Teoría de Cuerpos de Clase

Francisco García Cortés

18 de junio de 2021

El presente documento es la memoria que recoge los resultados estudiados durante el desarrollo de la Beca de Colaboración MEC con el Departamento de Álgebra de la Universidad de Sevilla, bajo la dirección y ayuda del Profesor Dr. Antonio Rojas León. El estilo del texto es algo informal y descuidado, en parte debido a que se escribió con la intención de comprender en profundidad los conceptos relevantes de la teoría de cuerpos de clase, así como desarrollar o fusionar demostraciones de la bibliografía que, según mi opinión, no fuesen suficientemente claras. La notación no es uniforme pues se ha usado distinta bibliografía para secciones diferentes. No se han reescrito las secciones para unificar la notación ya que también ha sido útil para abstraer las nociones y evitar la identificación notación-concepto que a menudo ocurre cuando se estudia algo por primera vez. La versión corregida, reducida y reestructurada es el documento presentado como memoria del Trabajo de Fin de Grado y que se puede usar como guión del presente texto.

Aprovecho esta introducción para agradecer al tutor Antonio Rojas el clima de trabajo del que me ha provisto así como su guía y ayuda en las partes difíciles de la teoría. También agradecer al departamento de Álgebra de la Universidad de Sevilla los espacios cedidos para el desarrollo de mi trabajo así como los materiales y los medios ofrecidos.

Índice general

Capítulo 1

Valoraciones

Comenzamos estudiando la teoría de valoraciones, el proceso de compleción y los resultados esenciales sobre extensión de valoraciones.

1.1. Primeras Definiciones

Definición 1.1.1. Un **valor absoluto** de un cuerpo k es una función

$$|\cdot| : k \to \mathbb{R}$$

verificando las propiedades siguientes:

`VA1.` $|x| \geq 0$ $\forall x$, y $|x| = 0$ si y sólo si $x = 0$.

`VA2.` $|xy| = |x||y|$ $\forall x, y \in k$.

`VA3.` $|x + y| \leq |x| + |y|$ $\forall x, y \in k$. (Desigualdad triangular)

Notar que un valor absoluto es, en particular, un homomorfismo entre el grupo $(k^\times, \cdot)$ y el grupo $(\mathbb{R}_{>0}, \cdot)$. De este modo, todo cuerpo admite el **valor absoluto trivial** dado por $|x| = 1$ si $x \neq 0$ y $|0| = 0$. En general dicho valor absoluto no será tenido en cuenta a menos que se indique lo contrario. Dado un cuerpo k con valor absoluto $|\cdot|$ podemos considerar la **distancia entre dos puntos** $x, y \in k$ definiendo $d(x, y) = |x - y|$. Esto hace que k sea un **espacio métrico** y, en particular, un espacio topológico. De hecho, es muy sencillo probar que k con dicha topología es un cuerpo topológico (suma, producto y $a \mapsto a^{-1}$ son operaciones continuas). Para nosotros será esencial dicha topología y por ello definimos:

Definición 1.1.2. Dos valores absolutos de k se dicen **equivalentes** si definen la misma topología.

Los valores absolutos equivalentes difieren tan sólo en un exponente:

Proposición 1.1.3. Dos valores absolutos $|\cdot|_1, |\cdot|_2$ en k son equivalentes si y sólo si existe un número real $s > 0$ tal que

$$|x|_1 = |x|_2^s \ \forall x \in k.$$

Demostración. La implicación $\Leftarrow$ es inmediata pues

$$|x-a|_1 < d \Leftrightarrow |x-a|_2^s < d \Leftrightarrow |x-a|_2 < d^{1/s},$$

es decir, $B_1(a,d) = B_2(a,d^{1/s})$. Con $B(a,d)$ estamos denotando a la bola de centro a y radio d.

Para el recíproco, observar que dado un valor absoluto $|\cdot|$ se cumple que $|x| < 1$ si y sólo si $x^n \to 0$ con respecto a $|\cdot|$. En consecuencia, si $|\cdot|_1, |\cdot|_2$ son equivalentes entonces $|x|_1 < 1$ implica que $|x|_2 < 1$. De hecho, $|x|_1 > 1$ implica que $|x|_2 > 1$ pues si $|x|_1 > 1$ entonces $|x^{-1}|_1 < 1$ y por ello $|x^{-1}|_2 < 1$, es decir, $|x^{-1}|_2 > 1$.

Como estamos suponiendo que nuestros valores absolutos son no triviales sabemos que existe $y \in k$ tal que $|y|_1 > 1$. Dado $x \in k \setminus \{0\}$ existe $\alpha \in \mathbb{R}$ tal que $|x|_1 = |y|_1^\alpha$. Sea m_i/n_i una sucesión de números racionales que converge a α y además verificando que $n_i > 0$ y $m_i/n_i \geq \alpha$. Entonces $|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i}$, luego

$$|\frac{x^{n_i}}{y^{m_i}}|_1 \Rightarrow |\frac{x^{n_i}}{y^{m_i}}|_2.$$

Por tanto es $|x|_2 \leq |y|_2^{m_i/n_i}$ para todo término de la sucesión y tomando límites concluimos que $|x|_2 \leq |y|_2^\alpha$. Usando una sucesión $m_i/n_i \leq \alpha$ y razonando como antes llegamos a que $|x|_2 \geq |y|_2^\alpha$, es decir, $|x|_2 = |y|_2^\alpha$. Para todo $x \in k \setminus \{0\}$ es

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} =: s,$$

y en consecuencia $|x|_1 = |x|_2^s$. Como $|y|_1 > 1$ implica que $|y|_2 > 1$ concluimos que $s > 0$.

□

Como hemos visto en la demostración, la equivalencia de $|\cdot|_1$ y $|\cdot|_2$ es equivalente a la condición

$$|x|_1 < 1 \Rightarrow |x|_2 < 1.$$

Usaremos esto para la demostración del siguiente resultado, **el teorema de aproximación**:

Teorema 1.1.4. Sean $|\cdot|_i, i = 1, \ldots, n$ valores absolutos de un cuerpo k tales que dos a dos no son equivalentes y consideremos $a_1, \ldots, a_n \in k$ elementos. Entonces para todo $\varepsilon > 0$ existe un $x \in k$ tal que

$$|x - a_i|_i < \epsilon \ \forall i = 1, \ldots, n.$$

Demostración. Al ser $|\cdot|_1$ y $|\cdot|_n$ valores absolutos no equivalentes sabemos que existe $\alpha \in k$ tal que $|\alpha|_1 < 1$ y $|\alpha|_n \geq 1$. Por la misma razón, existe $\beta \in k$ tal que $|\beta|_n < 1$ y $|\beta|_1 \geq 1$. Tomando $y = \beta/\alpha$ tenemos que $|y|_1 > 1$ y $|y|_n < 1$.

Ahora demostraremos por inducción en n que existe $z \in k$ tal que

$$|z|_1 > 1 \text{ y } |z|_j < 1 \text{ para } j = 2, \ldots, n.$$

Supongamos que hemos hallado $z \in k$ verificando que $|z|_1 > 1$ y $|z|_j < 1$ para todo $j = 2, \ldots, n-1$. Si $|z|_n \leq 1$ entonces bastaría considerar $z^m y$ con m suficientemente grande. Sin embargo, si $|z|_n > 1$, la sucesión $t_m = z^m/(1+z^m)$ converge a 1 con respecto a $|\cdot|_1$ y $|\cdot|_n$ pues $|z^m/(1+z^m) - 1|_i = 1/|z^m+1|_i \leq 1/(|z|_i^m - 1)$ para $i = 1, n$. Así mismo, $|z^m/(z^m+1)|_j = |1/(|z^{-1}|^m + 1)|_j$ para todo $j = 2, \ldots, n-1$ y por ello t_m converge a 0 respecto a dichos valores absolutos. Concluimos que con m suficientemente grande el elemento $t_m y$ cumpliría nuestros requisitos.

Demostrado lo anterior, para cada i podemos conseguir un elemento $z_i \in k$ tal que $|z_i|_i > 1$ y $|z_i|_j < 1$ para todo $j \neq i$. Como la sucesión $z_i^m/(z_i^m+1)$ converge a 1 respecto a $|\cdot|_i$ y a 0 respecto a $|\cdot|_j$ con $j \neq i$, dado $\varepsilon' > 0$ obtenemos para cada i un elemento $t_i \in k$ tal que $|t_i - 1|_i < \varepsilon'$ y $|t_i|_j < \varepsilon'$ para todo $j \neq i$. Si consideramos el elemento $x = a_1 t_1 + \cdots + a_n t_n$ concluimos que $|x - a_i|_i < \varepsilon$ para todo i (una vez elegido ε' adecuadamente).

□

Un corolario interesante es el siguiente:

Corolario 1.1.5. Sean $|\cdot|_i, i = 1, \ldots, n$ valores absolutos no equivalentes. Una relación de la forma

$$\prod_{i=1}^{n} |a|_i^{c_i} = 1$$

con $c_i \in \mathbb{R}$ será cierta para todo $a \in k \setminus \{0\}$ si y sólo si $c_i = 0$ para todo $i = 1, \ldots, n$.

Demostración. Supongamos que algún $c_i \neq 0$. Sea $a \in k \setminus \{0\}$ tal que $|a|_i$ es suficientemente grande y $|a|_j$ es suficientemente pequeño para todo $j \neq i$. Claramente a no verifica la igualdad.

□

Definición 1.1.6. Un valor absoluto $|\cdot|$ se dice **no arquimediano** si $|\underbrace{1 + \cdots + 1}_{n}|$ está acotado para todo $n \in \mathbb{N}$. En otro caso diremos que $|\cdot|$ es arquimediana.

Podemos caracterizar los valores absolutos no arquimedianos como sigue:

Proposición 1.1.7. EL valor absoluto $|\cdot|$ es no arquimediano si y sólo si se verifica la **desigualdad triangular fuerte**

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

Demostración. La implicación $\Leftarrow$ es sencilla pues si la desigualdad triangular fuerte se verifica entonces $|1+1| \leq \mathtt{max}\{|1|, |1|\} = |1| = 1$. Por inducción, si $|\underbrace{1 + \cdots + 1}_{n-1}| \leq 1$ entonces $|1 + \underbrace{1 + \cdots + 1}_{n-1}| \leq \mathtt{max}\{|1|, |\underbrace{1 + \cdots + 1}_{n-1}|\} \leq |1|$.

Para el recíproco, supongamos que existe $N \in \mathbb{R}$ tal que $|\underbrace{1+\cdots+1}_{n}| \leq N$ para todo $n \in \mathbb{N}$. Sean $x, y \in k$ y supongamos sin pérdida de generalidad que $|x| \geq |y|$. Entonces $|x|^j|y|^{n-j} \leq |x|^n$ para todo $n \in \mathbb{N}$ y todo $0 \leq j \leq n$. Entoces

$$|x+y|^n = \left|\sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}\right| \leq \sum_{j=0}^{n} \left|\binom{n}{j}\right| |x|^j|y|^{n-j} \leq N(n+1)|x|^n.$$

Por tanto, $|x+y| \leq N^{1/n}(n+1)^{1/n}\mathtt{max}\{|x|,|y|\}$ y haciendo $n \to \infty$ concluimos que $|x+y| \leq \mathtt{max}\{|x|,|y|\}$.

□

Como corolario del resultado anterior deducimos que si k es un cuerpo de característica positiva entonces k sólo admite valoraciones no arquimedianas pues el conjunto $\{n \cdot 1 := \sum_{j=1}^{n} 1 \mid n \in \mathbb{N}\}$ es finito.

La siguiente obervación será útil:

Lema 1.1.8. Sea $|\cdot|$ un valor absoluto no arquimediano. Dados $a_i \in k, i = 1, \ldots, n$ tales que $|a_1| > |a_j|$ para todo $j = 2, \ldots, n$ tenemos que

$$|a_1 + \cdots + a_n| = |a_1|.$$

Demostración. Razonamos por inducción. Para $n = 2$ tenemos que $|a_1| = |(a_1+a_2)-a_2| \leq \mathtt{max}\{|a_1+a_2|, |a_2|\}$. Debe ser $\mathtt{max}\{|a_1+a_2|, |a_2|\} = |a_1+a_2|$ pues en otro caso $|a_1| \leq |a_2|$ que es absurdo. Concluimos que $\mathtt{max}\{|a_1|, |a_2|\} = |a_1+a_2|$.

Supuesto el resultado cierto para $n-1$ elementos, i.e. $|a_1| = |a_1+\cdots+a_{n-1}|$, vamos a demostrarlo para n elementos. Tenemos que

$$|a_1| = \left|\sum_{j=1}^{n-1} a_j\right| = \left|\sum_{j=1}^{n} a_j - a_n\right| \leq \mathtt{max}\Big\{\left|\sum_{j=1}^{n} a_j\right|, |a_n|\Big\}.$$

Como antes, debe ser $\mathtt{max}\{|a_1+\cdots+a_n|, |a_n|\} = |a_1+\cdots+a_n|$ pues de otra forma sería $|a_1| \leq |a_n|$. Concluimos pues que $\mathtt{max}_i\{|a_i|\} = |a_1| \leq |a_1+\cdots+a_n| \leq \mathtt{max}_i\{|a_i|\}$.

□

El lema anterior suele presentarse en la siguiente forma:

$$a_1 + \cdots + a_n = 0 \Rightarrow \exists\ i \neq j : |a_i| = |a_j| = \mathtt{max}_r\{|a_r|\}.$$

Dada un **valor absoluto no arquimediano** $|\cdot|$ del cuerpo k definimos la aplicación

$$\begin{array}{rccc} \nu: & k & \to & \mathbb{R} \cup \{\infty\}, \\ & 0 & \mapsto & \infty, \\ & x \neq 0 & \mapsto & -\mathtt{log}|x|. \end{array}$$

La aplicación ν verifica las siguientes propiedades:

V1. $\nu(x) = \infty \Leftrightarrow x = 0$.

V2. $\nu(xy) = \nu(x) + \nu(y)$.

V3. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

Entenderemos que para todo $a \in \mathbb{R}$ es $a < \infty, a + \infty = \infty, \infty + \infty = \infty$. Una función ν en k verificando las propiedades anteriores se dice que es una **valoración** de k. Como antes, todo cuerpo admite la función trivial $\nu(x) = 0\ \forall x \neq 0$ y $\nu(0) = \infty$. Dos valoraciones ν_1, ν_2 son **equivalentes** si $\nu_1 = s\nu_2$ para algún número real $s > 0$. Dada una valoración ν podemos obtener un valor absoluto definiendo $|x| = q^{-\nu(x)}$, con $q > 1$ un número real fijado previamente. Es claro que los valores absolutos asociados a dos valoraciones equivalentes son también equivalentes. La siguiente proposición nos muestra la importancia de los valores absolutos no arquimedianas, o equivalentemente, las valoraciones:

Proposición 1.1.9. El subconjunto

$$o = \{x \in k \mid \nu(x) \geq 0\} = \{x \in k \mid |x| \leq 1\}$$

es un anillo con grupo de unidades

$$o^\times = \{x \in k \mid \nu(x) = 0\} = \{x \in k \mid |x| = 1\}$$

y con un único ideal maximal

$$\mathfrak{p} = \{x \in k \mid \nu(x) > 0\} = \{x \in k \mid |x| < 1\}.$$

Demostración. Para ver que o es un anillo basta probar que es cerrado para las dos operaciones de k y que contiene a los respectivos elementos neutros. Como $\nu(0) = \infty$ y $\nu(1) = 0$ tenemos que $0, 1 \in o$. Por otro lado, dados $x, y \in o$ tenemos que $\nu(xy) = \nu(x) + \nu(y) \geq 0$ y $\nu(x+y) \geq \min\{\nu(x), \nu(y)\} \geq 0$ luego $xy, x + y \in o$. Para las unidades de o tenemos las siguientes equivalencias:

$$x \in o^\times \Leftrightarrow \nu(x) = 0 \Leftrightarrow -\nu(x) = 0 \Leftrightarrow \nu(x^{-1} \in k) = 0 \Leftrightarrow x^{-1} \in o.$$

Es claro que $\mathfrak{p}$ es un ideal y como $o \setminus \mathfrak{p} = o^\times$ concluimos que o es un anillo local cuyo único ideal maximal es $\mathfrak{p}$.

□

Es importante resaltar que el anillo o sólo depende de la clase de equivalencia de la valoración ν, es decir, es un invariante algebraico de los valores absolutos no arquimedianos.

Observar que el anillo o verifica la siguiente condición:

$$\forall x \in k \Rightarrow x \in o \text{ o } x^{-1} \in o.$$

Además o es un dominio (subanillo de k) y por la propiedad anterior su cuerpo de fracciones coincide con k. Un anillo verificando la propiedad anterior se dice que es un **anillo de valoración**. Su único ideal maximal es $\mathfrak{p} = \{x \in o \mid x^{-1} \notin o\}$ y el cuerpo $o/\mathfrak{p}$ es el **cuerpo residual** de o. Todo anillo de valoración es **íntegralmente cerrado** pues si $x \in k$ es entero sobre o entonces verifica una ecuación de la forma

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, a_i \in o.$$

Supuesto que $x \notin o$ entonces $x^{-1} \in o$ y esto implica que $x = -a_1 - a_2 x^{-1} - \cdots - a_n (x^{-1})^{n-1} \in o$.

Introduciremos ahora una clase de valoraciones muy importante. Diremos que una valoración ν es **discreta** si existe $s \in \mathbb{R}_{>0}$ tal que $s = \mathtt{min}_{\{x \in k \mid \nu(x) > 0\}} \nu(x)$. Veamos que entonces es $\nu(k^\times) = \mathbb{Z}s = \langle s \rangle$. Claramente $\mathbb{Z}s = \nu(\{x^n\}_{n \in \mathbb{N}}) \subset \nu(k^\times)$. Para el recíproco, sea $t \in \nu(k^\times)$ y consideremos el elemento $t - s[t/s] \in \nu(k^\times)$, donde $[r] \in \mathbb{Z}$ es la parte entera del número real r. Sabemos que $[t/s] \in \mathbb{Z}$ es el único número entero tal que $[t/s] \leq t/s < [t/s] + 1$, luego $s[t/s] \leq t < s[t/s] + s$, de donde deducimos que $0 \leq t - s[t/s] < s$ y como $t - s[t/s] \in \nu(k^\times)$ la desigualdad contradice nuestra elección de s. Debe ser $t = s[t/s] \in \mathbb{Z}s$.

Si es $s = 1$ diremos que ν está normalizada. Es evidente que dada una valoración discreta siempre podemos normalizarla sin más que dividir por s y este proceso no cambia el anillo de valoración o. Podemos suponer sin pérdida de generalidad que ν está normalizada y consideramos $\pi \in o$ tal que $\nu(\pi) = 1$. Todo elemento π tal que $\nu(\pi) = 1$ (en general $\nu(\pi) = \text{mín}\{\nu(x) > 0\}$) diremos que es **un parámetro de uniformización**. Además todo parámetro de uniformización π es un **elemento primo**. En efecto, todo elemento $x \in k^\times$ admite una única representación de la forma $x = u\pi^m$ con $m \in \mathbb{Z}$ y $u \in o^\times$ ya que si $\nu(x) = m$ entonces $\nu(x\pi^{-m}) = 0$, es decir, $u = x\pi^{-m} \in o^\times$.

Tenemos el siguiente resultado:

Proposición 1.1.10. Si ν es una valoración discreta de k, entonces el anillo o es un dominio de ideales principales. Supongamos además que ν está normalizada. Entonces los ideales no nulos de o son las potencias de $\mathfrak{p}$:

$$\mathfrak{p}^n = o\pi^n = \{x \in k \mid \nu(x) \geq n\},\ n \geq 0,$$

donde π es un parámetro de uniformización. Además, $\mathfrak{p}^n/\mathfrak{p}^{n+1} \simeq o/\mathfrak{p}$.

Observación 1.1.11. En álgebra conmutativa los anillos que son dominios de ideales principales con un único ideal primo no nulo se denominan **anillos de valoración discreta**. Esta proposición

demuestra que si ν es una valoración discreta entonces su anillo de valoración asociado o es de hecho un anillo de valoración discreta.

Demostración. Sea $\mathfrak{a}$ un ideal de o y $x \neq 0$ un elemento de $\mathfrak{a}$ tal que $n := \nu(x) = \mathtt{min}_{y\in\mathfrak{a}}\{\nu(y)\}$. Entonces $x = u\pi^n$ con $u \in o^\times$, es decir, $o\pi^n \subset \mathfrak{a}$. Si $y = v\pi^m \in \mathfrak{a}$ es arbitrario con $v \in o^\times$, entonces $m = \nu(y) \geq n$ por construcción luego $y = (v\pi^{m-n})\pi^n \in o\pi^n$. Esto concluye que $\mathfrak{a} = o\pi^n$. Para la última parte del enunciado consideramos el homomorfismo o-lineal $\mathfrak{p}^n \to o/\mathfrak{p}$ tal que $a\pi^n \mapsto a + \mathfrak{p}$. Claramente es sobreyectivo pues $\mathfrak{p}^n = o\pi^n$, basta ver que su núcleo es $\mathfrak{p}^{n+1}$. Para ello, notar que la imagen de $a\pi^n$ es 0 si y sólo si $a \in \mathfrak{p} = o\pi$. Por tanto, $a\pi^n \mapsto 0$ si y sólo si $a\pi^n \in \mathfrak{p}^{n+1}$.

□

Dado un cuerpo k con valoración discreta la cadena de ideales

$$o \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \cdots$$

formada por los ideales del anillo de valoración o es una base de entornos de 0 para la topología de k. En efecto, si ν está normalizada y consideramos $|\cdot| = q^{-\nu}$ $(q > 1)$ un valor absoluto asociado, entonces

$$\mathfrak{p}^n = \{x \in k \mid \nu(x) \geq n\} = \{x \in k \mid |x| < 1/q^{n-1}\} = B(0, 1/q^{n-1}).$$

Como la aplicación $x \in k \mapsto 1 + x \in k$ es un automorfismo, tenemos que los conjuntos

$$U^{(n)} = 1 + \mathfrak{p}^n = \{x \in k \mid |1 - x| < 1/q^{n-1}\},\ n > 0$$

forman una base de entornos del 1. Además, los conjuntos $U^{(n)}$ no contienen al 0 y por ello los conjuntos $U^{(n)}$ también forman una base de entornos del 1 en $k^\times$ respecto a la topología inducida. De hecho $U^{(n)} = 1 + \mathfrak{p}^n$ es un conjunto cerrado para la multiplicación pues si $x, y \in U^{(n)}$ entonces $x-1, y-1 \in \mathfrak{p}^n$, i.e. existen $x', y' \in \mathfrak{p}^n$ con $x = 1+x', y = 1+y'$ y por ello $xy = 1+x'+y'+x'y' \in 1+\mathfrak{p}^n$. Así mismo, dado $x \in U^{(n)}$ entonces $|1 - x^{-1}| = |x|^{-1}|x - 1| = 1 \cdot |1 - x| < 1/q^{n-1}$ pues $x \notin \mathfrak{p}$ y es una unidad. Por tanto tenemos la siguiente cadena de **subgrupos**

$$o^\times = U^{(0)} \supset U^{(1)} \supset U^{(2)} \supset ...$$

Diremos que $U^{(n)}$ es el **grupo de unidades de altura** n y $U^{(1)}$ es el grupo de **unidades principales**. Tenemos el siguiente resultado:

Proposición 1.1.12. Existen isomorfismos de grupos $o^\times/U^{(n)} \simeq (o/\mathfrak{p}^n)^\times$ y $(U^{(n)}/U^{(n+1)}, \cdot) \simeq (o/\mathfrak{p}, +)$ para $n \geq 1$.

Demostración. Para el primer isomorfismo consideramos el homomorfismo de anillos sobreyectivo $o \to o/\mathfrak{p}^n$. Si lo restringimos a las unidades obtenemos un homomorfismo de grupos sobreyectivo $o^\times \to (o/\mathfrak{p}^n)^\times$ cuyo núcleo es el conjunto $1+\mathfrak{p}^n = U^{(n)}$.

Para el segundo, elegimos un parámetro de uniformización π y definimos

$$1 + o\pi^n = U^{(n)} \ni 1 + a\pi^n \overset{\varphi}{\mapsto} a + \mathfrak{p} \in o/\mathfrak{p}.$$

Es un homomorfismo de grupos pues

$$\varphi\big((1+a\pi^n)(1+b\pi^n)\big) = \varphi\big(1+(a+b+ab\pi^n)\big) = (a+b+ab\pi^n)+\mathfrak{p} = (a+\mathfrak{p})+(b+\mathfrak{p}) = \varphi(1+a\pi^n)+\varphi(1+b\pi^n).$$

Basta ahora observar que el homomorfismo φ es sobreyectivo y su núcleo es $U^{(n+1)}$.

□

1.2. Compleción

Definición 1.2.1. Un cuerpo con valoración $(k, |\cdot|)$ se dice **completo** si toda sucesión de Cauchy $\{a_n\}_{n\in\mathbb{N}}$ en k converge a un elemento $a \in k$, es decir,

$$\lim_{n\to\infty} |a_n - a| = 0.$$

La noción de sucesión de Cauchy en nuestro contexto es análoga a la estudiada en los cursos elementales de topología. A partir de un cuerpo con valor absoluto $(k, |\cdot|)$ obtenemos un cuerpo valorado completo $(\hat{k}, |\cdot|)$ por el proceso de **compleción**. A continuación describimos dicho proceso: Sea R el anillo formado por todas las sucesiones de Cauchy de $(k, |\cdot|)$ (cuyas operaciones son la suma y producto componente a componente) y $\mathfrak{m}$ el ideal formado por todas las sucesiones de Cauchy convergentes a 0.

Lema 1.2.2. Con la notación anterior, se verifica que el anillo cociente $R/\mathfrak{m}$ es un cuerpo. En particular, $\mathfrak{m}$ es un ideal maximal.

Demostración. Sea $(a_i)_{i\in\mathbb{N}}$ una sucesión que no pertenece a $\mathfrak{m}$. Veamos que el conjunto $I = \{i \in \mathbb{N} \ : \ a_i = 0\}$ es finito. Por definición de sucesion de Cauchy, dado $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $|a_i - a_j| < \varepsilon$ para todo $i, j \geq N$. Si I fuera infinito, existiría $i_N \in I$ verificando $i_N \geq N$ y tal que $|a_i - a_{i_N}| < \varepsilon$ para todo $i \geq N$. Como $i_N \in I$ entonces $a_{i_N} = 0$ y por ello $|a_i| \leq \varepsilon$ para todo $i \geq N$. Esto demostraría que la sucesión (a_i) converge a 0, contradiciendo la hipótesis $(a_i) \notin \mathfrak{m}$.

Podemos ahora demostrar el enunciado. Sea $(a_i) + \mathfrak{m} \in R/\mathfrak{m}$ un elemento no nulo. Sabemos que el conjunto de índices i tales que $a_i = 0$ es finito y por ello podemos suponer que $a_i \neq 0$ para todo

i, pues eso es irrelevante en lo que a convergencia se refiere (es decir, en la clase de equivalencia $(a_i)+\mathfrak{m}$). Como (a_n) es una sucesión de Cauchy, la sucesión $(|a_n|)$ también es una sucesión de Cauchy en $\mathbb{R}$ y esto implica que $(1/|a_n|)=(|a_n^{-1}|)$ es una sucesión de Cauchy. En particular, existe $M\in\mathbb{R}_{>0}$ tal que $|a_n^{-1}|\leq M$ para todo $n\in\mathbb{N}$. Dado $\varepsilon>0$, sea $N\in\mathbb{N}$ tal que $|a_n-a_m|<\varepsilon/M^2$ para todo $n,m\geq N$. Entonces $\left|1/a_n-1/a_m\right|=|a_n^{-1}a_m^{-1}||a_n-a_m|\geq M^2\cdot\varepsilon/M^2=\varepsilon$. En definitiva, $(1/a_n)\in R$ y obtenemos que $(1/a_n)+\mathfrak{m}$ es el inverso de $(a_n)+\mathfrak{m}$.

□

Este lema nos permite definir el cuerpo $\hat{k}$ como $\hat{k}=R/\mathfrak{m}$. Veamos que en $\hat{k}$ podemos encontrar, de manera natural, una valor absoluto a partir de $|\cdot|:k\to\mathbb{R}$. Para ello, antes observamos que dado $(a_n)\in R$ entonces $(|a_n|)$ es una sucesión de Cauchy de números reales y por ello existe el límite $\lim_{n\to\infty}|a_n|$. Definimos

$$|(a_n)+\mathfrak{m}|=\lim_{n\to\infty}|a_n|.$$

Veamos que la definición no depende del representante de la clase: Si $(a_n)+\mathfrak{m}=(b_n)+\mathfrak{m}$ entonces $(a_n-b_n)\in\mathfrak{m}$ y por ello $|a_n-b_n|\to 0$. Concluimos que $||a_n|-|b_n||\to 0$ y por ello $\lim_{n\to\infty}|a_n|=\lim_{n\to\infty}|b_n|$. Es sencillo comprobar que $(\hat{k},|\cdot|)$ es un cuerpo con valor absoluto.

Por otro lado, podemos ver k como subconjunto de $\hat{k}$ haciendo $a\mapsto\bar{a}:=(a,a,a,\dots)+\mathfrak{m}$. Esta identificación nos permite demostrar que k es un subcuerpo denso de $\hat{k}$. En efecto, dado $\alpha\in\hat{k}$, si la sucesión (a_n) es un representante de α entonces $\alpha=\lim_{n\to\infty}\overline{a_n}$ pues $|\alpha-\overline{a_m}|=\lim_{n\to\infty}|a_n-a_m|=0$ para m suficientemente grande. Hemos probado que todo elemento de $\hat{k}$ se puede aproximar por una sucesión de elementos de k. La densidad de k en $\hat{k}$ nos da como corolario que $\hat{k}$ es un cuerpo completo respecto a su valor absoluto, como vamos a ver: Sea $(\alpha_i)_{i\in\mathbb{N}}=((a_{ij})_{j\in\mathbb{N}}+\mathfrak{m})_{i\in\mathbb{N}}$ una sucesión de Cauchy de elementos de $\hat{k}$ y para cada i consideremos $a_i\in k$ tal que $|\alpha_i-\overline{a_i}|<1/i$. Entonces la sucesión $(\alpha_n-\overline{a_n})$ es una sucesión de Cauchy de elementos de $\hat{k}$ y por ello la sucesión $(\overline{a_n})$ también es de Cauchy. Esto último implica inmediatamente que (a_i) es una sucesión de Cauchy de elementos de k. Escribiendo $\alpha=(a_i)+\mathfrak{m}$ y tenemos que

$$\begin{aligned}
\lim_{n\to\infty}|\alpha_n-\alpha| &= \lim_{n\to\infty}\left(\lim_{m\to\infty}|a_{nm}-a_m|\right)\\
&= \lim_{n\to\infty}\left(\lim_{m\to\infty}|a_{nm}-a_n+a_n-a_m|\right)\\
&\leq \lim_{n\to\infty}\left(\lim_{m\to\infty}|a_{nm}-a_n|+\lim_{m\to\infty}|a_n-a_m|\right)\\
&= \lim_{n\to\infty}|\alpha_n-\overline{a_n}|+\lim_{n,m\to\infty}|a_n-a_m|=0.
\end{aligned}$$

Estas últimas observaciones prueban que la compleción de un cuerpo completo es el mismo. Además, la compleción de un cuerpo es única salvo isomorfismos:

Lema 1.2.3. Si $(\hat{k}', |\cdot|')$ es un cuerpo con valor absoluto completo que contiene a $(k, |\cdot|)$ como un subcuerpo denso, entonces es isomorfo a $(\hat{k}, |\cdot|)$ (isomorfismo compatible con las valoraciones).

Demostración. Como k es denso en $\hat{k}$, dado un elemento $\alpha \in \hat{k}$ tenemos que existe una sucesión (a_n) de elementos de k tal que $\alpha = \lim_{n\to\infty} a_n$ con respecto a $|\cdot|$. Consideramos $\sigma : \hat{k} \to \hat{k}'$ definido como $\sigma(\lim_{n\to\infty} a_n) = \lim_{n\to\infty} a_n$, donde el primer límite es respecto a $|\cdot|$ y el segundo respecto a $|\cdot|'$. Claramente $|\sigma a|' = |a|$ para todo $a \in k$. Es inmediato comprobar que σ es un homomorfismo biyectivo.

□

Una vez estudiado el concepto de cuerpo completo es interesante comprenderlo imponiendo restricciones a su valor absoluto. El siguiente teorema, que no demostraremos, nos dice que si el valor absoluto es arquimediano entonces se trata de $\mathbb{R}$ o $\mathbb{C}$ con el valor absoluto usual:

Teorema 1.2.4. Sea k un cuerpo que es completo respecto a un valor absoluto arquimediano $|\cdot|$. Entonces existe un isomorfismo σ de k en $\mathbb{R}$ o $\mathbb{C}$ verificando

$$|a| = |\sigma a|^s \ \forall\ a \in k$$

para algún $s \in (0, 1]$ fijo.

Demostración. Ver [**?**], Teorema II.4.2.

□

Visto el caso en que el valor absoluto es arquimediano pasamos a ver las implicaciones de que el valor absoluto sea no arquimediano. El primer paso es traducir la teoría al contexto de las valoraciones. Sea ν una valoración del cuerpo k. La extendemos canónicamente a una valoración $\hat{\nu}$ de la compleción $\hat{k}$ definiendo

$$\hat{\nu}(a) = \lim_{n\to\infty} \nu(a_n),$$

siendo $a = \lim_{n\to\infty} a_n = (a_n) + \mathfrak{m} \in \hat{k},\ a_n \in k$. Es sencillo comprobar que $\hat{\nu}$ está bien definida como aplicación y que es una valoración de $\hat{k}$.

Notemos que la sucesión $\nu(a_n)$ es constante a partir de cierto n_0 en adelante. En efecto, como $a = \lim_{n\to\infty} a_n$, sabemos que $\hat{\nu}(a - a_n) \to \infty$ y por ello, fijado $\hat{\nu}(a)$ existe $n_0 \in \mathbb{N}$ tal que $\hat{\nu}(a - a_n) > \hat{\nu}(a)$ para todo $n \geq n_0$. Entonces es $\min\{\hat{\nu}(a_n - a), \hat{\nu}(a)\} = \hat{\nu}(a_n - a + a) = \hat{\nu}(a_n)$ (ver 1.1.8). Concluimos que $\hat{\nu}(a_n) = \hat{\nu}(a)$ para todo $n \geq n_0$. Obtenemos que

$$\nu(k^\times) = \hat{\nu}(\hat{k}^\times),$$

es decir, el conjunto $\nu(k^\times) \subset \mathbb{R}$ es cerrado. En particular, si ν es discreta y normalizada entonces también lo es la extensión $\hat{\nu}$.

Una consecuencia importante de que el valor absoluto sea no arquimediano es que es particularmente sencillo hacer análisis sobre el cuerpo k. Concretamente, para que una sucesión $(a_n)_{n\in\mathbb{N}}$ de elementos de k sea de Cauchy es suficiente que la sucesión $(a_{n+1} - a_n)_{n\in\mathbb{N}}$ converja a 0. En efecto, como

$$\nu(a_n - a_m) = \nu\left(\sum_{i=m}^{n-1}(a_{i+1} - a_i)\right) \geq \min_{m\leq i<n}\{\nu(a_{i+1} - a_i)\},$$

concluimos que si los números $\nu(a_{i+1}-a_i)$ son muy grandes también lo serán los números $\nu(a_n-a_m)$. Este hecho, aplicado a la convergencia de una serie infinita $\sum_{i=0}^{\infty} a_i$ nos dice que la serie converge si y sólo si la sucesión (a_i) converge a 0.

Sea $\hat{o}$ (resp. $\hat{\mathfrak{p}}$) el anillo de valoración (resp. el ideal maximal) asociado a $\hat{\nu}$. Claramente, $\hat{o}$ es el conjunto de los límites de las sucesiones de Cauchy cuyos términos están en o y por ello $\hat{o}$ es la clausura topológica de o en $\hat{k}$. Lo mismo se tiene para $\hat{\mathfrak{p}}$. De hecho, $\hat{\mathfrak{p}}^n$ es la clausura de $\mathfrak{p}^n$ en $\hat{k}$ ($\forall\ n \geq 0$) pues $\mathfrak{p}^n = \{x \in k \mid \nu(x) \geq n\}$. El siguiente resultado es útil:

Proposición 1.2.5. Si $o \subset k$, resp. $\hat{o} \subset \hat{k}$, es el anillo de valoración de ν, resp. $\hat{\nu}$, y $\mathfrak{p}$, resp. $\hat{\mathfrak{p}}$, es el ideal maximal, tenemos entonces que

$$\hat{o}/\hat{\mathfrak{p}}^n \simeq o/\mathfrak{p}^n \ \forall\ n \geq 0.$$

Demostración. Sea ν una valoración (no arquimediana). Consideramos la inclusión $\iota : o \hookrightarrow \hat{o}$ (estamos usando la identificación $a \in k\ (a, a, a, \dots) + \mathfrak{m} \in \hat{k}$). Componemos ι con la proyección canónica $\pi : \hat{o} \to \hat{o}/\hat{\mathfrak{p}}^n$. Estudiamos la imagen y el núcleo de $\pi \circ \iota$:

- **Núcleo:** $\texttt{ker}(\pi \circ \iota) = \hat{\mathfrak{p}}^n \cap o = \mathfrak{p}^n$.
- **Imagen:** Sea $x \in \hat{o}$. Como $\hat{o} = \overline{o}^{\hat{k}}$ sabemos que existe $a \in o$ todo lo cerca de x que deseemos, por ejemplo, existe $a \in o$ tal que $\hat{\nu}(x-a) \geq n$. Concluimos que existe $a \in o$ tal que $x - a \in \hat{\mathfrak{p}}^n$, o equivalentemente, $x+\hat{\mathfrak{p}}^n = a+\hat{\mathfrak{p}}^n$. Esto concluye que $\pi\circ\iota$ es una homomorfismo sobreyectivo.

Gracias al primer teorema de isomorfia obtenemos que $\hat{o}/\hat{\mathfrak{p}}^n \simeq o/\mathfrak{p}^n$.

□

Tenemos el siguiente resultado que, intuitivamente, nos dice que el cuerpo $\hat{k}$ se obtiene a partir de o por medio de series de Laurent cuando la valoración ν es discreta:

Proposición 1.2.6. Sea (k, ν) un cuerpo con valoración discreta y sea $R \subset o$ un sistema de representantes para $o/\mathfrak{p}$ tal que $0 \in R$. Sea π un parámetro de uniformización de ν. Entonces todo $x \in \hat{k} \setminus \{0\}$ admite una única representación como una serie convergente

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$$

con $a_i \in R, a_0 \neq 0$ y $m \in \mathbb{Z}$.

Demostración. Sea $x = u\pi^m$ con $u \in \hat{o}^\times$. Como $\hat{o}/\hat{\mathfrak{p}} \simeq o/\mathfrak{p}$, la clase $u+\hat{p}$ tiene un único representante $a_0 \in R$ con $a_0 \neq 0$. Obtenemos entonces $u = a_0 + b_1\pi$ para algún $b_1 \in \hat{o}$.

Supongamos que hemos obtenido $a_0, a_1, \ldots, a_{n-1} \in R$ tales que

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + b_n\pi^n$$

para algún $b_n \in \hat{o}$ y que los a_i están únivocamente determinados por dicha ecuación. Entonces el representante $a_n \in R$ de $b_n + \hat{\mathfrak{p}} \in \hat{o}/\hat{p}$ está univocamente determinado por u y tenemos que $b_n = a_n + b_{n+1}\pi$ para algún $b_{n+1} \in \hat{o}$. Entonces

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n + b_{n+1}\pi^{n+1}.$$

Reiterando el proceso podemos hallar una serie infinita $\sum_{i=0}^{\infty} a_i\pi^i$ unívocamente determinada por u. La convergencia a u está garantizada pues el término residual $b_{n+1}\pi^{n+1}$ converge a 0.

