser abierto es equivalente a ser cerrado. Llegamos a que nuestros resultados nos dan la siguiente correspondencia biyectiva:

$$\left\{ \begin{array}{c} \text{Extensiones finitas} \\ \text{Lubin-Tate de } k: \\ k \subset k' \subset k^{\mathtt{LT}} \end{array} \right\} \xrightarrow{\mathtt{N}_{k'|k}(k'^\times)} \left\{ \begin{array}{c} \text{Subgrupos abiertos} \\ \text{con índice finito de } k^\times: \\ H \subset k^\times \end{array} \right\}$$

Esta correspondencia invierte las inclusiones (anti-isomorfismo) debido a 2.4.14.2. En particular, se

verifica que:

$$\mathtt{N}_{k'k''|k}((k'k'')^\times) = \mathtt{N}_{k'|k}(k'^\times) \cap \mathtt{N}_{k''|k}(k''^\times), \qquad \mathtt{N}_{k'\cap k''|k}((k' \cap k'')^\times) = \mathtt{N}_{k'|k}(k'^\times)\mathtt{N}_{k''|k}(k''^\times)$$

para cualesquiera extensiones Lubin-Tate finitas k', k'' de k.

2.5. Teorema de Kronecker-Weber para Cuerpos Locales

Hemos visto que las extensiones finitas de Lubin-Tate son suficiente para obtener la teoría de cuerpos de clase local. La razón es que la extensión de Lubin-Tate coincide con la extensión abeliana maximal y vamos a probarlo en esta sección. Para este resultado haremos uso de los los grupos de ramificación superiores y sus resultados más importantes, que repasamos brevemente en la siguiente subsección.

Grupos de Ramificación Superiores

Sea $L \supset k$ una extensión de Galois finita siendo k un cuerpo local con valoración normalizada ν_k y denotamos por $G := \mathtt{Gal}(L|k)$ al grupo de Galois de la extensión. Denotamos por ν_L a la valoración normalizada de L. Definimos el *grupo de ramificación i-ésimo de G* por

$$G_i := \{\sigma \in G \ : \ \sigma\alpha - \alpha \in \mathfrak{p}_L^{i+1} \text{ para todo } \alpha \in \mathcal{O}_L\}, \ i \geq -1.$$

Extendemos esta definición para valores reales del subíndice de la siguiente forma:

$$G_x := \{\sigma \in G \ : \ \nu_L(\sigma\alpha - \alpha) \geq x + 1 \text{ para todo } \alpha \in \mathcal{O}_L\}.$$

Claramente, $G_x = G_i$ con i el menor entero mayor o igual que x.

Tenemos las siguientes propiedades:

Lema 2.5.1. ([FV93], Subsection 4.3, Chapter II).

1. Sea H un subgrupo de G y $k' \supset k$ la extensión que verifica que $H = \mathtt{Gal}(L|k')$. Entonces $H_i = G_i \cap H$.

2. Los grupos G_i son normales en G.

3. Sea L_0 la extensión no ramificada maximal de k en L. Entonces $G_0 = \mathtt{Gal}(L|L_0)$ y el grupo i-ésimo de ramificación de G coincide con el de G_0 para $i \geq 0$. Además, el grupo i-ésimo de

ramificación de G_0 podemos describirlo como

$$(G_0)_i = \{\sigma \in G_0 \ : \ \sigma\pi - \pi \in \mathfrak{p}_L^{i+1}\}$$

con π un parámetro de uniformización de L.

4. Se tiene que $G_i = \{\mathtt{id}\}$ para i suficientemente grande.

Gracias al apartado **3.** podemos reducir el estudio a los grupos de ramificación de las extensiones totalmente ramificadas. Observar que además el apartado **3.** nos dice que $\sigma \in G_i$ si y sólo si $\sigma(\pi)/\pi \in 1 + \mathfrak{p}_L^{i+1} = U_L^{(i+1)}$. De forma más precisa, tenemos el siguiente resultado:

Proposición 2.5.2. ([Ser62], Proposition 7, Chapitre IV). Para cada $i \geq 0$ consideremos la aplicación

$$\begin{array}{ccc} G_i & \longrightarrow & U_L^{(i)}/U_L^{(i+1)}, \\ \sigma & \longmapsto & \sigma(\pi)/\pi \pmod{U_L^{(i+1)}}. \end{array}$$

El núcleo de esta aplicación es G_{i+1} de modo que pasando al cociente obtenemos una inyección de G_i/G_{i+1} en $U_L^{(i)}/U_L^{(i+1)}$. Esta inyección no depende del parámetro de uniformización π elegido.