□

Ahora vamos a describir el anillo de valoración discreta o por medio de cierto límite proyectivo. Para ello, sea k un cuerpo completo respecto a una valoración discreta con anillo de valoración o e ideal maximal $\mathfrak{p}$. Consideremos el sistema inverso formado por los morfismos

$$f_{nm} : o/\mathfrak{p}^m \to o/\mathfrak{p}^n$$

tal que $f_{nm}(a+\mathfrak{p}^m) = a+\mathfrak{p}^n$, con $m \geq n$. Es sencillo comprobar que el conjunto de morfismos dado forma un sistema inverso. Podemos obtener el límite proyectivo de dicho sistema

$$\varprojlim o/\mathfrak{p}^n = \{x \in \prod_{t=1}^{\infty} o/\mathfrak{p}^t \mid \Pi_i(x) = (f_{ij} \circ \Pi_j)(x) \ \forall\ i \leq j\}$$

que de manera natural tiene estructura de anillo. Si además consideramos que los anillos $o/\mathfrak{p}^n$ están dotados de la topología discreta, entonces el límite $\varprojlim o/\mathfrak{p}^n$ es un espacio topológico cuya topología es la topología inicial asociada a los homomorfismos canónicos de proyección $\Pi_n : \varprojlim o/\mathfrak{p}^n \to o/\mathfrak{p}^n$. Notar que dicha topología coincide con la de ser subespacio de $\prod o/\mathfrak{p}^t$ (con la topología producto) y además es cerrado. Tenemos el siguiente resultado:

Proposición 1.2.7. El morfismo canónico

$$\mathfrak{o} \to \varprojlim \mathfrak{o}/\mathfrak{p}^n$$

es un isomorfismo y un homeomorfismo. El mismo resultado es cierto para el morfismo

$$\mathfrak{o}^\times \to \varprojlim \mathfrak{o}^\times/U^{(n)}.$$

Demostración. Primero observar que el morfismo canónico del enunciado es el obtenido a partir de la propiedad universal del límite proyectivo aplicada al conjunto de homomorfismos (continuos) $p_n : \mathfrak{o} \to \mathfrak{o}/\mathfrak{p}^n$ (la continuidad se sigue de que $\{\mathfrak{p}^n\}$ es una base de entornos de 0). Por tanto existe un único morfismo $p : \mathfrak{o} \to \varprojlim \mathfrak{o}/\mathfrak{p}^n$ tal que $\Pi_n \circ p = p_n$, i.e. $p(a) = (a + \mathfrak{p}^n)_{n\in\mathbb{N}} \in \prod \mathfrak{o}/\mathfrak{p}^n$. Ahora es claro que el núcleo de p es el ideal $\cap_{i=1}^{\infty}\mathfrak{p}^i$ y dicha intersección es (0), luego p es inyectivo. Para la sobreyectividad tomamos un parámetro de uniformización π y $R \subset \mathfrak{o}, R \ni 0$ un sistema de representantes de $\mathfrak{o}/\mathfrak{p}$. Por 1.2.6 podemos escribir $a + \mathfrak{p}^n$ de manera única en la forma

$$a \equiv (a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}) + \mathfrak{p}^n,$$

con $a_i \in R$. Por tanto, cada elemento $s \in \varprojlim \mathfrak{o}/\mathfrak{p}^n$ está dado por una sucesión de sumas

$$s_n + \mathfrak{p}^n = (a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}) + \mathfrak{p}^n,\ n = 1, 2, \ldots$$

con coeficientes fijos $a_i \in R$. Basta ahora considerar el elemento $x = \sum_{i=0}^{\infty} a_i\pi^i \in \mathfrak{o}$ para concluir que p es sobreyectivo.

Veamos ahora la continuidad del homomorfismo biyectivo p : Los conjuntos $O_n = \prod_{j>n} \mathfrak{o}/\mathfrak{p}^j$ forman una base de entornos del 0 en el producto $\prod_{j=1}^{\infty} \mathfrak{o}/\mathfrak{p}^j$. La imagen por p de la base de entornos $\mathfrak{p}^n$ del 0 en $\mathfrak{o}$ es la base de entornos $O_n \cap \varprojlim \mathfrak{o}/\mathfrak{p}^i$ de 0 en $\varprojlim \mathfrak{o}/\mathfrak{p}^i$. Esto implica que p es un homeomorfismo.

Por último, p induce un isomorfismo y homeomorfismo en los grupos de unidades

$$\mathfrak{o}^\times \simeq \left(\varprojlim \mathfrak{o}/\mathfrak{p}^n\right)^\times \simeq \varprojlim (\mathfrak{o}/\mathfrak{p}^n)^\times \simeq \varprojlim \mathfrak{o}^\times/U^{(n)}.$$

El segundo isomorfismo se deduce a partir de la propiedad universal del límite y sabiendo que todo homomorfismo de anillos induce un homomorfismo entre los grupos de unidades.

□

La proposición anterior parece indicar que para las unidades también podemos obtener una expansión por medio de la filtración de los subgrupos de unidades $U^{(n)}$. Esto es lo que demostramos en el siguiente lema:

Lema 1.2.8. Sea (k,ν) un cuerpo con valoración discreta y sea $R \subset o$ un sistema de representantes de $o/\mathfrak{p}$ con $R \ni 0$. Sea π un parámetro de uniformización de ν. Entonces todo elemento $x \in \hat{k}^\times$ admite una única representación como un producto convergente:

$$x = \pi^m a_0 \prod_{i=1}^{\infty}(1 + a_i\pi^i)$$

con $a_i \in R,\ a_0 \neq 0$ y $m \in \mathbb{Z}$.

Demostración. Como $\hat{o}/\hat{p}^n \simeq o/\mathfrak{p}^n$ tenemos los isomorfismos canónicos

$$\frac{\hat{o}}{\hat{U}^{(n)}} \simeq \left(\frac{\hat{o}}{\hat{\mathfrak{p}}^n}\right)^\times \simeq \left(\frac{o}{\mathfrak{p}}\right)^\times \simeq \frac{o^\times}{U^{(n)}}.$$

Escribimos $x = u\pi^m$ con $m \in \mathbb{Z}$ y $u \in o^\times$. Denotemos el isomorfismo canónico $f_0 : o/U^{(1)} \to (o/\mathfrak{p})^\times,\ aU^{(1)} \mapsto a + p$. Tenemos que existe un único $a_0 \in R \setminus \{0\}$ tal que $f_0(uU^{(1)}) = a_0 + \mathfrak{p} = f_0(a_0U^{(1)})$ de modo que $ua_0^{-1} \in U^{(1)}$, es decir, existe $u_1 \in U^{(1)}$ con $u = a_0u_1$. Consideremos el isomorfismo de grupos $f_1 : U^{(1)}/U^{(2)} \to o/\mathfrak{p}$ que lleva $(1 + a\pi)U^{(2)}$ en $a + \mathfrak{p}$. Tenemos que existe un único $a_1 \in R$ tal que $f_1(u_1U^{(2)}) = a_1 + \mathfrak{p} = f_1((1 + a_1\pi)U^{(2)})$, es decir, existe $u_2 \in U^{(2)}$ tal que $u_1 = (1 + a_1\pi)u_2$. Si reiteramos este proceso (usando los isomorfismos $U^{(n)}/U^{(n+1)} \to o/\mathfrak{p}$) obtendremos la expansión única del enunciado.

□

Algo que nos interesa es saber resolver ecuaciones sobre cuerpos completos o equivalentemente estudiar las extensiones finitas de un cuerpo completo. Para ello sea k un cuerpo completo respecto a un valor absoluto no arquimediano $|\cdot|$, sea o su anillo de valoración con ideal maximal $\mathfrak{p}$ y cuerpo residual $\kappa = o/\mathfrak{p}$. Dado un polinomio $f(x) = a_nx^n + \cdots + a_1x + a_0 \in o[x]$ diremos que es **primitivo** si

$$|f| := \text{máx}\{|a_n|, \ldots, |a_0|\} = 1.$$

Tenemos el siguiente resultado conocido como **lema de Hensel**:

Teorema 1.2.9. Si un polinomio primitivo $f \in o[x]$ admite módulo $\mathfrak{p}[x]$ una factorización

$$f(x) + \mathfrak{p}[x] = \overline{g}(x)\overline{h}(x)$$

siendo $\overline{g}, \overline{h} \in \kappa[x]$ polinomios coprimos, entonces f admite una factorización

$$f = g \cdot h$$

con $g, h \in o[x]$ tal que $\mathtt{deg}(g) = \mathtt{deg}(\overline{g})$ y $g + \mathfrak{p}[x] = \overline{g},\ h + \mathfrak{p}[x] = \overline{h}$.

Demostración. Ver [**?**], página 129.

□

A partir de este resultado obtenemos el siguiente corolario:

Corolario 1.2.10. Sea k un cuerpo completo respecto a una valor absoluto no arquimediano $|\cdot|$. Entonces, para todo polinomio irreducible $f(x) = a_n x^n + \cdots + a_0 \in k[x]$ tal que $a_0 a_n \neq 0$, tenemos que $|f| = \text{máx}\{|a_0|, |a_n|\}$. En particular, $a_n = 1$ y $a_0 \in o$ implican que $f \in o[x]$.

Demostración. Sin pérdida de generalidad podemos suponer que $f \in o$ y tras dividir por un coeficiente a_i tal que $|f| = |a_i|$ podemos suponer que $|f| = 1$. Sea a_r el coeficiente de menor índice tal que $a_r = |f| = 1$. Tenemos que $f + \mathfrak{p}[x] = x^r(a_r + a_{r+1}x + \cdots + a_n x^{n-r}) + \mathfrak{p}[x]$. Si fuera $\mathtt{max}\{|a_0|, |a_n|\} < 1$ entonces $0 < r < n$ y la factorización anterior en módulo $\mathfrak{p}[x]$, gracias a 1.2.9, contradice la hipótesis $a_0 a_n \neq 0$.

□

Es interesante comentar que la función $|f| = \text{máx}(|a_n|, \ldots, |a_0|)$ da lugar a una función que verifica las propiedades de un valor absoluto si el valor absoluto $|\cdot|$ de k es no arquimediano (k no necesariamente completo). En efecto, la única propiedad no trivial es su carácter multiplicativo: Sean $f, g \in k[x]$ con $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i$ de modo que r y s son los menores índices verificando $|f| = |a_r|$ y $|g| = |b_s|$. Entonces se cumple que $|fg| = |a_r||b_s|$. Tenemos que

$$|\sum_{i=0}^{r+s} a_i b_{r+s-i}| = |a_r b_s|$$

pues $|a_r b_s| > |a_i b_{r+s-i}|$ para todo $i = 0, \ldots, r+s$. Por tanto,

$$|fg| = \max_k(|\sum_{i=0}^{k} a_i b_{k-i}|) = |a_r b_s| = |f||g|.$$

1.3. Extensión de Valoraciones e Identidad Fundamental

El último corolario demostrado nos permite probar el siguiente teorema sobre extensibilidad de valoraciones:

Teorema 1.3.1. Sea k completo respecto al valor absoluto $|\cdot|$ y sea $k \subset L$ una extensión algebraica. Entonces $|\cdot|$ puede ser extendida de manera única a un valor absoluto de L. Cuando $n := [k : L] < \infty$ la extensión de $|\cdot|$ viene dada por la fórmula $|x| = \sqrt[n]{|\mathtt{N_{L|k}(x)}|}$ y además L es de nuevo completo.

Observación: La norma debe entenderse como el producto de todos los conjugados de x contados con multiplicidad si la extensión $L \supset k$ no es separable, o si se prefiere como norma para extensiones de anillos. Para más información véase [Rib01], *Sección 12.2.*

Demostración. Tenemos que distinguir dos casos:

- $|\cdot|$ **es arquimediana:** Gracias al teorema 1.2.4 sabemos que k es isomorfo a $\mathbb{R}$ o $\mathbb{C}$. Sabemos que $\mathtt{N}_{\mathbb{C}|\mathbb{R}}(\mathtt{x}) = \mathtt{x}\overline{\mathtt{x}} = |\mathtt{x}|^2$ y nuestro teorema es inmediato pues es bien conocido que $\mathbb{C}$ es completo.

- $|\cdot|$ **es no arquimediana:** Vamos a reducirnos al caso en que $[L : k] < \infty$ pues, en caso contrario, dado $x \in L$ tenemos que $k \subset k(x) \subset L$ es una cadena de extensiones siendo $[k(x) : k] < \infty$ y por ello es suficiente demostrar que podemos extender la valoración original en el caso en que la extensión es finita (ver nota al final de la demostración). De nuevo, dividimos la prueba en dos etapas, primero existencia y después unicidad:

  - *Existencia:* Sea o el anillo de valoración de k y $\mathcal{O}$ su clausura integral en L. Veamos que se tiene la igualdad

    $$\mathcal{O} = \{\alpha \in L \mid \mathtt{N}_{\mathtt{L}|\mathtt{k}}(\alpha) \in \mathcal{O}\}.$$

    La inclusión $\subset$ es inmediata pues dado $x \in \mathcal{O}$ entonces su polinomio mínimo f sobre k tiene coeficientes en o y en particular $f(0) \in o$ (notar que la norma es, salvo signo, una potencia de dicho elemento en el caso más general). Para la otra contención tomamos $\alpha \in L^\times$ tal que $\mathtt{N}_{\mathtt{L}|\mathtt{k}}(\alpha) \in o$. Sea $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in k[x]$ el polinomio mínimo de α sobre k. Es conocido que (incluso sin hipótesis de separabilidad para $L \supset k$ ([Rib01], *Demostración de 12.2.J*).

    $$\mathtt{N}_{\mathtt{L}|\mathtt{k}}(\alpha) = (-\mathtt{1})^{[\mathtt{L}:\mathtt{k}]}\mathtt{f}(\mathtt{0})^{[\mathtt{L}:\mathtt{k}(\alpha)]} = (-\mathtt{1})^{\mathtt{n}}\mathtt{a}_{\mathtt{0}}^{[\mathtt{L}:\mathtt{k}(\alpha)]} \in o,$$

    es decir, $|a_0| \leq 1$ que equivale a que $a_0 \in o$. Gracias a 1.2.10 tenemos que $f \in o[x]$ y por ello $\alpha \in \mathcal{O}$.

    Ahora es claro que la función $|\alpha| = \sqrt[n]{|\mathtt{N}_{\mathtt{L}|\mathtt{k}}(\alpha)|}$ está bien definida y las propiedades $|\alpha| = 0 \Leftrightarrow \alpha = 0$, $|\alpha\beta| = |\alpha||\beta|$ son inmediatas. Falta comprobar la desigualdad triangular fuerte

    $$|\alpha + \beta| \leq \mathtt{max}\{|\alpha|, |\beta|\}$$

    que podemos reducirla a la implicación

    $$|\alpha| \leq 1 \Rightarrow |\alpha + 1| \leq 1$$

tras dividir por β o por α. Pero dicha implicación es trivial ya que equivale a la implicación

$$\alpha \in \mathcal{O} \Rightarrow \alpha + 1 \in \mathcal{O}$$

que es trivial. Concluimos que la fórmula $|\alpha| = \sqrt[n]{|\mathtt{N}_{\mathtt{L}|\mathtt{k}}(\alpha)|}$ define una valoración que extiende a la valoración original y que tiene a $\mathcal{O}$ como anillo de valoración.

- *Unicidad:* Sea $|\cdot|'$ otra valoración con anillo de valoración $\mathcal{O}'$. Sea $\mathfrak{P}$ (resp. $\mathfrak{P}'$) el ideal maximal de $\mathcal{O}$ (resp. $\mathcal{O}'$). Veamos que $\mathcal{O} \subset \mathcal{O}'$. Sea $\alpha \in \mathcal{O} \backslash \mathcal{O}'$ y consideremos el polinomio mínimo de α sobre k :

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_d.$$

Tenemos que $a_1, \ldots, a_d \in o$ y como $\mathcal{O}'$ es un anillo de valoración tenemos que $x^{-1} \in \mathcal{O}' \setminus \mathcal{O}'^{\times} = \mathfrak{P}'$. Esto implica que

$$1 = -a_d(x^{-1})^d - \cdots - a_1(x^{-1}) \in \mathfrak{P}',$$

que es absurdo. Concluimos que $\mathcal{O} \subset \mathcal{O}'$ que es equivalente a la implicación

$$|\alpha| \leq 1 \Rightarrow |\alpha|' \leq 1$$

y gracias a la demostración de 1.1.3 sabemos que esto implica que las valoraciones son equivalentes. Concluimos que $|\cdot|$ y $|\cdot|'$ son la misma valoración gracias a 1.1.3 pues coinciden sobre k.

Para concluir que L es completo respecto a dicha valoración necesitamos el siguiente resultado:

Proposición 1.3.2. Sea k un cuerpo completo respecto a la valoración $|\cdot|$ y sea V un k-espacio vectorial normado de dimensión finita n. Entonces la norma del máximo asociada a cualquier base es equivalente a la norma dada (inducen la misma topología). En particular V es completo y el isomorfismo de coordenadas $K^n \to V$ es un homeomorfismo.

Demostración. Ver [Art59], *página 54.*

■

Nota: Para ver que es suficiente probar el teorema sólo para extensiones finitas tenemos que demostrar que la expresión obtenida es independiente de la extensión finita que elijamos. Para ello, sea $L|k$ una extensión algebraica, $x \in L$ y sea $K|k$ una extensión finita tal que $x \in K$. Tenemos entonces la cadena de extensiones finitas $k \subset k(x) \subset K$ y usando la fórmula del

grado ($[K:k] = [K:k(x)][k(x):k]$) y la transitividad de la norma ($\mathtt{N}_{k(x)|k} \circ \mathtt{N}_{K|k(x)} = \mathtt{N}_{K|k}$) deducimos:

$$\begin{aligned} |x|_K &= |\mathtt{N}_{K|k}(x)|^{1/[K:k]} \\ &= |\mathtt{N}_{k(x)|k}(\mathtt{N}_{K|k(x)}(x))|^{1/[K:k(x)]\cdot 1/[k(x):k]} \\ &= |\mathtt{N}_{k(x)|k}(x^{[K:k(x)]})|^{1/[K:k(x)]\cdot 1/[k(x):k]} \\ &= |\mathtt{N}_{k(x)|k}(x)|^{1/[k(x):k]} = |x|_{k(x)}. \end{aligned}$$

□

De 1.3.1 deducimos inmediatamente que una valoración ν de k asociada $|\cdot|$ se extiende de manera única a L. La extensión ω está dada por la formula

$$\omega(\alpha) = \frac{1}{n}\nu(\mathtt{N}_{\mathtt{L}|\mathtt{k}}(\alpha))$$

si $n = [L:k] < \infty$. Si denotamos por κ al cuerpo residual de ν y λ al cuerpo residual de ω, hemos obtenido las inclusiones

$$\nu(k^\times) \subset \omega(L^\times),\ \kappa \subset \lambda.$$

Consideramos los índices

$$e = e(\omega|\nu) = (\omega(L^\times) : \nu(k^\times)),\ f = f(\omega|\nu) = [\lambda : \kappa].$$

El número e se dirá que es el índice de ramificación de la extensión $L|k$ y f es el grado de inercia. Observar que e mide cuántos nuevos valores puede tomar ω respecto a ν. Si ν es discreta, y en dicho caso también lo será $\omega = \frac{1}{n}\nu \circ \mathtt{N}_{\mathtt{L}|\mathtt{k}}$, podemos considerar el anillo de valoración o, el ideal maximal $\mathfrak{p}$ y un parámetro de uniformización π de k (resp. $\mathcal{O}, \mathfrak{P}, \Pi$ de L), entonces $e = (\langle\omega(\Pi)\rangle : \langle\nu(\pi)\rangle)$, luego $\nu(\pi) = e\omega(\Pi)$ si e es finito (ver 1.3.3) y vemos que $\pi = u\Pi^e$ para alguna unidad $u \in \mathcal{O}^\times$, o equivalentemente

$$\mathcal{O}\mathfrak{p} = \mathcal{O}\pi = \mathcal{O}\Pi^e = \mathfrak{P}^e.$$

Proposición 1.3.3. Se verifica la desigualdad $[L:k] \geq ef$, en particular $e, f < \infty$. Además, se da la igualdad si la valoración es discreta y el cuerpo k es completo para dicha valoración.

Demostración. Sean $w_1, \ldots, w_s \in \mathcal{O}$ elementos tales que el conjunto $\{w_1 + \mathfrak{P}, \ldots, w_s + \mathfrak{P}\}$ es linealmente independiente sobre $o/\mathfrak{p}$. Así mismo, sean $\pi_1, \ldots, \pi_r \in L^\times$ tales que $\omega(\pi_1), \ldots, \omega(\pi_r)$ son valores distintos entre sí. Vamos a ver que los elementos $\pi_i\omega_j,\ i = 1, \ldots, r,\ j = 1, \ldots, s$ son

linealmente independientes sobre K de modo que $rs \leq [L:k]$. Esto implicaría que e y f son finitos y $ef \leq [L:k]$.

Supongamos que

$$\sum_{i=1}^{r}\sum_{j=1}^{s} a_{ij}w_j\pi_i = 0$$

con $a_{ij} \in k$ y no todos nulos. Entonces existen combinaciones lineales no nulas $s_i = \sum_{j=1}^{s} a_{ij}w_j$, y siempre que $s_i \neq 0$ deducimos que $\omega(s_i) \in \nu(k^\times)$. En efecto, si a_{it} es tal que $\nu(a_{it}) = \mathtt{min}\{\nu(a_{ij})\}$, dividiendo s_i por a_{it} obtenemos una combinación lineal de los elementos $w_1, \ldots, w_s$ con coeficientes en el anillo $o \subset k$ siendo uno de ellos igual a 1. Dicha combinación es distinta de 0 en módulo $\mathfrak{P}$ (el conjunto $\{w_1 + \mathfrak{P}, \ldots, w_s + \mathfrak{P}\}$ es linealmente independiente). En definitiva, s_i/a_{it} es una unidad de $\mathcal{O}$ y por ello $\omega(s_i) = \omega(a_{it}) = \nu(a_{it}) \in \nu(k^\times)$.

En la suma $\sum_{i=0}^{r} s_i\pi_i$ dos sumandos no nulos deben tener el mismo valor (i.e. $\omega(s_i\pi_i) = \omega(s_j\pi_j),\ i \neq j$) pues si no dicha suma no puede ser nula (ver observación que sigue al lema 1.1.8). Se sigue que

$$\omega(\pi_i) + \nu(k^\times) = (\omega(\pi_j) + \omega(s_j) - \omega(s_i)) + \nu(k^\times) = \omega(\pi_j) + \nu(k^\times),$$

que por hipótesis es imposible.

Hemos concluido la prueba de la desigualdad, ahora vamos a ver la demostración de la segunda afirmación. Esta vez tomamos para cada $i \in \mathbb{Z}$ un elemento $\Pi_i \in L$ tal que $\omega(\Pi_i) = i$ y $w_1, \ldots, w_f$ como antes. Sea $\alpha \in L$ tal que $\omega(\alpha) \geq i$. Entonces $\alpha/\Pi_i \in \mathcal{O}$ pues $\omega(\alpha/\Pi_i) \geq 0$. Escribamos $\alpha/\Pi_i + \mathfrak{P} = \sum_{j=1}^{f}(a_j + \mathfrak{p})(w_j + \mathfrak{P})$ y si denotamos $A = \sum_{j=1}^{f} a_j w_j$ tenemos que $\omega(\alpha/\Pi_i - A) \geq 1 = \omega(\Pi_1)$, es decir,

$$\omega(\alpha + A\Pi_i) \geq i + 1.$$

Si tomamos ahora un valor $\alpha \in \mathcal{O}$, por iteración del razonamiento anterior tenemos que existe una combinación lineal A_0 tal que $\omega(\alpha - A_0\Pi_0) \geq 1$, existe A_1 tal que $\omega(\alpha - A_0\Pi_0 - A_1\Pi_1) \geq 2$. En general, para cada n, sabemos que existen combinaciones lineales A_i $(i = 0, \ldots, n)$ tales que $\omega(\alpha - \sum_{i=0} A_i\Pi_i) \geq n + 1$. Lo anterior implica que podemos representar α por la serie

$$\alpha = \sum_{i=0}^{\infty} A_i\Pi_i,$$

siendo los coeficientes A_i combinaciones lineales de los $w_j,\ j = 1, \ldots, f$ y coeficientes en o.

Ahora vamos a elegir Π_i de forma adecuada. Si tenemos que $\mathfrak{p} = o\pi$ y $\mathfrak{P} = \mathcal{O}\Pi$ entonces definimos $\Pi_i = \Pi^j\pi^r$ de modo que $i = j + er$, $j = 0, \ldots, e-1$ y $r \in \mathbb{Z}$. Obtenemos entonces

$$\alpha = \sum_{r=0}^{\infty}\sum_{j=0}^{e-1}(a_{i1}w1 + \cdots + a_{if}w_f)\pi^r\Pi^j.$$

La serie $a_{is}\sum_{r=0}^{\infty}\pi^r$ converge y de hecho lo hace a un elemento $b_{js}\in o$ pues k es completo, podemos intercambiar los sumatorios y llegamos a que

$$\alpha=\sum_{j=0}^{e-1}(b_{j1}w_1+\cdots+b_{jf}w_f)\Pi^j,$$

con $b_{js}\in o$.

Hemos conseguido demostrar el resultado para $\alpha\in L$ con $\omega(\alpha)\geq 0$, vamos a extender el resultado a los elementos α tales que $\omega(\alpha)<0$. Para ello, elegimos $a\in k\setminus\{0\}$ tal que $\nu(a)>0$. Dado $\alpha\in L$ tal que $\omega(\alpha)<0$ tenemos que existe $r\in\mathbb{Z}$ tal que $\omega(\alpha a^r)\geq 0$ de modo que podemos escribir αa^r, y en particular α, como combinación lineal sobre k de los elementos $w_j\Pi^j$. Concluimos que $ef\geq[L:k]$. Notar que también hemos demostrado que $\{w_j\Pi^i\}$ es una o-base integral de $\mathcal{O}$.

□

Nota: Supongamos que $[L:k]<\infty$. Si la valoración ν es discreta, y por ello también ω, podemos normalizarlas. En general, la valoración normalizada de ω, que denotamos por ν_L, no extiende a la valoración normalizada de ν, denotada ν_k, sin embargo están relacionadas por la siguiente fórmula:

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

En efecto, podemos suponer que la valoración $\nu=\nu_k$ ya está normalizada y la extenemos a L de modo que $\omega=(1/n)\cdot\nu_k\circ\mathtt{N}_{L|k}$. Sean π,Π parámetros de uniformización de k,L respectivamente. Supongamos que $\pi=u\Pi^{e(\omega|\nu)}$ con $u\in\mathcal{O}^\times$. Entonces $e(\omega|\nu)\omega(\Pi)=\omega(\pi)=(1/n)\nu_k(\pi^n)=1$. Deducimos que para normalizar ω es suficiente multiplicarla por $e(\omega|\nu)$ y basta tener en cuenta que $[L:k]=n=e(\omega|\nu)f(\omega|\nu)$. Observar que ahora $(\nu_L)_{|k^\times}=e(k'|k)\nu_k$.

Ahora vamos a estudiar como extender una valoración arbitraria ν de k a una extensión algebraica finita L cuando k no es necesariamente completo respecto a ν. A partir de ahora vamos a denotar por ν a las valoraciones tanto arquimedianas (valores absolutos) como no arquimedianas y por el contexto estará claro que tipo de valoración es. Si es necesario distinguir, dada una valoración ν denotaremos un valor absoluto asociado por $|\cdot|_\nu$ y la complección por $\hat{k}_\nu$.

Dada una valoración ν arbitraria de k consideramos su complección $\hat{k}_\nu$ con la extensión canónica de ν denotada por $\hat{\nu}$. La clausura algebraica de $\hat{k}_\nu$ la denotaremos por $\overline{k}_\nu$ y la extensión de $\hat{\nu}$ a $\overline{k}_\nu$ la denotamos por $\overline{\nu}$.

Sea $L\supset k$ una extensión algebraica de k con $[L:k]<\infty$. Sea $\tau:L\to\overline{k}_\nu$ una k-inmersión. Dicha inmersión existe pues $\overline{k}_\nu$ es algebraicamente cerrado. Restringiendo la valoración $\overline{\nu}$ a τL obtenemos la valoración $w=\overline{\nu}\circ\tau$ que extiende la valoración ν de k a L. Con esta valoración, la aplicación $\tau:L\to\overline{k}_\nu$ es continua pues $\overline{\nu}(\tau a-\tau b)=(\overline{\nu}\circ\tau)(a-b)=w(a-b)$. De hecho, esto demuestra que

sucesiones de Cauchy respecto de w se transforman en sucesiones de Cauchy respecto de $\overline{\nu}$ a través de τ. Esto sugiere que definamos la extensión de τ a la complección de L respecto de w, $\hat{L}_w$, como sigue:

$$\tau(\lim_{n\to\infty} a_n) = \lim_{n\to\infty} \tau a_n.$$

Una vez demostrado que esta definición es correcta tendremos que $\tau : \hat{L}_w \to \overline{k}_\nu$ es un K-homomorfismo continuo. Para ver que está bien definido tenemos que demostrar que la sucesión τa_n converge respecto a $\overline{\nu}$. En este sentido, consideremos la extensión finita $\tau L \cdot \hat{k}_\nu \supset \hat{k}_\nu$ (es finita pues $L \supset k$ lo es) y usando 1.3.1 concluimos que existe una única valoración u extendiendo a $\hat{\nu}$ que además hace que $\tau L\hat{k}_\nu$ sea completo respecto a dicha valoración. Ahora bien, tenemos que $(\overline{\nu}_{|L\hat{k}_\nu})_{|\hat{k}_\nu} = \overline{\nu}_{\hat{k}_\nu} = \hat{\nu}$, por unicidad concluimos que $\overline{\nu}_{|L\hat{k}_\nu} = u$. Como u coincide con $\hat{\nu}_{|L\hat{k}_\nu}$ y $\tau : L \to \overline{k}_\nu$ lleva sucesiones de Cauchy en sucesiones de Cauchy, concluimos que $\tau : L \to L\hat{k}_\nu$ también y al ser $\tau L\hat{k}_\nu$ completo llegamos a que la sucesión τa_n converge en $\tau L\hat{k}_\nu \subset \overline{k}_\nu$.

De hecho, si consideramos el cuerpo $L \cdot \hat{k}_\nu$ de manera abstracta como la menor extensión que contiene a $L \cup \hat{k}_\nu$, sabemos que es completo y por ello $L \cdot \hat{k}_\nu \subset \hat{L}_w$. Como $L \subset L\hat{k}_\nu$ tenemos que $\hat{L}_w \subset L\hat{k}_\nu \subset \hat{L}_w$ y por ello coinciden. Esta información la recogemos en el siguiente diagrama:

$$\begin{array}{ccc} k & \longrightarrow & L \\ \downarrow & & \downarrow \\ \hat{k}_\nu & \longrightarrow & \hat{L}_w \end{array}$$

que nos muestra como pasar de la información global $L \supset k$ a la información local $\hat{L}_w \supset \hat{k}_\nu$. Este método se conoce como el **Principio local a global**. Si la extensión $\hat{L}_w \supset \hat{k}_\nu$ tiene grado $n < \infty$ tenemos la siguiente relación:

$$|x|_{\hat{w}} = \sqrt[n]{|\mathtt{N}_{\hat{L}_w|\hat{k}_\nu}(x)|_{\hat{\nu}}} \quad \forall x \in \hat{L}_\nu.$$

Hemos visto que toda k-inmersión $\tau : L \to \overline{k}_\nu$ da lugar a una extensión $w = \overline{\nu} \circ \tau$ de ν. Para cada $\hat{k}_\nu$-automorfismo σ de $\overline{k}_\nu$ (i.e. $\sigma \in \mathtt{Gal}(\overline{k}_\nu|\hat{k}_\nu)$) obtenemos por composición $L \xrightarrow{\tau} \overline{k}_\nu \xrightarrow{\sigma} \overline{k}_\nu$ una nueva k-inmersión $\tau' = \sigma \circ \tau$ de L. Diremos que τ' es conjugada a τ sobre $\hat{k}_v$. Claramente la relación de ser conjugados es de equivalencia pues procede de la acción (natural) del grupo de Galois $\mathtt{Gal}(\overline{k}_\nu|\hat{k}_\nu)$ sobre el conjunto de las k-inmersiones $L \to \overline{k}_\nu$. Usando esta relación de equivalencia podemos describir completamente las extensiones de ν a L cuando $[L : k] < \infty$:

Proposición 1.3.4. Sea $L \supset k$ una extensión algebraica finita y ν una valoración de k. Se cumple lo siguiente:

1. Toda extensión w de ν es de la forma $w = \overline{\nu} \circ \tau$ para alguna k-inmersión $\tau : L \to \overline{k}_\nu$.

2. Dos extensiones $\overline{\nu}\circ\tau$ y $\overline{\nu}\circ\tau'$ son iguales si y sólo si τ y τ' son conjugadas sobre $\hat{k}_\nu$.

Demostración. 1. Sea w una extensión de ν a L y $\hat{L}_w$ la complección con valoración $\hat{w}$. Esta valoración $\hat{w}$ es la única extensión de la valoración $\hat{\nu}$ de $\hat{k}_\nu$ a $\hat{L}_w$. Dada una $\hat{k}_\nu$-inmersión $\tau : \hat{L}_w \to \overline{k}_\nu$, la valoración $\overline{\nu}\circ\tau$ extiende a $\hat{\nu}$ y por unicidad debe coincidir con $\hat{w}$. La restricción de τ a L es la k-inmersión que hace $w = \overline{\nu}\circ\tau_{|L}$.

2. Sea $\tau : L \to \overline{k}_\nu$ una k-inmersión y $\sigma \in \mathtt{Gal}(\overline{k}_\nu|\hat{k}_\nu)$ un $\hat{k}_\nu$-automorfismo de $\overline{k}_\nu$. Como $\overline{v}$ es la única extensión de la valoración $\hat{\nu}$ a $\overline{k}_\nu$, tenemos que $\overline{\nu} = \overline{\nu}\circ\sigma$ y por ello $\overline{\nu}\circ\tau = \overline{\nu}\circ(\sigma\circ\tau)$.

   Recíprocamente, sean $\tau, \tau' : L \to \overline{k}_\nu$ dos k-inmersiones tales que $\overline{\nu}\circ\tau = \overline{\nu}\circ\tau'$. Sea

$$\sigma : \tau L \xrightarrow{\tau^{-1}} L \xrightarrow{\tau'} \tau' L.$$

   Veamos como extender σ a un $\hat{k}_\nu$-isomorfismo $\sigma : \tau L\hat{k}_\nu \to \tau' L\hat{k}_\nu$. Como $\tau L\hat{k}_\nu \simeq \hat{L}_{\overline{\nu}\circ\tau}$, tenemos que τL es denso en $\tau L\hat{k}_\nu$ y para cada $x \in \tau L\hat{k}_\nu$ obtenemos una sucesión de términos $x_n \in L$ de modo que $x = \lim_{n\to\infty} \tau x_n$. Como $\overline{\nu}\circ\tau = \overline{\nu}\circ\tau'$, la sucesión $\tau' x_n = (\sigma\circ\tau)(x_n)$ es convergente en $\tau' L\hat{k}_\nu$ (notar que $\overline{\nu}(\tau x_n - \tau x_m) = \overline{\nu}(\tau' x_n - \tau' x_m)$). Si escribimos

$$\sigma x = \lim_{n\to\infty} (\sigma\circ\tau)(x_n)$$

   obtenemos una posible extensión de σ. Veamos que esta definición es correcta y que la aplicación obtenida es un $\hat{k}_\nu$-isomorfismo:

   a. σ **está bien definida:** Sean $(x_n), (y_n)$ sucesiones de elementos de L tales que $\lim \tau x_n = \lim \tau y_n = x$. Entonces $\lim \tau(x_n - y_n) = 0$, es decir, $(\overline{\nu}\circ\tau)(x_n - y_n) \to \infty$ cuando $n \to \infty$. Como $\overline{\nu}\circ\tau = \overline{\nu}\circ\tau'$ concluimos que $\lim \tau'(x_n - y_n) = 0$, es decir, $\lim(\sigma\circ\tau)(x_n) = \lim(\sigma\circ\tau)(y_n)$.

   b. σ **es homomorfismo:** Inmediato pues τ' y lím son homomorfismos.

   c. σ **es inyectivo:** Si $\sigma x = \lim \tau' x_n = 0$ entonces $(\overline{\nu}\circ\tau')(x_n) \to \infty$ cuando $n \to \infty$. Usando de nuevo que $\overline{\nu}\circ\tau' = \overline{\nu}\circ\tau$ concluimos que $x = \lim \tau x = 0$.

   d. σ **es sobreyectivo:** Inmediato usando que $\tau' L$ es denso en $\tau' L\hat{k}_\nu$.

   e. σ **es $\hat{k}_\nu$-homomorfismo:** Sea $x \in \hat{k}_\nu$. Como k es denso en $\hat{k}_\nu$ tenemos que existe una sucesión (x_n) de elementos de k tal que $x = \lim x_n$. Entonces

$$\sigma x = \lim(\sigma\circ\tau)(x_n) = \lim x_n = x.$$

   Considerando ahora una extensión de σ a un $\hat{k}_\nu$-automorfismo $\overline{\sigma} \in \mathtt{Gal}(\overline{k}_\nu|\hat{k}_\nu)$ tenemos que $\tau' = \overline{\sigma}\circ\tau$, de modo que τ y τ' son conjugados sobre $\hat{k}_\nu$.

□

Es interesante ver la forma que toman nuestros resultados cuando la extensión L es de la forma $L = k(\alpha)$ siendo α una raíz de un polinomio irreducible $f(x) \in k[x]$. Tenemos el siguiente resultado:

Proposición 1.3.5. Supongamos que la extensión $L \supset k$ es de la forma $L = k(\alpha)$ con α una raíz del polinomio irreducible $f(x) \in k(x)$.

Entonces las valoraciones $w_1, \ldots, w_r$ que extienden ν a L están en correspondencia biyectiva con los factores $f_1, \ldots, f_r$ en la descomposición

$$f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}$$

de f sobre la compleción $\hat{k}_\nu$.

Demostración. Las k-inmersiones $\tau : L \to \overline{k}_\nu$ están determinadas por las raíces β de $f(x)$ (sin pérdida de generalidad suponemos que están en $\overline{k}_\nu$,) es decir, $\tau_\beta : L \to \overline{k}_\nu$, $\tau_\beta(\alpha) = \beta$. Las k-inmersiones $\tau_\beta, \tau_{\beta'}$ serán conjugadas sobre $\hat{k}_\nu$ si y sólo si las raíces β y β' son conjugadas sobre $\hat{k}_\nu$, es decir, si y sólo si son raíces del mismo polinomio irreducible f_i. Usando 1.3.4 concluimos el resultado. □

La valoración w_i asociada a f_i se obtiene explícitamente a partir de este polinomio como sigue: sea $\alpha_i \in \overline{k}_\nu$ una raíz de f_i y consideremos la k-inmersión $\tau_i := \tau_{\alpha_i}$. Obtenemos que $w_i = \overline{\nu} \circ \tau_i$. Además, τ_i podemos extenderlo de forma canónica a una $\hat{k}_\nu$-inmersión continua $\tau_i : \hat{L}_{w_i} \to \overline{k}_\nu$. La imagen de dicha extensión es el cuerpo $\hat{k}_\nu(\alpha_i) = \tau_i L \cdot \hat{k}_\nu$, lo que demuestra que τ_i se extiende a un isomorfismo (para todas las estructuras que intervienen) $\tau_i : \hat{L}_{w_i} \to \hat{k}_\nu(\alpha_i)$.

Sea de nuevo $L \supset k$ una extensión finita arbitraria. Vamos a escribir $w|\nu$ para indicar que w es una extensión de la valoración ν a L. Consideremos para cada $w|\nu$ el homomorfismo

$$a \otimes b \in L \otimes_k \hat{k}_\nu \mapsto ab \in \hat{L}_w.$$

Este homomorfismo está bien definido pues $L \cup \hat{k}_\nu \subset \hat{L}_w$. De hecho, este homomorfismo de k-espacios vectoriales se puede ver como un homomorfismo de $\hat{k}_\nu$-álgebras considerando en $L \otimes_k \hat{k}_\nu$ la acción de $\hat{k}_\nu$ dada por $(\lambda, a \otimes b) \mapsto a \otimes (\lambda b)$. Todos estos homomorfismos podemos "combinarlos" y obtener un homomorfismo canónico

$$\varphi : L \otimes_k \hat{k}_\nu \to \prod_{w|\nu} \hat{L}_w.$$

De nuevo, este homomorfismo es válido al nivel de $\hat{k}_\nu$-álgebras.

La siguiente proposición nos da una condición suficiente para que $L \otimes_k \hat{k}_\nu \to \prod_{w|\nu} \hat{L}_w$ sea un isomorfismo:

Proposición 1.3.6. Si la extensión $L \supset k$ es separable, entonces

$$L \otimes_k \hat{k}_\nu \simeq \prod_{w|\nu} \hat{L}_w.$$

Demostración. Sea α un elemento primitivo para $L \supset k$ de modo que $L = k(\alpha)$ y sea $f(x) \in k[x]$ su polinomio mínimo. Para cada $w|\nu$ tenemos un factor irreducible $f_w \in \hat{k}_\nu[x]$ y por la hipótesis de separabilidad concluimos que $f = \prod_{w|\nu} f_w$. Supongamos que los cuerpos $\hat{L}_w$ están contenidos en una clausura algebraica $\overline{k}_\nu$ de $\hat{k}_\nu$ y vamos a denotar por α_w la imagen de α bajo las inmersiones $L \to \hat{L}_w$. Sabemos entonces que $\hat{L}_w = \hat{k}_\nu(\alpha_w)$ y f_w es el polinomio mínimo de α_w sobre $\hat{k}_\nu$.

Como $k[x]/\langle f\rangle \simeq k(\alpha) = L$ tenemos que $\hat{k}_\nu[x]/\langle f\rangle \simeq L \otimes_k \hat{k}_\nu$ vía el isomorfismo que hace $(x + \langle f\rangle) \mapsto \alpha \otimes 1$. Así mismo, para cada $w|\nu$ tenemos que $\hat{k}_\nu[x]/\langle f_w\rangle \simeq \hat{k}_\nu(\alpha_w) = \hat{L}_w$. Todos estos isomorfismos podemos reunirlos en el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \hat{k}_\nu[x]/\langle f\rangle & \longrightarrow & \prod_{w|\nu} \hat{k}_\nu[x]/\langle f_w\rangle \\ \downarrow & & \downarrow \\ L \otimes_k \hat{k}_\nu & \longrightarrow & \prod_{w|\nu} \hat{L}_w \end{array},$$

siendo las flechas verticales los isomorfismos descritos y la flecha horizontal superior el isomorfismo que se obtiene al aplicar el teorema chino del resto. Además el diagrama es válido al nivel de $\hat{k}_\nu$-álgebras de modo que el isomorfismo del enunciado es de $\hat{k}_\nu$-álgebras.

□

Obtenemos el siguiente corolario:

Corolario 1.3.7. Si $L \supset k$ es separable, entonces tenemos que

$$[L : k] = \sum_{w|\nu} [\hat{L}_w : \hat{k}_\nu]$$

y

$$\mathtt{N}_{L|k}(\alpha) = \prod_{w|\nu} \mathtt{N}_{\hat{L}_w|\hat{k}_\nu}(\alpha),\ \mathtt{Tr}_{L|k}(\alpha) = \sum_{w|\nu} \mathtt{Tr}_{\hat{L}_w|\hat{k}_\nu}(\alpha).$$

Demostración. Para la formula de las dimensiones basta recordar que

$$[L : k] = \mathtt{dim}_k(L) = \mathtt{dim}_{\hat{k}_\nu}(L \otimes_k \hat{k}_\nu).$$

Para la norma y la traza, sabemos que los polinomios característicos de la aplicaciones lineales que consisten en multiplicar por $\alpha \in L$ en $L \otimes \hat{k}_\nu$ y $\prod_{w|\nu} \hat{L}_w$ coinciden, de modo que

$$\mathtt{char.pol}_{L|k}(\alpha) = \prod_{w|\nu} \mathtt{char.pol}_{\hat{L}_w|\hat{k}_\nu}(\alpha).$$

□

Si además suponemos que ν es una valoración no arquimediana, podemos definir el índice de ramificación (local) de una extensión $w|\nu$ como

$$e_w = (w(L^\times) : \nu(K^\times))$$

y el grado de inercia (local)

$$f_w = [\lambda_w : \kappa],$$

siendo λ_w, resp. κ, el cuerpo residual de w, resp. v. Sabemos por 1.3.3 que $[\hat{L}_w : \hat{k}_\nu] = e_w f_w$ y usando 1.3.7 obtenemos **la identidad fundamental de la teoría de valoraciones:**

Proposición 1.3.8. Si ν es discreta y $L \supset k$ es separable, entonces

$$[L : k] = \sum_{w|v} e_w f_w.$$

Es interesante resaltar que si la valoración ν es discreta, y en ese caso también lo serán sus extensiones w, entonces la intersección $\cap_{w|\nu}\mathcal{O}_w$ es la clausura integral de o_ν en L. Para una demostración de este resultado mirar [AM69] *página 66, teorema 5.21.* y usar el hecho de que un anillo de valoración discreta induce de manera canónica una valoración discreta.

1.4. Valores Absolutos de $\mathbb{Q}$ y la Fórmula del Producto

Para nosotros será esencial comprender en profundidad la teoría de valoraciones en el caso de los números racionales. Observar que $\mathbb{Q}$ admite un gran número de valores absolutos distintos del valor absoluto usual $|a|_\infty = \mathtt{sgn}(a) \cdot a$: En efecto, sea $p > 0$ un número primo en $\mathbb{Z}$ y dado $a \in \mathbb{Z}$ denotemos por $\mathtt{ord}_p(a)$ el mayor número natural tal que $p^{\mathtt{ord}_p(a)}$ divide a a. Podemos entonces definir la función

$$\nu_p : \mathbb{Q} \to \mathbb{Z}$$

dada por

$$\nu_p(a/b) = \mathtt{ord}_p(a) - \mathtt{ord}_p(b).$$

Es inmediato que ν_p así definida es una valoración (no arquimediana) discreta normalizada de $\mathbb{Q}$ y tenemos una para cada número primo $p \in \mathbb{Z}_{\geq 0}$. Observar que si definimos una función análoga para el número 0 obtendremos la valoración trivial asumiendo que $0^0 = 1$. Por último, notar que el anillo de valoración de ν_p es el conjunto de todas las fracciones con denominador coprimo con p, su ideal maximal es el conjunto de las fracciones cuyo denominador es coprimo con p y el numerador es divisible por p y las unidades es el conjunto de las fracciones tales que numerador y denominador son ambos coprimos con p. Ssalvo equivalencia, hemos encontrado todas las valoraciones de $\mathbb{Q}$:

Proposición 1.4.1. Sea $\nu : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ una valoración. Entonces ν es la valoración trivial o ν es equivalente a ν_p para algún número primo $p > 0$. En particular toda valoración de $\mathbb{Q}$ no trivial es discreta.

Demostración. Sea $o \subset \mathbb{Q}$ el anillo de valoración de ν con ideal maximal $\mathfrak{p}$. Como o tiene característica 0 y $1 \in o$ tenemos que $\mathbb{Z} \subset o$. Obtenemos que $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$. Se presentan dos casos:

1. $\mathfrak{p} \cap \mathbb{Z} = 0$. En este caso todo entero no nulo es una unidad de o y por ello $\mathbb{Q}\backslash\{0\} \subset o^\times \subset \mathbb{Q}\backslash\{0\}$. Concluimos que $o = \mathbb{Q}$ y que ν es la valoración trivial.

2. $\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z}p$ con $p > 0$ primo. Entonces todo número entero coprimo con p es una unidad de o, lo que implica que el anillo de valoración de ν_p, $o_p = \mathbb{Z}_{(p)}$, está contenido en o. De hecho, podemos demostrar que $o = \mathbb{Z}_{(p)}$ pues el anillo $\mathbb{Z}_{(p)}$ tiene dimensión 1 ya que es un anillo de valoración discreta. En efecto, supongamos que existe $x \in o \setminus \mathbb{Z}_{(p)}$. Como $\mathbb{Z}_{(p)}$ es un anillo de valoración de $\mathbb{Q}$, $x \in o \setminus \{0\} \subset \mathbb{Q} \setminus \{0\}$ y $x \notin \mathbb{Z}_{(p)}$ concluimos que $x^{-1} \in \mathbb{Z}_{(p)}$. De hecho, $x^{-1} \in \mathbb{Z}_{(p)} \setminus \mathbb{Z}_{(p)}^\times$. Por hipótesis $\mathbb{Z} \cap \mathfrak{p} \neq 0$ luego $\mathbb{Z}_{(p)} \cap \mathfrak{p} \neq 0$ y al ser $\mathbb{Z}_{(p)}$ un anillo de dimensión 1 concluimos que $\mathbb{Z}_{(p)} \cap \mathfrak{p} = \mathbb{Z}_{(p)} \setminus \mathbb{Z}_{(p)}^\times$ es el ideal maximal del anillo local $\mathbb{Z}_{(p)}$, de modo que $x^{-1} \in \mathbb{Z}_{(p)} \cap \mathfrak{p} \subset \mathfrak{p}$. Ahora bien, $x \in o$ y $x^{-1} \in \mathbb{Z}_{(p)} \subset o$ luego $x^{-1} \in o^\times = o \setminus \mathfrak{p}$. Concluimos que $x^{-1} \in o^\times \cap \mathfrak{p} = \emptyset$ que es absurdo. Por tanto, $o = o_p$ y por ello, salvo equivalencia, ν coincide con ν_p.

□

Visto que las valoraciones de $\mathbb{Q}$ son todas de la forma ν_p nuestro próximo objetivo es hallar los posibles valores absolutos de $\mathbb{Q}$. Asociado a cada valoración ν_p hay un valor absoluto canónico, que es aquel dado por

$$|\cdot|_p = p^{-\nu_p(\cdot)}.$$

Diremos que este es el **valor absoluto normalizado** asociado al número primo p. Todos estos valores absolutos junto con el valor absoluto usual son, salvo equivalencia, todos los posibles valores absolutos sobre $\mathbb{Q}$. Tenemos el siguiente resultado debido a **Ostrowski:**

Proposición 1.4.2. Sea $|\cdot|$ un valor absoluto en $\mathbb{Q}$.

1. Si $|\cdot|$ es arquimediano entonces es equivalente al valor absoluto usual, denotado $|\cdot|_\infty$.

2. Si $|\cdot|$ es no arquimediano entonces es equivalente al un valor absoluto $|\cdot|_p$ para un único primo p.

Demostración. Sean $m, n > 1$ números enteros. Podemos escribir

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

con a_i enteros tales que $0 \leq a_i < n$ y $n^r \leq m$. Usando la desigualdad triangular deducimos que es

$$|m| \leq \sum |a_i||n|^i \leq \sum |a_i| \operatorname{máx}(1, |n|)^r.$$

Además, $r \leq \log(m)/\log(n)$ y de nuevo por la desigualdad triangular tenemos que

$$|a_i| = |\underbrace{1 + \cdots + 1}_{a_i}| \leq a_i < n.$$

Combinando estas desigualdades encontramos que

$$|m| \leq (1+r)n \operatorname{máx}(1, |n|)^r \leq \left(1 + \frac{\log(m)}{\log(n)}\right) n \operatorname{máx}(1, |n|)^{\frac{\log(n)}{\log(n)}}.$$

Si escribimos esta desigualdad con m^t en lugar de m (siendo $t \in \mathbb{N}$) y tomando la raíz t-ésima obtenemos:

$$|m| \leq \left(1 + \frac{t\log(m)}{\log(n)}\right)^{1/t} n^{1/t} \operatorname{máx}(1, |n|)^{\frac{\log(n)}{\log(n)}}.$$

Haciendo $t \to \infty$ llegamos a

$$|m| \leq \operatorname{máx}(1, |n|)^{\frac{\log(m)}{\log(n)}}$$

para todos los enteros $m, n > 1$. Tenemos dos casos:

a. Existe $n > 1$ tal que $|n| \leq 1$. Entonces $|m| \leq 1$ para todo $m \in \mathbb{N}$ de modo que $|\cdot|$ es arquimediano y existe un único ideal primo p tal que $|\cdot|$ es equivalente a $|\cdot|_p$.

b. Para todo número natural $n > 1$ es $|n| > 1$. Entonces la desigualdad deducida antes se reduce a

$$|m|^{1/\log(m)} \leq |n|^{1/\log(n)}$$

y por simetría la desigualdad debe ser una igualdad, de modo que existe $c > 1$ tal que $c = |n|^{1/\log(n)}$ para todo entero $n > 1$. Concluimos que

$$|n| = c^{\log(n)} = n^{\log(c)}$$

para todo $n \in \mathbb{N}$. Si escribimos $a := \log(c)$ llegamos a que

$$|n| = |n|_\infty^a \ \forall n \in \mathbb{N}.$$

Ahora bien, $|\cdot|$ y $|\cdot|_\infty^a$ son homomorfismos de $\mathbb{Q}^\times \to \mathbb{R}_{>0}$ verificando que $|-1| = 1 = |-1|_\infty^a$ y $|n| = |n|_\infty^a$ para todo $n > 1$, luego $|\cdot| = |\cdot|_\infty^a$ en todo $\mathbb{Q}^\times$.

□

Es conocido que la compleción de $\mathbb{Q}$ respecto a $|\cdot|_\infty$ coincide con $\mathbb{R}$. La compleción de $\mathbb{Q}$ respecto a $|\cdot|_p$ es el cuerpo de los números p-ádicos que denotaremos por $\mathbb{Q}_p$. Su anillo de valoración discreta es el anillo de los enteros p-ádicos que denotamos por $\mathbb{Z}_p$. En 1.1.5 vimos que un conjunto finito de valores absolutos son independientes, sin embargo, si consideramos el conjunto de todos los valores absolutos de $\mathbb{Q}$ la situación es distinta y se tiene la conocida **Fórmula del Producto para $\mathbb{Q}$:**

Teorema 1.4.3. Para cada $p = 2, 3, 5, 7, \ldots, \infty$ sea $|\cdot|_p$ el valor absoluto normalizado asociado. Entonces se cumple que

$$\prod_p |a|_p = 1$$

para todo $a \in \mathbb{Q} \setminus \{0\}$ y esta fórmula es esencialmente única, es decir, cualquier otra fórmula de la forma

$$\prod_p |a|_p^{c_p} = 1$$

que se cumpla para todo $a \in \mathbb{Q} \setminus \{0\}$ debe verificar que $c_p = c_q$ para todo $p \neq q$.

Demostración. Consideremos el producto

$$\varphi(a) = \prod_p |a|_p^{c_p}$$

con $a \in \mathbb{Q}\setminus\{0\}$. Este producto está bien definido pues es $|a|_p = 1$ para casi todo p (en la factorización de a sólo aparecen un número finito de primos) y por ello el producto $\varphi(a)$ es un producto finito para cada $a \in \mathbb{Q} \setminus \{0\}$. De hecho, $\varphi : \mathbb{Q}^\times \to \mathbb{R}^\times$ es un homomorfismo y se verifica que para todo primo p la función φ toma el valor

$$\varphi(p) = |p|_\infty^{c_\infty} |p|_p^{c_p} = p^{c_\infty - c_p}.$$

Además, $\varphi(-1) = 1$ y todos estos valores determinan a la función φ. Concluimos que φ es el homomorfismo trivial si y sólo $c_\infty = c_p$ para todo p.

□

1.5. Cuerpos Locales

Terminamos el capítulo de valoraciones estudiando una clase de cuerpos importantes y sobre la que trabajaremos principalmente.

Definición 1.5.1. Un **cuerpo local** k es un cuerpo con un valor absoluto no trivial $|\cdot|$ que es localmente compacto bajo la topología inducida por $|\cdot|$.

Como nuestras topologías son de Hausdorff, podemos tomar como definición de espacio localmente compacto aquel que para cada punto existe un entorno con clausura compacta. En símbolos, un espacio X es localmente compacto si para todo $x \in X$ existe $U \subset X$ abierto con $x \in U$ y $\overline{U}$ compacto. En realidad como nuestros cuerpos son espacios métricos tenemos que X es localmente compacto si y sólo si para todo $x \in X$ existe una bola cerrada compacta que contenga a x. En efecto, si X es localmente compacto y $x \in X$ existe U entorno abierto de x tal que $\overline{U}$ es compacto. Sea $\varepsilon > 0$ con $\varepsilon \in |k^\times|$ tal que $B(x, \varepsilon) \subset U$. Entonces $x \in \overline{B(x,\varepsilon)} \subset \overline{U}$. Como $\overline{U}$ es compacto y $\overline{B(x,\varepsilon)}$ es cerrado concluimos que la bola es compacta y contiene a x. La otra implicación es trivial.

Vamos a clasificar a los cuerpos locales. Usaremos con frecuencia que en un espacio métrico no arquimediano, i.e. se cumple la desigualdad triangular fuerte, las bolas abiertas son también cerradas y viceversa. La demostración de este hecho se basa en la propiedad *extraña* que cumplen las bolas no arquimedianas:

> Sea $x \in X$ con (X, d) espacio métrico no arquimediano y $\varepsilon > 0$. Entonces para todo $y \in B(x, \varepsilon)$ es $B(y, \varepsilon) = B(x, \varepsilon)$. En palabras, todo punto de una bola es centro de la misma.

Demostración. Consideremos $z \in B(y, \varepsilon)$. Entonces $d(y, z) < \varepsilon$ y

$$d(x, z) \leq \text{máx}\{d(x, y), d(y, z)\} < \text{máx}\{\varepsilon, \varepsilon\} = \varepsilon.$$

Luego $z \in B(x, \varepsilon)$. Como $x \in B(y, \varepsilon)$, por simetría concluimos que ambas bolas coinciden.

□

Como consecuencia, dos bolas cualesquiera son disjuntas o concéntricas. También es importante observar que en general no todos los números de $\mathbb{R}$ pueden aparecer como radio de una bola. Por ejemplo, considerar un valor absoluto obtenido a partir de una valoración discreta. En este caso el número posible de radios es numerable y este hecho tiene consecuencias no triviales para la topología.

Tenemos la siguiente caracterización:

Lema 1.5.2. Sea k un cuerpo con un valor absoluto no trivial $|\cdot|$. Entonces k es un cuerpo local si y sólo si toda bola cerrada en k es compacta.

Demostración. Supongamos que k es un cuerpo local. Como es usual en un grupo topológico, es suficiente demostrar el resultado para el punto $x = 0$ pues en otro caso podemos usar una traslación que es un homeomorfismo. Considerando $0 \in k$, por definición existe una bola cerrada compacta $\overline{B(0, r)}$ que contiene a 0. Podemos suponer que el centro de la bola es 0 pues la métrica es no arquimediana. Fijemos $\alpha \in k^\times$ con $|\alpha| > 1$, que existe pues el valor absoluto lo hemos supuesto no trivial. La aplicación $x \mapsto \alpha x$ es continua y multiplicativa por tanto las bolas $\overline{B(0, |\alpha|^n r)}$ son

compactas pues son la imagen continua de un compacto. Obtenemos que existen bolas compactas conteniendo a 0 de radio lo grande que se desee y por esta razón concluimos que toda bola cerrada que contenga a 0 es compacta pues será un cerrado contenido en un compacto.

Para el recíproco, basta aplicar la definición y la hipótesis de que $|\cdot|$ es no trivial.

□

Observar que en la demostración no sólo se demuestra que k es un cuerpo local si toda bola cerrada es compacta si no que es suficiente encontrar una bola cerrada compacta para concluir que k es un cuerpo local.

Corolario 1.5.3. Sea k un cuerpo local con valor absoluto $|\cdot|$. Entonces k es completo.

Demostración. Por reducción al absurdo, supongamos que existe una sucesión de Cauchy (x_n) de k con límite $x \in \hat{k} \setminus k$. Sea $N \in \mathbb{N}$ tal que $|x_n - x|_{\hat{k}} < 1/2$ para todo $n \geq N$. Consideremos la bola cerrada $B = \overline{B(x_N, 1)} \subset k$. Dicha bola es compacta gracias al lema anterior. Gracias a que k es un espacio métrico podemos usar la caracterización secuencial de la compacidad y deducir que la sucesón de Cauchy $(x_n)_{n \geq N}$ posee una subsucesión contenida en B con límite en B. Pero dicho límite debe coincidir con $x \notin B$.

□

Proposición 1.5.4. Sea k un cuerpo con valor absoluto no arquimediano $|\cdot|_\nu$ inducido por una valoración discreta ν de k con anillo de valoración $\mathcal{O}_\nu$ e ideal primo $\mathfrak{p}_\nu$. Entonces k es un cuerpo local si y sólo si k es completo y el cuerpo residual $\overline{k} = \mathcal{O}_\nu/\mathfrak{p}_\nu$ es finito.

Demostración. Si k es un cuerpo local entonces k es completo gracias a 1.5.3. Además, el anilo de valoración

$$\mathcal{O}_\nu = \{x \in k || x|_\nu \leq 1\}$$

es una bola cerrada y debido a 1.5.2 es compacto. Cada clase de equivalencia $x + \mathfrak{p}_\nu$ son bolas abiertas pues $y \in x + \mathfrak{p}_\nu$ si y sólo si

$$y - x \in \mathfrak{p}_v = \{z \in k || z|_\nu < 1\}.$$

La colección de clases de equivalencia $\{x + \mathfrak{p}_\nu | x \in \mathcal{O}_\nu\}$ es un recubrimiento abierto de $\mathcal{O}_\nu$ por bolas disjuntas y como $\mathcal{O}_\nu$ es compacto el número de bolas en dicha colección debe ser finito.

Recíprocamente, supongamos que k es completo y $\overline{k}$ es finito. Entonces también es completo el anillo $\mathcal{O}_\nu$ y se tiene el isomorfismo

$$A \simeq \varprojlim \frac{\mathcal{O}_\nu}{\mathfrak{p}_\nu^n}.$$

Como $\overline{k}$ es finito tenemos que $\mathcal{O}_\nu/\mathfrak{p}_\nu^n$ es finito para todo $n \in \mathbb{N}$ y por tanto compacto con la topología discreta. Se puede comprobar que el límite proyectivo de un sistema de espacios topológicos compactos es compacto *(Ver capítulo 4)*, es decir, $\mathcal{O}_\nu$ es compacto. El lema 1.5.2 implica que k es un cuerpo local pues $|\cdot|_\nu$ es no trivial. □

Particularizamos nuestros resultados al caso en k tiene característica 0 :

Corolario 1.5.5. Se L una extensión finita de $\mathbb{Q}$ con valor absoluto $|\cdot|_\nu$. Entonces la compleción $\hat{L}_\nu$ es un cuerpo local.

Demostración. Sea $\mathcal{O}$ la clausura integral de $\mathbb{Z}$ en L. Sabemos que $\mathcal{O}$ es un dominio de Dedekind. Hay dos posibles casos:

1. $|\cdot|_\nu$ *es arquimediano.* La compleción $\hat{L}_\nu$ contiene la compleción de $\mathbb{Q}$ respecto de la restricción de $|\cdot|_\nu$ a $\mathbb{Q}$, que debe ser isomorfa a $\mathbb{R}$. Por tanto $\hat{L}_\nu$ es una extensión finita de $\mathbb{R}$ y debe ser isomorfo a $\mathbb{R}$ o $\mathbb{C}$, ambos cuerpos locales.

2. $|\cdot|_\nu$ *es no arquimediano.* En este caso $|\cdot|_\nu$ está inducido por una valoración discreta ν de L. En efecto, sea
$$\mathcal{O}_\nu = \{x \in L | |x|_\nu \leq 1\}$$
el anillo de valoración de $|\cdot|_\nu$, con ideal maximal $\mathfrak{p}_\nu$ que es no nulo pues $|\cdot|_\nu$ es no trivial.

   La restricción de $|\cdot|_\nu$ a $\mathbb{Q}$ es un valor absoluto no arquimediano y por el *teorema de Ostrowski* sabemos que tiene que ser equivalente al valor absoluto asociadoa una de las valoraciones discretas de $\mathbb{Q}$. En particular, $|n|_\nu \leq 1$ para todo $n \in \mathbb{Z}$, es decir, $\mathbb{Z} \subset \mathcal{O}_\nu$. Como $\mathcal{O}_\nu$ es integralmente cerrado en su cuerpo de fracciones L, debe contener a $\mathcal{O}$ pues $\mathcal{O}$ es la clausura integral de $\mathbb{Z}$ en L. El ideal $\mathfrak{p} = \mathcal{O} \cap \mathfrak{p}_\nu$ es maximal y el localizado $\mathcal{O}_\mathfrak{p}$ está contenido en $\mathcal{O}_\nu$, pero como ambos tienen el mismo cuerpo de fracciones deben ser iguales. Concluimos que cualquier valor absoluto obtenido a partir de $\mathtt{ord}_\mathfrak{q}$ es equivalente a $|\cdot|_\nu$ pues tienen el mismo anillo de valoración. Eligiendo $c \in (0,1)$ apropiado, podemos asumir que $|\cdot|_\nu = c^{\mathtt{ord}_\mathfrak{q}(\cdot)}$ y esto demuestra nuestra afirmación.

   El cuerpo residual $\mathcal{O}_\nu/\mathfrak{p}_\nu \simeq \mathcal{O}/\mathfrak{p}$ es finito pues es una extensión finita del cuerpo finito $\mathbb{Z}/(\mathfrak{p}\cap\mathbb{Z})$. Si consideramos la compleción $\hat{L}_\nu$ con anillo de valoración $\hat{\mathcal{O}}_\nu$ e ideal maximal $\hat{P}_\nu$ tenemos los siguientes isomorfismos:
$$\frac{\mathcal{O}_\nu}{\mathfrak{p}_\nu} \simeq \frac{\mathcal{O}}{\mathfrak{p}} \simeq \frac{\hat{\mathcal{O}}_\nu}{\hat{\mathfrak{p}}_\nu}$$
y por ello $\hat{L}_\nu$ es un cuerpo completo con cuerpo residual finito y gracias a 1.5.4 es $\hat{L}_\nu$ un cuerpo local.

□

Ya podemos probar el teorema principal de la sección. El siguiente lema será utilizado en la demostración:

Lema 1.5.6. Sea k un cuerpo completo valorado cuya topología no es discreta. Todo espacio vectorial topológico de Hausdorff V sobre k que admita un entorno de 0 con clausura compacta es de dimensión finita.

Demostración. Ver [Bou81] *Capítulo I, §2, Sección 4, Teorema 3.*

□

Teorema 1.5.7. Sea L un cuerpo local de característica nula. Si L es arquimediano entonces es isomorfo a $\mathbb{R}$ o $\mathbb{C}$, si L es no arquimediano entonces es isomorfo a una extensión finita de $\mathbb{Q}_p$, para algún p primo.

Demostración. Como la característica de L es nula, el cuerpo primo que contiene L es $\mathbb{Q}$ y contiene la compleción de $\mathbb{Q}$ respecto a la restricción del valor absoluto $|\cdot|$ de L. Por el teorema de Ostrowski la restricción de $|\cdot|$ a $\mathbb{Q}$ es equivalente al valor absoluto arquimediano $|\cdot|_\infty$ de $\mathbb{Q}$ o aun valor absoluto p-ádico para algún primo p. Por tanto nuestro cuerpo L contiene un subcuerpo k isomorfo a $\mathbb{R}$ o a $\mathbb{Q}_p$ para algún primo p.

Si k es arquimediano entonces $k = \mathbb{R}$ y es un cuerpo local. Si k es no arquimediano entonces $k = \mathbb{Q}_p$ para algún primo p y en este caso k es un cuerpo de valoración discreta completo con cuerpo residual finito y por 1.5.4 es un cuerpo local. En ambos casos, k es un cuerpo local no discreto (el valor absoluto es no trivial). Gracias a 1.5.6 sabemos que $L \supset k$ es una extensión finita. Si $k = \mathbb{R}$ entonces $L = \mathbb{R}$ o $L = \mathbb{C}$. Si $k = \mathbb{Q}_p$ entonces L es una extensión finita de $\mathbb{Q}_p$.

□

Nota: Nuestros resultados también son ciertos para cuerpos de característica finita. De hecho, las mismas demostraciones funcionan una vez se han resuelto las cuestiones de separabilidad que surgen en el contexto de la característica finita. En el caso no arquimediano, los cuerpos de *series de Laurent* $\mathbb{F}_q((t))$ juegan el papel de los cuerpos $\mathbb{Q}_p$. Para una descripción más detallada ver [Neu99].

Para finalizar vamos a ver que las unidades de un cuerpo completo poseen una descomposición que será muy útil en lo que sigue:

Proposición 1.5.8. Sea k un cuerpo local, entonces el grupo multiplicativo $k^\times$ admite la siguiente descomposición:

$$k^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)},$$

donde π es un parámetro de uniformización de k, q es el cardinal del cuerpo residual $\overline{k} = \mathcal{O}/\mathfrak{p}$, $U^{(1)} = 1 + \mathfrak{p}$ es el grupo de unidades principales y μ_{q-1} es el grupo de las raíces $q-1$-ésimas de la unidad.

Demostración. Sabemos que todo elemento $\alpha \in k^\times$ se puede escribir como $\alpha = u\pi^n$ con $u \in \mathcal{O}^\times$ y $n \in \mathbb{Z}$. Por tanto $k^\times = \pi^{\mathbb{Z}} \times \mathcal{O}^\times$. Como el cuerpo residual $\overline{k}$ es el cuerpo finito con q elementos, el polinomio $X^{q-1} - 1 \in \mathcal{O}[X]$ se descompone en factores lineales gracias al lema de Hensel (1.2.9). Por tanto, $\mathcal{O}^\times$ contiene al grupo de las raíces $q-1$-ésimas de la unidad μ_{q-1}. Observar que $\overline{k}^\times = \mu_{q-1} + \mathfrak{p}$. Sabemos que el homomorfismo $\mathcal{O}^\times \to \overline{k}^\times$ es sobreyectivo con núcleo $U^{(1)}$ y además, restringido sobre μ_{q-1} es un isomorfismo pues si $\zeta \in \mu_{q-1}$ es una raíz $q-1$-ésima primitiva de la unidad y es $\zeta^k + \mathfrak{p} = 1 + \mathfrak{p}$ con $0 \leq k < q-1$ entonces $q-1|k$ y debe ser $k = 0$, es decir, el homomorfismo restringido a μ_{q-1} es una aplicación inyectiva entre conjuntos finitos del mismo cardinal y por ello es biyectiva. En definitiva, $\mathcal{O}^\times = \mu_{q-1} \times U^{(1)}$.

□

Capítulo 2

Teoría de Divisibilidad para Ideales

En este capítulo queremos obtener el concepto de dominio de Dedekind a partir de la teoría de valoraciones. Comenzamos con algunas definiciones:

Definición 2.0.1. Sea o un dominio con cuerpo de fracciones k. Dado un o-módulo $\mathfrak{a} \subset k$ diremos que es un **ideal fraccionario** de o si existe $d \in o \setminus \{0\}$ tal que $d\mathfrak{a} \subset o$. Los ideales fraccionarios contenidos en o (es decir, los ideales usuales) se llamarán **ideales enteros** de o.

Dados dos ideales fraccionarios $\mathfrak{a}, \mathfrak{b}$ de o podemos definir su suma como

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

y su producto como

$$\mathfrak{ab} = \{\sum a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}.$$

Notar que para la definición del producto estamos usando que $\mathfrak{a}, \mathfrak{b} \subset k$ de modo que podemos multiplicar elementos. Es inmediato que la suma o producto de ideales fraccionarios dan lugar a un ideal fraccionario.

Ahora vamos a definir lo que entenderemos por valoración de ideales. Para ello, supongamos que el dominio o está contenido en el anillo de valoración de cierta valoración **discreta normalizada** ν de k, es decir, $r \in o \Rightarrow \nu(r) \geq 0$. Dado un ideal fraccionario $\mathfrak{a}$ de o definimos

$$\nu(\mathfrak{a}) := \min_{a \in \mathfrak{a}} \nu(a).$$

Veamos que esta definición es consistente, es decir, que dicho mínimo siempre existe: Por definición de ideal fraccionario existe $d \in o \setminus \{0\}$ tal que para todo $a \in \mathfrak{a}$ se tiene que $da \in o$, es decir, para todo $a \in \mathfrak{a}$ es $\nu(a) \geq -\nu(d)$. Como los valores de ν son enteros concluimos que dicho mínimo existe y además se alcanza para algún $a \in \mathfrak{a}$.

Proposición 2.0.2. Dados $\mathfrak{a}, \mathfrak{b}$ ideales fraccionarios de o se cumplen las siguientes propiedades:

1. $\nu(\mathfrak{a} + \mathfrak{b}) = \min(\nu(\mathfrak{a}), \nu(\mathfrak{b}))$,
2. $\nu(\mathfrak{ab}) = \nu(\mathfrak{a}) + \nu(\mathfrak{b})$,
3. Dado $a \in o$ es $\nu(oa) = \nu(a)$.

Demostración. 1. Sabemos que dados $a, b \in k$ entonces $\nu(a+b) \geq \min(\nu(a), \nu(b))$, por tanto

$$\begin{aligned}\nu(\mathfrak{a}+\mathfrak{b}) &= \min_{a\in\mathfrak{a}, b\in\mathfrak{b}} (\nu(a+b), \nu(a), \nu(b)) \\ &= \min_{a\in\mathfrak{a}, b\in\mathfrak{b}} (\nu(a), \nu(b)) \\ &= \min(\nu(\mathfrak{a}), \nu(\mathfrak{b})).\end{aligned}$$

2. Es $\nu(\sum a_i b_i) \geq \min_i(\nu(a_i b_i))$ de modo que

$$\begin{aligned}\nu(\mathfrak{a}\mathfrak{b}) &= \min_{a\in\mathfrak{a}, b\in\mathfrak{b}} (\nu(ab)) \\ &= \min_{a\in\mathfrak{a}, b\in\mathfrak{b}} (\nu(a)+\nu(b)) \\ &= \nu(\mathfrak{a})+\nu(\mathfrak{b}).\end{aligned}$$

3. Para todo $x \in o$ es $\nu(x) \geq 0$ y para $x = 1$ es $\nu(1) = 0$ por tanto

$$\nu(oa) = \min_{x\in o}(\nu(a)+\nu(x)) = \nu(a).$$

□

2.1. Divisores

Con las definiciones introducidas podemos desarrollar nuestra teoría de divisibilidad para los ideales de un anillo o. Para ser más explícitos, nuestro objetivo es comprobar que bajo ciertas hipótesis lo siguiente se verifica:

1. Existe un conjunto de valoraciones normalizadas de k cuyos anillos de valoración contienen a o y tales que los ideales fraccionarios de o están determinados unívocamente por el valor de dichas valoraciones sobre estos.

2. Dado un cierto número entero y una valoración del conjunto anterior existe un ideal fraccionario de modo que el valor de dicha valoración sobre este ideal es el número entero dado.

Las propiedades anteriores no se tienen en general y vamos a ver qué condiciones exigimos a k para que se cumplan. Para ello introducimos los dos axiomas siguientes:

`Ax.1` *El cuerpo k tiene un conjunto Σ de valoraciones discretas normalizadas no equivalentes $\mathfrak{p}$, que denotaremos por $|\cdot|_\mathfrak{p}$ o $\nu_\mathfrak{p}$, de modo que para todo $a \in k$ es*

$$|a|_\mathfrak{p} \leq 1 \text{ (equiv. } \nu_\mathfrak{p}(a) \geq 0) \text{ para todo } \mathfrak{p} \text{ salvo un número finito.}$$

`Ax.2` *Dado un conjunto finito de valoraciones* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \Sigma$, *un número real* $\varepsilon > 0$ *y* r *elementos* $a_1, \ldots, a_r \in k$ *existe un elemento* $c \in k$ *tal que*

$$|c - a_i|_{\mathfrak{p}_i} \leq \varepsilon \ i = 1, 2, \ldots, r$$
$$|c|_{\mathfrak{p}} \leq 1 \text{ para todo } \mathfrak{p} \in \Sigma \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}.$$

Notemos que `Ax.1` es equivalente a la siguiente propiedad más fuerte: Dado $a \in k \setminus \{0\}$ la aplicación del axioma `Ax.1` a a^{-1} nos dice que

$$|a|_{\mathfrak{p}} = 1 \text{ para casi todo } \mathfrak{p} \in \Sigma.$$

De hecho, supongamos que tenemos o un anillo contenido en todos los anillos de valoración correspondientes a $\mathfrak{p} \in \Sigma$ y $\mathfrak{a}$ un ideal fraccionario no nulo de o. Por definición existe $d \in o \setminus \{0\}$ tal que $d\mathfrak{a} \subset o$ y por ello $\nu_{\mathfrak{p}}(\mathfrak{a}) \geq -\nu_{\mathfrak{p}}(d)$ para casi todo $\mathfrak{p} \in \Sigma$. Usando que $\nu_{\mathfrak{p}}(d) = 0$ para casi todo $\mathfrak{p}$ tenemos que $\nu_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ para casi todo $\mathfrak{p}$. Ahora bien, para todo $a \in \mathfrak{a}$ es $\nu_p(\mathfrak{a}) \leq \nu_{\mathfrak{p}}(a)$ y aplicando de nuevo que $\nu_{\mathfrak{p}}(a) = 0$ para casi todo $\mathfrak{p}$ concluimos que $\nu_{\mathfrak{p}}(\mathfrak{a}) = 0$ para casi todo $\mathfrak{p} \in \Sigma$.

Esta observación motiva la siguiente definición:

Definición 2.1.1. Un **divisor** θ de k es un producto formal de potencias de valoraciones $\mathfrak{p} \in \Sigma$:

$$\theta = \prod_{\mathfrak{p} \in \Sigma} \mathfrak{p}^{v_{\mathfrak{p}}}, \ v_{\mathfrak{p}} \in \mathbb{Z}$$

tal que $v_{\mathfrak{p}} = 0$ para casi todo $\mathfrak{p} \in \Sigma$.

Para simplificar la notación solemos representar los divisores como el producto finito de aquellas valoraciones con exponente no nulo, elevadas a dicho exponente. Definimos el **orden de un divisor** $\theta = \prod_{\mathfrak{p} \in \Sigma} \mathfrak{p}^{v_{\mathfrak{p}}}$ en una valoración $\mathfrak{p}$ como

$$\mathtt{ord}_{\mathfrak{p}}(\theta) := v_{\mathfrak{p}}.$$

Para unificar la notación también denotaremos dicho orden por $\nu_{\mathfrak{p}}(\theta)$.

Diremos que un divisor es **entero** si $\mathtt{ord}_{\mathfrak{p}} \geq 0$ para todo $\mathfrak{p} \in \Sigma$. Para dos divisores $\theta_1 = \prod \mathfrak{p}^{v_{\mathfrak{p}}}, \theta_2 = \prod \mathfrak{p}^{u_{\mathfrak{p}}}$ de k definimos su producto y su suma como sigue:

$$\theta_1 \theta_2 := \prod_{\mathfrak{p} \in \Sigma} \mathfrak{p}^{v_{\mathfrak{p}} + u_{\mathfrak{p}}},$$
$$\theta_1 + \theta_2 := \prod_{\mathfrak{p} \in \Sigma} \mathfrak{p}^{\min(v_{\mathfrak{p}}, u_{\mathfrak{p}})}.$$

Con esta definición es claro que el conjunto de los divisores de k es un grupo con la multiplicación isomorfo a la suma directa $\sum_{\mathfrak{p}\in\Sigma}\mathbb{Z}$.