Combinando estos homomorfismos con los isomorfismos $\mathcal{O}_L^\times/U_L^{(1)} \simeq (\overline{L})^\times$ y $U_L^{(i)}/U_L^{(i+1)} \simeq \overline{L}$ deducimos que el índice $(G_0 : G_1)$ divide a $q_L - 1$ y los índices $(G_i : G_{i+1})$ dividen a q_L con $q_L = |\overline{L}|$. Cuando la extensión $L \supset k$ es totalmente ramificada entonces $q_L = q_k = |\overline{k}|$.

Hemos visto que los grupos de ramificación con enumeración inferior tienen un buen comportamiento con los subgrupos y las intersecciones. Sin embargo, no se comportan bien con los cocientes de modo que necesitamos los grupos de ramificación enumerados de otra forma. Para ello introducimos la siguiente definición: Sea $\phi : \mathbb{R}_{\geq 0} \to \mathbb{R}$ la única función continua y que es lineal a trozos verificando las siguientes dos condiciones:

$$\phi(0) = 0, \qquad \phi'(u) = (G_0 : G_u)^{-1} \text{ para } u \notin \mathbb{Z}.$$

Esta función es creciente y cóncava. Se puede comprobar que se verifica la siguiente fórmula:

$$\phi(m) = \frac{1}{|G_0|} \sum_{i=1}^{m} |G_i|, \quad \forall\ m \in \mathbb{N}.$$

Definimos la *enumeración superior* de forma que $G^v = G_u$ si y sólo si $v = \phi(u)$. Tenemos el siguiente resultado:

Proposición 2.5.3. (Teorema de Herbrand, [Ser62], Proposition 14, Chapitre IV). Sean $L' \supset L \supset k$

extensiones de Galois con grupos $G = \mathtt{Gal}(L'|k), H = \mathtt{Gal}(L'|L), G/H = \mathtt{Gal}(L|k)$. Entonces

$$(G/H)^v = G^v H/H.$$

Es decir, si $\mathtt{res} : \mathtt{Gal}(L'|k) \to \mathtt{Gal}(L|k)$ es el homomorfismo restricción, entonces $\mathtt{res}(\mathtt{Gal}(L'|k)^v) = \mathtt{Gal}(L|k)^v$.

Nos interesa saber cuando en la filtración de los grupos de ramificación aparece un nuevo grupo y por ello introducimos la siguiente definición:

Definición 2.5.4. (Salto). *En la filtración $\{G^v\}$, decimos que $r \in \mathbb{R}$ es un salto si para todo $\varepsilon > 0$ es $G^r \neq G^{r+\varepsilon}$.*

El siguiente teorema es un resultado profundo y será esencial para la Teoría de Cuerpos de Clase Local:

Teorema 2.5.5. (Teorema de Hasse-Arf, [Ser62], §7, Chapitre V). Si G es un grupo abeliano y v es un salto de la filtración $\{G^v\}$ entonces $v \in \mathbb{Z}$.

El teorema de Hasse-Arf se usa únicamente en la segunda parte del siguiente lema. No lo volveremos a necesitar.

Lema 2.5.6. ([Yos08], Corollary 6.13).

1. Sean $L_1 \supset k$ y $L_2 \supset k$ dos extensiones de Galois finitas contenidas en algún cuerpo común y $v \geq 0$. Si $\mathtt{Gal}(L_1|k)^v = \mathtt{Gal}(L_2|k)^v = \{\mathtt{id}\}$ entonces también $\mathtt{Gal}(L_1L_2|k)^v = \{\mathtt{id}\}$.
2. Supongamos que $L \supset k$ es una extensión totalmente ramificada con grupo de Galois abeliano G. Entonces $(G : G^m)$ divide a $(q-1)q^m$ para todo $m \geq 1$.