De nuevo, supuesto que tenemos un anillo o contenido en todos los anillos de valoración, podemos asignar de manera canónica a cada ideal fraccionario $\mathfrak{a}\neq(0)$ de o un divisor:

$$\mathfrak{a}\mapsto\prod_{\mathfrak{p}\in\Sigma}\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}.$$

Análogamente, para cada $a\in k\setminus\{0\}$ podemos definir

$$a\mapsto\prod_{\mathfrak{p}\in\Sigma}\mathfrak{p}^{\nu_{\mathfrak{p}}(a)}.$$

Gracias a 2.0.2 tenemos que la aplicación que asigna a cada ideal $\mathfrak{a}$ su divisor canónico es un homomorfismo del semigrupo multiplicativo de los ideales en el grupo multiplicativo de los divisores y también es un homomorfismo del semigrupo aditivo de los ideales en el semigrupo aditivo de los divisores.

Denotaremos por $\mathcal{D}iv$ al grupo de divisores del cuerpo k y al divisor asociado a un ideal $\mathfrak{a}$ (resp. un elemento $a\in k$) por $\mathtt{div}(\mathfrak{a})$ (resp. $\mathtt{div}(a)$).

Nosotros vamos a definir el anillo o que buscamos como $o:=\cap_{\mathfrak{p}\in\Sigma}o_{\mathfrak{p}}$, siendo $o_{\mathfrak{p}}$ el anillo de valoración discreta asociado a la valoración $\mathfrak{p}$:

$$o_{\mathfrak{p}}=\{a\in k\mid|a|_{\mathfrak{p}}\leq 1\}.$$

Tenemos que verificar que o es efectivamente el objeto que buscamos. Antes necesitaremos hacer un estudio breve de la resolución de ecuaciones diofánticas sobre el anillo o.

2.1.1. Ecuaciones Diofánticas

Consideremos el siguiente sistema:

$$\begin{aligned}
y_1&=a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n+b_1,\\
y_2&=a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n+b_2,\\
&\vdots\\
y_m&=a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n+b_m.
\end{aligned}$$

con $a_{ij}\in k$ y $b_i\in k$. Nuestro objetivo es estudiar la resolubilidad de este sistema sobre o, es decir de manera global. Vamos a ver que existe una solución global si y sólo si existe una solución local para cada valoración $\mathfrak{p}$, esto es, sobre $o_{\mathfrak{p}}$ para todo $\mathfrak{p}\in\Sigma$. En realidad, el problema que nosotros queremos

resolver es el de buscar x_j en el anillo adecuado de manera que las sumas $\sum a_{ij}x_j + b_i$ pertenezcan al mismo anillo para todo i, es decir, para nosotros no será esencial hallar los valores y_j si no los valores x_i y saber cuando las combinaciones lineales dan lugar a un elemento en el mismo anillo. El siguiente teorema garantiza la equivalencia de la versión local y la versión global del problema:

Teorema 2.1.2. Consideremos el sistema de ecuaciones

$$\begin{array}{rl} y_1 & = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n + b_1, \\ y_2 & = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n + b_2, \\ & \vdots \\ y_m & = a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n + b_m, \end{array} \qquad \text{con } a_{ij} \in k, b_i \in k.$$

Entonces existen $x_1, \ldots, x_n, y_1, \ldots, y_m \in \mathcal{o}$ solución (global) del sistema si y sólo si para cada $\mathfrak{p} \in \Sigma$ existe una solución $x_1(\mathfrak{p}), \ldots, x_n(\mathfrak{p}), y_1(\mathfrak{p}), \ldots, y_m(\mathfrak{p}) \in \mathcal{o}_\mathfrak{p}$ solución (local en $\mathfrak{p}$) del sistema.

Demostración. La definición $\mathcal{o} = \cap_{\mathfrak{p}\in\Sigma}\mathcal{o}_\mathfrak{p}$ hace trivial la implicación $\Rightarrow$ pues $\mathcal{o} \subset \mathcal{o}_\mathfrak{p}$ para todo $\mathfrak{p} \in \Sigma$. Para la otra implicación hacemos algunas observaciones que simplificarán la tarea:

a. Si $\mathfrak{p}$ es una valoración para la cual

$$|a_{ij}|_\mathfrak{p} \leq 1, \ |b_i|_\mathfrak{p} \leq 1 \ \forall i, j$$

entonces todas la n-uplas $x_1, x_2, \ldots, x_n$ verificando $|x_j|_\mathfrak{p} \leq 1$ para todo j dan lugar a una solución local al problema para la valoración $\mathfrak{p}$. En efecto, supuesto que se verifica lo anterior, basta tomar $y_i = \sum_{j=1}^n a_{ij}x_j + b_i$ pues

$$|\sum a_{ij}x_j + b_i|_\mathfrak{p} \leq \max_j(|a_{ij}x_j|_\mathfrak{p}, |b_i|_\mathfrak{p}) \leq 1.$$

b. Supongamos que tenemos una solución local $\underline{x}(\mathfrak{p}) = (x_1(\mathfrak{p}), \ldots, x_n(\mathfrak{p}))$ para la valoración $\mathfrak{p}$. Sea $\underline{x}'(\mathfrak{p}) = (x_1'(\mathfrak{p}), \ldots, x_n'(\mathfrak{p}))$ tal que $|x_j(\mathfrak{p}) - x_j'(\mathfrak{p})|_\mathfrak{p}$ es suficientemente pequeño. Entonces $\underline{x}'(\mathfrak{p})$ es una solución local. En efecto, supongamos que $\max_j |x_j(\mathfrak{p}) - x_j'(\mathfrak{p})|_\mathfrak{p} < \varepsilon$ con ε tal que

$\varepsilon \cdot (\text{máx}_j\, |a_{ij}|_{\mathfrak{p}}) \leq 1$ para todo $i = 1, \ldots, m$. Tenemos que

$$\begin{aligned}
|\sum_{j=0}^{n} a_{ij}x'_j(\mathfrak{p}) + b_i|_{\mathfrak{p}} &= |\sum_{j=0}^{n} a_{ij}x'_j(\mathfrak{p}) + b_i \pm (\sum_{j=0}^{n} a_{ij}x_j(\mathfrak{p}) + b_i)|_{\mathfrak{p}} \\
&= |\sum_{j=0}^{n} a_{ij}(x'_j(\mathfrak{p}) - x_j(\mathfrak{p})) + \sum_{j=0}^{n} a_{ij}x_j(\mathfrak{p}) + b_i|_{\mathfrak{p}} \\
&\leq \text{máx}(|\sum_{j=0}^{n} a_{ij}(x'_j(\mathfrak{p}) - x_j(\mathfrak{p}))|_{\mathfrak{p}}, |\sum_{j=0}^{n} a_{ij}x_j(\mathfrak{p}) + b_i|_{\mathfrak{p}}) \\
&\leq \text{máx}(|\sum_{j=0}^{n} a_{ij}(x'_j(\mathfrak{p}) - x_j(\mathfrak{p}))|_{\mathfrak{p}}, 1) \\
&\leq \text{máx}(\max_j |a_{ij}|_{\mathfrak{p}} \cdot |x'_j(\mathfrak{p}) - x_j(\mathfrak{p})|_{\mathfrak{p}}, 1) \\
&= \text{máx}((\max_j |a_{ij}|_{\mathfrak{p}}) \cdot (\max_j |x'_j(\mathfrak{p}) - x_j(\mathfrak{p})|_{\mathfrak{p}}), 1) \\
&< \text{máx}(\varepsilon \cdot (\max_j |a_{ij}|_{\mathfrak{p}}), 1) = 1 \ \forall i = 1, \ldots, m.
\end{aligned}$$

Si tenemos una solución local $\underline{x}(\mathfrak{p})$ para cada valoración $\mathfrak{p}$, por `Ax.1` sabemos que para todo $\mathfrak{p}$ excepto un conjunto finito $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ es $|a_{ij}|_{\mathfrak{p}} \leq 1$ y $|b_i|_{\mathfrak{p}} \leq 1$. Para todos esos $\mathfrak{p}$ ya sabemos que todos los elementos de $o_{\mathfrak{p}}$ son solución. Para el conjunto finito $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, usando `Ax.2`, obtenemos para cada $j = 1, \ldots, n$ un $x_j \in k$ tal que

$$|x_j - x_j(\mathfrak{p}_i)|_{\mathfrak{p}_i} < \varepsilon, \ i = 1, \ldots, r,$$

$$|x_j|_{\mathfrak{p}} \leq 1 \ \forall \ \mathfrak{p} \neq \mathfrak{p}_i,$$

siendo ε un número real lo suficientemente pequeño de modo que la observación *b.* es aplicable. Tenemos entonces que los números $(x_1, \ldots, x_n)$ son una solución local para todo $\mathfrak{p}$ que es independiente de $\mathfrak{p}$. Por definición de o concluimos que $x_j \in o$ para todo $j = 1, \ldots, n$ e $y_i \in o$ para todo $i = 1, \ldots, m$. Hemos visto como construir una solución global a partir de las soluciones locales y esto concluye la demostración.

□

De este resultado podemos obtener el siguiente corolario:

Corolario 2.1.3. Un sistema de ecuaciones

$$\sum_{j=0}^{n} a_{ij}x_j = b_i \ i = 1, \ldots, m$$

con $a_{ij}, b_i \in k$ tiene solución en o si y sólo si tiene solución en $o_{\mathfrak{p}}$ para todo $\mathfrak{p} \in \Sigma$.

Demostración. De nuevo, la implicación $\Rightarrow$ es trivial. Para la otra implicación, si suponemos que tenemos una solución local para todo $\mathfrak{p}$, como $o_{\mathfrak{p}} \subset k$ tenemos que el sistema de ecuaciones lineales del enunciado admite al menos una solución en k. Por álgebra lineal sabemos que hay dos posibilidades:

a. Si el sistema tiene una única solución sobre k entonces todas las soluciones locales coinciden y esa solución debe ser global.

b. Si el sistema k tiene más de una solución entonces alguna de las variables x_i se puede expresar como combinación lineal del resto. Si ahora denotamos dicha variable x_i por y_i vemos que el problema queda reducido a 2.1.2.

□

Nosotros solo haremos uso del teorema en el caso de una sola ecuación. En este caso nuestro análisis se reduce al siguiente criterio:

Corolario 2.1.4. Una ecuación lineal

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \; a_i, b \in k$$

admite una solución sobre o si y sólo si para todo $\mathfrak{p} \in \Sigma$ se cumple la desigualdad

$$|b|_{\mathfrak{p}} \leq \max_{1\leq i\leq n} |a_i|_{\mathfrak{p}}.$$

Demostración. Para demostrar el resultado es suficiente probar que la desigualdad anterior es una condición necesaria y suficiente para que la ecuación tenga solución local en $o_{\mathfrak{p}}$. Sin pérdida de generalidad vamos a suponer que al menos un coeficiente a_i es no nulo, digamos que $a_n \neq 0$. Obtenemos la igualdad equivalente:

$$x_n = -\sum_{i=1}^{n-1} \frac{a_i}{a_n} x_i - \frac{-b}{a_n}.$$

Para estudiar dicha ecuación vamos a ver cuando una ecuación de la forma

$$y = a_1x_1 + \cdots + a_{n-1}x_{n-1} + b$$

tiene solución en $o_{\mathfrak{p}}$. Notemos que si conocemos una solución entonces es $b = y - \sum_{j=1}^{n-1} a_jx_j$ y por ello

$$|b|_{\mathfrak{p}} \leq \max(1, |a_1|_{\mathfrak{p}}, \ldots, |a_{n-1}|_{\mathfrak{p}}).$$

Recíprocamente, supongamos que esta desigualdad es cierta. Tenemos dos casos:

a. *El máximo es* 1. Entonces $|a_i|_\mathfrak{p} \leq 1$ para todo i y $|b|_\mathfrak{p} \leq 1$. Cualquier conjunto de valores $x_1, \ldots, x_{n-1}$ con $|x_i|_\mathfrak{p} \leq 1$ (i.e. $x_i \in o_\mathfrak{p}$) es una solución local.

b. *El máximo es* $|a_1|$. Entonces $|b|_\mathfrak{p} \leq |a_1|_\mathfrak{p}$ con $|a_1|_\mathfrak{p} \geq 1$. Si tomamos $x_1 = -b/a_1, x_2 = x_3 = \cdots = x_{n-1} = 0$ obtenemos una solución local con $y = 0$. Notar que $|-b/a_1|_\mathfrak{p} \leq 1$.

Esto demuestra que la ecuación $y = a_1x_1 + \cdots + a_{n-1}x_{n-1} + b$ tiene solución en $o_\mathfrak{p}$ si y sólo si $|b|_\mathfrak{p} \leq \text{máx}(1, |a_1|_\mathfrak{p}, \ldots, |a_{n-1}|_\mathfrak{p})$. Reescribiendo esta desigualdad para nuestra ecuación $x_n = -(a_1/a_n)x_1 - \cdots - (a_{n-1}/a_n)x_{n-1} - (-b/a_n)$ obtenemos que la ecuación del enunciado tiene solución local si y sólo si

$$\left|\frac{b}{a_n}\right|_\mathfrak{p} \leq \text{máx}(1, \left|\frac{a_1}{a_n}\right|_\mathfrak{p}, \ldots, \left|\frac{a_{n-1}}{a_n}\right|_\mathfrak{p}).$$

□

Observar que, si para cada coeficiente a_i consideramos su divisor asociado $\prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(a_i)}$ y análogamente para b obtenemos $\prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(b)}$, la condición anterior se convierte en

$$\texttt{div}b \text{ es divisible por } \texttt{div}a_1 + \cdots + \texttt{div}a_2,$$

definiendo la divisibilidad entre divisores en un sentido natural. Además esta observación nos indica que la suma de divisores debemos considerarla como el máximo común divisor de los divisores en cuestión.

2.1.2. Teoría de Divisibilidad para Ideales

Usando el teorema sobre ecuaciones diofánticas podemos demostrar que la teoría de divisibilidad de ideales se sigue de nuestros dos axiomas:

1. *k es el cuerpo de fracciones de o:* Dado $a \in k \setminus \{0\}$, por `Ax.1` es $|a|_\mathfrak{p} \leq 1$ para todo $\mathfrak{p} \in \Sigma$ salvo para un número finito $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Si consideramos en `Ax.2` los valores $a_1 = \cdots = a_r = a^{-1}$ tenemos que para todo $\varepsilon > 0$ existe un $x_\varepsilon \in k$ tal que $|x_\varepsilon - a^{-1}|_{\mathfrak{p}_i} < \varepsilon$ para todo $i = 1, \ldots, r$ y $|x_\varepsilon|_\mathfrak{p} \leq 1$ para todo $\mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Las condiciones que verifica x_ε podemos reescribirlas como

$$|x_\varepsilon - a^{-1}|_\mathfrak{p} < \varepsilon \text{ si } |a|_\mathfrak{p} > 1,$$
$$|x_\varepsilon|_\mathfrak{p} \leq 1 \text{ en otro caso.}$$

   Por tanto, teniendo en cuenta que $|a|_\mathfrak{p} > 1$ implica $|a^{-1}|_\mathfrak{p} < 1$, obtenemos que $|a|_\mathfrak{p} > 1$ implica $|x_\varepsilon|_\mathfrak{p} = |x_\varepsilon \pm a^{-1}|_\mathfrak{p} \leq \text{máx}(|x_\varepsilon - a^{-1}|, |a^{-1}|_\mathfrak{p}) < \text{máx}(\varepsilon, 1) < 1$ para $\varepsilon < \text{mín}(1, |a^{-1}|_{\mathfrak{p}_1}, \ldots, |a^{-1}|_{\mathfrak{p}_r})$. Notar además que si tomamos ε como antes entonces $x_\varepsilon \neq 0$ pues en caso contrario, cuando $|a|_\mathfrak{p} > 1$, tendríamos que $|a^{-1}|_\mathfrak{p} < \epsilon$ que es absurdo.

Por tanto, $x_\epsilon \in \mathfrak{o}$ y

$$|ax_\varepsilon - 1|_\mathfrak{p} < \varepsilon |a|_\mathfrak{p} \text{ si } |a|_\mathfrak{p} > 1,$$
$$|ax_\varepsilon|_\mathfrak{p} \leq 1 \text{ en otro caso.}$$

De nuevo, tomando ε suficientemente pequeño podemos conseguir también $ax \in \mathfrak{o}$. Entonces $a = \frac{ax}{x}$ con $ax, x \in \mathfrak{o}$.

2. *Caracterizar ideales por sus órdenes $\nu_\mathfrak{p}$ para todo $\mathfrak{p}$.* Sea $\mathfrak{a}$ un ideal fraccionario de $\mathfrak{o}$ y $v_\mathfrak{p} = \nu_\mathfrak{p}(\mathfrak{a})$. Sea $a \in \mathfrak{a}$ un elemento no nulo. Entonces $\nu_\mathfrak{p}(a) \geq v_\mathfrak{p}$ para todo $\mathfrak{p}$. Sabemos que $\nu_\mathfrak{p}(a)$ y $v_\mathfrak{p}$ son cero para casi todo $\mathfrak{p}$, de modo que el conjunto de valoraciones $\mathfrak{p} \in \Sigma$ tales que $\nu_\mathfrak{p}(a) \neq v_\mathfrak{p}$ es finito, digamos que sus elementos son $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Para cada $i = 1, \ldots, r$ tomamos un $a_i \in \mathfrak{a}$ tal que $\nu_{\mathfrak{p}_i}(a_i) = v_{\mathfrak{p}_i}$ y consideramos la ecuación diofántica

$$ax + a_1x_1 + \cdots + a_rx_r = b,\ b \in k.$$

Sabemos que esta ecuación tendrá solución local en $\mathfrak{p}$ si y sólo

$$\nu_\mathfrak{p}(b) \geq \text{mín}(\nu_\mathfrak{p}(a), \nu_\mathfrak{p}(a_1), \ldots, \nu_\mathfrak{p}(a_r)).$$

Notar que si $\mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ entonces el mínimo es $\nu_\mathfrak{p}(a) = v_\mathfrak{p}$ mientras que si $\mathfrak{p} = \mathfrak{p}_i$ para algún i entonces el mínimo es $\nu_{\mathfrak{p}_i}(a_i) = v_{\mathfrak{p}_i}$. En definitiva, tenemos que la ecuación tiene solución global si y sólo si para todo $\mathfrak{p} \in \Sigma$ es

$$\nu_\mathfrak{p}(b) \geq v_\mathfrak{p}.$$

Esto último nos dice que todo elemento b verificando dicha desigualdad lo podemos expresar como $b = ax + \sum_{i=1}^r a_ix_i,\ x, x_i \in \mathfrak{o}$ y como $a, a_i \in \mathfrak{a}$ tenemos que dicho b pertenece a $\mathfrak{a}$. Concluimos que el ideal $\mathfrak{a}$ coincide con el conjunto $\{b \in k \mid \nu_\mathfrak{p}(b) \geq v_\mathfrak{p}\ \forall\ \mathfrak{p} \in \Sigma\}$, es decir, $\mathfrak{a}$ está determinado por sus órdenes. Observar que, además, hemos demostrado que todo ideal fraccionario de $\mathfrak{o}$ es finitamente generado, en particular, $\mathfrak{o}$ es noetheriano. Si queremos interpretar esta propiedad abstractemente hemos demostrado que el homomorfismo $\mathfrak{a} \mapsto \mathtt{div}(\mathfrak{a}) = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}$ es inyectivo.

3. *Dados órdenes siempre existe un ideal con dichos órdenes.* Queremos demostrar que el homomorfismo $\mathfrak{a} \mapsto \mathtt{div}(\mathfrak{a}) = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}$ es sobreyectivo. Será suficiente demostrar el siguiente lema:

Lema 2.1.5. Dados $v_{\mathfrak{p}_1}, \ldots, v_{\mathfrak{p}_r}$ números enteros existe $a \in k$ tal que

$$\nu_{\mathfrak{p}_i}(a) = v_{\mathfrak{p}_i},\ i = 1, \ldots, r,$$
$$\nu_\mathfrak{p}(a) \geq 0 \text{ para cualquier otra } \mathfrak{p}.$$

Demostración. Para cada i tomamos un $a_i \in k$ tal que $\nu_{\mathfrak{p}_i}(a_i) = v_{\mathfrak{p}_i}$. Consideremos $a \in k$ tal que

$$|a - a_i|_{\mathfrak{p}_i} < |a_i|_{\mathfrak{p}_i} \ i = 1, \ldots, r,$$
$$|a|_{\mathfrak{p}} \leq 1 \text{ para cualquier otra valoración } \mathfrak{p}.$$

Como $|a|_{\mathfrak{p}_i} = |a_i + (a - a_i)|_{\mathfrak{p}_i} = |a_i|_{\mathfrak{p}_i}$, el lema se concluye reexpresando lo anterior en términos de valoraciones exponenciales.

□

Supongamos que tenemos números enteros $v_{\mathfrak{p}}$ para cada $\mathfrak{p} \in \Sigma$ de modo que son todos nulos salvo un número finito de ellos, digamos $v_{\mathfrak{p}_1}, \ldots, v_{\mathfrak{p}_r}$. Por `Ax.2` (versión para valoraciones) podemos hallar $a \in k$ tal que $\nu_{\mathfrak{p}_i}(a) \geq v_{\mathfrak{p}_i}$ para $i = 1, \ldots, r$ y $\nu_{\mathfrak{p}}(a) \geq 0$ para el resto de valoraciones $\mathfrak{p}$, por tanto $\nu_{\mathfrak{p}}(a =\geq v_{\mathfrak{p}}$ para todo $\mathfrak{p} \in \Sigma$. Sean $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \in \Sigma$ valoraciones tales que $\nu_{\mathfrak{p}}(a) = 0$ si $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$. De este modo tenemos que $\nu_{\mathfrak{p}_i}(a) \geq v_{\mathfrak{p}_i}$, $\nu_{\mathfrak{q}_j}(a) > 0$ y $\nu_{\mathfrak{p}}(a) = 0$ para el resto de valoraciones $\mathfrak{p}$.

Aplicando el lema 2.1.5 sabemos que existe $b \in k$ de modo que $\nu_{\mathfrak{p}}(b) = v_{\mathfrak{p}}$ para $\mathfrak{p} = \mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ y en el resto de valoraciones es $\nu_{\mathfrak{p}}(b) \geq 0$. Si comparamos los valores $\nu_{\mathfrak{p}}(a)$ y $\nu_{\mathfrak{p}}(b)$ para todo $\mathfrak{p}$ vemos que

$$\text{mín}(\nu_{\mathfrak{p}}(a), \nu_{\mathfrak{p}}(b)) = \begin{cases} v_{\mathfrak{p}} & \text{si } \mathfrak{p} = \mathfrak{p}_1, \ldots, \mathfrak{p}_r, \\ 0 & \text{si } \mathfrak{p} = \mathfrak{q}_1, \ldots, \mathfrak{q}_s, \\ 0 & \text{en otro caso.} \end{cases}$$

Concluimos que el divisor asociado al ideal $\mathfrak{o}a + \mathfrak{o}b$ es $\prod_{\mathfrak{p}} \mathfrak{p}^{\text{mín}(\nu_{\mathfrak{p}}(a), \nu_{\mathfrak{p}}(b))} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}$.

Observar que gracias a que `div` es un isomorfismo, todo ideal $\mathfrak{a}$ de $\mathfrak{o}$ puede ser generado por dos elementos a, b pudiéndose elegir $a \in \mathfrak{a}$ arbitrario. En efecto, una vez elegido $a \in \mathfrak{a}$ tenemos que $\nu_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}$ para toda valoración $\mathfrak{p}$ y ahora tan sólo hay que seguir con la prueba como antes.

Así mismo, debido a que `div` es un isomorfismo sabemos que el conjunto de ideales fraccionarios de $\mathfrak{o}$ forman un grupo. Los ideales fraccionarios enteros se corresponden con los divisores enteros, es decir, son los ideales $\mathfrak{a}$ tales que $\nu_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ para todo $\mathfrak{p}$. Vamos a ver cuáles son los divisores asociados a los ideales primos de $\mathfrak{o}$. Primero introducimos la noción de divisibilidad entre ideales: *Dados dos ideales* $\mathfrak{a}, \mathfrak{b}$ *decimos que* $\mathfrak{b}$ **divide a** $\mathfrak{a}$ *(notado* $\mathfrak{b}|\mathfrak{a}$*) si el ideal* $\mathfrak{b}^{-1}\mathfrak{a}$ *es entero.*

La definición anterior es equivalente a que se verifique la inclusión $\mathfrak{a} \subset \mathfrak{b}$ pues $\mathfrak{a} = \{x \in k | \nu_{\mathfrak{p}}(x) \geq \nu_{\mathfrak{p}}(\mathfrak{a})\}$. Vista la noción de divisibilidad, supongamos que tenemos un ideal $\mathfrak{a}$ entero tal que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ con $\mathfrak{b} \neq \mathfrak{o}, \mathfrak{c} \neq \mathfrak{o}$. Tenemos entonces que $\mathfrak{b}|\mathfrak{a}, \mathfrak{c}|\mathfrak{a}$. Es $\mathfrak{a} \subset \mathfrak{b}$ con $\mathfrak{a} \neq \mathfrak{b}$ y análogamente $\mathfrak{a} \subset \mathfrak{c}$ con $\mathfrak{a} \neq \mathfrak{c}$.

Esto implica que existen $b \in \mathfrak{b}, c \in \mathfrak{c}$ tales que $b, c \notin \mathfrak{a}$ y $bc \in \mathfrak{a}$, es decir, $\mathfrak{a}$ no es un ideal primo. Esto nos indica que para que un ideal $\mathfrak{a}$ sea primo entonces $\mathtt{div}(\mathfrak{a})$ debe tener sólo un factor. Veamos que de hecho los divisores que tienen un único factor son todos los ideales primos no nulos de o. Si $\mathfrak{a}$ es un ideal tal que $\mathtt{div}(\mathfrak{a}) = \mathfrak{p}$, como

$$\mathfrak{a} = \{x \in k \mid \nu_{\mathfrak{p}}(a) \geq 1, \nu_{\mathfrak{q}}(a) \geq 0 \ \forall \mathfrak{q} \neq \mathfrak{p}\}$$

tenemos que si $ab \in \mathfrak{a}$ con $a, b \in o$ entonces

$$\nu_{\mathfrak{p}}(ab) = \nu_{\mathfrak{p}}(a) + \nu_{\mathfrak{p}}(b) \geq 1, \nu_{\mathfrak{p}}(a), \nu_{\mathfrak{p}}(b) \geq 0$$
$$\nu_{\mathfrak{q}}(ab) = \nu_{\mathfrak{q}}(a) + \nu_{\mathfrak{q}}(b) \geq 0, \nu_{\mathfrak{q}}(a), \nu_{\mathfrak{q}}(b) \geq 0 \ \forall \ \mathfrak{q} \neq \mathfrak{p}$$

Estas condiciones implican que se cumplen las condiciones

$$\nu_{\mathfrak{p}}(a) \geq 1, \nu_{\mathfrak{q}}(a) \geq 0 \ \forall \ \mathfrak{q} \neq \mathfrak{p},$$

o las condiciones

$$\nu_{\mathfrak{p}}(b) \geq 1, \nu_{\mathfrak{q}}(b) \geq 0 \ \forall \ \mathfrak{q} \neq \mathfrak{p}.$$

Es decir $a \in \mathfrak{a}$ o $b \in \mathfrak{a}$, i.e., $\mathfrak{a}$ es un ideal primo que denotaremos simplemente por $\mathfrak{p}$.

Concluimos que los ideales primos no nulos de o están en biyección con el conjunto de valoraciones Σ y por ello todo ideal de o se descompone de manera esencialmente única como producto de ideales primos. Por último, el anillo $o = \cap_{\mathfrak{p}} o_{\mathfrak{p}}$ es integralmente cerrado pues si un elemento $\alpha \in k$ es raíz de un polinómio mónico $f \in o[x]$ entonces α es un elemento entero de todos los anillos $o_{\mathfrak{p}}$ y sabido que estos anillos de valoración discreta son integralmente cerrados concluimos que $\alpha \in \cap_{\mathfrak{p}} o_{\mathfrak{p}} = o$. Es importante observar que los anillos de valoración $o_{\mathfrak{p}} = \{x \in k \mid \nu_{\mathfrak{p}}(x) \geq 0\}$ coinciden con la localización $S^{-1}o$ del anillo o con $S = o \setminus \mathfrak{p}$ para todo ideal primo $\mathfrak{p}$ no nulo de o.

2.1.3. Carácter Necesario de los Axiomas

Hemos visto que los axiomas `Ax.1` y `Ax.2` tienen como consecuencia más importante que el conjunto de ideales fraccionarios del anillo o es un grupo con el producto. Ahora vamos a ver que el recíproco es cierto, es decir, tenemos la siguiente proposición:

Proposición 2.1.6. Sea o un dominio con cuerpo de fracciones k y cuyos ideales fraccionarios no nulos forman un grupo, entonces el cuerpo k verifica los axiomas `Ax.1` y `Ax.2`.

Demostración. La demostración se desarrolla en numerosas etapas:

1. **Todo ideal fraccionario de o es finitamente generado.** Supongamos que $\mathfrak{a}$ es un ideal fraccionario de o con inverso $\mathfrak{b}$ de modo que $\mathfrak{ab} = o$. Entonces existen $a_1, \ldots, a_r \in \mathfrak{a}, b_1, \ldots, b_r \in \mathfrak{b}$ tales que
$$1 = \sum_{i=1}^{r} a_i b_i.$$
Consideremos el ideal $\mathfrak{a}' = oa_1 + \cdots + oa_r \subset \mathfrak{a}$. Tenemos que $\mathfrak{a}' = \mathfrak{a}$ pues $\mathfrak{a}'\mathfrak{b} \subset \mathfrak{ab} = o$ y $1 \in \mathfrak{a}'\mathfrak{b}$ luego $\mathfrak{a}'\mathfrak{b} = \mathfrak{ab}$, es decir, multiplicando por $\mathfrak{a}$ llegamos a $\mathfrak{a} = \mathfrak{a}'$. Observar que esto se tiene sin necesidad de usar que el conjunto de ideales fraccionarios de o es un grupo.

   En particular, el anillo o es noetheriano. De hecho, usando esto, deducimos que dados dos ideales fraccionarios $\mathfrak{a}, \mathfrak{b}$ se verifican las siguientes equivalencias:
$$\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow \mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1} \subset o \Leftrightarrow \mathfrak{a} = \mathfrak{b}\mathfrak{c},\ \mathfrak{c} \subset o \Leftrightarrow \mathfrak{b}|\mathfrak{a}.$$

2. **Todo ideal entero de o podemos escribirlo como producto de ideales maximales.** Concretamente vamos a demostrar que dado un ideal entero no nulo $\mathfrak{a} \subset o$ se tiene que es $\mathfrak{a} = o$, o $\mathfrak{a}$ es un ideal maximal o $\mathfrak{a}$ es producto de ideales maximales. En efecto, sea A el conjunto de aquellos ideales enteros de o que no cumplen ninguna de las propiedades anteriores. Si A es no vacío, como o es noetheriano sabemos que existe un elemento maximal $\mathfrak{m} \in A$. En particular $\mathfrak{m} \neq o$ y por ello existe un ideal maximal $\mathfrak{p}$ tal que $\mathfrak{m} \subset \mathfrak{p}$. Esto último equivale a que $\mathfrak{p}|\mathfrak{m}$, es decir, existe un ideal entero $\mathfrak{c} \subset o$ tal que $\mathfrak{m} = \mathfrak{p}\mathfrak{c}$ con $\mathfrak{m} \subset \mathfrak{c}, \mathfrak{c} \neq \mathfrak{m}, \mathfrak{c} \neq o$. Como $\mathfrak{m}$ es maximal en A tenemos que $\mathfrak{c} \notin A$ y por ello $\mathfrak{c}$ es o un ideal maximal o un producto de ideales maximales, en cualquier caso $\mathfrak{m}$ también lo es contradiciendo que $\mathfrak{m} \in A$.

3. **La descomposición de un ideal entero como producto de ideales maximales es única salvo reordenación.** En efecto, primeros notemos que si $\mathfrak{a}, \mathfrak{b}$ son dos ideales enteros y $\mathfrak{p}$ es un ideal maximal con $\mathfrak{p} \not| \mathfrak{a}$ ($\mathfrak{a} \not\subset \mathfrak{p}$) y $\mathfrak{p}|\mathfrak{ab}$ entonces $\mathfrak{a} + \mathfrak{p} = o$ y multiplicando por $\mathfrak{b}$ concluimos que $\mathfrak{b} = \mathfrak{ab} + \mathfrak{pb} \subset \mathfrak{p}$, es decir, $\mathfrak{p}|\mathfrak{b}$. Con esto mente, si tenemos dos descomposiciones
$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$
con ideales maximales $\mathfrak{p}_i, \mathfrak{q}_j$, tenemos que $\mathfrak{p}_1|\mathfrak{q}_1 \cdots \mathfrak{q}_s$ y por ello $\mathfrak{p}_1$ divide a algún factor que podemos suponer que es $\mathfrak{q}_1$. Por maximalidad concluimos que $\mathfrak{p}_1 = \mathfrak{q}_1$. Si reiteramos este proceso llegamos a que $r = s$ y que los factores que intervienen son los mismos salvo reordenación.

   Concluimos que todo ideal entero $\mathfrak{a}$ se puede escribir como producto de potencias de ideales maximales:
$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}}\ \ v_\mathfrak{p} \geq 0 \text{ y para casi todo } \mathfrak{p} \text{ es } v_\mathfrak{p} = 0.$$

Las descomposiciones también se tienen para los ideales fraccionarios pues dado un ideal fraccionario $\mathfrak{a}$ entonces existe $d \in o$ tal que $d\mathfrak{a} \subset o$. Obtenemos entonces una descomposición:

$$d\mathfrak{a} = (o d)\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{u_{\mathfrak{p}}},\ u_{\mathfrak{p}} \geq 0 \text{ y para casi todo } \mathfrak{p} \text{ es } u_{\mathfrak{p}} = 0,$$
$$o d = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}},\ e_{\mathfrak{p}} \geq 0 \text{ y para casi todo } \mathfrak{p} \text{ es } e_{\mathfrak{p}} = 0.$$

Por tanto,

$$\mathfrak{a} = (oc)^{-1}(d\mathfrak{a}) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}, v_p = u_p - e_p \text{ y para casi todo } \mathfrak{p} \text{ es } v_{\mathfrak{p}} = 0.$$

La unicidad es inmediata usando que todo ideal fraccionario $\mathfrak{a}$ podemos escribirlo como $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ con $\mathfrak{b}, \mathfrak{c}$ ideales enteros sin factores comunes en sus descomposiciones. Entonces

$$\frac{\mathfrak{b}}{\mathfrak{c}} = \frac{\mathfrak{b}_1}{\mathfrak{c}_1} \Rightarrow \mathfrak{b}\mathfrak{c}_1 = \mathfrak{b}_1\mathfrak{c} \Rightarrow \mathfrak{b} | \mathfrak{b}_1\mathfrak{c} \Rightarrow \mathfrak{b} | \mathfrak{b}_1 \Rightarrow \mathfrak{b}_1 \subset \mathfrak{b}.$$

Análogamente concluimos que $\mathfrak{b} \subset \mathfrak{b}_1$, es decir, $\mathfrak{b} = \mathfrak{b}_1$. Esto implica que $\mathfrak{c} = \mathfrak{c}_1$ lo que nos da la unicidad de la descomposición.

4. **Cada ideal maximal $\mathfrak{p}$ induce una valoración discreta normalizada de** k. Sea $a \in k \backslash \{0\}$ y consideremos la descomposición
$$oa = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}.$$
Definimos $\nu_{\mathfrak{p}}(a) = v_{\mathfrak{p}}$ si $a \neq 0$ y $\nu_{\mathfrak{p}}(0) = \infty$. La definición es consistente gracias a la unicidad de las factorizaciones y ahora vamos a ver que es una valoración discreta. La primera propiedad es inmediata por construcción y la segunda se obtiene a partir de
$$o(ab) = (oa)(ob) \text{ para } a, b \neq 0.$$
Para la tercera propiedad observar que es suficiente demostrar que $\nu_{\mathfrak{p}}(a) \geq 0$ implica $\nu_{\mathfrak{p}}(1+a) \geq 0$. La implicación anterior es claro que se cumple para $a = 0, -1$. Si $a \neq 0, -1$ entonces $\nu_{\mathfrak{p}}(a) \geq 0$ implica que $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ con $\mathfrak{b}, \mathfrak{c}$ enteros y $\mathfrak{p} \not| \mathfrak{c}$. Entonces $o(1+a) \subset o + oa = \mathfrak{c}/\mathfrak{c} + \mathfrak{b}/\mathfrak{c} = (\mathfrak{c}+\mathfrak{b})/\mathfrak{c}$ usando que la ley distributiva se tiene para la suma y multiplicación de ideales de un anillo. Concluimos que
$$o(1+a) = \frac{\mathfrak{c}+\mathfrak{b}}{\mathfrak{b}}\mathfrak{d} \text{ con } \mathfrak{d} \text{ entero y } \mathfrak{p} \not| \mathfrak{c},$$
es decir, $\nu_{\mathfrak{p}}(1+a) \geq 0$. Veamos que esta valoración es discreta, de hecho vamos a ver que está normalizada. Para ello, notar que $\mathfrak{p}^2 \subset \mathfrak{p}$ con $\mathfrak{p}^2 \neq \mathfrak{p}$ de modo que existe $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, es decir, $\mathfrak{p} | o\pi$ pero $\mathfrak{p}^2 \not| o\pi$ luego $\nu_{\mathfrak{p}}(\pi) = 1$. Por último comprobemos que dos ideales maximales

$\mathfrak{p}, \mathfrak{q}$ distintos inducen valoraciones distintas. Como los ideales son maximales tenemos que $\mathfrak{p} + \mathfrak{q} = o$ y por ello existen $\pi \in \mathfrak{p}, \tau \in \mathfrak{q}$ tales que $\pi + \tau = 1$. Como $1 \notin \mathfrak{p}$ tenemos que $\tau \notin \mathfrak{p}$ y por ello $\nu_{\mathfrak{p}}(\tau) \leq 0$ y $\nu_{\mathfrak{q}}(\tau) > 0$.

5. `Axioma 1.` Esta propiedad es trivial pues dado $a \in k \setminus \{0\}$ tenemos que sólo un número finito de ideales maximales aparecen en la factorización de oa, de modo que $\nu_{\mathfrak{p}}(a) = 0$ para casi todo $\mathfrak{p}$.

6. `Axioma 2.` Para ello, observar que un elemento $a \in k$ pertenece a o si y sólo si $oa \subset o$, es decir, $\nu_{\mathfrak{p}}(a) \geq 0$ para todo $\mathfrak{p}$. Si denotamos por $o_{\mathfrak{p}}$ al anillo de valoración asociado a la valoración $\nu_{\mathfrak{p}}$ vemos que $o = \cap_{\mathfrak{p}} o_{\mathfrak{p}}$.

   Si $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ son un número finito de ideales maximales distintos entonces para cada $N \geq 1$ es

   $$\mathfrak{p}_1^N + \mathfrak{p}_2^N \cdots \mathfrak{p}_s^N = o$$

   pues la suma de ideales es el máximo comun divisor de estos. Luego existe una representación $\alpha + x = 1$ con $\alpha, x \in o, \mathfrak{p}_1^N | o\alpha, \mathfrak{p}_i^N | ox$ $(i = 2, \ldots, s)$. Eligiendo N suficientemente grande tenemos

   $$\begin{cases} |x-1|_{\mathfrak{p}_1} \text{ pequeño,} \\ |x|_{\mathfrak{p}_i} \text{ pequeño para } i = 2, \ldots, s, \\ |x|_{\mathfrak{p}} \leq 1 \text{ para cualquier otro } \mathfrak{p}. \end{cases}$$

   Supongamos que tenemos $a \in k$ e ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distintos dos a dos y sean $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ ideales primos que dividen a $(oa)^{-1}$ y es $\mathfrak{q}_i \neq \mathfrak{p}_j$ para todo par de índices i, j. Si procedemos como antes pero esta vez sobre el conjunto de ideales $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$ obtenemos que existe $x \in k$ tal que

   $$\begin{cases} |x-1|_{\mathfrak{p}_1} < \varepsilon \\ |x|_{\mathfrak{p}_i} < \varepsilon \ i = 2, \ldots, r, \\ |x|_{\mathfrak{q}_j} < \varepsilon \ j = 1, \ldots, s, \\ |x|_{\mathfrak{p}} \leq 1 \text{ en cualquier otro caso.} \end{cases}$$

   Observar que la tercera propiedad es equivalente a

   $$|x|_{\mathfrak{p}} < \varepsilon \text{ para todo } \mathfrak{p} \neq \mathfrak{p}_i \text{ y tal que } |a|_{\mathfrak{p}} > 1.$$

Si consideramos el elemento $y = ax \in k$ tenemos que se verifican las siguientes desigualdades:

$$\begin{cases} |y-a|_{\mathfrak{p}_1} < \varepsilon |a|_{\mathfrak{p}_1} \\ |y|_{\mathfrak{p}_i} < \varepsilon |a|_{\mathfrak{p}_i} \ i = 2, \ldots, r, \\ |y|_{\mathfrak{p}} < \varepsilon |a|_{\mathfrak{p}} \text{ para todo } \mathfrak{p} \neq \mathfrak{p}_i \text{ y tal que } |a|_{\mathfrak{p}} > 1, \\ |y|_{\mathfrak{p}} \leq |a|_{\mathfrak{p}} \leq 1 \text{ en cualquier otro caso.} \end{cases}$$

Usando lo anterior podemos concluir que se cumple el axioma 2. Para ello, consideramos de nuevo r ideales primos distintos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, y r elementos de k $a_1, \ldots, a_r$ y un número real $\varepsilon > 0$. Podemos encontrar $y_1, \ldots, y_r \in k$ verificando las siguientes desigualdades para cada $i = 1, \ldots, r$:

$$\begin{cases} |y_i - a_i|_{\mathfrak{p}_i} < \varepsilon \\ |y_i|_{\mathfrak{p}_j} < \varepsilon \ i \neq j, j = 1, \ldots, r, \\ |y_i|_{\mathfrak{p}} \leq 1 \text{ en cualquier otro caso.} \end{cases}$$

Basta ahora considerar el elemento $y = y_1 + y_2 + \cdots + y_r \in k$ pues verifica

$$\begin{cases} |y - a_i|_{\mathfrak{p}_i} < \varepsilon \ i = 1, \ldots, r, \\ |y|_{\mathfrak{p}} \leq 1 \text{ en cualquier otro caso.} \end{cases}$$

□

2.1.4. Transición a una Extensión Finita

Proposición 2.1.7. Si los axiomas `Ax.1` y `Ax.2` se verifican en un cuerpo k, entonces también se verifican para cualquier extensión finita $L \supset k$.

Demostración. Sea o el anillo de k correspondiente a las valoraciones $\mathfrak{p} \in \Sigma$:

$$o = \cap_{\mathfrak{p}} o_{\mathfrak{p}}.$$

Sabemos que los ideales fraccionarios de o forman un grupo. El conjunto de valoraciones $\overline{\Sigma}$ de L se define como el conjunto de todas las posibles extensiones $\mathfrak{P}$ de las valoraciones $\mathfrak{p} \in \Sigma$ de k. Sabemos que entonces las valoraciones $\mathfrak{P}$ son también discretas. Recordar que para indicar que una valoración $\mathfrak{P}$ extiende una valoración $\mathfrak{p}$ escribíamos $\mathfrak{P}|\mathfrak{p}$. Veamos que se verifican los axiomas:

`Ax.1` Sabemos que dada una valoración $\mathfrak{p} \in \Sigma$ sólo hay un número finito de extensiones $\mathfrak{P} \in \overline{\Sigma}$. Entonces, dado $\alpha \in L$ sabemos que verifica una ecuación de la forma

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0, \ a_i \in k.$$

Se verifican los axiomas para k y por ello para todo i es $|a_i|_{\mathfrak{p}} \leq 1$ para casi todo $\mathfrak{p}$. Y usando que hay un número finito de extensiones $\mathfrak{P}|\mathfrak{p}$ concluimos que $\max_{i=1,\dots,n} |a_i|_{\mathfrak{P}} \leq 1$ para casi todo $\mathfrak{P} \in \overline{\Sigma}$. Entonces

$$|\alpha|_{\mathfrak{P}}^n \leq \max(|a_1|_{\mathfrak{P}}|\alpha|_{\mathfrak{P}}^{n-1}, \dots, |a_{n-1}|_{\mathfrak{P}}|\alpha|_{\mathfrak{P}}, |a_0|_{\mathfrak{P}}) \leq (\max_i |a_i|_{\mathfrak{P}})(\max_{j=0,\dots,n-1}(|\alpha|_{\mathfrak{P}}^j).$$

Por tanto, para casi todo $\mathfrak{P}$ es $|\alpha|_{\mathfrak{P}}^n \leq \max_{j=0,\dots,n-1}(|\alpha|_{\mathfrak{P}}^j) = \max(|\alpha|_{\mathfrak{P}}^{n-1}, 1)$. Si es $|\alpha|_{\mathfrak{P}}^n \leq 1$ hemos acabado. En el otro caso, si $|\alpha|_{\mathfrak{P}}^n \leq |\alpha|_{\mathfrak{P}}^{n-1}$ entonces $|\alpha|_{\mathfrak{P}} \leq 1$. Concluimos que para casi todo $\mathfrak{P} \in \overline{\Sigma}$ es $|\alpha|_{\mathfrak{P}} \leq 1$.

`Ax.2` Sean $\mathfrak{P}_1, \dots, \mathfrak{P}_r \in \overline{\Sigma}$ valoraciones distintas, $\alpha_1, \dots, \alpha_r \in L$ y $\varepsilon > 0$. Supongamos que $b_1, \dots, b_n \in L$ es una k-base de la extensión $L \supset k$. Sean $\mathfrak{P}_{r+1}, \dots, \mathfrak{P}_s \in \overline{\Sigma}$ valoraciones tales que se verifica lo siguiente:

> Si para algún índice i es $|b_i|_{\mathfrak{P}} > 1$ entonces existe $j \in \{1, \dots, r, r+1, \dots, s\}$ con $\mathfrak{p} = \mathfrak{p}_j$.

Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_t \in \Sigma$ las valoraciones de k obtenidas a partir de las $\mathfrak{P}_j$ por restricción a k. Consideremos el conjunto de todas las valoraciones de $\overline{\Sigma}$ que extienden a las valoraciones $\mathfrak{p}_i$. Dicho conjunto contiene a las valoraciones $\mathfrak{P}_j$ y tras reordenación podemos suponer que son $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ el conjunto de todas las valoraciones que son extensión de alguna $\mathfrak{p}_i$. Definimos los números $\alpha_{r+1} = \cdots = \alpha_t = 0$ y asumiremos que $\varepsilon < 1$. Por 1.1.4 sabemos que existe $\beta \in L$ tal que

$$|\beta - \alpha_i|_{\mathfrak{P}_i} < \varepsilon \ i = 1, \dots, t.$$

Supongamos que es $\beta = x_1 b_1 + \cdots + x_n b_n$, con $x_i \in k$. Aplicando `Ax.2` a los x_j en k tenemos que para cada $j \in \{1, \dots, n\}$ existe y_j verificando

$$|y_j - x_j|_{\mathfrak{p}_i} < \varepsilon, \ i = 1, \dots, q,$$
$$|y_j|_{\mathfrak{p}} \leq 1 \text{ en cualquier otro caso.}$$

con $\varepsilon' > 0$ número real (más adelante quedará claro como hay que elegir ε'.) Consideramos el elemento

$$\gamma = y_1 b_1 + \cdots + y_n b_n \in L.$$

Tomando ε' lo suficientemente pequeño podemos conseguir que se verifiquen las desigualdades

$$|\gamma - \beta|_{\mathfrak{P}_i} \leq \varepsilon' \cdot \max_j |b_j|_{\mathfrak{P}_i} < \varepsilon, \ i = 1, \dots, t.$$

Obtenemos entonces las siguientes desigualdades:

$$|\gamma - \alpha_i|_{\mathfrak{P}_i} = |\gamma - \beta + \beta - \alpha_i|_{\mathfrak{P}_i} < \varepsilon, \ i = 1, \dots, t,$$
$$|\gamma|_{\mathfrak{P}} \leq 1 \text{ en cualquier otro caso.}$$

Usando que $\alpha_i = 0$ para $i \geq r+1$ y $\varepsilon < 1$ concluimos que se verifica `Ax.2` para L pues se tienen las desigualdades

$$|\gamma - \alpha_i|_{\mathfrak{P}_i} < \varepsilon,\ i = 1, \ldots, r,$$
$$|\gamma|_{\mathfrak{P}} \leq 1 \text{ en cualquier otro caso.}$$

□

Es importante observar que el anillo $\mathcal{O} = \cap_{\mathfrak{P}} \mathcal{O}_{\mathfrak{P}}$ es la clausura integral de o en L. En efecto, como $\mathcal{O}$ es íntegralmente cerrado en L y $o \subset \mathcal{O}$ concluimos que la clausura integral de o está contenida en $\mathcal{O}$. Para el recíproco: sea $\alpha \in \mathcal{O} = \cap_{\mathfrak{P}} \mathcal{O}_{\mathfrak{P}}$, entonces para todo $\mathfrak{p} \in \Sigma$ tenemos que $\alpha \in \cap_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}$, es decir, α es entero sobre $o_{\mathfrak{p}}$. Esto implica que para cada $\mathfrak{p} \in \Sigma$ existe $f_{\mathfrak{p}} \in o_{\mathfrak{p}}[x]$ polinomio mónico tal que $f_{\mathfrak{p}}(\alpha) = 0$. Si denotamos por $|f_{\mathfrak{p}}|_{\mathfrak{p}}$ al máximo valor que toma $|\cdot|_{\mathfrak{p}}$ en los coeficientes de $f_{\mathfrak{p}}$ tenemos que $|f_{\mathfrak{p}}| = 1$ pues $f_{\mathfrak{p}} \in o_{\mathfrak{p}}[x]$ y es mónico. Consideremos ahora el polinomio mínimo $f \in k[x]$ de α sobre k. Veamos que $f \in o[x]$, es decir, $|f|_{\mathfrak{p}} \leq 1$ para todo $\mathfrak{p} \in \Sigma$. Por reducción al absurdo, supongamos que existe $\mathfrak{p}$ tal que $|f|_{\mathfrak{p}} > 1$. Como f es el polinomio mínimo de α sabemos que $f | f_{\mathfrak{p}}$ y por ello existe $g \in k[x]$ tal que $f_p = g \cdot f$. Tenemos entonces que $1 = |f_{\mathfrak{p}}|_{\mathfrak{p}} = |g|_{\mathfrak{p}} |f|_{\mathfrak{p}} > |g|_{\mathfrak{p}}$, es decir, $1 > |g|_{\mathfrak{p}}$. Como f y $f_{\mathfrak{p}}$ son mónicos y es $f_{\mathfrak{p}} = g \cdot f$, debe ser g mónico, por ejemplo, $g = x^m + b_1 x^{m-1} + \cdots + b_m$. Entonces $1 > |g|_{\mathfrak{p}} = \text{máx}(1, |b_1|_{\mathfrak{p}}, \ldots, |b_m|_{\mathfrak{p}})$ es absurdo pues obtenemos $1 > 1$. Concluimos que $|f|_{\mathfrak{p}} \leq 1$ para todo $\mathfrak{p}$, es decir, α es entero sobre o.

2.2. Dominios de Dedekind

Un dominio de integridad o es un **dominio de Dedekind** si el conjunto de sus ideales fraccionarios forman un grupo, es decir, su cuerpo de fracciones k verifica los axiomas `Ax.1` y `Ax.2`. Gracias a los resultados probados en la sección anterior sabemos que un dominio de Dedekind o es un anillo noetheriano, integralmente cerrado, todo ideal primo no nulo de o es maximal y la localización de o en uno de dichos ideales primos es un anillo de valoración discreta. A menudo, sólo un subconjunto de estas propiedades son suficientes para concluir que un anillo es un dominio de Dedekind. En este sentido tenemos la proposición se siguiente:

Proposición 2.2.1. Sea A un dominio. Son equivalentes:

1. A es un dominio de Dedekind.
2. A es noetheriano, integralmente cerrado y todo ideal primo no nulo es maximal.
3. Para todo ideal primo $\mathfrak{p}$ no nulo de A la localización $A_{\mathfrak{p}}$ es un anillo de valoración discreta.

Demostración. Ver [Ser62] *Capítulo 1, Proposición 4.*

□

Durante nuestro estudio de los axiomas y sus implicaciones vimos que los ideales de un dominio de Dedekind son finitamente generados y de hecho podemos generarlos por dos elementos, uno de ellos se puede tomar arbitrariamente en el ideal dado. Así mismo, nuestro teorema de transición a extensiones finitas lo podemos interpretar como sigue:

> Sea o un dominio de Dedekind con cuerpo de fracciones k y $L \supset k$ una extensión finita. Entonces la clausura integral de o en L también es un dominio de Dedekind.

Este resultado se conoce por el nombre de **Teorema de Krull-Akizuki.** Observar que la teoría, tal y como la hemos presentado, es muy versátil pues si restringimos el conjunto de valoraciones Σ podemos deducir resultados más fuertes. Un ejemplo de esto es el siguiente lema:

Lema 2.2.2. Sea k un cuerpo y Σ un conjunto *finito* de valoraciones discretas normalizadas de k de modo que se cumplen `Ax.1` y `Ax.2`. Entonces el anillo $o = \cap_{\mathfrak{p}\in\Sigma} o_p$ asociado a esta teoría es un dominio de ideales principales.

Demostración. Teniendo en cuenta que los ideales de o se expresan como producto de ideales primos es suficiente demostrar que todo ideal primo es principal. Para ello, si es $\Sigma = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ aplicamos 2.1.5 usando todos los ideales y tomando $v_{\mathfrak{p}_1} = 1$ y $v_{\mathfrak{p}_i} = 0$ para todo $i \neq 1$. Concluimos que existe $a \in k$ tal que $\nu_{\mathfrak{p}_1}(a) = 1$ y $\nu_{\mathfrak{p}_i}(a) = 0$ para todo $i \neq 1$, es decir, $a \in o$ y $oa = \mathfrak{p}_1$.

□

Un dominio de ideales principales es un dominio de Dedekind pues la ley de factorización única de elementos del cuerpo de fracciones se extiende a los ideales fraccionarios. En particular, $\mathbb{Z}$ es un dominio de Dedekind y por ello la clausura íntegra de $\mathbb{Z}$ en cualquier extensión finita de $\mathbb{Q}$ también es un dominio de Dedekind, o equivalentemente, en todos los cuerpos de números se verifican los axiomas. Aunque nosotros no vamos a estudiar el caso de los cuerpos de funciones merece la pena comentar que nuestra teoría podemos aplicarla al cuerpo $k(t)$ de funciones racionales con coeficientes en k. Algo interesante que podemos ver a partir de este otro ámbito es la sensibilidad de la teoría a la elección del conjunto de valoraciones pues si Σ es el conjunto de todas las valoraciones no arquimedianas normalizadas de $k(t)$ tales que su restricción a k es la valoración trivial tenemos que no se verificaría `Ax.2`, pues el anillo o coincidiría con k que es demasiado "pequeño". Sin embargo, si omitimos una de ellas obtendremos que o es isomorfo al anillo de polinomios $k[t]$.

2.2.1. Valores Absolutos Normalizados. Fórmula del Producto

Observar que dada una extensión finita $L \supset \mathbb{Q}$ tenemos que el cuerpo residual de L en un primo $\mathfrak{P}$ es finito pues el anillo de enteros de L es una extensión integral de $\mathbb{Z}$ y esta propiedad se preserva tras tomar cocientes. A partir de ahora denotaremos por $\mathtt{N}(\mathfrak{P})$ al número de elementos del cuerpo residual de L en $\mathfrak{P}$. Diremos que el **valor absoluto normalizado** de L asociado a $\mathfrak{P}$ es el que viene dado por $|\cdot|_{\mathfrak{P}} = \mathtt{N}(\mathfrak{P})^{-\nu_{\mathfrak{P}}(\cdot)}$ siendo $\nu_{\mathfrak{P}}$ la valoración discreta normalizada asociada a $\mathfrak{P}$. Notar que si $\mathfrak{p}$ es un ideal primo de k y $\mathfrak{P}|\mathfrak{p}$ entonces $\mathtt{N}(\mathfrak{P}) = \mathtt{N}(\mathfrak{p})^{f(\mathfrak{P}|\mathfrak{p})}$.

En general, dado un cuerpo de números algebraicos k o un cuerpo local en cada clase de equivalencia de valores absolutos $|\cdot|$ seleccionamos un valor absoluto normalizado $\|\cdot\|$ como sigue:

- Para cada inmersión $\sigma : k \to \mathbb{R}$ definimos $\|\cdot\| = |\sigma(\cdot)|$.
- Para cada par de inmersiones conjugadas $\sigma : k \to \mathbb{C}$ definimos $\|\cdot\| = |\sigma(\cdot)|^2$. En este caso $\|\cdot\|$ no define un valor absoluto pues no cumple la propiedad triangular pero salvo equivalencia lo hace. La aparición del cuadrado es que las inmersiones complejas van por pares (conjugadas) y por ello deben ser contadas con multiplicidad.
- Para cada ideal primo p de k $\|\cdot\|_{\mathfrak{p}} = \mathtt{N}(\mathfrak{p})^{-\nu_{\mathfrak{p}}(\cdot)}$ con $\nu_{\mathfrak{p}}$ la valoración discreta normalizada asociada a $\mathfrak{p}$.

En realidad estos valores absolutos se pueden definir de manera natural (sin distinguir entre arquimedianos y no arquimedianos) considerando cierta acción natural del grupo de Galois de la clausura normal de L sobre k.

Si $L \supset k$ es una extensión finita y k es un cuerpo local respecto $|\cdot|$ y consideramos la extensión única de $|\cdot|$ a L queremos saber cuál es la relación entre el único valor absoluto extendido y el valor absoluto normalizado. Tenemos el siguiente resultado:

Lema 2.2.3. Sea k un cuerpo local con valor absoluto $|\cdot|_k$ de modo que se puede hablar del valor absoluto normalizado. Sea $L \supset k$ una extensión finita y sea

$$|\cdot|_L = |\mathtt{N}_{L|k}(\cdot)|_k^{\frac{1}{[L:k]}}$$

la única extensión de $|\cdot|_k$ a L. Denotemos por $\|\cdot\|_L$ al valor absoluto normalizado correspondiente a $|\cdot|_L$. Se tiene la igualdad

$$\|\cdot\|_L = |\cdot|_L^{[L:k]}.$$

Demostración. Si $|\cdot|_k$ es arquimediano no hay nada que probar. Supongamos que $|\cdot|_k$ es no arquimediano. Por hipótesis $\|\cdot\|_L = |\cdot|_L^c$ para algún c. Tenemos que verificar que la fórmula se cumple para

un parámetro de uniformización $\pi \in k$. Sea Π un parámetro de uniformización de L y consideremos los ideales primos $\mathfrak{P} = (\Pi), \mathfrak{p} = (\pi)$ de modo que $\mathfrak{p} = \mathfrak{P}^e$. Entonces

$$\|\pi\|_L = \|\Pi^e\|_L = \mathtt{N}(\mathfrak{P})^{-e(\mathfrak{P}|\mathfrak{p})} = \mathtt{N}(\mathfrak{p})^{-e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})} = |\pi|_L^{[L:k]}.$$

□

La importancia de los valores absolutos normalizados la encontramos en la siguiente proposición:

Proposición 2.2.4. Sea $L \supset k$ una extensión finita de cuerpos de números algebraicos. Para cada primo $\mathfrak{p}$ de k y $\alpha \in L$ se cumple la igualdad:

$$\prod_{\mathfrak{P}|\mathfrak{p}} \|\alpha\|_{\mathfrak{P}} = \left\|\mathtt{N}_{L|k}(\alpha)\right\|_{\mathfrak{p}}.$$

En particular, la fórmula del producto se verifica para todo cuerpo de números algebraicos k, es decir, para todo $a \in k$ es

$$\prod_{\mathfrak{p}} \|a\|_{\mathfrak{p}} = 1$$

donde $\mathfrak{p}$ recorre todos los primos de k, arquimedianos y no arquimedianos.

Demostración. Para la primera afirmación basta tener en cuenta las siguientes igualdades:

$$\left\|\mathtt{N}_{L|k}(\alpha)\right\|_{\mathfrak{p}} = \left\|\prod_{\mathfrak{P}|\mathfrak{p}} \mathtt{N}_{\hat{L}_{\mathfrak{P}}|\hat{k}_{\mathfrak{p}}}(\alpha)\right\|_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \left\|\mathtt{N}_{\hat{L}_{\mathfrak{P}}|\hat{k}_{\mathfrak{p}}}(\alpha)\right\|_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} |\alpha|_{\mathfrak{P}}^{[\hat{L}_{\mathfrak{P}}:\hat{k}_{\mathfrak{p}}]} = \prod_{\mathfrak{P}|\mathfrak{p}} \|\alpha\|_{\mathfrak{P}}.$$

La segunda afirmación es inmediata usando lo anterior y teniendo en cuenta que la fórmula del producto es cierta sobre $\mathbb{Q}$.

□

2.2.2. Factorización de Ideales

Conocido que dado un dominio de Dedekind o su clausura integral en cualquier extensión finita L de su cuerpo de fracciones k da lugar a un dominio de Dedekind $\mathcal{O}$ es natural preguntarse por la factorización de un ideal primo $\mathfrak{p}$ de o en $\mathcal{O}$. Este problema ya lo hemos resuelto usando el lenguaje de las valoraciones, es suficiente probar el siguiente resultado:

Proposición 2.2.5. Sea o un dominio de Dedekind con cuerpo de fracciones k, L una extensión finita de k y $\mathcal{O}$ la clausura integral de o en L, que es un dominio de Dedekind. Dado un ideal primo $\mathfrak{p}$ de o tenemos que el conjunto de los ideales primos $\mathfrak{P}$ de $\mathcal{O}$ diviendo a $\mathfrak{p}$ está en biyección con el conjunto de las valoraciones discretas de L que extienden a la valoración $\nu_{\mathfrak{p}}$ de k. De hecho, si $\omega_{\mathfrak{P}}$ es una valoración de L extendiendo a $\nu_{\mathfrak{p}}$ tenemos que el índice de ramificación $e(\omega_{\mathfrak{P}}|\nu_{\mathfrak{p}})$ coincide con el exponente de $\mathfrak{P}$ en la factorización de $\mathfrak{p}$.

Demostración. Sea $\mathfrak{P}|\mathfrak{p}$ y supongamos que $\mathcal{O}\mathfrak{p} = \prod_{\mathfrak{Q}|\mathfrak{p}} \mathfrak{Q}^{e_\mathfrak{Q}}$ es la factorización en factores primos de $\mathcal{O}\mathfrak{p}$. Localizando obtenemos que

$$(\mathcal{O}\mathfrak{p})_\mathfrak{P} = \left(\prod_{\mathfrak{Q}|\mathfrak{p}} \mathfrak{Q}^{e_\mathfrak{Q}}\right)_\mathfrak{P} = \prod_{\mathfrak{Q}|\mathfrak{p}} \mathfrak{Q}_\mathfrak{P}^{e_\mathfrak{Q}} = \prod_{\mathfrak{Q}|\mathfrak{p}} (\mathcal{O}_\mathfrak{P}\mathfrak{Q})^{e_\mathfrak{Q}} = (\mathcal{O}_\mathfrak{P}\mathfrak{P})^{e_\mathfrak{P}}.$$

Deducimos que para todo $m \in \mathbb{Z}$ es $\mathcal{O}_\mathfrak{P}\mathfrak{p}^m = (\mathcal{O}_\mathfrak{P}\mathfrak{P})^{e_\mathfrak{P} m}$. Entonces $\omega_\mathfrak{P}(\mathcal{O}_\mathfrak{P}\mathfrak{p}^m) = e_\mathfrak{P} m = e_\mathfrak{P}\nu_\mathfrak{p}(o_\mathfrak{p}\mathfrak{p}^m)$ y por ello para todo ideal fraccionario de o concluimos que es $\omega_\mathfrak{P}(\mathcal{O}_\mathfrak{P} I) = e_\mathfrak{P}\nu_\mathfrak{p}(o_\mathfrak{p} I)$. En particular, para todo $x \in k^\times$ tenemos que $\omega_\mathfrak{P}(x) = \omega_\mathfrak{P}(\mathcal{O}_\mathfrak{P} x) = e_\mathfrak{P}\nu_\mathfrak{p}(o_\mathfrak{p} x) = e_\mathfrak{P}\nu_\mathfrak{p}(x)$, lo que demuestra que $\omega_\mathfrak{P}$ extiende a $\nu_\mathfrak{p}$ y el índice de ramificación es $e_\mathfrak{P}$.

Esto demuestra que podemos asignar a cada ideal primo $\mathfrak{P}|\mathfrak{p}$ la valoración $\omega_\mathfrak{P}$. Veamos que esta aplicación es biyectiva:

a. Para la inyectividad, si $\mathfrak{P}, \mathfrak{P}'$ son ideal primos distintos de $\mathcal{O}$ dividiendo $\mathfrak{p}$ entonces las valoraciones asociadas $\omega_\mathfrak{P}, \omega_{\mathfrak{P}'}$ son distinas.

b. Sea ω una valoración (discreta) normalizada de L extendiendo a $\nu_\mathfrak{p}$. Consideremos su anillo de valoración discreta R y su ideal maximal $\mathfrak{m}$. Como $\omega_{|k} = e\nu_\mathfrak{p}$, tenemos que $o \subset R$. Por definición de $\mathcal{O}$ sabemos además que $\mathcal{O} \subset R$. El ideal primo $\mathfrak{P} = R \cap \mathfrak{m}$ está sobre $\mathfrak{p}$ pues $\mathfrak{p} = \mathfrak{m} \cap o = \mathfrak{P} \cap o$, ya que $\mathfrak{p} = o_\mathfrak{p}\mathfrak{p} \cap o = (\mathfrak{m} \cap o_\mathfrak{p}) \cap o$. Deducimos que $\mathcal{O}_\mathfrak{P} \subset R$ pues $\mathcal{O} \setminus \mathfrak{P} \subset R \setminus \mathfrak{m} = R^\times$. Entonces obtenemos que R es un anillo de valoración discreta (necesariamente distinto de su cuerpo de fracciones L) que contiene a otro anillo de valoración discreta $\mathcal{O}_\mathfrak{P}$ de L, es necesario que ambos coincidan y $\omega_\mathfrak{P} = \omega$ (ambas son normalizadas).

□

Además, es bien conocido que $o_\mathfrak{p}/o_\mathfrak{p}\mathfrak{p} \simeq o/\mathfrak{p}$ pues $\mathfrak{p}$ es un ideal maximal y por ello concluimos que $f(\mathfrak{P}|\mathfrak{p}) = [\mathcal{O}_\mathfrak{P}/\mathcal{O}_\mathfrak{P}\mathfrak{P} : o_\mathfrak{p}/o_\mathfrak{p}\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : o/\mathfrak{p}]$. Esta última igualdad junto con 1.3.8 nos dice que si obtenemos una factorización de la forma $\mathcal{O}\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$ entonces

$$[L : k] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p}).$$

Capítulo 3

Ramificación

En este capítulo vamos a estudiar el fenómeno de ramificación en extensiones finitas. Comenzaremos con un estudio general y posteriormente comprenderemos la ramificación bajo la hipótesis de que las extensiones en cuestión son de Galois.

Nota: **Reducción a Cuerpos Completos**

Como vimos antes, dado un dominio de Dedekind o con cuerpo de fracciones k y una extensión $L \supset k$ finita tenemos que la clausura integral de o en L es un dominio de Dedekind $\mathcal{O}$ de modo que tiene sentido plantearse el problema de la factorización de los primos $\mathfrak{p}$ de o en $\mathcal{O}$. Además, sabemos que la factorización de $\mathcal{O}\mathfrak{p}$ en $\mathcal{O}$ es equivalente a hallar todas las posibles extensiones de la valoración discreta $\nu_{\mathfrak{p}}$ de k a L con sus índices de ramificación. Como venimos haciendo, nosotros usaremos ambas nociones indistintamente. De este modo, si tenemos una valoración discreta ν de k con extensiones ω a L, diremos que ν **ramifica** en L si para alguna extesión ω $e(\omega|\nu) > 1$. Si para toda extensión ω de ν a L es $e(\omega|\nu) = 1$ decimos que ν no ramifica en L.

Para ver que el estudio de la ramificación se puede reducir al estudio local necesitamos demostrar que los índices de ramificación y el grado de inercia se preservan al pasar a la localización y esto es precisamente lo que se demostró en 2.2.5.

Usando esto, si tenemos una valoración discreta ν de k con extensión ω a L, denotando por $(\hat{k}, \hat{\nu}), (\hat{L}, \hat{\omega})$ las compleciones y extensiones respectivas, sabemos que $\hat{\nu}(\hat{k}^{\times}) = \nu(k^{\times})$ luego $e(\hat{\nu}|\nu) = 1$. Así mismo, si es o_ν el anillo de valoración discreta asociada a ν con ideal maximal $\mathfrak{p}_\nu$ y análogamente $\hat{o}_\nu, \hat{\mathfrak{p}}_\nu$ sabemos que $\hat{o}_\nu/\hat{\mathfrak{p}}_\nu \simeq o_\nu/\mathfrak{p}_\nu$ luego $f(\hat{\nu}|\nu) = 1$. Lo mismo se obtiene para $\omega, \hat{\omega}$ y esto demuestra que además de poder reducir nuestro análisis a anillos de valoración discreta podemos reducirnos a anillos de valoración discreta cuyo cuerpo de fracciones es completo.

3.1. Extensiones No Ramificadas

Sea k un cuerpo con valoración (no arquimediana) ν respecto a la cual es completo y $L \supset k$ una extensión *finita*, siendo ω la única extensión de ν a L. Vamos a denotar por $\mathcal{O}_k$ al anillo de valoración de ν, por $\mathfrak{p}_k$ su ideal maximal y por $\overline{k}$ al cuerpo residual $\mathcal{O}_k/\mathfrak{p}_k$. Análogamente, para ω

denotaremos los correspondientes objetos por $\mathcal{O}_L, \mathfrak{p}_L, \overline{L}$. La imagen de $x \in \mathcal{O}_k$ en $\overline{k}$ la denotaremos por $\overline{x}$. Tenemos la siguiente definición:

Definición 3.1.1. La extensión finita $L \supset k$ se dice **no ramificada** si la extensión $\overline{L} \supset \overline{k}$ es separable y $[L : k] = [\overline{L} : \overline{k}] = f(\omega|\nu)$.

Gracias a 1.3.3 sabemos que la definición anterior implica que $e(\omega|\nu) = 1$. Observar que en general la condición $e(\omega|\nu) = 1$ no es equivalente a $f(\omega|\nu) = [L : k]$ y sólo tenemos la equivalencia cuando la igualdad $[L : k] = e(\omega|\nu)f(\omega|\nu)$ se cumple, por ejemplo, cuando la valoración de k es discreta.

El siguiente resultado resuelve completamente el estudio de las extensiones finitas no ramificadas:

Proposición 3.1.2. Siguiendo con la notación anterior:

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 $\overline{L} = \overline{k}(\overline{\alpha})$.

Demostración. 1. Como $\mathcal{O}_L$ es la clausura integral de $\mathcal{O}_k$ en L sabemos que el polinomio mínimo de $\alpha \in \mathcal{O}_L$ tiene coeficientes en $\mathcal{O}_k$. Tenemos que $f(\alpha) = 0$ luego $\overline{f}(\overline{\alpha}) = 0$, con $\mathtt{deg}(f) = \mathtt{deg}(\overline{f})$ pues f es mónico. Además,

$$[L : k] \geq [k(\alpha) : k] = \mathtt{deg}(f) = \mathtt{deg}(\overline{f}) \geq [\overline{k}(\overline{\alpha}) : \overline{k}] = [L : k].$$

Concluimos que $L = k(\alpha)$ y $\overline{\alpha}$ es una raíz simple del polinomio irreducible $\overline{f}$, es decir, $\overline{f}$ es el polinómio mínimo de $\overline{\alpha}$ sobre $\overline{k}$. Como la extensión $\overline{L} \supset \overline{k}$ es separable sabemos que $\overline{f}'(\overline{\alpha}) = \overline{f'(\alpha)} \neq 0$ y por ello $f'(\alpha) \neq 0$ pues $0 \in \mathfrak{P}$, es decir, α es separable sobre k. Para la igualdad $\mathcal{O}_L = \mathcal{O}_k[\alpha]$ basta aplicar las conclusiones obtenidas en la demostración de 1.3.3 en el caso en que $e = 1$.

2. Sea $f = \prod_{i=1}^{n} f_i$ la descomposición de f como producto de polinómios mónicos irreducibles en $k[x]$. Sabemos que los factores f_i pertenecen a $\in \mathcal{O}_k[x]$ (para probarlo usar el "valor absoluto" en polinomios para deducir el lema de Gauss para cuerpos no arquimedianos). Supongamos, sin pérdida de generalidad, que α es una raíz de f_1, en particular $\alpha \in \mathcal{O}_L$. Como $\overline{f}$ es mónico separable sobre $\overline{k}$ sabemos que también lo es $\overline{f}_1$ sobre $\overline{k}$. Por el lema de Hensel 1.2.9 sabemos

que además $\overline{f}_1$ es irreducible sobre $\overline{k}$. Obtenemos entonces que $\overline{L} \supset \overline{k}(\overline{\alpha})$. Para concluir la igualdad basta tener en cuenta lo siguiente:

$$\mathtt{deg}(f_1) = [L : k] \geq [\overline{L} : \overline{k}] \geq [\overline{k}(\overline{\alpha}) : \overline{k}] = \mathtt{deg}(\overline{f}_1) = \mathtt{deg}(f_1).$$

□

Gracias a este resultado podemos demostrar las siguientes propiedades de las extensiones finitas no ramificadas:

Corolario 3.1.3. 1. Si $L \supset k, M \supset L$ son extensiones finitas no ramificadas entonces $M \supset k$ es finita no ramificada.

2. Sea $L \supset k$ es una extensión finita no ramificada y $M \supset k$ otra extensión algebraica (ambas en una misma clausura algebraica de k) tal que M es completo respecto a la valoración extendida. Entonces la extensión $LM \supset M$ es finita no ramificada.

3. Toda subextensión de una extensión finita no ramificada es no ramificada.

4. Si $L_1 \supset k, L_2 \supset k$ son extensiones finitas no ramificadas entonces $L_1L_2 \supset k$ es finita no ramificada.

Demostración. 1. Tenemos que $\overline{L} \supset \overline{k}$ y $\overline{M} \supset \overline{L}$ son extensiones separables de grados $[L : k]$ y $[M : L]$ respectivamente. Concluimos que la extensión $\overline{M} \supset \overline{k}$ es separable de grado $[M : k]$.

2. Usando 3.1.2(1) podemos suponer que es $L = k(\alpha)$ con $\alpha \in \mathcal{O}_L$ y $f \in \mathcal{O}_k[x]$ como en el enunciado (1) de la proposición. Entonces $\overline{L} = \overline{k}(\overline{\alpha})$ y por ello $\alpha \notin \mathfrak{P}$. Como $ML = M(\alpha)$ podemos considerar el polinomio mínimo de α sobre M que denotaremos por f_1. Además sabemos que $f_1 \in \mathcal{O}_M[x]$. Gracias al lema de Hensel 1.2.9 sabemos que $\overline{f}_1$ es una potencia de un polinomio irreducible de $\overline{M}[x]$. Por último, como $\overline{f}_1$ divide a $\overline{f}$ concluimos que $\overline{f}_1$ es un polinomio irreducible separable. Ahora basta aplicar 3.1.2(2) para concluir que la extensión $LM \supset M$ es no ramificada finita.

3. Usando el apartado 2 de este mismo enunciado, si tenemos una extensión finita no ramificada $L \supset k$ y consideramos una subextensión $L \supset M \supset k$, entonces la extensión $L \supset M$ es no ramificada. Por la fórmula del producto:

$$[\overline{M} : \overline{k}] = \frac{[\overline{L} : \overline{k}]}{[\overline{L} : \overline{M}]} = \frac{[L : k]}{[L : M]} = [M : k].$$

4. De nuevo, gracias al apartado 2 de este mismo enunciado, la extensión $L_1L_2 \supset L_2$ es finita no ramificada. Usando el razonamiento del apartado 3 (i.e. la separabilidad es una propiedad transitiva y el grado es multiplicativo) concluimos que $L_1L_2 \supset k$ es finita no ramificada.

□

Este último corolorario nos lleva a considerar de manera natural la composición de todas las extensiones finitas no ramificadas del cuerpo k. Esta extensión no es finita en general y sin embargo parece que es no ramificada en algún sentido. Por ello introducimos la siguiente definición:

Definición 3.1.4. Sea k un cuerpo con valoración ν respecto a la cual es completo. Una extensión algebraica $L \supset k$ se dice **no ramificada** si L es una unión de extensiones finitas no ramificadas. Equivalentemente, toda subextensión finita de $L \supset k$ es no ramificada.

Usando 3.1.3(4), sabemos que la composición de dos extensiones finitas no ramificadas es no ramificada. Sea k^{ur} la composición de todas las extensiones finitas no ramificadas de k, que llamaremos la **extensión maximal no ramificada de** k. Es inmediato comprobar que k^{ur} es la unión de todas las extensiones finitas no ramificadas de k y por ello $k^{ur} \supset k$ es una extensión no ramificada. En general k^{ur} no es completo respecto a la única extensión de ν. Una propiedad que será esencial para nosotros es que $k^{ur} \supset k$ es una extensión de Galois, que se comprueba inmediatamente usando cualquier automorfismo $\sigma \in \mathtt{Gal}(k^{sep}|k)$ y considerando la caracterización 3.1.2. Otra propiedad importante de la extensión $k^{ur} \supset k$ es que el índice de ramificación es igual a 1. En efecto, si es ν^{ur} la única extensión de ν a k^{ur}, por definición es $e(\nu^{ur}|\nu) = (\nu^{ur}((k^{ur})^\times) : \nu(k^\times))$ y si consideramos $r = \nu^{ur}(\alpha)$ con $\alpha \in k^{ur}$ tenemos que $\nu^{ur}(\alpha)$ coincide con el valor que toma la extensión de la valoración ν a la extensión finita no ramificada $k(\alpha) \supset k$ y este valor pertenece a $\nu(k^\times)$ debido a la ausencia de ramificación. En definitiva, $\nu^{ur}((k^{ur})^\times) = \nu(k^\times)$.

El siguiente resultado muestra la interrelación entre extensiones no ramificadas y extensiones de Galois:

Proposición 3.1.5.

1. Sea $L \supset k$ una extensión finita 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 finita 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

$$\overline{\sigma}\ \overline{\alpha} = \overline{\sigma\alpha}\ \forall \alpha \in \mathcal{O}_L.$$

Demostración. 1. Sea $L \supset k$ una extensión finita no ramificada. Supongamos que es $\overline{L} = \overline{k}(\theta)$ y sea g el polinomio mónico irreducible de θ sobre $\overline{k}$. Entonces

$$g = \prod_{i=1}^{n}(X - \theta_i)$$

con $\theta_i \in \overline{L}, \theta_1 = \theta$. Sea $f \in \mathcal{O}_k$ un polinomio mónico del mismo grado que g y tal que $\overline{f} = g$. La aplicación reiterada del lema de Hensel a f implica que la factorización de g en $\overline{L}[X]$ podemos elevarla a $\mathcal{O}_L[X]$ y obtener una expresión de la forma

$$f = \prod_{i=1}^{n}(X - \alpha_i)$$

con $\alpha_i \in \mathcal{O}_L, \overline{\alpha_i} = \theta_i$. La proposición 3.1.2 demuestra que $L = k(\alpha_1)$ y concluimos que $L \supset k$ es una extensión de Galois.