La última proposición que necesitamos para poder demostrar el teorema de Kronecker-Weber para cuerpos locales es la siguiente

Proposición 2.5.7. ([Yos08], Proposition 6.4). Sea $x \in k^\times$ con $\nu_k(x) = n > 0$. Sea $\pi \in k_n$ con $\mathtt{N}_{k_n|k}(\pi) = x$ y $f \in \mathcal{O}_{k_n}[X]$ un polinomio de Frobenius para π. Consideramos la extensión $(k_n)_f^m$. Entonces tenemos que $\mathtt{Gal}((k_n)_f^m|k_n)^m = \{\mathtt{id}\}$ para todo $m \geq 1$.

2.5.1. Kronecker-Weber para Cuerpos Locales

Teorema 2.5.8. (Teorema de Kronecker-Weber Local) Toda extensión finita abeliana del cuerpo local k es una extensión finita de Lubin-Tate, i.e., $k^{\mathtt{LT}} = k^{\mathtt{ab}}$.

Demostración. Consideramos $\varphi^{-1} \in \mathtt{W}(k^{\mathtt{LT}}|k)$ el inverso del elemento de Frobenius. Extendemos φ^{-1} de forma arbitraria a $\sigma \in \mathtt{W}(k^{\mathtt{ab}}|k)$ y consideramos su cuerpo fijo $(k^{\mathtt{ab}})^{\sigma}$ en $k^{\mathtt{ab}}$. Tenemos

$$(k^{\mathtt{ab}})^{\sigma} \cap k^{\mathtt{ur}} = (k^{\mathtt{ur}})^{\varphi^{-1}} = k$$

de modo que $(k^{\mathtt{ab}})^{\sigma} \supset k$ es una extensión totalmente ramificada. Por teoría de Galois $\mathtt{Gal}(k^{\mathtt{ab}}|(k^{\mathtt{ab}})^{\sigma}) = \overline{\langle\sigma\rangle} \simeq \hat{\mathbb{Z}}$, con el isomorfismo definido por $\sigma \mapsto 1$. Por otro lado, también gracias a la teoría de Galois,

$$\mathtt{Gal}(k^{\mathtt{ur}}(k^{\mathtt{ab}})^{\sigma}/(k^{\mathtt{ab}})^{\sigma}) \simeq \mathtt{Gal}(k^{\mathtt{ur}}|k) = \overline{\langle\varphi^{-1}\rangle} = \overline{\langle\sigma_{|k^{\mathtt{ur}}}\rangle}$$

de modo que de nuevo $\mathtt{Gal}(k^{\mathtt{ur}}(k^{\mathtt{ab}})^{\sigma}/(k^{\mathtt{ab}})^{\sigma}) \simeq \hat{\mathbb{Z}}$ vía $\sigma \mapsto 1$. Llegamos a

$$\mathtt{Gal}(k^{\mathtt{ab}}|(k^{\mathtt{ab}})^{\sigma}) \simeq \mathtt{Gal}(k^{\mathtt{ur}}(k^{\mathtt{ab}})^{\sigma}/(k^{\mathtt{ab}})^{\sigma})$$

y por tanto $k^{\mathtt{ab}} = k^{\mathtt{ur}}(k^{\mathtt{ab}})^{\sigma}$.

Ahora fijemos $\pi = \mathtt{Art}_k^{-1}(\varphi^{-1})$, que es un parámetro de uniformización de k. Como vimos en la prueba de 2.4.4 sabemos que $\cup_{m\geq 1}(k_1)_f^m \subset (k^{\mathtt{ab}})^{\sigma}$ para cierto polinomio de Frobenius f asociado a π. Con la igualdad $k^{\mathtt{LT}} = k^{\mathtt{ur}} \cup_{m\geq 1} (k_1)_f^m$ es suficiente probar que $(k^{\mathtt{ur}})^{\sigma} \subset \cup_{m\geq 1}(k_1)_f^m$. Sea $k' \supset k$ una extensión finita de Galois contenida en el cuerpo $(k^{\mathtt{ab}})^{\sigma}$. Al ser $(k^{\mathtt{ab}})^{\sigma} \supset k$ totalmente ramificada deducimos que $k' \supset k$ también es totalmente ramificada y $\mathtt{Gal}(k'|k)^m = \{\mathtt{id}\}$ para m suficientemente grande. Como tenemos la igualdad $\mathtt{Gal}((k_1)_f^m|k_1)^m = \{\mathtt{id}\}$ gracias a 2.5.7, usando 2.5.6.1 llegamos a

$$\mathtt{Gal}(k'(k_1)_f^m|k_1)^m = \{\mathtt{id}\}$$

de modo que

$$[k'(k_1)_f^m : k] = |\mathtt{Gal}(k'(k_1)_f^m|k_1)| = |\mathtt{Gal}(k'(k_1)_f^m|k_1)/\mathtt{Gal}(k'(k_1)_f^m|k_1)^m|$$

divide a $q^{m-1}(q-1) = [(k_1)_f^m : k]$ por 2.5.6.2. Concluimos que $k'(k_1)_f^m \subset (k_1)_f^m$, es decir, $k' \subset \cup_{m\geq 1}(k_1)_f^m$.

□

Corolario 2.5.9. $(\mathbb{Q}_p^{\mathtt{ab}} = \cup_{n\geq 1}\mathbb{Q}_p(\mu_n))$. Para todo número primo p la extensión abeliana maximal de $\mathbb{Q}_p$ coincide con $\mathbb{Q}_p(\cup_{n\geq 1}\mu_n)$.

Demostración. En efecto, $\cup_{m\geq 1}(\mathbb{Q}_p)_{f_p}^m = \mathbb{Q}_p(\cup_{m\geq 1}\mu_{p^m})$ y $\mathbb{Q}_p^{\mathtt{ur}} = \mathbb{Q}_p(\cup_{(n,p)=1}\mu_n)$ de modo que $\mathbb{Q}_p^{\mathtt{ab}} = \mathbb{Q}_p^{\mathtt{LT}} = \mathbb{Q}_p(\cup_{m\geq 1}\mu_{p^m})\mathbb{Q}_p(\cup_{(n,p)=1}\mu_n) = \mathbb{Q}_p(\cup_{n\geq 1}\mu_n)$.

□

2.5.2. Teorema de Kronecker-Weber

Para la demostración haremos uso del siguiente lema. En [Š51] aparece con el nombre de **Monodromía Aritmética** y su demostración se basa en el resultado de **Minkowski** por el cual sabemos que $\mathbb{Q}$ no admite extensiones no ramificadas no triviales.

Lema 2.5.10. ([Cas86], Theorem 12.1, Chapter 10). Sea $k \supset \mathbb{Q}$ una extensión finita de Galois con grupo de Galois G. Entonces G está generado por los grupos de inercia de los ideales primos $\mathfrak{p}$ de k que están ramificados en la extensión $k \supset \mathbb{Q}$.

El teorema de Kronecker-Weber es el siguiente:

Teorema 2.5.11. (Teorema de Kronecker-Weber). Toda extensión abeliana de $\mathbb{Q}$ está contenida en una extensión ciclotómica.

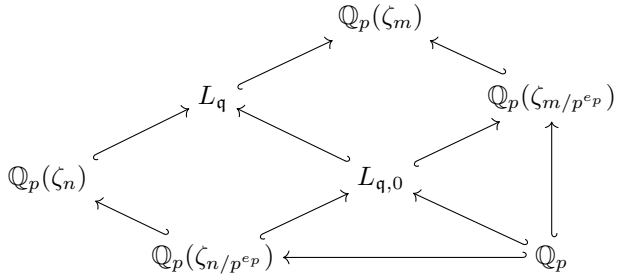
Demostración. Sea $k \supset \mathbb{Q}$ una extensión abeliana. Para cada número primo p de $\mathbb{Q}$ que ramifica en la extensión $k \supset \mathbb{Q}$ consideramos un primo $\mathfrak{p}$ de k sobre p y consideramos la compleción $k_{\mathfrak{p}}$ de k en $\mathfrak{p}$. Gracias al isomorfismo de grupos $\mathtt{Gal}(k_{\mathfrak{p}}|\mathbb{Q}_p) \simeq \mathtt{G}_{\mathfrak{p}}(k|\mathbb{Q}) \subset \mathtt{Gal}(k|\mathbb{Q})$ con $\mathtt{G}_{\mathfrak{p}}(k|\mathbb{Q})$ el grupo de descomposición de $\mathfrak{p}$, vemos que la extensión $k_{\mathfrak{p}} \supset \mathbb{Q}_p$ es abeliana y finita (recordar que al ser la extensión $k \supset \mathbb{Q}$ abeliana los grupos de descomposición e inercia sólo dependen del primo p). Por el teorema de Kronecker-Weber para $\mathbb{Q}_p$ sabemos que existen números naturales $n_p \in \mathbb{N}$ tales que para cada primo p se tiene la inclusión $k_{\mathfrak{p}} \subset \mathbb{Q}_p(\zeta_{n_p})$ con ζ_{n_p} una raíz primitiva n_p-ésima de la unidad. El número n_p sólo depende de p pues el grupo de Galois $\mathtt{Gal}(k|\mathbb{Q})$ actúa transitivamente sobre el conjunto de primos de k sobre p. Sea p^{e_p} la máxima potencia de p dividiendo a n_p, es decir, $e_p = \nu_p(n_p)$ y consideremos el número $n = \prod_{p \text{ ramifican}} p^{e_p}$, que es un producto finito pues el número de primos que ramifican es finito (divisores del discriminante de la extensión).