2. Comenzamos observando que $\overline{\sigma}$ está bien definido, supuesto demostrado que $\overline{L} \supset \overline{k}$ es una extensión de Galois. Es claro que dado $\beta \in \mathcal{O}_L$ entonces $\sigma\beta \in \mathcal{O}_L$ pues β verifica es raíz de un polinomio mónico con coeficientes en $\mathcal{O}_k \subset k$. Por otro lado, como $\sigma : \mathcal{O}_L \to \mathcal{O}_L$ es un automorfismo del anillo concluimos que lleva ideales primos no triviales en ideales primos no triviales y como en $\mathcal{O}_L$ sólo tenemos el ideal primo no nulo $\mathfrak{p}_L$ concluimos que $\sigma\mathfrak{p}_L = \mathfrak{p}_L$. Por la propiedad universal del cociente obtenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} L & \xleftrightarrow{\sigma} & L \\ \uparrow & & \uparrow \\ \mathcal{O}_L & \xleftrightarrow{\sigma_{|\mathcal{O}_L}} & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \overline{L} & \xleftrightarrow{\overline{\sigma}} & \overline{L} \end{array}$$

Aplicando lo anterior a $\sigma^{-1}, \sigma\tau$ concluimos que son $\overline{\sigma^{-1}} = \overline{\sigma}^{-1}$ y $\overline{\sigma\tau} = \overline{\sigma}\ \overline{\tau}$ probando así que $\overline{\sigma} \in \mathtt{Gal}(\overline{L}|\overline{k})$ y que la aplicación $\sigma \mapsto \overline{\sigma}$ es un homomorfismo. Queda probar que $\overline{L} \supset \overline{k}$ es una extensión de Galois y que el homomorfismo anterior es un isomorfismo. Para ello suponemos que $\overline{L} = \overline{k}(\theta), \alpha \in \mathcal{O}_L$ tal que $\overline{\alpha} = \theta$ y $f \in \mathcal{O}_k[X]$ el polinomio mínimo de α sobre k. Como todas las raíces de f están en L obtenemos que todas las raíces de $\overline{f}$ están en $\overline{L}$ y $\overline{L} \supset \overline{k}$ es una extensión de Galois pues $\overline{f}$ es el polinomio mínimo irreducible de θ sobre $\overline{k}$. Para ver que es isomorfismo es suficiente probar que la aplicación es sobreyectiva pues los grupos $\mathtt{Gal}(L|k)$ y $\mathtt{Gal}(\overline{L}|\overline{k})$ tienen el mismo orden. La sobreyectividad se sigue de la siguiente observación: La condición $\overline{\sigma}\theta = \theta_i$ implica que es $\sigma\alpha = \alpha_i$ con α_i raíz de f tal que $\overline{\alpha_i} = \theta_i$. Como todo elemento de $\mathtt{Gal}(\overline{L}|\overline{k})$ está determinado por la imagen de θ concluimos el resultado.

□

El resultado anterior se cumple en general para extensiones de Galois infinitas. Nosotros no necesitaremos esa generalidad y sólo probamos el siguiente resultado:

Proposición 3.1.6. El cuerpo residual de k^{ur} coincide con la clausura separable $\overline{k}^{sep}$ de $\overline{k}$ y $\mathtt{Gal}(k^{ur}|k) \simeq \mathtt{Gal}(\overline{k}^{sep}|\overline{k})$.

Demostración. Sea $\theta \in \overline{k}^{sep}$, g el polinomio mínimo de θ sobre $\overline{k}$ y $f \in \mathcal{O}_k[X]$ del mismo grado que g con $\overline{f} = g$. Sean $\alpha_1, \ldots, \alpha_n$ todas las raíces de f y consideremos $L = k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1) \cdot k(\alpha_2) \cdots k(\alpha_n)$. Tenemos que $L \subset k^{ur}$ por la maximalidad de k^{ur} y $\theta = \overline{\alpha_i} \in \overline{k^{ur}}$ para un índice i adecuado. Concluimos que $\overline{k^{ur}} = \overline{k}^{sep}$.

Un elemento de $\mathtt{Gal}(k^{ur}|k)$ determina para cada subextensión finita de Galois $k^{ur} \supset L \supset k$ un automorfismo $\sigma_{|L} \in \mathtt{Gal}(L|k)$ con la propiedad de que para una cadena de subextensiones $k^{ur} \supset L' \supset L \supset k$ se verifica que $(\sigma_{|L'})_{|L} = \sigma_{|L}$. Recíprocamente, toda colección de automorfismos compatibles determinan de forma única automorfismo de k^{ur}. De manera completamente análoga podemos razonar para el grupo $\mathtt{Gal}(\overline{k}^{sep}|\overline{k})$. Concluimos que para describir la imagen de un elemento $\sigma \in \mathtt{Gal}(k^{ur}|k)$ es suficiente describir la imagen de sus restricciones $\sigma_{|L} \in \mathtt{Gal}(L|k)$ para cada subextensión finita de Galois $L \supset k$ y esperar que dichas imágenes sean compatibles. Para toda extensión finita no ramificada $L \supset k$ tenemos el isomorfismo canónico $\varphi_L : \mathtt{Gal}(L|k) \to \mathtt{Gal}(\overline{L}|\overline{k})$ de la proposición 3.1.5 y es este el que usaremos para definir la imagen en las subextensiones finitas de Galois. Falta comprobar que son compatibles, es decir, para cada cadena de subextensions de Galois (respecto a k) $k^{ur} \supset L' \supset L \supset k$ el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathtt{Gal}(L'|k) & \xrightarrow{res} & \mathtt{Gal}(L|k) \\ \downarrow{\scriptstyle \varphi_{L'}} & & \downarrow{\scriptstyle \varphi_L} \\ \mathtt{Gal}(\overline{L'}|\overline{k}) & \xrightarrow{res} & \mathtt{Gal}(\overline{L}|\overline{k}). \end{array}$$

Las flechas horizontales son los homomorfismos de restricción. Efectivamente este diagrama es conmutativo por construcción de los homomorfismos φ_L.

□

Las consideraciones anteriores podemos hacerlas de forma relativa, es decir, respecto a una extensión finita $L \supset k$ prefijada. Para evitar saturar la notación asumiremos que k y L comparten una clausura algebraica, i.e. $k^{alg} = L^{alg}$.

Tenemos el siguiente resultado:

Proposición 3.1.7. Siguiendo con la configuración anterior, se cumplen las siguientes propiedades:

1. $L^{ur} = L \cdot k^{ur}$.

2. $L_0 = L \cap k^{ur}$ es la subextensión maximal no ramificada de $L \supset k$. Además, la extensión $\overline{L} \supset \overline{L_0}$ es una extensión inseparable pura.

Demostración. 1. Gracias a 3.1.3.2 tenemos que para toda extensión finita no ramificada $M \supset k$ la extensión $ML \supset L$ es finita no ramificada y en particular $ML \subset L^{ur}$. Como $k^{ur} = \bigcup M$ donde M recorre el conjunto de las extensiones finitas no ramificadas de k, concluimos que $Lk^{ur} \subset L^{ur}$. Para la otra inclusión observar que el cuerpo residual $\overline{Lk^{ur}}$ contiene los cuerpos $\overline{L}$ y $\overline{k^{ur}} = \overline{k}^{sep}$ y por definición de composición de cuerpos también contiene al cuerpo $\overline{L}\ \overline{k}^{sep}$. Veamos que, como la extensión $\overline{L} \supset \overline{k}$ es algebraica, la composición $\overline{L}\ \overline{k}^{sep}$ coincide con la clausura separable de $\overline{L}$. En efecto, si la característica de $\overline{k}$ es 0 no hay nada que probar y suponemos que la característica de $\overline{k}$ es $p > 0$. Es claro que $\overline{L}\ \overline{k}^{sep} \subset \overline{L}^{sep}$. Para la otra inclusión, sabemos que $\overline{L}^{sep} = \overline{L}\left(\overline{L}^{sep}\right)^{p^m}$ para todo $m \in \mathbb{N}$ (ver [Hun80] *Capítulo 5, Corolario 6.9*). Sea $n \in \mathbb{N}$ tal que $p^n = [\overline{L} : \overline{k}]_i$ coincide con el grado de inseparabilidad (ver [Hun80] *Capítulo 5, Corolario 6.5*). Dado $\alpha \in \overline{L}^{sep}$ sabemos que $\alpha^{[\overline{k}(\alpha):\overline{k}]_i}$ es separable sobre $\overline{k}$ (ver [Hun80] Capítulo 5, Corolario 6.14). Ahora bien, sabiendo que el grado de inseparabilidad es multiplicativo tenemos las siguientes igualdades:

$$\begin{aligned}[\overline{L}(\alpha) : \overline{k}]_i &= [\overline{L}(\alpha) : \overline{L}]_i [\overline{L} : \overline{k}]_i \\ &= [\overline{L} : \overline{k}]_i, \\ [\overline{L}(\alpha) : \overline{k}]_i &= [\overline{L}(\alpha) : \overline{k}(\alpha)]_i [\overline{k}(\alpha) : \overline{k}]_i.\end{aligned}$$

En definitiva, $[\overline{k}(\alpha) : \overline{k}]_i$ divide a $[\overline{L} : \overline{k}]_i$ para todo $\alpha \in \overline{L}^{sep}$. Podemos concluir que $\left(\overline{L}^{sep}\right)^{p^n} \subset \overline{k}^{sep}$ y deducimos que

$$\overline{L}^{sep} = \overline{L}\left(\overline{L}^{sep}\right)^{p^n} \subset \overline{L}\ \overline{k}^{sep}.$$

2. Claramente L_0 contiene toda extensión no ramificada de k contenida en L y la extensión $L_0 \supset k$ es no ramificada. Veamos que la extensión $\overline{L} \supset \overline{L_0}$ no tiene elementos separables. Sea $\theta \in \overline{L}$ separable sobre $\overline{k}$ siendo g su polinomio mínimo sobre $\overline{k}$. Sea $f \in \mathcal{O}_L[X]$ un polinomio mónico del mismo grado que g y tal que $\overline{f} = g$. Usando el lema de Hensel (para L) concluimos que existe $\alpha \in \mathcal{O}_L$ raíz de f tal que $\overline{\alpha} = \theta$. Gracias a 3.1.2 sabemos que $k(\alpha) \supset k$ es una extensión no ramificada y por ello $\theta \in \overline{L_0}$.

□

Si a lo anterior añadimos la hipótesis de que la extensión $\overline{L} \supset \overline{k}$ es separable obtenemos resultados más fuertes:

(a) Consideremos la extensión $L \supset L_0$. Sabemos que $\overline{L} \supset \overline{L_0}$ es una extensión inseparable pura pero al ser la extensión $\overline{L} \supset \overline{k}$ separable concluimos que la extensión $\overline{L} \supset \overline{L_0}$ también es separable de donde se deduce la igualdad $\overline{L} = \overline{L_0}$. Si denotamos por $f(L|L_0)$ al grado de inercia de la extensión y por $e(L|L_0)$ al índice de ramificación concluimos que $f(L|L_0) = 1$ y $e(L|L_0) = [L : L_0]$.

(b) La otra extensión que podemos estudiar es $L^{ur} \supset k^{ur}$. En este caso, sabemos que

$$\overline{L^{ur}} = \overline{L}^{sep} = \overline{L}\ \overline{k}^{sep} = \overline{k}^{sep}$$

usando para la última igualdad que la extensión $\overline{L} \supset \overline{k}$ es separable. De nuevo, concluimos que $f(L^{ur}|k^{ur}) = 1$ y $e(L^{ur}|k^{ur}) = [L^{ur} : k^{ur}]$.

(c) Se cumple además que $[L : L_0] = [L^{ur} : k^{ur}]$. Si denotamos los índices de ramificación y los grados de inercia como antes, al ser $e(k^{ur}|k) = 1$ tenemos que

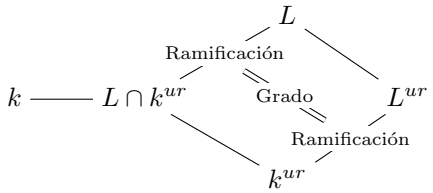
$$e(L^{ur}|k^{ur}) = e(L^{ur}|k^{ur})e(k^{ur}|k) = e(L^{ur}|k) = e(L^{ur}|L)e(L|L_0)e(L_0|k).$$

Como las extensiones $L^{ur} \supset L, L_0 \supset k$ son no ramificadas obtenemos la igualdad

$$e(L^{ur}|k^{ur}) = e(L|L_0).$$

Concluimos que $[L : L_0] = [L^{ur} : k^{ur}]$.

A modo de diagrama, podemos indicar estas propiedades como sigue:



Observar que lo que hemos conseguido con la introducción del cuerpo $L_0 = L \cap k^{ur}$ es "separar" el fenómeno de la ramificación del fenómeno de la inercia en dos pasos, en el primer paso correspondiente a $k \subset L_0$ nuestro primo $\mathfrak{p}_k$ no factoriza (tiene lugar la *inercia*) y en el segundo paso correspondiente a $L_0 \subset L$ el primo $\mathfrak{p}_k$ ramifica completamente (con completamente queremos decir que el exponente de la factorización coincide con el grado de la extensión). De hecho, vista la propiedad que comparten las extensiones $L \supset L_0$ y $L^{ur} \supset k^{ur}$ parece sensato darle nombre:

Definición 3.1.8. Sea (k, ν) un cuerpo completo respecto a la valoración discreta ν y (L, ω) una extensión finita de (k, ν). Decimos que la extensión $L \supset k$ está **totalmente ramificada** si $f(\omega|\nu) = 1$. En general, si la extensión $L \supset k$ es algebraica infinita, se dice que es totalmente ramifica si toda subextensión finita es totalmente ramificada.

Todas nuestras afirmaciones se reducen al siguiente resultado:

Corolario 3.1.9. Sea L una extensión finita de un cuerpo discreto completo k, con $\overline{L} \supset \overline{k}$ una extensión separable. Entonces L es una extensión totalmente ramificada de L_0, L^{ur} es una extensión totalmente ramificada de k^{ur}, y $[L : L_0] = [L^{ur} : k^{ur}]$.

3.1.1. Extensiones No Ramificadas de un Cuerpo Local

Antes de comenzar el estudio de las extensiones totalmente ramificadas vamos a considerar las extensiones no ramificadas de un cuerpo local y veremos que la teoría toma una forma particularmente sencilla. Fijamos el contexto: k denotará a un cuerpo local, esto es, un cuerpo completo respecto a una valoración discreta que es localmente compacto y con cuerpo residual finito. Denotamos el cardinal de $\overline{k} \sim \mathbb{F}_q$ por $q = |\overline{k}|$.

Por 3.1.2 sabemos que las extensiones finitas no ramificadas de k se corresponden con las extensiones separables finitas del cuerpo residual, que en este caso, al tratarse de un cuerpo finito, sabemos que para número natural n posee una única extensión (salvo isomorfismo) de grado n, a saber, el cuerpo finito con q^n elementos $\mathbb{F}_{q^n}$. Como es bien conocido, $\mathbb{F}_{q^n}$ se obtiene a partir de $\mathbb{F}_q$ como el conjunto de las raíces del polinomio $X^{q^n} - X$. Por el *lema de Hensel* se demuestra que la correspondiente extensión no ramificada de k coincide con el cuerpo de descomposición del polinomio $X^{q^n} - X$ sobre k. Deducimos que dado un cuerpo local no arquimediano k para cada $n \in \mathbb{N}$ existe, salvo isomorfismos, una única extensión no ramificada de grado n y que además es de Galois con grupo de Galois cíclico. Esta extensión la denotaremos usualmente por k_n.

Además, como el grupo de Galois $\mathtt{Gal}(\mathbb{F}q^n|\mathbb{F}_q)$ está generado por el automorfismo de Frobenius $x \mapsto x^q$, sabemos que el grupo de Galois $\mathtt{Gal}(k_n|k)$ está generado por el único k-automorfismo φ_n de k_n de modo que $\overline{\varphi_n} = (x \mapsto x^q)$ (3.1.5.2), es decir, $\varphi_n(x) + \mathfrak{p}_{k_n} = x^q + \mathfrak{p}_{k_n}$ para todo $x \in \mathcal{O}_{k_n}$. Este automorfismo φ_n lo llamamos **automorfismo de Frobenius de** k o simplemente **el elemento de Frobenius de** k. Obviamente, el elemento de Frobenius φ_n tiene orden n.

Observar que cada cuerpo k_n es un cuerpo local cuyo cuerpo residual tiene q^n elementos y k_n contiene a las raíces $q^n - 1$-ésimas de la unidad. Gracias a la demostración de 1.5.8 sabemos que este conjunto de raíces de la unidad, denotado

$$\mu_{q^n-1} \cup \{0\} = \{\alpha \in k_n \mid \alpha^{q^n} = \alpha\},$$

forma un sistema de representantes de $\overline{k}$ de modo que todo elemento admite una π-expansión con coeficientes estas raíces y π un parámetro de uniformización de k_n. Además, como la extensión $k_n \supset k$ es no ramificada, todo parámetro de uniformización de k también lo es de k_n y de esta forma, usando que el elemento de Frobenius φ_n es un k-automorfismo continuo, podemos conocer

explícitamente su acción sobre k_n si conocemos como actúa sobre las raíces de $X^{q^n-1}-1$ pues deja invariante a π. En este sentido, tenemos el siguiente resultado:

Lema 3.1.10. Sea k un cuerpo local no arquimediano con valoración normalizada ν_k y cuerpo residual $\overline{k}$ con q elementos. El homomorfismo de anillos $\mathcal{O}_k \to \mathcal{O}_k/\mathfrak{p}_k = \overline{k}$ induce un isomorfismo de grupos multiplicativos

$$\mu_{q-1} \to \overline{k}^{\times}.$$

En particular, μ_{q-1} es un grupo cíclico con $q-1$ elementos.

Demostración. Sabemos que $\mu_{q-1} \cup \{0\}$ es un sistema de representantes de $\mathcal{O}_k$ gracias al lema de Hensel. Como $\overline{k}$ y μ_{q-1} tienen el mismo número de elementos, es inmediato que el homomorfismo canónico de proyección es un isomorfismo de grupos multiplicativos.

□

Usando este resultado, tenemos que para todo $n \in \mathbb{N}$, el conjunto μ_{q^n-1} es isomorfo al grupo cíclico $\mathbb{F}_{q^n}^{\times}$. Además, como $\varphi_n(\alpha) + \mathfrak{p}_{k_n} = \alpha^q + \mathfrak{p}_{k_n}$ y sabemos que $\varphi_n(\mu_{q^n-1}) \subset \mu_{q^n-1}$, usando que $\mathcal{O}_{k_n} \to \overline{k_n}$ induce un isomorfismo $\mu_{q^n-1} \simeq \overline{k_n}^{\times}$, concluimos que φ_n actúa sobre las raíces de la unidad μ_{q^n-1} elevándolas a q. Esto, junto a las observaciones anteriores, nos dice que dado $\pi \in k$ parámetro de uniformización y $a \in k_n$ que se escribe de manera única como

$$a = \sum_{j=-m}^{\infty} \alpha_j \pi^j, \quad \alpha_j \in \mu_{q^n-1} \cup \{0\}, m \in \mathbb{Z}$$

entonces

$$\varphi_n(a) = \sum_{j=-m}^{\infty} \alpha_j^q \pi^j.$$

Si consideramos los elementos de Frobenius para cada n vemos que obtenemos una sucesión de automorfismos compatibles entre sí de modo que podemos definir un automorfismo φ_k en la unión $\cup_{n\geq 1} k_n$. Esta unión coincide con $k^{\mathtt{ur}}$ pues antes hemos visto que para cada entero n existe una única extensión de grado n salvo isomorfismo. Este k-automorfismo φ_k de $k^{\mathtt{ur}}$ coincide sobre $\overline{k}^{\mathtt{sep}} = \overline{k^{\mathtt{ur}}}$ con el $\mathbb{F}_q$-automorfismo de $\mathbb{F}_q^{\mathtt{sep}} = \overline{k^{\mathtt{ur}}}$ que consiste en hacer la potencia q-ésima. Sabemos que dicho $\mathbb{F}_q$-automorfismo es el generador topológico (ver Capítulo 4) del grupo de Galois, es decir $\mathtt{Gal}(\mathbb{F}_q^{\mathtt{sep}}|\mathbb{F}_q) = \overline{\langle x \mapsto x^q \rangle} \simeq \hat{\mathbb{Z}}$ y gracias al isomorfismo 3.1.6 deducimos que $\mathtt{Gal}(k^{\mathtt{ur}}|k) = \overline{\langle \varphi_k \rangle}$. En particular la extensión $k^{\mathtt{ur}} \supset k$ es procíclica. Decimos que φ_k es el **elemento de Frobenius de** k.

Como ya se comentó, en general el cuerpo $k^{\mathtt{ur}}$ no es completo respecto a la valoración que extiende a ν_k. Para nosotros será útil disponer de la completitud y a menudo trabajaremos sobre la compleción $\hat{k}^{\mathtt{ur}}$ de $k^{\mathtt{ur}}$ respecto a la valoración anterior. Sabemos que $e(\hat{k}^{\mathtt{ur}}|k^{\mathtt{ur}}) = 1$ y $f(\hat{k}^{\mathtt{ur}}|k^{\mathtt{ur}}) = 1$ de modo que en cierto sentido la extensión $\hat{k}^{\mathtt{ur}} \supset k$ no ramifica ni hay inercia. En realidad no se puede hablar

ni de ramificación ni inercia pues de forma general la extensión $\hat{k}^{\mathtt{ur}} \supset k^{\mathtt{ur}}$ no es algebraica, razón por la que tampoco podemos hablar de grupo de Galois. En este sentido, abusaremos del lenguaje y hablaremos del grupo de Galois $\mathtt{Gal}(\hat{k}^{\mathtt{ur}}|k)$ para referirnos al grupo $\mathtt{Aut}_k(\hat{k}^{\mathtt{ur}})$ de k-automorfismos de $\hat{k}^{\mathtt{ur}}$. Extendemos φ_k a $\hat{k}^{\mathtt{ur}}$ por continuidad y obtenemos un elemento que denotamos de nuevo por φ_k que pertenece a $\mathtt{Gal}(\hat{k}^{\mathtt{ur}}|k)$. Teniendo en cuenta que $f(\hat{k}^{\mathtt{ur}}|k^{\mathtt{ur}}) = 1$, un sistema de representantes de $\mathcal{O}_{k^{\mathtt{ur}}}$ será también un sistema de representantes de $\mathcal{O}_{\hat{k}^{\mathtt{ur}}}$. Sabemos que para todo $n \in \mathbb{N}$ el conjunto $\mu_{q^n-1} \cup \{0\}$ es un sistema de representantes de $\mathcal{O}_{k_n}$ y deducimos que la unión $\cup_{n\geq 0}\mu_{q^n-1}$ es un sistema de representantes de $\mathcal{O}_{k^{\mathtt{ur}}}$. Además, los isomorfismos $\mu_{q^n-1} \simeq \overline{k_n}^{\times}$ son compatibles entre sí y vemos que el homomorfismo canónico $\mathcal{O}_{k^{\mathtt{ur}}} \to \overline{k}^{\mathtt{sep}}$ induce un isomorfismo $\cup_{n\geq 0}\mu_{q^n-1} \simeq \overline{k}^{\mathtt{sep},\times}$. Como antes, podemos demostrar que el elemento de Frobenius de k actúa sobre el conjunto $\cup_{n\geq 0}\mu_{q^n-1}$ elevando a q. Concluimos que si $\pi \in k$ es un parámetro de uniformización y tenemos $a \in \hat{k}^{\mathtt{ur}}$ expresado de manera única como

$$a = \sum_{j=m}^{\infty} \alpha_j \pi^j, \quad \alpha_j \in \cup_{n\geq 0}\mu_{q^n-1}, m \in \mathbb{Z}$$

entonces

$$\varphi_k(a) = \sum_{j=m}^{\infty} \alpha_j^q \pi^j.$$

Este descripción relativamente explícita del elemento de Frobenius se probará muy útil a la hora de estudiar la Teoría de Cuerpos de Clase Local.

Por último, es importante comparar elementos de Frobenius de distintos cuerpos locales. Para ello, supongamos que tenemos una extensión finita separable $k' \supset k$ con cuerpos residuales de q', q elementos respectivamente, grado residual $f(k'|k)$ e índice de ramificiación $e(k'|k)$. Sean $\varphi_{k'}, \varphi_k$ los elementos de Frobenius de k', k respectivamente. Es $k'^{\mathtt{ur}} = k'k^{\mathtt{ur}}$ de modo que $k^{\mathtt{ur}} \subset k'^{\mathtt{ur}}$ y podemos restringir $\varphi_{k'}$ a $k^{\mathtt{ur}}$. Se verifica la siguiente relación:

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

Por 3.1.5 tenemos los isomorfismos

$$\begin{array}{ccccc} \mathtt{Gal}(k'^{\mathtt{ur}}|k') & \xrightarrow{\simeq} & \mathtt{Gal}(\overline{k'}^{\mathtt{sep}}|\overline{k'}), & \text{y} & \mathtt{Gal}(k^{\mathtt{ur}}|k) \xrightarrow{\simeq} \mathtt{Gal}(\overline{k}^{\mathtt{sep}}|\overline{k}), \\ \sigma' & \longmapsto & \overline{\sigma'}, & & \sigma \longmapsto \overline{\sigma}. \end{array}$$

Podemos verlos conjuntamente en el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathtt{Gal}(k'^{\mathtt{ur}}|k') & \xrightarrow{\simeq} & \mathtt{Gal}(\overline{k'}^{\mathtt{sep}}|\overline{k'}) \\ \downarrow & & \downarrow \\ \mathtt{Gal}(k^{\mathtt{ur}}|k) & \xrightarrow{\simeq} & \mathtt{Gal}(\overline{k}^{\mathtt{sep}}|\overline{k}) \end{array}$$

donde los morfismos verticales son restricciones. Como $q' = q^{f((k'|k)}$, tenemos $\overline{\varphi_{k'}}_{|\overline{k}} = \overline{\varphi_k}^{f(k'|k)} = \overline{\varphi_k^{f(k'|k)}}$. Trazando el elemento de Frobenius $\varphi_{k'}$ a lo largo del diagrama:

$$\overline{(\varphi_{k'})_{|k^{\mathrm{ur}}}} = (\overline{\varphi_{k'}})_{|\overline{k}} = \overline{\varphi_k^{f(k'|k)}}.$$

Concluimos con la igualdad $(\varphi_{k'})_{|k^{\mathrm{ur}}} = \varphi_k^{f(k'|k)}$.

3.2. Extensiones Totalmente Ramificadas

En la sección anterior hemos encontrado ejemplos naturales de extensiones totalmente ramificadas. En esta sección vamos a estudiarlas y concluir que son de un tipo muy concreto, a saber, extensiones simples cuyo generador es una raíz de un polinomio de Eisenstein. Vamos a introducir estas nociones y demostrar el resultado principal.

Sea (k, ν) un cuerpo completo respecto de la valoración discreta ν. Un polinomio

$$g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_k[X]$$

es un **polinomio de Eisenstein** si

$$a_0, \ldots, a_{n-1} \in \mathfrak{p}_k,\ a_0 \notin \mathfrak{p}_k^2.$$

Se cumple el siguiente resultado:

Proposición 3.2.1. 1. Un 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.

Demostración. 1. Escribiremos $L = k(\Pi), e = e(\omega|\nu), f = f(\omega|\nu)$. Como Π es una raíz de g tenemos que

$$n\omega(\Pi) = \omega\left(\sum_{i=0}^{n-1} a_i\Pi^i\right) \geq \mathtt{min}_{0\leq i\leq n-1}(\nu(a_i) + i\omega(\Pi)).$$

Es claro que debe ser $\omega(\Pi) > 0$ pues si no obtenemos una contradicción con la desigualdad anterior. Además, como el polinomio es de Eisenstein, tenemos que $\nu(a_0) = 1 \leq \nu(a_i) < \nu(a_i) + i\omega(\Pi)$ para todo $i > 0$. Como se tiene la igualdad $g(\Pi) = 0$ sabemos que ω alcanza el valor mínimo en al menos dos de los sumandos que intervienen y como $\omega(a_0) < \omega(a_i\Pi^i)$ para todo $i > 0$ concluimos que debe ser

$$n\omega(\Pi) = \omega(\Pi^n) = \omega(a_0) = 1.$$

Recordando que la expresión de ω es $1/n \cdot \nu \circ \mathtt{N}_{L|k}$ vemos que $\nu(\mathtt{N}_{L|k}(\Pi)) = 1$, es decir, $\mathtt{N}_{L|k}(\Pi) = \varepsilon\pi$ con $\varepsilon \in \mathcal{O}_k^\times$. Veamos que $e \geq n$ y que Π es un elemento primo de L. Sea $\hat{\Pi}$ un elemento primo de L y escribamos $\Pi = a\hat{\Pi}^k, \pi = b\hat{\Pi}^e,\ a, b \in \mathcal{O}_L^\times$. Tomando normas, deducimos las igualdades

$$\mathtt{N}_{L|k}(\Pi) = \mathtt{N}_{L|k}(a)\mathtt{N}_{L|k}(\hat{\Pi})^k,\ \pi^n = \mathtt{N}_{L|k}(\pi) = \mathtt{N}_{L|k}(b)\mathtt{N}_{L|k}(\hat{\Pi})^e.$$

Usando que $\mathtt{N}_{L|k}(\Pi) = \varepsilon\pi$:

$$\mathtt{N}_{L|k}(a)^n\mathtt{N}_{L|k}(\hat{\Pi})^{nk} = \varepsilon^n\pi^n = \varepsilon^n\mathtt{N}_{L|k}(b)\mathtt{N}_{L|k}(\hat{\Pi})^e.$$

Deducimos que $\hat{\Pi}^{kn-e}$ es una unidad de $\mathcal{O}_L$, es decir, $kn = e$. De aquí deducimos que es $e \geq n = [L : k] = ef \geq e$, es decir, $e = n, f = 1, k = 1$. Concluimos que el polinomio $g(X)$ es irreducible, que Π es un elemento primo de L. Por último para probar que es $\mathcal{O}_L = \mathcal{O}_k[\Pi]$ basta usar (la demostración de) 1.3.3.

2. Sea Π un elemento primo de L. De nuevo, gracias a (la demostración de) 1.3.3, es $L = k(\Pi)$. Sea $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ el polinomio mínimo de Π sobre k. Es $n = e$ y

$$n\omega(\Pi) = \mathtt{min}_{0\leq i\leq m-1}(\nu(a_i) + i\omega(\Pi)) = \nu(a_0).$$

Como $\omega(\Pi) = 1/n$ tenemos que $\nu(a_0) = 1$ y $\nu(a_i) \geq 1$ para todo i con $\nu(a_0) = 1$.

□

3.3. Ramificación y Extensiones de Galois

Hemos estudiado la ramificación para extensiones locales en general. Ahora estamos interesados en comprender la ramificación en extensiones de Galois sin que el cuerpo base k sea necesariamente un cuerpo completo. Vamos a ver la influencia que tiene el grupo de Galois en las factorizaciones así como la "monitorización" que nos permite hacer de las mismas.

Comenzamos con un cuerpo k con un valor absoluto ν. Como en el capítulo de extensiones, vamos a denotar los valores absolutos y las valoraciones con los mismos símbolos ν, ω. Cuando el valor absoluto sea no arquimediano quedará claro por el contexto si estamos usando una valoración o un valor absoluto. Si fuese necesario distinguir usaremos ν para valoraciones y $|\cdot|_\nu$ para valores absolutos.

Sea $L \supset k$ una extensión finita de Galois y ω una extensión de ν a L. Para cada $\sigma \in G = \mathtt{Gal}(L|k)$ consideramos $w \circ \sigma$, que también extiende a ν. De este modo obtenemos una acción de G sobre el conjunto de extensiones $\omega|\nu$. Como es de esperar, esta acción es transitiva y lo demostramos en la siguiente proposición:

Proposición 3.3.1. El grupo G actúa transitivamente en el conjunto de extensiones $\omega|\nu$.

Demostración. Sean ω, ω' dos extensiones de ν a L. Por reducción al absurdo, si estas extensiones no son conjugadas entonces los conjuntos

$$\{\omega \circ \sigma | \sigma \in G\} \text{ y } \{\omega' \circ \sigma | \sigma \in G\}$$

serían disjuntos. Por el teorema de aproximación 1.1.4 hallamos un elemento $x \in L$ tal que

$$|\sigma x|_\omega < 1 \text{ y } |\sigma x|_{\omega'} > 1$$

para todo $\sigma \in G$. Obtendríamos entonces que

$$|\mathtt{N}_{L|k}(x)|_\nu = \prod_{\sigma \in G} |\sigma x|_\omega < 1,$$

y análogamente también obtendríamos $|\mathtt{N}_{L|k}(x)|_\nu > 1$ que es absurdo.

□

Definición 3.3.2. El **grupo de descomposición** de una extensión ω de ν a L se define como

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

Cuando ν es una valoración no arquimediana el grupo de descomposición G_ω contiene un subgrupo canónico I_ω que definimos a continuación. Denotamos el anillo de valoración, ideal maximal y cuerpo residual de k respecto a ν (resp. L respecto a ω) por $\mathcal{O}_\nu, \mathfrak{p}_\nu, \overline{k}_\nu$ (resp. $\mathcal{O}_\omega, \mathfrak{p}_\omega, \overline{L}_\omega$).

Definición 3.3.3. Sea ν una valoración no arquimediana y $\omega|\nu$. El **grupo de inercia** de ω se define como

$$I_\omega = I_\omega(L|k) = \{\sigma \in G_\omega | \sigma x + \mathfrak{p}_\omega = x + \mathfrak{p}_\omega \ \forall x \in \mathcal{O}_\omega\}.$$

La definición asume que dado $x \in \mathcal{O}_\omega$ entonces $\sigma x \in \mathcal{O}_\omega$ para todo $\sigma \in G_\omega$. Esta propiedad se cumple pues un elemento $\sigma \in G_\omega$ verifica que $\omega \circ \sigma = \omega$ y por tanto $|\sigma x|_\omega = |x|_\omega$ y si $|x|_\omega \leq 1$ entonces $|\sigma x|_\omega \leq 1$.

Veamos algunas propiedades funtoriales de los grupos G_ω, I_ω. Consideremos dos extensiones de Galois finitas $L \supset k, L' \supset k'$ y un diagrama conmutativo

$$\begin{array}{ccc} L & \xrightarrow{\tau} & L' \\ \uparrow & & \uparrow \\ k & \xrightarrow{\tau} & k'. \end{array}$$

Este diagrama induce un homomorfismo

$$\begin{array}{rccc} \tau^* : \mathtt{Gal}(L'|k') & \to & \mathtt{Gal}(L|k), \\ \sigma' & \mapsto & \tau^{-1}\sigma'\tau. \end{array}$$

Observar que al ser la extensión $L \supset k$ normal también lo es $\tau L \supset \tau k$ y por ello tenemos que $\sigma'\tau L \subset \tau L$ de modo que podemos componer con τ^{-1}.

Sea ω' una valoración de L' de modo que $\omega := \omega' \circ \tau$ con $\nu := \omega_{|k}$. En k' consideramos la valoración $\nu' := \omega'_{|k'}$. Se cumple la siguiente proposición:

Proposición 3.3.4. El homomorfismo $\tau^* : \mathtt{Gal}(L'|k') \to \mathtt{Gal}(L|k)$ induce homomorfismos:

$$\begin{aligned} G_{\omega'}(L'|k') &\to G_\omega(L|k), \\ I_{\omega'}(L'|k') &\to I_\omega(L|k). \end{aligned}$$

En el último homomorfismo ν debe ser no arquimediana.

Demostración. Sea $\sigma' \in G_{\omega'}(L'|k')$ y $\sigma = \tau^*(\sigma')$. Entonces

$$\omega \circ \sigma = \omega \circ \tau^{-1} \circ \sigma' \circ \tau = \omega' \circ \sigma' \circ \tau = \omega' \circ \tau = \omega$$

luego $\sigma \in G_\omega(L|k)$.

Si $\sigma' \in I_{\omega'}(L'|k')$ y $x \in \mathcal{O}_\omega$:

$$\omega(\sigma x - x) = \omega(\tau^{-1}(\sigma'\tau x - \tau x)) = \omega'(\sigma(\tau x) - (\tau x)) > 0$$

pues $\tau x \in \mathcal{O}_{\omega'}$.

□

Cuando los homomorfismos $\tau : L' \to L$ y $\tau : k' \to k$ son isomorfismos deducimos que los homomorfismos anteriores son también isomorfismos. En particular, en el caso en que $k' = k, L' = L$ vemos que para todo $\tau \in \mathtt{Gal}(L|k)$ se verifican las identidades:

$$G_{\omega\circ\tau} = \tau^{-1} G_\omega \tau, \; I_{\omega\circ\tau} = \tau^{-1} I_\omega \tau,$$

es decir, los grupos de descomposición e inercia de valoraciones conjugadas son conjugados.

Otro caso particular es cuando partimos de una subextensión intermedia $L \supset M \supset k$, que representamos por medio del diagrama siguiente:

$$\begin{array}{ccc} L & = & L \\ | & & | \\ k & \hookrightarrow & M. \end{array}$$

En este caso τ^* es la inclusión $\mathtt{Gal}(L|M) \hookrightarrow \mathtt{Gal}(L|k)$ y de manera trivial obtenemos las siguientes relaciones:

Corolario 3.3.5. Para las extensiones $k \subset M \subset L$ tenemos:

$$\begin{aligned} G_\omega(L|M) &= G_\omega(L|k) \cap \mathtt{Gal}(L|M), \\ I_\omega(L|M) &= I_\omega(L|k) \cap \mathtt{Gal}(L|M). \end{aligned}$$

Aplicamos nuestras propiedades al diagrama *global a local*:

$$\begin{array}{ccc} (L,\omega) & \longrightarrow & (\hat{L}_\omega,\hat{\omega}) \\ \Big| & & \Big| \\ (k,\nu) & \longrightarrow & (\hat{k}_\nu,\hat{\nu}). \end{array}$$

Para la extensión local $\hat{L}_\omega \supset \hat{k}_\nu$ denotaremos los grupos de descomposición e inercia por $G_{\hat{\omega}}(\hat{L}_\omega|\hat{k}_\nu)$, $I_{\hat{\omega}}(\hat{L}_\omega|\hat{k}_\nu)$. De hecho, la unicidad de la extensión de cuerpos valorados $(\hat{L}_\omega,\hat{\omega}) \supset (\hat{k}_\nu,\hat{\nu})$ implica que $G_{\hat{\omega}}(\hat{L}_\omega|\hat{k}_\nu) = \mathtt{Gal}(\hat{L}_\omega|\hat{k}_\nu)$. En este caso, el homomorfismo $\tau^* : \mathtt{Gal}(\hat{L}_\omega|\hat{k}_\nu) \to \mathtt{Gal}(L|k)$ es simplemente la restricción $\sigma \mapsto \sigma_{|L}$.

Tenemos los siguientes isomorfismos:

Proposición 3.3.6.

$$G_\omega(L|k) \simeq \mathtt{Gal}(\hat{L}_\omega|\hat{k}_\nu),$$
$$I_\omega(L|k) \simeq I(\hat{L}_\omega|\hat{k}_\nu).$$

Demostración. La proposición se basa en la siguiente propiedad:

> *El grupo de descomposición $G_\omega(L|k)$ está constituido por los automorfismos $\sigma \in \mathtt{Gal}(L|k)$ que son continuos respecto a la valoración ω.*
>
> *Demostración.* Es inmediata la continuidad de un elemento $\sigma \in G_\omega(L|k)$, de hecho σ es una isometría. Para el recíproco, sea σ un automorfismo continuo respecto a ω. Si es $x \in L$ tal que $|x|_\omega < 1$ entonces x^n converge a cero respecto a ω. Como σ es continua entonces también converge a cero $(\sigma x)^n$ y por ello $|\sigma x|_\omega < 1$. Concluimos que se verifica la implicación
>
> $$|x|_\omega < 1 \Rightarrow |\sigma x|_\omega = |x|_{\omega\circ\sigma} < 1.$$
>
> Esta propiedad sabemos que implica que ω y $\omega \circ \sigma$ son equivalentes pero como ω y $\omega \circ \sigma$ coinciden sobre k concluimos que son iguales y por ello $\sigma \in G_\omega(L|k)$.
>
> ■
>
> Para concluir el resultado, recordar que L es denso en L_ω y por ello, visto que $\sigma \in G_\omega(L|k)$ si y sólo si es continuo, vemos que **existe una única** extensión de σ a un $\hat{k}_\nu$-automorfismo $\hat{\sigma}$ de $\hat{L}_\omega$. Además, es claro que $\hat{\sigma} \in I_{\hat{\omega}}(\hat{L}_\omega|\hat{k}_\nu)$ si $\sigma \in I_\omega(L|k)$.
>
> □

La importancia de este último resultado es que de nuevo podemos reducir nuestro estudio de una valoración a la situación local sin perder demasiada información en lo que al grupo de Galois se refiere.

De ahora en adelante abusaremos de la notación e identificaremos los grupos de descomposición e inercia con sus versiones locales tal y como la proposición 3.3.6 sugiere.

Ya podemos comprender el significado práctico de los grupos introducidos en esta sección. El grupo de descomposición G_ω controla la extensión de ν a L desde el punto de vista de la teoría de grupos. De hecho, una propiedad importante de este grupo es que el índice de grupos $(G : G_\omega)$ es igual al número de posibles extensiones de ν a L.

Definición 3.3.7. El cuerpo fijo de G_ω,

$$Z_\omega = Z_\omega(L|k) = \{x \in L | \sigma x = x \ \forall \sigma \in G_\omega\},$$

es el **cuerpo de descomposición** de ω sobre k.

Z_ω verifica las siguientes propiedades:

1. La restricción de ω a Z_ω, denotada ω_Z, se extiende de manera única a L.

   Demostración. Una extensión arbitraria ω' de ω_Z a L es conjugada con ω sobre Z_ω, luego $\omega' = \omega \circ \sigma$ para algún $\sigma \in \mathtt{Gal}(L|Z_\omega)$. Como $\mathtt{Gal}(L|Z_\omega) = G_\omega(L|k)$ por definición, concluimos que $\omega' = \omega \circ \sigma = \omega$.

   □

2. $Z_\omega = L \cap \hat{k}_\nu$ (considerándose la intersección dentro de $\hat{L}_\omega$).

   Demostración. Tenemos el isomorfismo $G_\omega(L|k) \simeq \mathtt{Gal}(\hat{L}_\omega|\hat{k}_\nu)$ que lleva σ en su extensión (por continuidad) $\hat{\sigma}$. El inverso es simplemente la restricción. De este modo,

   $$\begin{aligned} Z_\omega &= \{x \in L | \sigma x = x \ \forall \sigma \in G_\omega(L|k)\} \\ &= \{x \in L | \hat{\sigma} x = x \ \forall \sigma \in G_\omega(L|k)\} \\ &= \{x \in L | \alpha x = x \ \forall \alpha \in \mathtt{Gal}(\hat{L}_\omega|\hat{k}_\nu)\} \\ &= L \cap Z_\omega = L \cap \hat{k}_\nu. \end{aligned}$$

   □

3. Si ν es no arquimediana, ω_Z tiene el mismo cuerpo residual y el mismo grupo de valores que ν.

Demostración. Sabemos que $\hat{k}_\nu$ tiene el mismo grupo de valores y el mismo cuerpo residual que k. Como $k \subset Z_\omega \subset \hat{k}_\nu$ concluimos que k y Z_ω tienen el mismo grupo de valores. De manera análoga se ve que poseen el mismo cuerpo residual.

□

El grupo de inercia $I_\omega(L|k)$ se puede obtener a partir del grupo de descomposición como el núcleo de un homomorfismo natural. Para construir dicho homomorfismo, si $\mathcal{O}_\omega$ es el anillo de valoración de ω con ideal maximal $\mathfrak{p}_\omega$ entonces, como $\sigma\mathcal{O}_\omega = \mathcal{O}_\omega, \sigma\mathfrak{p}_\omega = \mathfrak{p}_\omega$ para todo $\sigma \in G_\omega(L|k)$, vemos que los elementos de $G_\omega(L|k)$ inducen un $\overline{k}_\nu$-automorfismo de $\overline{L}_\omega$:

$$\begin{array}{ccc} \overline{\sigma} : \overline{L}_\omega & \to & \overline{L}_\omega \\ x + \mathfrak{p}_\omega & \mapsto & \sigma x + \mathfrak{p}_\omega \end{array}$$

y obtenemos un homomorfismo

$$G_\omega(L|k) \to \mathtt{Aut}_{\overline{k}_\nu}(\overline{L}_\omega)$$

con núcleo $I_\omega(L|k)$.

En realidad, el grupo de automorfismos en la llegada es en realidad un grupo de Galois pues la extensión $\overline{L}_\omega \supset \overline{k}_\nu$ es una extensión normal y dicho homomorfismo es sobreyectivo.

Demostración. Como el cuerpo de descomposición Z_ω tiene el mismo cuerpo residual que k podemos suponer sin pérdida de generalidad que $G_\omega(L|k) = \mathtt{Gal}(L|k)$. Sea $\alpha \in \mathcal{O}_\omega$ siendo $f \in \mathcal{O}_\nu[X]$ su polinomio mínimo sobre k y consideremos $\alpha + \mathfrak{p}_\omega \in \overline{L}_\omega$ con polinomio mínimo $\overline{g} \in (\overline{k}_\nu)[X]$. Tenemos que $\alpha + \mathfrak{p}_\omega$ es una raíz del polinomio $\overline{f}(X) = f(X) + \mathfrak{p}_\omega[X]$ y por ello $\overline{g}|\overline{f}$. Como la extensión $L \supset k$ es normal, f factoriza como producto de polinomios lineales en $\mathcal{O}_\omega[X]$. Por tanto, $\overline{f}$ factoriza como producto de polinomios lineales en $\overline{L}_\omega$ y por tanto lo mismo se cumple para $\overline{g}$.

Para la sobreyectividad, vamos a suponer que la extensión de los cuerpos residuales es separable pues es el contexto en el que nos encontraremos, si bien, el resultado sigue siendo cierto en el caso en que la extensión no es separable. Sea $\alpha + \mathfrak{p}_\omega \in \overline{L}_\omega$ un generador de la extensión $\overline{L}_\omega \supset \overline{k}_\nu$. Con nuestras hipótesis, sea $\tilde{\sigma}$ un $\overline{k}_\nu$-automorfismo de $\overline{L}_\omega$ y sea $\alpha + \mathfrak{p}_\omega \in \overline{L}_\omega$ como antes. Entonces $\tilde{\sigma}(\alpha + \mathfrak{p}_\omega)$ es una raíz de $\overline{g}$ y por ello también lo es de $\overline{f}$, es decir, existe $\alpha' \in \mathcal{O}_\omega$ raíz de f tal que $\alpha' + \mathfrak{p}_\omega = \tilde{\sigma}(\alpha + \mathfrak{p}_\omega)$. α' es conjugado de α de modo que existe $\sigma \in \mathtt{Gal}(L|k)$ verificando $\alpha' = \sigma\alpha$. Como $\sigma\alpha + \mathfrak{p}_\omega = \tilde{\sigma}(\alpha + \mathfrak{p}_\omega)$ concluimos que $\tilde{\sigma} = \overline{\sigma}$ y el homomorfismo es sobreyectivo.

□

En definitiva, obtenemos para cada $\omega|\nu$ tenemos el isomorfismo del grupo de descomposición $G_\omega(L|k) \simeq \mathtt{Gal}(\hat{L}_\omega|\hat{k}_\nu)$ y un homomorfismo sobreyectivo canónico

$$G_\omega(L|k) \to \mathtt{Gal}(\overline{L}_\omega|\overline{k}_\nu)$$

cuyo núcleo es el grupo de inercia $I_\omega(L|k)$.

Definición 3.3.8. El cuerpo fijo de $I_\omega(L|k)$,

$$T_\omega = \{x \in L | \sigma x = x \ \forall \sigma \in I_\omega(L|k)\},$$

se llama **cuerpo de inercia** de ω sobre k.

Como $I_\omega(L|k)$ es un subgrupo normal de $G_\omega(L|k)$ tenemos que la extensión $T_\omega \supset Z_\omega$ es de Galois. De hecho, tenemos el isomorfismo

$$\texttt{Gal}(T_\omega|Z_\omega) \simeq G_\omega(L|k)/I_\omega(L|k) \simeq \texttt{Gal}\left(\overline{L}_\omega|\overline{k}_\nu\right).$$

El cuerpo T_ω verifica la siguiente propiedad:

Proposición 3.3.9. La extensión $T_\omega \supset Z_\omega$ es la subextensión maximal no ramificada de $L \supset Z_\omega$.

Demostración. Por 3.3.6 podemos asumir que k es completo de modo que $k = Z_\omega$. Sea $T \supset k$ la suebxtensión maximal no ramificada de $L \supset k$. Sabemos que dicha extensión es de Galois y por 3.1.6 tenemos que el cuerpo residual de T es la clausura separable de $\overline{k}$ en $\overline{L}$ junto con el isomorfismo

$$\texttt{Gal}(T|k) \to \texttt{Gal}(\overline{L}^{sep} \cap \overline{k}|\overline{k}).$$

Para concluir la demostración, observar que un elemento $\sigma \in \texttt{Gal}(L|k)$ pertenece a $I_\omega(L|k)$, i.e., σ induce la identidad en $\overline{L}$ (equivalentemente en $\overline{L}^{sep} \cap \overline{k}$) si y sólo si pertenece a $\texttt{Gal}(L|T)$. Concluimos que $\texttt{Gal}(L|T) = I_\omega(L|k)$ y $T = T_\omega$.

□

Veamos que hemos obtenido hasta ahora. Sea ν una valoración no arquimediana de k y $L \supset k$ una extensión de Galois finita, con $\omega|\nu$ una valoración extendiendo ν a L. Denotamos por ω_Z la extensión de ν a Z_ω y por ω_T la extensión de ν a T_ω. Supuesto que la extensión $\overline{L}_\omega \supset \overline{k}_\nu$ es separable, se cumplen las siguientes propiedades:

1. ω_Z admite una única extensión a L.
2. La extensión de ω_Z a T_ω, ω_T, no ramifica y $f(\omega_T|\omega_Z) = f(\omega|\nu)$.

   En efecto, la extensión $T_\omega \supset Z_\omega$ es la subextensión maximal no ramificada de $L \supset Z_\omega$ de modo que $[T_\omega : Z_\omega] = [\overline{T_\omega} : \overline{Z_\omega}] = f(\omega_T|\omega_Z)$. Además

   $$[T_\omega : Z_\omega] = \#\texttt{Gal}(T_\omega|Z_\omega) = \#\texttt{Gal}(\overline{L}_\omega|\overline{k}_\nu) = f(\omega|\nu).$$

3. La valoración ω_T ramifica completamente en L y se cumple que $e(\omega|\omega_T) = e(\omega|\nu)$.

   Tenemos que la extensión $L \supset T_\omega$ es totalmente ramificada luego $f(\omega|\omega_T) = 1$ y

   $$e(\omega|\omega_T) = e(\omega|\omega_T)e(\omega_T|\omega_Z)e(\omega_Z|\nu) = e(\omega|\nu).$$

   Observar además que

   $$e(\omega|\omega_T) = e(\omega|\omega_T)f(\omega|\omega_T) = [L : T_\omega] = \#\mathtt{Gal}(L|T_\omega) = \#I_\omega(L|T).$$

4. Tenemos la siguiente fórmula

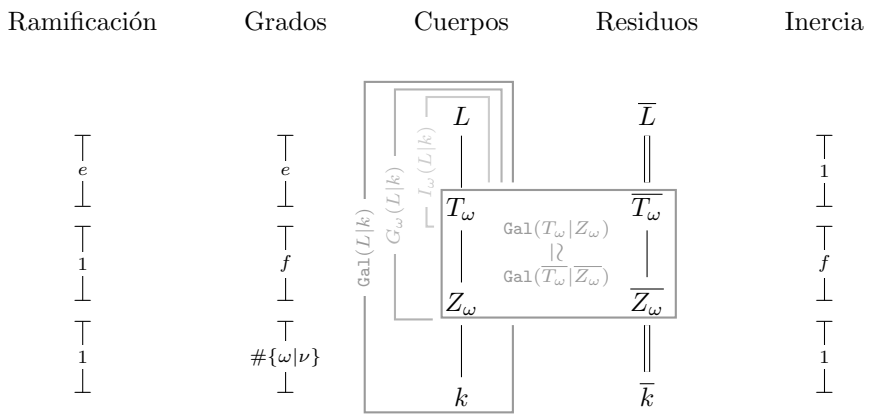
   $$\begin{aligned}[L : k] &= (G : G_\omega)\#G_\omega \\ &= (G : G_\omega)\#\left(G_\omega/I_\omega\right)\#I_\omega \\ &= (G : G_\omega)\#\mathtt{Gal}(\overline{L}_\omega|\overline{k}_\nu)\#I_\omega \\ &= (G : G_\omega)e(\omega|\nu)f(\omega|\nu)\end{aligned}$$

   para todo par $\omega|\nu$. Recordar que el número $(G : G_\omega)$ es el número de posibles extensiones ω de ν.

5. Si el grupo de descomposición G_ω es normal en $G = \mathtt{Gal}(L|k)$ (por ejemplo cuando la extensión $L \supset k$ es abeliana) entonces todos los grupos de descomposición de las extensiones de ν a L coinciden al igual que los cuerpos de descomposición. Podemos hablar entonces del grupo de descomposición de ν a secas y que denotaremos por G_ν. Concluimos que para toda extensión $\omega|\nu$ es $e(\omega_Z|\nu) = 1$ y $f(\omega_Z|\nu) = 1$. Si suponemos que ν es discreta con ideal maximal asociado $\mathfrak{p}_\nu$, este resultado equivale a la siguiente factorización

   $$\mathcal{O}_{L^{G_\nu}}\mathfrak{p}_\nu = \prod_{\sigma G_\nu \in G/G_\nu} \sigma\mathfrak{P}_{\omega,L^{G_\nu}}$$

   con $\mathfrak{P}_{\omega,L^{G_\nu}}$ el ideal maximal de L^{G_ν} asociado a una de las extensiones $\omega|\nu$. En general, el grupo $G_\omega(L|k)$ no es normal y lo único que podemos afirmar es que en la factorización anterior, el exponente que acompaña a $\mathfrak{P}_{\omega,L^{G_\nu}}$ es igual a 1.



3.4. Grupos Superiores de Ramificación

Los grupos de descomposición e inercia solo son dos términos de una sucesión decreciente de grupos llamados *grupos de ramificación (superiores)*. Veamos cómo se definen y algunas de sus propiedades elementales. No demostraremos muchos resultados aquí, el objetivo de esta sección es introducir conceptos que necesitaremos a modo de herramientas.

Sea $L \supset k$ una extensión de Galois finita con k un cuerpo local no arquimediano 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 3.4.1. 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 maximal no ramificada 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.

Demostración. 1. Es inmediato a partir de las definciones.

2. Sean $\sigma \in G_i, \alpha \in \mathcal{O}_L$. Entonces $\sigma\alpha - \alpha \in \mathfrak{p}_L^{i+1}$ y como $\sigma(\mathfrak{p}_L) = \mathfrak{p}_L$ deducimos que $\alpha - \sigma^{-1}\alpha \in \mathfrak{p}_L^{i+1}$ de modo que $\sigma^{-1} \in G_i$. Sean $\sigma, \tau \in G_i$. Entonces

$$\sigma\tau(\alpha) - \alpha = \sigma(\tau\alpha - \alpha) + \sigma\alpha - \alpha \in \mathfrak{p}_L^{i+1},$$

luego $\sigma\tau \in G_i$. Por último, sean $\sigma \in G_i, \tau \in G$. Entonces $\tau\alpha \in \mathcal{O}_L$ y $\sigma\tau\alpha - \tau\alpha \in \mathfrak{p}_L^{i+1}$, luego $\tau^{-1}\sigma\tau\alpha - \alpha \in \mathfrak{p}_L^{i+1}$ y concluimos que $\tau^{-1}\sigma\tau \in G_i$.

3. Sabemos que G_0 coincide con el núcleo del homomorfismo canónico $\mathtt{Gal}(L|k) \to \mathtt{Gal}(\overline{L}|\overline{k})$, es decir, G_0 es el grupo de inercia de la extensión de modo que $G_0 = \mathtt{Gal}(L|L \cap k^{\mathtt{ur}})$. Gracias al apartado 1. tenemos que $(G_0)_i = G_i \cap G_0 = G_i$ usando que $G_i \subset G_0$. Además, como la extensión $L \supset L \cap k^{\mathtt{ur}}$ es totalmente ramificada, para cualquier parámetro de uniformización π de L tenemos que $\mathcal{O}_L = \mathcal{O}_{L\cap k^{\mathtt{ur}}}[\pi]$. Sea $\alpha \in \mathcal{O}_L$ de modo que $\alpha = \sum_{i=0}^{n} a_i\pi^i$ con $a_i \in \mathcal{O}_{L\cap k^{\mathtt{ur}}}$. Como $\sigma a_i = a_i$ para $\sigma \in G_0$ vemos que

$$\sigma\alpha - \alpha = \sum_{i=0}^{n} a_i(\sigma(\pi^i) - \pi^i).$$

Llegamos a que es suficiente tener $\sigma\pi - \pi \in \mathfrak{p}_L^{i+1}$ para obtenerlo para el resto de elementos.

4. Gracias al apartado 3. vemos que si $i \geq \mathtt{max}\{\nu_L(\sigma\pi - \pi\} \ : \ \sigma \in G\}$ entonces $G_i = \{\mathtt{id}\}$.

□

Gracias al apartado 3. generalmente nos reduciremos al estudio de 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 3.4.2. 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.

Demostración. Si π' es otro parámetro de uniformización tenemos que $\pi' 0 \pi u$ con $u \in \mathcal{O}_L^\times$ de modo que $\sigma(\pi')/\pi' = \sigma(\pi)/\pi \cdot \sigma(u)/u$. Si $s \in G_i$, tenemos que $\sigma(u) + \mathfrak{p}_L^{i+1} = u + \mathfrak{p}_L^{i+1}$ de modo que $\sigma(u)/u \cdot U_L^{(i+1)} = U_L^{(i+1)}$ y esto demuestra la independencia de la aplicación. Si $\sigma, \tau \in G_i$ entonces $\sigma\tau(\pi)/\pi = \sigma(\pi)/\pi \cdot \tau(\pi)/\pi \cdot \sigma(u)/u$ con $u = \tau(\pi)/\pi \in \mathcal{O}_L^\times$. Como $\sigma \in G_i$ volvemos a obtener que $\sigma(u)/u \cdot U_L^{(i+1)} = U_L^{(i+1)}$ de modo que

$$\sigma\tau(\pi)/\pi \cdot U_L^{(i+1)} = \sigma(\pi)/\pi \cdot \tau(\pi)/\pi \cdot U_L^{(i+1)}.$$

Por último, supongamos que $\sigma \in G_i$ es tal que $\sigma(\pi)/\pi \cdot U_L^{(i+1)} = U_L^{(i+1)}$. Entonces existe $u \in U_L^{(i+1)}$ tal que $\sigma(\pi) = u\pi$. Si escribimos $u = 1 + \alpha\pi^{i+1}$ con $\alpha \in \mathcal{O}_L$ entonces $\sigma\pi - \pi \in \mathfrak{p}_L^{i+1}$ y $\sigma \in G_i$.

□

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 $q_L - 1$ y los índices $(G_i : G_{i+1})$ dividen 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 los grupos de ramificación con enumeración inferior que 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:

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

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

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

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

Proposición 3.4.3. 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 $\mathtt{res}(\mathtt{Gal}(L'|k)^v) = \mathtt{Gal}(L|k)^v$.

Demostración. Ver [Ser62] *página 81, Proposicion 14.*

□

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

Definición 3.4.4. 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 fuerte y será esencial para la Teoría de Cuerpos de Clase Local:

Teorema 3.4.5. (Teorema de Hasse-Arf)

Si G es un grupo abeliano y v es un salto de la filtración $\{G^v\}$ entonces $v \in \mathbb{Z}$.

Demostración. Ver [Ser62] *Capítulo V, §7.*

□

Un comentario importante sobre este teorema es que la hipótesis de separabilidad sobre la extensión $\overline{L} \supset \overline{k}$ es necesaria, de modo que en este caso dicha hipótesis no se hace simplemente para simplificar el enunciado.

Los siguientes resultados serán útiles:

Lema 3.4.6.

1. Sean $L_1 \supset k$ y $L_2 \supset k$ dos extensiones de Galois finitas y $v \geq 0$. Si $\texttt{Gal}(L_1|k)^v = \texttt{Gal}(L_2|k)^v = \{\texttt{id}\}$ entonces también $\texttt{Gal}(L_1L_2|k)^v = \{\texttt{id}\}$.

2. Supongamos que $L \supset k$ es una extensión totalmente ramificada con grupo de Galois abeliano G. Entonces $(G : G^m)$ divide $(q-1)q^m$ para todo $m \geq 1$.

Demostración.

1. Denotamos $G : \texttt{Gal}(L_1L_2|k)$ y $H_i := \texttt{Gal}(L_1L_2|L_i)$ para $i = 1, 2$. Gracias a 3.4.3 obtenemos
$$G^v H_i/H_i = (G/H_i)^v = \texttt{Gal}(L_i|k)^v = \{\texttt{id}\}.$$
Se sigue que $G^v H_i \subset H_i$ para $i = 1, 2$ de modo que
$$G^v \subset H_1 \cap H_2 = \texttt{Gal}(L_1L_2|L_1) \cap \texttt{Gal}(L_1L_2|L_2) = \{\texttt{id}\}.$$

2. Notar que $G_0 = G$ pues la extensión es totalmente ramificada. Tenemos $G^m = G_{\phi^{-1}(m)}$. Por tanto si $n - 1 < \phi^{-1}(m) \leq n$ entonces $G^m = G_n$. Consideramos la descomposición
$$(G : G^m) = (G : G_n) = (G : G_1)(G_1 : G_2) \cdots (G_{n-1} : G_n).$$

Gracias a la observación realizada tras 3.4.2 sabemos que $(G : G_1)$ divide a $q-1$ y $(G_i : G_{i+1})$ divide a q para todo entero $i \geq 1$.

Por otro lado, el teorema de Hasse-Arf 3.4.5 nos dice que si $G_i \neq G_{i+1}$ para algún $0 \leq i \leq n-1$, entonces $\phi(i) \in \mathbb{Z}$. Pero como

$$0 \geq \phi(i) \leq \phi(n-1) < \phi(\phi^{-1}(m) = m,$$

vemos que se pueden producir como máximo $m-1$ con $i > 1$.

□

Capítulo 4

Teoría de Galois y Topología de Krull. Grupos Profinitos

4.1. Topología de Krull

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:

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

Vamos a ver que la topología de Krull hace que G sea un grupo topológico. Probaremos el resultado para la composición, siendo la demostración para la inversión totalmente análoga.

Continuidad de la composición: Sean σ, τ elementos de G de modo que $\sigma\tau \in \gamma\mathtt{Gal}(L|F)$. Entonces $(\sigma\tau)_{|F} = \gamma_{|F}$, es decir, $\sigma_{|\tau F}\tau_{|F} = \gamma_{|F}$. Como la extensión $F \supset k$ es normal entonces $\tau F \subset F$ y por ello $\sigma_{|F}\tau_{|F} = \gamma_{|F}$. Vamos a ver que el abierto $U := \sigma\mathtt{Gal}(L|F) \times \tau\mathtt{Gal}(L|F)$ de $G \times G$ está contenido en la imagen inversa por $(a, b) \in G \times G \mapsto ab \in G$ de $\gamma\mathtt{Gal}(L|F)$. Para ello, notar que si $(a, b) \in U$ entonces $a_{|F} = \sigma_{|F},\ b_{|F} = \tau_{|F}$ de modo que se tienen las igualdades (usaremos que $F \supset k$ es una extensión normal):

$$\begin{aligned}(ab)_{|L} &= a_{|b(F)}b_{|F} = a_{|F}b_{|F} \\ &= \sigma_{|L}\tau_{|L} = \sigma_{|\tau L}\tau_{|L} \\ &= (\sigma\tau)_{|L} = \gamma_{|L}.\end{aligned}$$

Concluimos que U es un entorno abierto de (σ, τ) contenido en la imagen inversa de $\gamma\mathtt{Gal}(L|F)$.

En la demostración hemos usado que $\sigma \in \tau\mathtt{Gal}(L|F)$ si y sólo si $\sigma_{|F} = \tau_{|F}$. Esta observación nos da la intuición que hay detrás de la topología de Krull: *dos elementos σ, τ están cerca si y sólo si coinciden sobre una subextensión finita de Galois $L \supset F \supset k$ grande.*

Denotaremos de ahora en adelante la base de entornos de $1 \in G$ por $\mathcal{S}$.

La topología de Krull verifica las siguientes propiedades:

Proposición 4.1.1. Sea $L \supset k$ una extensión de Galois con grupo de Galois G. Entonces G con la topología de Krull es un espacio topológico de **Hausdorff**, **compacto** y **totalmente disconexo**.

Demostración. Para ver que es de Hausdorff, sea $\mathcal{F}_n$ el conjunto de todas las subextensiones $L \supset F \supset k$ finitas de Galois. Tenemos que

$$\bigcap_{U \in \mathcal{S}} U = \bigcap_{F \supset k \in \mathcal{F}_n} \mathtt{Gal}(L|F) = \{1\}$$

pues

$$L = \bigcup_{F \supset k \in \mathcal{F}_n} F,$$

es decir, si $\sigma \in G$ es tal que $\sigma_{|F} = \mathtt{id}_F$ para toda subextensión finita de Galois $F \supset k$ entonces $\sigma = \mathtt{id}_L = 1$. Entonces, dados $\sigma, \tau \in G$ con $\sigma \neq \tau$ tendremos que $\sigma^{-1}\tau \neq 1$ luego existe $U_0 \in \mathcal{S}$ de modo que $\sigma^{-1}\tau \notin U_0$. Esto implica que $\tau \notin \sigma U_0$. En particular, $\tau U_0 \cap \sigma U_0 = \emptyset$.

Veamos la compacidad de G. Consideramos el homomorfismo

$$\begin{array}{ccc} f : G & \longrightarrow & \displaystyle\prod_{F \supset k \in \mathcal{F}_n} \mathtt{Gal}(F|k), \\ \sigma & \mapsto & (\sigma_{|F})_{F \supset k \in \{_n}. \end{array}$$

f es un homomorfismo pues los elementos de $\mathcal{F}_n$ son subextensiones finitas de Galois. Observar que el producto $\prod \mathtt{Gal}(F|k)$ es compacto cuando consideramos cada grupo finito $\mathtt{Gal}(F|k)$ con la topología discreta. Vamos a ver que f es una aplicación continua e inyectiva, que su imagen es cerrada en la llegada y $f : G \to f(G)$ es una aplicación abierta. Esto probaría que G es homeomorfo al espacio compacto $f(G)$, pues todo subespacio cerrado de un espacio compacto es compacto.

Inyectividad: Sea $\sigma \in G$ con $f(\sigma) = 1$. Entonces $\sigma_{|F} = 1$ para todo elemento $F \supset k \in \mathcal{F}_n$. Como $L = \bigcup_{F \supset k \in \mathcal{F}_n} F$ concluimos que $\sigma = 1$ y f es inyectiva.

Continuidad: Consideremos la composición

$$G \xrightarrow{f} \prod_{F \supset k \in \mathcal{F}_n} \mathtt{Gal}(F|k) \xrightarrow{\pi_{F|k}} \mathtt{Gal}(F|k)$$

siendo $\pi_{F|k}$ la proyección canónica. Es suficiente probar que cada una de estas composiciones es continua. La continuidad de las composiciones se sigue de la siguiente obsevación:

$$(\pi_{F|k} \circ f)^{-1}(\{1\}) = \mathtt{Gal}(L|F) \in \mathcal{S}$$

y teniendo en cuenta que en $\mathtt{Gal}(F|k)$ consideramos la topología discreta.

Imagen cerrada: Consideremos una cadena de extensiones $L \supset F_1 \supset F_2 \supset k$ con $F_1 \supset k, F_2 \supset k \in \mathcal{F}_n$ y asociemos a esta cadena el siguiente conjunto:

$$M_{F_1|F_2} = \left\{ (\sigma_F)_{F\supset k\in\mathcal{F}_n} \in \prod_{F\supset k\in\mathcal{F}_n} \mathtt{Gal}(F|k) \;\middle|\; (\sigma_{|F_1})_{|F_2} = \sigma_{|F_2} \right\}.$$

Estos conjuntos son todos cerrados. En efecto, si $\mathtt{Gal}(F_2|k) = \{\sigma_1, \ldots, \sigma_r\}$ y es A_i el conjunto de todas las extensiones de f_i a F_1, entonces

$$M_{F_1|F_2} = \bigcup_{i=1}^{r} \left(\left(\prod_{\substack{F\neq F_1,F_2 \\ F\supset k\in\mathcal{F}_n}} \mathtt{Gal}(F|k) \right) \times A_i \times \{f_i\} \right)$$

es unión finita de cerrados. Claramente,

$$f(G) \subset \bigcap_{F_1\supset F_2} M_{F_1|F_2}.$$

De hecho se tiene la igualdad pues si $(\tau_F)_{F\supset k\in\mathcal{F}_n} \in \cap_{F_1\supset F_2} M_{F_1|F_2}$ entonces (τ_F) es una cadena de aplicaciones compatibles entre si y podemos definir un k-automorfismo $\tilde{\tau} : L \to L$ de modo que $f(\tilde{\tau}) = (\tilde{\tau}_{|F})_{F\supset k\in\mathcal{F}_n} = (\tau_F)$.

Abierta sobre la imagen: Si $F \supset k \in \mathcal{F}_n$, entonces

$$f(\mathtt{Gal}(L|F)) = f(G) \cap \left(\left(\prod_{\substack{F'\neq F \\ F'\supset k\in\mathcal{F}_n}} \mathtt{Gal}(F'|k) \right) \times \{\mathtt{id}_F\} \right),$$

que es abierto en $f(G)$.

Por último probamos que G es totalmente disconexo. Gracias a la homogeneidad de los grupos topológicos, es suficiente probar que la componente conexa del elemento neutro $\mathtt{id}$ es $\{\mathtt{id}\}$. Denotamos la componente conexa de $\mathtt{id}$ por H. De manera general, para los grupos topológicos, es conocido que la componente conexa del elemento neutro es un subgrupo. Fijemos un abierto básico $U \in \mathcal{S}$ y consideremos el conjunto $U_H = U \cap H$. Claramente U_H es abierto en H. Por otro lado, definimos

$$V_H = \bigcup_{x\in H\setminus U_H} xU_H,$$

que es abierto de H pues xU_H es abierto de H para todo $x \in H$. Es claro que $U_H \cup V_H = H$. Sin embargo, $U_H \cap V_H = \emptyset$ ya que un elemento $\alpha \in U_H \cap V_H$ implica que existe $x \in H, x \notin U_H$ tal que $\alpha \in xU_H$, pero como $\alpha \in U_H$ y U_H es un subgrupo de G concluimos que $x \in U_H$, que es absurdo.

Como H es conexo y hemos encontrado dos abiertos que lo descomponen, siendo $U_H \neq \emptyset$ concluimos que es $V_H = \emptyset$. En definitiva, hemos probado que $H = H \cap U$ para cada $U \in \mathcal{S}$. Por tanto

$$\{\mathtt{id}\} \subset H \subset \bigcap_{U \in \mathcal{S}} U = \{\mathtt{id}\}.$$

□

Estas propiedades del grupo de Galois de una extensión infinita nos indican que dicho grupo es un *grupo profinito*. En la siguiente sección vamos a estudiar los grupos profinitos en general y veremos algunos ejemplos.

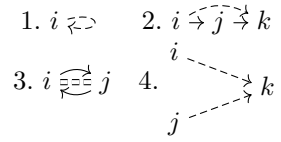
4.2. Grupos Profinitos

4.2.1. Generalidades Sobre Límites Proyectivos

Para la teoría de grupos profinitos debemos comprender qué es el límite proyectivo de una familia de conjuntos. Vamos a repasar este concepto que ya nos apareció en el primer capítulo. Sea $(I, \leq)$ un **conjunto dirigido parcialmente ordenado**, esto es, un conjunto I con una relación binaria $\leq$ verificando las siguientes condiciones:

1. Para todo $i \in I$, $i \leq i$.
2. Las condiciones $i \leq j,\ j \leq k$ implican $i \leq k$, para $i, j, k \in I$.
3. Si es $i \leq j$ y $j \leq i$ entonces $i = j$ para $i, j \in I$.
4. Si $i, j \in I$ entonces existe $k \in I$ tal que $i, j \leq k$.

Para ayudar a recordar los axiomas anteriores vamos a visualizarlos representando la condición $i \leq j$ como una flecha $i \to j$. De este modo los axiomas tienen los siguientes diagramas asociados:



Nota: Los tres primeros diagramas vienen a decir que $(I, \leq)$ es una categoría, sus objetos son los elementos de I y sus conjuntos de morfismos están formados por un único elemento para indicar que cierto par de elementos verifican la relación binaria $\leq$. El cuarto diagrama es un axioma no derivable a partir de los anteriores y que exigimos que cumplan estas categorías especiales.

Un **sistema proyectivo** de conjuntos sobre I es una colección de $\{X_i | i \in I\}$ de conjuntos indexado por I y una colección de aplicaciones $\varphi_{ij} : X_i \to X_j$ definida siempre que $i \geq j$ verificando que los diagramas de la forma

$$\begin{array}{ccc} X_i & \xrightarrow{\varphi_{ik}} & X_k \\ & {\scriptstyle\varphi_{ij}}\searrow \quad \nearrow{\scriptstyle\varphi_{jk}} & \\ & X_j & \end{array}$$

conmutan siempre que $i, j, k \in I$ con $i \geq j \geq k$. En definitiva, un sistema proyectivo no es más que un funtor contravariante de la categoría $(I, \leq)$ en la categoría de los conjuntos. Claramente, podemos modificar la categoría de llegada por la categoría de espacios topológicos o grupos abelianos (con sus respectivos morfismos) y obtener un sistema proyectivo de espacios topológicos o grupos abelianos, por ejemplo. Si el funtor es covariante obtenemos la noción dual a los sistemas proyectivos llamados **sistemas inductivos**. Denotaremos los sistemas proyectivos por $\{X_i, \varphi_{ij}, I\}$ o simplemente por $\{X_i, \varphi_{ij}\}$ si el conjunto I se sobreentiende por el contexto. A partir de ahora trabajaremos principalmente con grupos topológicos pues es la categoría que nos interesa, la mayor parte de nuestras construcciones se pueden llevar a cabo en otras categorías.

Sea Y un grupo topológico, $\{X_i, \varphi_{ij}, I\}$ un sistema proyectivo de grupos topológicos sobre el conjunto dirigido parcialmente ordenado I y sea $\psi_i : Y \to X_i$ un homomorfismo de grupos continuo para cada $i \in I$. Estas aplicaciones ψ_i se dicen **compatibles** si $\varphi_{ij}\psi_i = \psi_j$ siempre que $i \geq j$.

Diremos que un grupo topológico X junto con homomorfismos continuos compatibles $\varphi_i : X \to X_i$ $(i \in I)$ es un **límite proyectivo** del sistema proyectivo $\{X_i, \varphi_{ij}, I\}$ si la siguiente propiedad universal se cumple:

> *Para todo grupo topológico Y y un conjunto de homomorfismos continuos compatibles $\psi_i : Y \to X_i$ $(i \in I)$, existe un único homomorfismo continuo $\psi : Y \to X$ tal que $\varphi_i\psi = \psi_i$ para todo $i \in I$.*

$$\begin{array}{ccc} Y & \overset{\psi}{\dashrightarrow} & X \\ & {\scriptstyle\psi_i}\searrow & \downarrow{\scriptstyle\varphi_i} \\ & & X_i \end{array}$$

Las aplicaciones $\varphi_i : X \to X_i$ las llamamos **proyecciones**. Veamos que para los grupos topológicos existe el límite proyectivo de cualquier sistema proyectivo. Observar que este resultado no se cumple para todas las categorías.

Proposición 4.2.1. Sea $\{X_i, \varphi_{ij}, I\}$ un sistema proyectivo de grupos topológicos sobre un conjunto dirigido parcialmente ordenado I. Entonces

1. Existe un límite proyectivo del sistema proyectivo $\{X_i, \varphi_{ij}, I\}$.
2. El límite es único salvo isomorfismo topológico. En concreto, dados dos límites proyectivos $(X, \varphi_i), (Y, \psi_i)$ del sistema proyectivo $\{X_i, \varphi_{ij}, I\}$ existe un único isomorfismo continuo $\varphi : X \to Y$ tal que $\psi_i \varphi = \varphi_i$ para todo $i \in I$.

Demostración. La demostración de la segunda propiedad es rutinaria usando la propiedad universal como es usual.

Vamos a definir el límite proyectivo, que efectivamente es un límite proyectivo así como que el límite es de nuevo un grupo topológico se sigue facilmente. Para ello consideremos el producto directo $\prod_{i\in I} X_i$ con la topología producto y la operación de grupo definida componente a componente. Definimos X como sigue:

$$X = \{(x_i) \in \prod_{i\in I} X_i \mid \varphi_{ij}(x_i) = x_j \text{ si } i \geq j\}.$$

Definimos $\varphi_i : X \to X_i$ la restricción de la proyección canónica $\prod_{i\in I} X_i \to X_i$.

□

El límite proyectivo del sistema $\{X_i, \varphi_{ij}, I\}$ lo denotaremos por $\varprojlim X_i$. Ahora vamos a estudiar algunas propiedades de estos límites y como interaccionan con la topología de los conjuntos X_i.

Lema 4.2.2. Si $\{X_i, \varphi_{ij}\}$ es un sistema proyectivo de grupos topológicos de Hausdorff, entonces $\varprojlim X_i$ es un subgrupo cerrado de $\prod_{i\in I} X_i$.

Demostración. Veamos que es cerrado. Sea $(x_i) \in \prod_{i\in I} X_i \setminus \varprojlim X_i$ de modo que existen índices $r, s \in I$ con $r \geq s$ tales que $\varphi_{rs}(x_r) \neq x_s$. Sean U, V entornos abiertos disjuntos de $\varphi_{rs}(x_r)$ y x_s en X_s respectivamente. Definimos $U' = \varphi_{rs}^{-1}(U)$ que es un entorno abierto de x_r en X_r. Consideremos el abierto básico de $\prod_{i\in I} X_i$ dado por

$$W := \prod_{i\in I} V_i,\ V_r = U', V_s = V, V_i = X_i\ i \neq r, s.$$

Tenemos que W es un entorno abierto (x_i) que no corta con $\varprojlim X_i$. En efecto, si existe $(y_i) \in W \cap \varprojlim X_i$ entonces $y_r \in U', y_s \in V$ con $\varphi_{rs}(y_r) = y_s$. Esto es absurdo pues $\varphi_{rs}(y_r) \in U \cap V = \emptyset$. Concluimos que $\varprojlim X_i$ es cerrado.

□

Recordemos que un espacio topológico se dice **totalmente disconexo** si todo punto en el espacio es su propia componente conexa. Por ejemplo, un espacio con la topología discreta es totalmente disconexo pero hay espacios totalmente disconexos con una topología subyacente que no es la topología discreta. La propiedad de desconexión total también se preserva por paso al límite:

Lema 4.2.3. Sea $\{X_i, \varphi_{ij}, I\}$ un sistema proyectivo de grupos topológicos compactos, Hausdorff y totalmente disconexos sobre el conjunto dirigido parcialemnte ordenado I. Entonces $\varprojlim X_i$ es también un grupo topológico compacto de Hausdorff totalmente disconexo.