Consideramos la extensión $L = k(\zeta_n)$. Queremos demostrar que $L = \mathbb{Q}(\zeta_n)$. La extensión $L \supset \mathbb{Q}$ es abeliana por ser composición de extensiones abelianas. Para cada primo $\mathfrak{q}$ de L tal que $\mathfrak{q}|\mathfrak{p}$ esta vez tenemos (sin hacer uso directo del teorema de Kronecker-Weber para $\mathbb{Q}_p$) que $L_{\mathfrak{q}} = k_{\mathfrak{p}}\mathbb{Q}_p(\zeta_n) \subset \mathbb{Q}_p(\zeta_{n_p})\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{\mathtt{mcm}(n_p,n)})$, y sabemos por construcción que $\nu_p(\mathtt{mcm}(n_p, n)) = \nu_p(n_p) = e_p$. De ahora en adelante denotaremos $m := \mathtt{mcm}(n_p, n)$. En definitiva, lo que tenemos es que $L \supset \mathbb{Q}$ es una extensión abeliana y para cualquier primo $\mathfrak{q}$ de L sobre p (p ramifica) tenemos la siguiente cadena de extensiones:

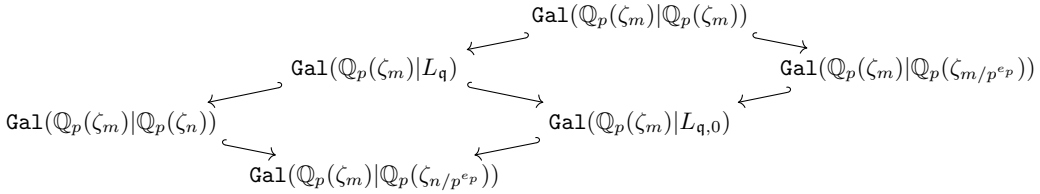
$$\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_n) \subset L_{\mathfrak{q}} \subset \mathbb{Q}_p(\zeta_m),$$

con $\nu_p(n) = \nu_p(m) = e_p$.

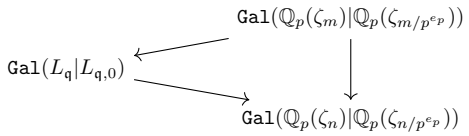
Sea $L_{\mathfrak{q},0}$ la extensión maximal no ramificada de $\mathbb{Q}_p$ en $L_{\mathfrak{q}}$ de modo que $L_{\mathfrak{q}} \supset L_{\mathfrak{q},0}$ es una extensión totalmente ramificada de Galois con grupo de Galois isomorfo al grupo de inercia de la extensión $L \supset \mathbb{Q}$ en $\mathfrak{q}$. Resaltar una vez más que debido a la abelianidad de la extensión $L \supset \mathbb{Q}$, estos grupos de inercia sólo dependen del primo racional p. Como sabemos gracias a la teoría de Lubin-Tate, la extensión maximal no ramificada de $\mathbb{Q}_p$ en $\mathbb{Q}_p(\zeta_n)$ (resp. en $\mathbb{Q}_p(\zeta_m)$) es la extensión $\mathbb{Q}_p(\zeta_{n/p^{e_p}})$ (resp. $\mathbb{Q}_p(\zeta_{m/p^{e_p}})$). Tenemos el siguiente retículo de extensiones:



Si consideramos los correspondientes grupos de Galois respecto a $\mathbb{Q}_p(\zeta_m)$ obtenemos el siguiente retículo de subgrupos:

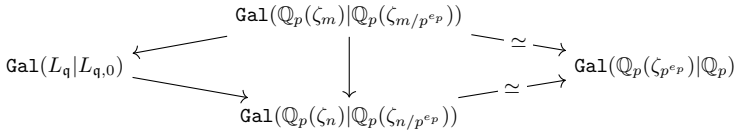


Usando la conmutatividad de los cuadrados de estos diagramas y recordando que $\mathtt{Gal}(F_2|F_1) \simeq \mathtt{Gal}(F_3|F_2)/\mathtt{Gal}(F_3|F_1)$ en general, obtenemos los siguientes homomorfismos bien definidos que se corresponden con la restricción y que nos dan el triángulo conmutativo:



Observar que los grupos que aparecen en este último diagrama son isomorfos a los grupos de inercia de las extensiones correspondientes. Por otro lado, este diagrama podemos completarlo como sigue: Sabemos que $\mathbb{Q}_p(\zeta_m) = \mathbb{Q}_p(\zeta_{m/p^{e_p}})\mathbb{Q}_p(\zeta_{p^{e_p}})$ y $\mathbb{Q}_p(\zeta_{m/p^{e_p}}) \cap \mathbb{Q}_p(\zeta_{p^{e_p}}) = \mathbb{Q}_p$ debido a que una extensión es no ramificada y la otra es totalmente ramificada. Deducimos por teoría de Galois que $\mathtt{Gal}(\mathbb{Q}_p(\zeta_m)|\mathbb{Q}_p(\zeta_{m/p^{e_p}})) \simeq \mathtt{Gal}(\mathbb{Q}_p(\zeta_{p^{e_p}})|\mathbb{Q}_p)$ vía el homomorfismo de restricción. De manera análoga deducimos que $\mathtt{Gal}(\mathbb{Q}_p(\zeta_n)|\mathbb{Q}_p(\zeta_{n/p^{e_p}})) \simeq \mathtt{Gal}(\mathbb{Q}_p(\zeta_{p^{e_p}})|\mathbb{Q}_p)$ vía la restricción. Por tanto

obtenemos el siguiente diagrama donde ambos triángulos conmutan:



Podemos concluir

$$|\mathtt{I}_p(L|\mathbb{Q})| = |\mathtt{I}_p(\mathbb{Q}(\zeta_m)|\mathbb{Q})| = |\mathtt{I}_p(\mathbb{Q}(\zeta_{p^{e_p}})|\mathbb{Q})| = [\mathbb{Q}(\zeta_{p^{e_p}}) : \mathbb{Q}] = \Phi(p^{e_p}),$$

siendo Φ la función indicatriz de Euler. Gracias a 2.5.10 sabemos que el grupo de Galois de la extensión $L \supset \mathbb{Q}$ está generado por todos los grupos de inercia de los primos que dividen a los primos racionales p que ramifican en la extensión, de este modo llegamos a

$$\begin{aligned}
[L : \mathbb{Q}] &= |\mathtt{Gal}(L|\mathbb{Q})| \\
&\leq \prod_{p \text{ ramifica}} |\mathtt{I}_p(L|\mathbb{Q})| \\
&= \prod_{p \text{ ramifica}} \Phi(p^{e_p}) = \Phi(n) \\
&= [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \\
&\leq [L : \mathbb{Q}].
\end{aligned}$$

Es decir, $k \subset L = \mathbb{Q}(\zeta_n)$ como queríamos demostrar. □

Esta demostración que acabamos de ver se debe a [Š51] e ilustra muy bien la filosofía del *principio local a global*. Se pueden dar ejemplos de extensiones finitas de $\mathbb{Q}$ tales que poseen extensiones abelianas no contenidas en una extensión ciclotómica, es decir, el teorema de Kronecker-Weber no se cumple en general para todos los cuerpos globales y no se debe esperar que la demostración anterior se pueda extender para obtener un resultado análogo para otros cuerpos globales. En cierto modo, la demostración anterior nos dice una vez más lo especial que es el cuerpo de los números racionales $\mathbb{Q}$.

Bibliografía

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., 1969.

[Art59] E. Artin, *Theory of Algebraic Numbers*, 1959, Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester, 1956/7, Translated by George Striker.

[Bou81] N. Bourbaki, *Espaces Vectoriels Topologiques. Chapitres 1 à 5*, Masson, Paris, 1981, Éléments de mathématique.

[Cas86] J. W. S. Cassels, *Local Fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986.

[Che40] C. Chevalley, *La théorie du corps de classes*, Ann. of Math. (2) **41** (1940), 394–418.

[Coh91] P. M. Cohn, *Algebra. Vol. 3*, second ed., John Wiley & Sons, Ltd., Chichester, 1991.

[Col79] R. Coleman, *Division Values in Local Fields*, Invent. Math. **53** (1979), no. 2, 91–116.

[Cona] B. Conrad, *Galois Groups and Abelianizations*, Disponible On-line en: `virtualmath1.stanford.edu/~conrad/249BW09Page/handouts/profinite.pdf`.

[Conb] ———, *History of Class Field Theory*, Disponible On-line en: `virtualmath1.stanford.edu/~conrad/249BW09Page/handouts/cfthistory.pdf`.

[Cp86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, London, Academic Press Inc., 1986.

[FV93] I. B. Fesenko and S. V. Vostokov, *Local Fields and Their Extensions*, Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 1993.

[GC] F. García Cortés, *Teoría de Cuerpos de Clase.* Memoria del Proyecto de Beca de Colaboración, 2021, Disponible On-line en: `www.github.com/FranGarciaCo/Report-BCMEC`.

[Hun80] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York-Berlin, 1980.

[Iwa86] K. Iwasawa, *Local Class Field Theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1986.

[Lan94] S. Lang, *Algebraic Number Theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[Lan02] ———, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Lem00] F. Lemmermeyer, *Reciprocity Laws*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, From Euler to Eisenstein.

[LT65] J. Lubin and J. Tate, *Formal Complex Multiplication in Local Fields*, Ann. of Math. (2) **81** (1965), 380–387.

[Mila] J. S. Milne, *Class Field Theory*, Disponible On-line en: `www.jmilne.org/math/CourseNotes/cft.html`.

[Milb] ———, *Fields and Galois Theory*, Disponible On-line en: `www.jmilne.org/math/CourseNotes/ft.html`.

[MP05] Y. I. Manin and Alexei A. Panchishkin, *Introduction to Modern Number Theory*, second ed., Encyclopaedia of Mathematical Sciences, vol. 49, Springer-Verlag, Berlin, 2005.

[Neu99] J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

[PS04] B. Petri and N. Schappacher, *From Abel to Kronecker: episodes from 19th century algebra*, The Legacy of Niels Henrik Abel, Springer, Berlin, 2004, pp. 227–266.

[Rib01] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Universitext, Springer-Verlag, New York, 2001.

[Rib13] L. Ribes, *Introduction to Profinite Groups*, Travaux mathématiques. Vol. XXII, Trav. Math., vol. 22, Fac. Sci. Technol. Commun. Univ. Luxemb., Luxembourg, 2013, pp. 179–230.

[RZ10] L. Ribes and P. Zalesskii, *Profinite Groups*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 40, Springer-Verlag, Berlin, 2010.

[Ser62] Jean-Pierre Serre, *Corps Locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, VIII, Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.

[Sut19] A. Sutherland, *Local Fields and Hensel's Lemmas*, Disponible On-line en: `ocw.mit.edu/courses/mathematics/18-785-number-theory-i-fall-2019/lecture-notes/MIT18_785F19_lec9.pdf`, 2019.

[Tak94] Masahito Takase, *Three Aspects of the Theory of Complex Multiplication*, The intersection of history and mathematics, Sci. Networks Hist. Stud., vol. 15, Birkhäuser, Basel, 1994, pp. 91–108.

[Š51] I. R. Šafarevič, *A New Proof of the Kronecker-Weber Theorem* (in Russian), Trudy Mat. Inst. Steklov., v. 38, Izdat. Akad. Nauk SSSR, Moscow, 1951, pp. 382–387.

[Yos08] T. Yoshida, *Local Class Field Theory via Lubin-Tate Theory*, Ann. Fac. Sci. Toulouse Math. (6) **17** (2008), no. 2, 411–438.