Demostración. Observar que se tiene las siguientes propiedades para espacios topológicos de Hausdorff (resp. totalmente disconexos):

a. Dada una colección de espacios topológicos de Hausdorff E_i, indexada por cierto conjunto I, el producto $\prod_i E_i$ es también un espacio de Hausdorff. En efecto, si consideramos $\alpha = (a_i), \beta = (b_i) \in \prod_i E_i$ distintos, entonces existe $j \in I$ tal que $a_j \neq b_j$. Como X_j es un espacio de Hausdorff, sean A, B abiertos de X_j tales que $a_j \in A, b_j \in B$ y $A \cap B = \emptyset$. Entonces los conjuntos $\tilde{A} = \prod_{i \neq j} E_i \times A, \tilde{B} = \prod_{i \neq j} E_i \times B$ son abiertos de $\prod_i E_i$ disjuntos y contienen a α y β respectivamente.

b. Si los espacios E_i son totalmente disconexo también lo será el producto. En efecto, sea $\alpha \in \prod_i E_i$ de modo que $\alpha = (a_i)$ y sea C su componente conexa en $\prod_i E_i$. Para cada $j \in I$ tenemos la proyección π_j sobre la componente j-ésima del producto, que es continua y sobreyectiva. De este modo, $\pi_j(C)$ es conexo para todo $j \in I$. Como hemos supuesto los E_i totalmente disconexos obtenemos que $\pi_j(C) = \{a_j\}$, pues $a_j = \pi_j(\alpha) \in \pi_j(C)$. Sea ahora $\beta = (b_i) \in C$, entonces para todo $i \in I$ es $b_i = \pi_i(\beta) = a_i$. Concluimos que $\beta = \alpha$.

Así mismo, gracias al *teorema de Tychonoff* sabemos que el producto de espacios topológicos compactos es compacto. Podemos concluir entonces que $\varprojlim X_i$ es un espacio de Hausdorff, totalmente disconexo y compacto pues hereda las dos primeras propiedades por ser subespacio de $\prod_i X_i$ y es compacto pues es un subconjunto cerrado de un compacto.

□

Es interesante ver la demostración de que el límite proyectivo es no vacío si los espacios X_i son de Hausdorff, compactos y no vacíos.

Lema 4.2.4. Sea $\{X_i, \varphi_{ij}\}$ un sistema proyectivo de espacios de Hausdorff compactos no vacíos sobre el conjunto dirigido parcialmente ordenado I. Entonces $\varprojlim X_i$ es no vacío. En particular, el límite proyectivo de un sistema proyectivo de conjuntos finitos no vacíos es no vacío.

Demostración. Para cada $j \in I$, definimos el subconjunto de $\prod_i X_i$ siguiente:

$$Y_j = \{(x_i) \in \prod_i X_i \mid \varphi_{jk}(x_j) = x_k \ \forall\ k \leq j\}.$$

Vamos a ver algunas propiedades de estos conjuntos:

a. Si es $j \leq j'$ entonces $Y_j \supset Y_j'$ gracias a la compatibilidad de las funciones φ...

b. Los conjuntos Y_j son no vacíos gracias al *axioma de elección.*

c. La propiedad anterior implica que la familia $\{Y_j \mid j \in I\}$ tiene la propiedad de intersección finita. En efecto, sean $j_1, \ldots, j_n \in I$ índices. Por inducción podemos obtener un índice $k \in I$ tal que $j_i \leq k$ para todo $i = 1, \ldots, n$. Entonces $Y_k \subset Y_{j_i}$ para todo $i = 1, \ldots, n$ y por ello $\cap_{i=1}^n Y_{j_i} \supset Y_k \neq \emptyset$.

d. Los conjuntos Y_j son cerrados. En efecto, sea $\alpha \in \prod_i X_i \setminus Y_j$ (si no existe hemos terminado). Como $\alpha \notin Y_j$ existe un índice $k_0 \leq j$ tal que $\varphi_{jk_0}(x_j) \neq x_{k_0}$. Sean U, V abiertos de X_{k_0} tales que $\varphi_{jk_0}(x_j) \in U, x_{k_0} \in V$ y $U \cap V = \emptyset$. Consideremos $U' = \varphi_{jk_0}^{-1}(U)$ abierto de X_j. Si tomamos el abierto
$$W = \prod_{i \neq j, k_0} X_i \times U' \times V$$
de $\prod_i X_i$ tenemos que $\alpha \in W$ pero $W \cap Y_j = \emptyset$. Concluimos que Y_j es cerrado para todo $j \in I$.

e. Por construcción, es inmediato que la intersección $\cap Y_j$ coincide con el límite proyectivo $\varprojlim X_i$.

Gracias a la compacidad del espacio $\prod_i X_i$ y a que la familia $\{Y_j\}_{j \in I}$ tiene la propiedad de intersección finita concluimos que $\cap Y_j = \varprojlim X_i$ es no vacío.

□

Por último veamos la noción de aplicación entre sistemas proyectivos. Sean $\{X_i, \varphi_{ij}, I\}, \{X_i', \varphi_{ij}', I\}$ dos sistemas proyectivos de grupos topológicos (o en cualquier otra categoría) sobre el mismo conjunto dirigido parcialmente ordenado I. Una aplicación de sistemas proyectivos

$$\Psi : \{X_i, \varphi_{ij}\} \to \{X_i', \varphi_{ij}'\}$$

es una colección de homomorfismos continuos $\psi_i X_i \to X_i'$ para cada $i \in I$ tales que si $i \leq j$ entonces el siguiente diagrama conmuta:

$$\begin{array}{ccc} X_j & \xrightarrow{\varphi_{ji}} & X_i \\ {\scriptstyle \psi_j}\downarrow & & \downarrow{\scriptstyle \psi_i} \\ X_j' & \xrightarrow{\varphi_{ji}'} & X_i' \end{array}.$$

Las aplicaciones ψ_i las llamaremos componentes de Ψ.

En términos de la teoría de categorías, una aplicación entre los sistemas proyectivos correspondientes a dos funtores $F : (I, \leq) \to \mathcal{C}, G : (I, \leq) \to \mathcal{C}$ es simplemente una transformación natural entre estos, siendo $\mathcal{C}$ una categoría prefijada. Vemos que podemos considerar la categoría de los funtores con salida $(I, \leq)$ y llegada $\mathcal{C}$, i.e. sistemas proyectivos, y con morfismos las transformaciones naturales entre estos, i.e. aplicaciones entre sistemas proyectivos.

Sean $\{X_i, \varphi_{ij}\}, \{X'_i, \varphi'_{ij}\}$ dos sistemas proyectivos sobre el mismo conjunto dirigido I, y consideremos sus correspondientes límites proyectivos $(X = \varprojlim X_i, \varphi_i), (X' = \varprojlim X'_i, \varphi'_i)$. Supongamos que tenemos una aplicación de sistemas proyectivos

$$\Psi : \{X_i, \varphi_{ij}\} \to \{X'_i, \varphi'_{ij}\}$$

con componentes ψ_i. Entonces la colección de aplicaciones compatibles

$$\psi_i \circ \varphi_i : X \to X'_i$$

induce un homomorfismo continuo de $X = \varprojlim X_i$ en $X' = \varprojlim X'_i$ que denotamos por $\varprojlim \Psi = \varprojlim \psi_i$.

Es claro que $\varprojlim$ es un funtor de la categoría de sistemas proyectivos en la categoría de grupos topológicos. Es sencillo comprobar que si las componentes de una aplicación entre sistemas proyectivos son inyectivas entonces el límite también sigue siendo inyectivo. Sin embargo, en general, si las componentes son sobreyectivas el límite no será sobreyectivo. Tenemos el siguiente resultado que nos indica cuándo si será el límite sobreyectivo:

Lema 4.2.5. Sea $\Psi : \{X_i, \varphi_{ij}, I\} \to \{X'_i, \varphi'_{ij}, I\}$ una aplicación entre sistemas proyectivos de grupos topológicos compactos de Hausdorff y supongamos que todas las componentes $\psi_i : X_i \to X'_i$ son sobreyectivas. Entonces

$$\varprojlim \Psi : \varprojlim X_i \to \varprojlim X'_i$$

también es sobreyectiva.

Demostración. Sea $(x'_i) \in \varprojlim X'_i$. Consideramos los subgrupos $\tilde{X}_i = \psi_i - 1(x'_i)$ con $i \in I$. Como $\tilde{X}_i$ es cerrado en el espacio compacto X_i, concluimos que $\tilde{X}_i$ es compacto para todo $i \in I$. Además, observar que $\varphi_{ij}(\tilde{X}_i) \subset \tilde{X}_j$ para $i \geq j$ pues

$$(\psi_j \varphi_{ij})(\psi_i^{-1}(x_i)) = (\varphi'_{ij}\psi_i)(\psi_i^{-1}(x_i)) \subset \{x_j\}.$$

Obtenemos, mediante restricciones, el sistema proyectivo $\{\tilde{X}_i, \varphi_{ij}\}$ de grupos topológicos compactos no vacíos. Gracias 4.2.4, $\varprojlim \tilde{X}_i \neq \emptyset$. Dado un elemento arbitrario $(x_i) \in \varprojlim \tilde{X}_i \subset \varprojlim X_i$ tenemos que $(\varprojlim \Psi)(x_i) = (x'_i)$.

□

Para acabar definimos la clase de espacios que más nos interesarán en lo que sigue:

Definición 4.2.6. Sea X un conjunto. Diremos que X es un **espacio profinito** si es isomorfo al límite proyectivo de un sistema proyectivo de conjuntos finitos no vacíos.

En la definición hemos definido espacio profinito en lugar de conjunto profinito, la razón es que todo conjunto obtenido como límite de un sistema proyectivo de conjuntos finitos no vacíos posee una topología canónica, aquella obtenida en el límite una vez considerados los conjuntos finitos espacios topológicos compactos de Hausdorff totalmente disconexos. Curiosamente, estas tres propiedades para un espacio topológico son suficientes para concluir que un espacio es profinito:

Teorema 4.2.7. Sea X un espacio topológico. Las siguientes condiciones son equivalentes:

1. X es un espacio profinito.
2. X es un espacio de Hausdorff, compacto y totalmente disconexo.
3. X es un espacio de Hausdorff compacto y su topología admite una base de conjuntos simultáneamente abiertos y cerrados.

Demostración. Ver [RZ10] *Teorema 1.1.12.*

□

4.2.2. Grupos Profinitos

Ya estamos en disposición de ver el concepto central de este capítulo, algunas de sus propiedades y ejemplos que serán importantes para la teoría local de cuerpos de clase.

Lema 4.2.8. Sea $G = \varprojlim G_i$, con $\{G_i, \varphi_{ij}\}$ un sistema proyectivo de grupos finitos y sean $\varphi_i : G \to G_i$ los homomorfismos de proyección. Entonces la familia $\{\texttt{Ker}(\varphi_i)\}_{i\in I}$ es un sistema fundamental de entornos abiertos del elemento neutro $e_G \in G$.

Demostración. Dotamos a los grupos finitos G_i con la topología discreta. Consideramos la familia de entornos del elemento neutro e de $\prod_{i\in I} G_i$ de la forma

$$\left(\prod_{i\neq i_1,\ldots,i_t} G_i\right) \times \{e_{i_1}\} \times \cdots \times \{e_{i_t}\},$$

para una colección finita de índices $i_1, \ldots, i_t \in I$. e_k denota al elemento neutro del grupo G_k. Como cada G_i posee la topología discreta, esta familia es un sistema fundamental de entornos del elemento

neutro e. Sea $i_0 \in I$ un índice tal que $i_0 \geq i_1, \ldots, i_t$. Entonces

$$G \cap \left[\left(\prod_{i \neq i_0} G_i \right) \times \{e_{i_0}\} \right] = G \cap \left[\left(\prod_{i \neq i_1, \ldots, i_t} G_i \right) \times \{e_{i_1}\} \times \cdots \times \{e_{i_t}\} \right]$$

gracias a la definición de G. Por tanto la familia de entornos de e_G en G de la forma

$$G \cap \left[\left(\prod_{i \neq i_0} G_i \right) \times \{e_{i_0}\} \right]$$

es un sistema fundamental de entornos abiertos de e_G. Es inmediata la comprobación de la siguiente igualdad:

$$G \cap \left[\left(\prod_{i \neq i_0} G_i \right) \times \{e_{i_0}\} \right] = \texttt{Ker}(\varphi_i).$$

□

Un resultado muy útil que se obtiene gracias a la compacidad es el siguiente:

Lema 4.2.9. En un grupo topológico compacto G, un subgrupo U es abierto si y sólo si U es cerrado y tiene índice finito en G.

Demostración. $\Rightarrow$ Sea $G/U \subset G$ un conjunto de representantes de las clases a izquierda del subgrupo U. Obtenemos el siguiente recubrimiento por abiertos de G

$$G = \coprod_{g \in G/U} gU.$$

Como estos abiertos son disjuntos y G es compacto concluimos que el conjunto G/U es finito, es decir, $(G : U) < \infty$. Para ver que es cerrado, sea $a \in G \setminus U$, en particular $a \neq e$. El conjunto aU es abierto pues $x \mapsto ex$ es un homeomorfismo y además $aU \cap U = aU \cap eU = \emptyset$ luego $aU \subset G \setminus U$ prueba que U es cerrado. Para esta segunda parte no ha sido necesaria la hipótesis de compacidad.

$\Leftarrow$ Para esta implicación tampoco usaremos la compacidad de G. Sean $g_0 = e, g_1, \ldots, g_n$ tales que $G = \coprod_{i=0}^{n} g_i U$. Supuesto que U es cerrado y usando de nuevo que las traslaciones son homeomorfismos obtenemos que $g_i U$ es cerrado para todo i. Concluimos que $G \setminus U = \coprod_{i=1}^{n} g_i G$ es una unión finita de cerrados, luego U es abierto.

□

Definición 4.2.10. Sea $\{G_i, \varphi_{ij}\}$ un sistema proyectivo de grupos finitos dotados de la topología discreta. Diremos que el límite proyectivo $\varprojlim G_i$ es un **grupo profinito**.

Claramente todo grupo profinito es un grupo topológico de Hausdorff, compacto y totalmente disconexo. El siguiente resultado que nos da diversas caracterizaciones de los grupos profinitos:

Proposición 4.2.11. Las siguientes condiciones sobre un grupo topológico compacto G son equivalentes:

1. G es un grupo profinito,
2. G es compacto Hausdorff totalmente disconexo y para cada subgrupo normal abierto U de G, el cociente G/U es finito.
3. G es compacto y el elemento neutro e de G admite un sistema fundamental $\mathcal{U}$ de entornos abiertos U tales que $\cap_{U\in\mathcal{U}}U = \{e\}$ y cada U es un subgrupo normal abierto de índice finito en G.
4. El elemento neutro $e \in G$ admite un sistema fundamental $\mathcal{U}$ de entornos abiertos U tal que cada U es un subgrupo normal abierto de índice finito y

$$G = \varprojlim_{U\in\mathcal{U}} G/U.$$

Demostración. Ver [RZ10] *Teorema 2.1.3.*

□

Ejemplo 4.2.12. Los grupos de Galois $\mathtt{Gal}(L|k)$ son grupos profinitos como vimos en 4.1.1. Si $K \supset k$ varía en el conjunto de las subextensiones finitas de Galois de $L \supset k$, entonces por definición de la topología de Krull, $\mathtt{Gal}(L|K)$ varía en el conjunto de los subgrupos abiertos normales de $\mathtt{Gal}(L|k)$. Gracias al isomorfismo $\mathtt{Gal}(K|k) \simeq \mathtt{Gal}(L|k)/\mathtt{Gal}(L|K)$ y a 4.2.11 obtenems el grupo de Galois $\mathtt{Gal}(L|k)$ como el límite proyectivo $\mathtt{Gal}(L|k) \simeq \varprojlim \mathtt{Gal}(K|k)$ de los grupos de Galois finitos $\mathtt{Gal}(K|k)$.

Esto explica que en nuestras demostraciones para la topología de Krull hicieramos uso del espacio $\prod \mathtt{Gal}(K|k)$.

Ejemplo 4.2.13. Sea $\mathcal{O}$ un anillo de valoración discreta asociado a un cuerpo local k de característica 0, con ideal maximal $\mathfrak{p}$. Los ideales $\mathfrak{p}^n, n \in \mathbb{N}$ forman una base de entornos de 0 en $\mathcal{O}$. $\mathcal{O}$ es Hausdorff y compacto, por 4.2.11 sabemos que $\mathcal{O}$ es un anillo profinito (observar que hemos cambiado subgrupos por ideales). Los anillos $\mathcal{O}/\mathfrak{p}^n, n \in \mathbb{N}$ son finitos y tenemos un isomorfismo topológico

$$\mathcal{O} \simeq \varprojlim \mathcal{O}/\mathfrak{p}^n.$$

Este resultado ya lo estudiamos en el capítulo 1.

Así mismo, el grupo de unidades $\mathcal{O}^\times$ es compacto y Hausdorff (es subgrupo cerrado de $\mathcal{O}$) y los subgrupos $U^{(n)}, n \in \mathbb{N}$ forman una base de entornos de 1 en $\mathcal{O}^\times$. De nuevo usando 4.2.11 es $\mathcal{O}^\times \simeq \varprojlim \mathcal{O}^\times/U^{(n)}$ un grupo profinito.

Ejemplo 4.2.14. En los números naturales $\mathbb{N}$ siempre tenemos la relación de orden usual, sin embargo, podemos definir una relación de orden de naturaleza más aritmética como sigue: *Dados $n, m \in \mathbb{N}$ diremos que $n \leq' m$ si y sólo si n divide a m.* Es claro que esta relación de orden junto con la existencia del máximo común divisor hacen que $(\mathbb{Z}, \leq')$ sea un conjunto dirigido parcialmente ordenado. De hecho, este conjunto dirigido es "isomorfo" (noción que no hemos definido pero está clara) al conjunto dirigido formado por los subgrupos no nulos de $\mathbb{Z}$ ordenados por inclusión invertida, i.e. contención. Si a cada natural n le asignamos el anillo $\mathbb{Z}/\mathbb{Z}n$ y al par $n \leq' m$ le asignamos el morfismo natural $\mathbb{Z}/\mathbb{Z}m \to \mathbb{Z}/\mathbb{Z}n$ dado por $x + \mathbb{Z}m \mapsto x + \mathbb{Z}n$ obtenemos un sistema proyectivo. El límite proyectivo

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/\mathbb{Z}n$$

se denomina el anillo de los enteros profinitos. Es interesante observar que el *Teorema Chino del Resto* podemos usarlo para conseguir una descomposición de $\widehat{\mathbb{Z}}$ como el producto de los anillos de enteros p-ádicos $\mathbb{Z}_p$:

Para cada primo p consideramos las proyecciones continuas $\widehat{\mathbb{Z}} \to \mathbb{Z}/\mathbb{Z}p^n$. Todas estas aplicaciones son compatibles entre sí y pasando al límite obtenemos un homomorfismo continuo $\widehat{\mathbb{Z}} \to \mathbb{Z}_p$. Conseguimos así un homomorfismo continuo $f : \widehat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p$. Veamos que f es un isomorfismo:

1. *Sobreyectiva:* Será suficiente probar que $f(\widehat{\mathbb{Z}})$ es denso en $\prod_p \mathbb{Z}_p$ pues $\widehat{\mathbb{Z}}$ es compacto luego su imagen es compacta y por ello cerrada. Un abierto básico de $\prod_p \mathbb{Z}_p$ es de la forma:

$$U = (x_1 + \mathbb{Z}_{p_1} p_1^{n_1}) \times \cdots \times (x_r + \mathbb{Z}_{p_r} p_r^{n_r}) \times \prod_{q \neq p_i} \mathbb{Z}_q,$$

y para demostrar la densidad de la imagen de f es suficiente demostrar que las composiciones

$$\widehat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p \to \mathbb{Z}/\mathbb{Z}p_1^{n_1} \times \cdots \times \mathbb{Z}/\mathbb{Z}p_r^{n_r}$$

son sobreyectivas. Por el teorema Chino del Resto tenemos los diagramas conmutativos siguientes:

$$\begin{array}{ccc} \widehat{\mathbb{Z}} & \longrightarrow & \prod_p \mathbb{Z}_p \\ \downarrow & & \downarrow \\ \mathbb{Z}/\mathbb{Z}m & \longrightarrow & \mathbb{Z}/\mathbb{Z}p_1^{n_1} \times \cdots \times \mathbb{Z}/\mathbb{Z}p_r^{n_r} \end{array}$$

con $m = p_1^{n_1} \cdots p_r^{n_r}$. Como la proyección $\widehat{\mathbb{Z}} \to \mathbb{Z}/\mathbb{Z}m$ es sobreyectiva, concluimos que la imagen de f es densa y por ello f es sobreyectiva.

2. *Inyectiva:* Sea $x \in \widehat{\mathbb{Z}} \setminus \{0\}$. Por definición, existe $m \in \mathbb{N}$ tal que la imagen de x por la proyección $\widehat{\mathbb{Z}} \to \mathbb{Z}/\mathbb{Z}m$ es distinta de cero. Usando el diagrama anterior para una factorización $m = p_1^{n_1} \cdots p_r^{n_r}$ concluimos que la imagen de x por f es no trivial.

Notar que esta descomposición demuestra que $\widehat{\mathbb{Z}}$ no es un dominio de integridad. Así mismo, vemos que $\mathbb{Z}$ es denso en $\widehat{\mathbb{Z}}$, identificando $\mathbb{Z}$ con su imagen por el homomorfismo natural inyectivo obtenido de considerar las aplicaciones naturales $\mathbb{Z} \to \mathbb{Z}/\mathbb{Z}n$ con $n \in \mathbb{N}$. Los subgrupos $\widehat{\mathbb{Z}}n$ forman un sistema de entornos del 0 y como el núcleo de la proyección $\widehat{\mathbb{Z}} \to \mathbb{Z}/\mathbb{Z}n$ es $\widehat{\mathbb{Z}}n$, tenemos los isomorfismos $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}n \simeq \mathbb{Z}/\mathbb{Z}n$. Además, bajo el isomorfismo $\widehat{\mathbb{Z}} \simeq \prod \mathbb{Z}_p$, $\mathbb{Z}$ corresponde a la diagonal del producto. Por último veamos que los subgrupos abiertos de $\widehat{\mathbb{Z}}$ son los subgrupos $\widehat{\mathbb{Z}}n$. Para ver que todo subgrupo $\widehat{\mathbb{Z}}n$ es abierto basta tener en cuenta que, como hemos comentado, $\widehat{\mathbb{Z}}n$ es el núcleo de la proyección $\widehat{\mathbb{Z}} \to \mathbb{Z}/\mathbb{Z}n$ y por ello es un subgrupo abierto. Para el recíproco, si U es un subgrupo abierto, tenemos que el conjunto $U \cap \mathbb{Z}$ es denso en U pues $\mathbb{Z}$ es denso en $\widehat{\mathbb{Z}}$. Ahora bien, la intersección $U \cap \mathbb{Z} = \mathbb{Z}n$ para cierto $n \in \mathbb{N}$ pues es un subgrupo de $\mathbb{Z}$. Si denotamos por $\overline{\mathbb{Z}n}^U$ a la clausura de $\mathbb{Z}n$ en U, entonces $U = \overline{\mathbb{Z}n}^U = \overline{\mathbb{Z}n} \cap U$. Claramente $\overline{\mathbb{Z}n} = \widehat{\mathbb{Z}}n$ y por tanto $U \subset \widehat{Z}n$. Como $\mathbb{Z}n \subset U \subset \widehat{Z}n$ y U es cerrado por ser $\widehat{\mathbb{Z}}$ compacto, concluimos que $U = \widehat{\mathbb{Z}}n$.

En este ejemplo hemos considerado la familia de todos los subgrupos normales de índice finito de un grupo dado y obtenido el límite proyectivo correspondiente al sistema proyectivo formado por estos subgrupos ordenados por inclusión inversa. Este proceso es lo que llamamos **compleción profinita** de un grupo y el grupo obtenido es el **completado profinito** del grupo. Es importante resaltar que si el grupo de partida posee una topología la familia que se elige para hacer la compleción es la familia de subgrupos normales *abiertos* de índice finito y en este caso se dice que estamos haciendo la **compleción profinita** de un grupo *topológico.* Si por el contexto no está claro que compleción estamos realizando se indicará explícitamente.

Ejemplo 4.2.15. Consideremos un cuerpo finito $\mathbb{F}_q$ con $q = p^n$ elementos. Para cada $m \in \mathbb{N}$ tenemos los isomorfismos

$$\begin{array}{rcl} \mathtt{Gal}\left(\mathbb{F}_{q^m}|\mathbb{F}_q\right) & \xrightarrow{\sim} & \mathbb{Z}/\mathbb{Z}m, \\ \sigma_m : x \mapsto x^q & \longmapsto & 1 + \mathbb{Z}m. \end{array}$$

Como la clausura algebraica de $\mathbb{F}_q$ es el límite inductivo $\bigcup_{m\in\mathbb{N}} \mathbb{F}_{q^m}$, tenemos que el grupo de Galois $\mathtt{Gal}\left(\overline{\mathbb{F}_q}|\mathbb{F}_q\right)$ coincide con el límite proyectivo $\varprojlim \mathtt{Gal}\left(\mathbb{F}_{q^m}|\mathbb{F}_q\right) \simeq \varprojlim \mathbb{Z}/\mathbb{Z}m = \widehat{\mathbb{Z}}$. En definitiva, concluimos que

$$\mathtt{Gal}\left(\overline{\mathbb{F}_q}|\mathbb{F}_q\right) \simeq \widehat{\mathbb{Z}}.$$

Bajo este isomorfismo continuo, el automorfismo de Frobenius $\sigma : x \mapsto x^q$ se corresponde con el $1 \in \mathbb{Z} \subset \widehat{\mathbb{Z}}$, luego el subgrupo cíclico generado por σ es denso en $\mathtt{Gal}\left(\overline{\mathbb{F}_q}|\mathbb{F}_q\right)$.

Definición 4.2.16. Decimos que un grupo profinito G es **procíclico** si está generado topológicamente por un elemento $g \in G$, es decir, la clausura del subgrupo cíclico $\langle g \rangle$ coincide con G. En este caso, decimos que g es un **generador topológico** del grupo G.

Hasta ahora hemos visto dos ejemplos de grupos procíclicos, los enteros p-ádicos $\mathbb{Z}_p$ y los enteros profinitos $\widehat{\mathbb{Z}}$ ya que en ambos casos $\mathbb{Z} = \langle 1 \rangle$ es un subgrupo denso. Es sencillo probar que todo grupo procíclico es el límite proyectivo de un sistema de grupos cíclicos finitos, en particular todo grupo procíclico es abeliano. Vimos que los subgrupos abiertos de $\widehat{\mathbb{Z}}$ son todos de la forma $\widehat{\mathbb{Z}}n$, este resultado es cierto en general para grupos procíclicos:

Si consideramos el subgrupo G^n formado por todas las potencias n-ésimas de los elementos de G (recordar que G es abeliano por ser procíclico), entonces G^n es cerrado pues es la imagen de G por el homomorfismo continuo $x \in G \mapsto x^n \in G$. Si dotamos a G/G^n con la topología cociente (que hace que G/G^n sea un grupo profinito), tenemos el homomorfismo sobreyectivo continuo $\pi : G \to G/G^n$ y es $G/G^n = \pi(G) = \pi\left(\overline{\langle g \rangle}\right) \subset \overline{\pi(\langle g \rangle)} = \overline{\langle gG^n \rangle}$, de modo que $\langle gG^n \rangle$ es un subgrupo denso de G/G^n. Como G/G^n es Hausdorff y el conjunto $\langle gG^n \rangle$ es finito, debe ser cerrado y por ello $G/G^n = \langle gG^n \rangle$, es decir, el grupo G/G^n es finito y $(G : G^n) = n$. Como G es compacto, esto prueba que G^n es abierto. Recíprocamente, sea H un subgrupo abierto de G de índice n de modo que $G^n \subset H \subset G$ y por ello $n = (G : H) \leq (G : G^n) = n$, es decir $(H : G^n) = 1$ luego $H = G^n$.

Por último, comentar que todo grupo procíclico es un cociente del grupo $\widehat{\mathbb{Z}}$ ya que si $G = \overline{\langle g \rangle}$ entonces para cada n tenemos el homomorfismo sobreyectivo

$$\begin{array}{ccc} \mathbb{Z}/\mathbb{Z}n & \longrightarrow & G/G^n, \\ 1 + \mathbb{Z}n & \longmapsto & gG^n. \end{array}$$

Pasando al límite y usando que la sobreyectividad se preserva cuando los sistemas profinitos son de espacios compactos, obtenemos un homomorfismo sobreyectivo $\widehat{\mathbb{Z}} \to G$, pues $\varprojlim G/G^n$ es la compleción profinita topológica de G.

4.3. Teoría de Galois Infinita

Antes de comenzar con el resultado principal de la sección veamos el siguiente lema:

Lema 4.3.1. Sea $L \supset k$ una extensión de Galois con grupo de Galois G.

1. Sea K una subextensión de $L \supset k$. Entonces $L \supset K$ es una extensión de Galois, el grupo de Galois $\mathtt{Gal}(L|K)$ es cerrado en G y $L^{\mathtt{Gal}(L|K)} = K$.

2. Para todo subgrupo H de G, $\mathtt{Gal}(L|L^H)$ es la clausura de H en G.

Demostración. 1. Es conocido que $L \supset K$ es de Galois. Tenemos la igualdad siguiente:

$$\texttt{Gal}(L|K) = \{\sigma \in G \mid \sigma\alpha = \alpha \ \forall \ \alpha \in K\} = \bigcap_{\alpha \in K} \texttt{Gal}(L|k(\alpha)),$$

pero el grupo $\texttt{Gal}(L|k(\alpha))$ es abierto pues contiene a $\texttt{Gal}(L|F)$ con F la clausura normal de $k(\alpha)$ en L (gracias a la homogeneidad de los grupos topológicos se demuestra que es abierto). En particular, $\texttt{Gal}(L|k(\alpha))$ es cerrado pues G es compacto. Concluimos que el conjunto $\texttt{Gal}(L|K)$ es cerrado. Por último, es claro que $K \subset L^{\texttt{Gal}(L|K)}$ y para el recíproco tomamos $\alpha \in L$ tal que $\sigma\alpha = \alpha$ para todo $\sigma \in \texttt{Gal}(L|K)$. Consideramos la subextensión $L \supset K(\alpha) \supset K$. Si es F la clausura normal de $K(\alpha)$ en L, tenemos que el homomorfismo de restricción $\texttt{Gal}(L|K) \to \texttt{Gal}(F|K)$ es sobreyectiva pues $F \supset K$ es una extensión finita de Galois de K. Concluimos que para todo $\tau \in \texttt{Gal}(F|K)$ es $\tau\alpha = \alpha$ pues existe $\sigma \in \texttt{Gal}(L|K)$ verificando $\sigma_{|F} = \tau$, esto implica que $\alpha \in K$ gracias a la teoría de Galois de extensiones finitas.

2. Por lo anterior sabemos que $\texttt{Gal}(L|L^H)$ es un subgrupo cerrado. Además este subgrupo contiene a H y por ello debe contener también a su clausura. Para la otra inclusión, sea $\sigma \in G \setminus \overline{H}$ y veamos que σ no deja invariante a algún elemento de L^H. Como σ no está en la clausura de H sabemos que $\sigma\texttt{Gal}(L|K) \cap H = \emptyset$ para alguna subextensión $L \supset K \supset k$ finita de Galois. Si consideramos el homomorfismo sobreyectivo de restricción $\varphi : G \to \texttt{Gal}(K|k)$ entonces $\sigma_{|E} \notin \varphi(H)$ pues en caso contrario existiría $\tau \in H$ tal que $\tau_{|E} = \sigma_{|E}$, es decir, $\tau \in \sigma\texttt{Gal}(L|K) \cap H$. Por teoría finita de Galois, σ mueve algún elemento de $K^{\varphi(H)} \subset L^H$.

□

Podemos enunciar el teorema de correspondencia de Galois para extensiones infinitas:

Teorema 4.3.2. Sea $L \supset k$ una extensión de Galois con grupo de Galois G. Las aplicaciones

$$\begin{array}{ccccccc} \{G:1\} & \longrightarrow & \{L:k\} & \quad & \{L:k\} & \longrightarrow & \{G:1\} \\ H & \longmapsto & L^H & & K & \longmapsto & \texttt{Gal}(L|K) \end{array}$$

son biyecciones una inversa de la otra entre los retículos de subextensiones de $L \subset k$ 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 $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$, $\texttt{Gal}(L|\sigma K) = \sigma\texttt{Gal}(L|K)\sigma^{-1}$.

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 $\texttt{Gal}(L^H|k) \simeq G/H$.

Demostración. Tenemos que probar que las aplicaciones $H \mapsto L^H, K \mapsto \texttt{Gal}(L|K)$ son inversas una de la otra. Sea H un subgrupo cerrado de G. Entonces la extensión $L \supset L^H$ es de Galois y su grupo de Galois es $\texttt{Gal}(L|L^H) = H$ pues H es cerrado (4.3.1).

Por otro lado, si K es una subextensión intermedia, entonces $\texttt{Gal}(L|K)$ es un subgrupo cerrado de G y $L^{\texttt{Gal}(L|K)} = K$ gracias a 4.3.1.

Veamos las otras propiedades:

1. Es inmediato que si tenemos la contención de subgrupos cerrados $H_1 \supset H_2$ entonces $L^{H_1} \subset L^{H_2}$ pues los elementos de L fijos bajo la acción de todos los elementos de H_1 también serán fijos bajo la acción del subgrupo H_2. Así mismo, esta última inclusión implica que $\texttt{Gal}(L|L^{H_1}) \supset \texttt{Gal}(L|L^{H_2})$ pues un elemento que fije a todos los elementos de L^{H_2} fijará todos los elementos del subcuerpo L^{H_1}. Ahora bien, como H_1, H_2 son subgrupos cerrados de G, concluimos que la última igualdad es equivalente a $H_1 \supset H_2$. En conclusión, hemos obtenido la equivalencia $H_1 \supset H_2 \Leftrightarrow L^{H_1} \subset L^{H_2}$.

2. Si H es un subgrupo abierto existe cierta extensión finita de Galois $K \supset k$ lo suficientemente grande de modo que $\texttt{Gal}(L|K) \subset H$. Como G es un grupo topológico compacto sabemos que H también es cerrado y por ello $H = \texttt{Gal}(L|L^H)$. De la inclusión $\texttt{Gal}(L|K) \subset \texttt{Gal}(L|L^H)$ deducimos que $L^H \subset K$ y esto demuestra que la extensión $k \subset L^H$ es finita.

   Recíprocamente, si tenemos una subextensión finita $L \supset K \supset k$ y consideramos la clausura normal de K en L que denotamos por F, entonces $\texttt{Gal}(L|F) \subset \texttt{Gal}(L|K)$ lo que demuestra que $\texttt{Gal}(L|K)$ es abierto pues $F \supset k$ es finita debido a que $K \supset k$ lo es.

   Para concluir que $(G : H) = [L^H : L]$ razonamos como sigue. Consideramos la aplicación entre *conjuntos*

$$\begin{array}{ccc} G/H & \longrightarrow & \texttt{Hom}_k(L^H, L), \\ \sigma H & \longmapsto & \sigma_{|L^H}, \end{array}$$

   con G/H el conjunto de clases de equivalencia a derecha de H en G. La aplicación está bien definida pues si $\sigma H = \tau H$ entonces $\tau^{-1}\sigma \in H$ y para todo $\alpha \in H$ es $\sigma\alpha = \tau\alpha$, es decir, $\sigma_{|L^H} = \tau_{|L^H}$. De hecho estas condiciones son equivalentes lo que demuestra que la aplicación es inyectiva. Así mismo la aplicación es sobreyectiva pues todo k-homomorfismo $f : L^H \to L$ (necesariamente inyectivo) admite una extensión a un k-automorfismo de L $\tilde{f} : L \to L$ y deducimos que f es la imagen de $\tilde{f}H$. Por último, sabiendo que la extensión $L^H \supset k$ es finita, un resultado de la teoría de cuerpos (ver [Hun80] *Capítulo V, Propoposición 6.12*) nos dice que

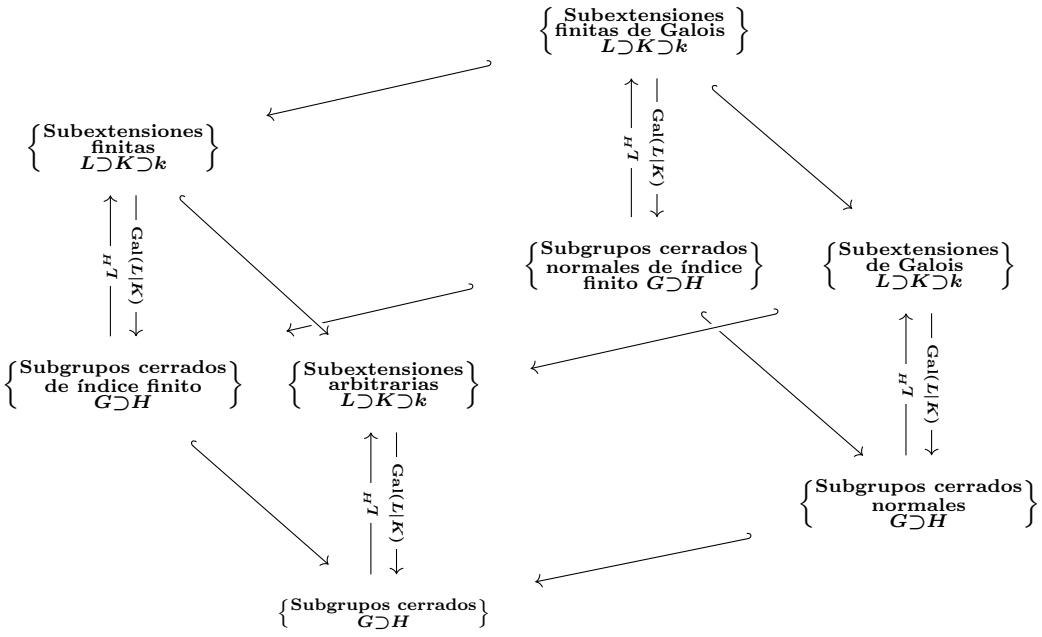
el cardinal de $\mathtt{Hom}_k(L^H, L)$ coincide con el grado de la extensión $L^H \supset k$ y gracias a nuestra biyección concluimos que $(G : H) = [L^H : k]$.

3. Dado $\tau \in G$ y $\alpha \in L$, se cumple que $\tau\alpha = \alpha$ si y sólo si $(\sigma\tau\sigma^{-1})(\sigma\alpha) = \sigma\alpha$. Por tanto $\mathtt{Gal}(L|\sigma K) = \sigma\mathtt{Gal}(L|K)\sigma^{-1}$ y por ello $\sigma\mathtt{Gal}(L|M)\sigma^{-1}$ corresponde a la subextensión σK.

4. Sea K un subextensión de $L \supset k$ asociada al grupo H. H es normal si y sólo si $\sigma H\sigma^{-1} = H$ para todo $\sigma \in G$. Ahora bien, por el apartado anterior, $\sigma H\sigma^{-1}$ corresponde a la subextensión σK y concluimos que debe ser $\sigma K = K$ para todo $\sigma \in G$. Se sigue que $K \supset k$ es una extensión de Galois. Como el homomorfismo de restricción $\mathtt{Gal}(L|k) \to \mathtt{Gal}(K|k)$ es sobreyectivo y su núcleo es $\mathtt{Gal}(L|K)$, obtenemos la última parte del enunciado.

□

Este resultado podemos resumirlo con el siguiente esquema:



Los siguientes resultados serán útiles:

Proposición 4.3.3. 1. Sea $L \supset k$ una extensión de Galois, sea $K \supset k$ una extensión arbitraria. 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. Entonces $L_1L_2 \supset k$ es de Galois. Si denotamos por G al grupo de Galois de la extensión $L_1L_2 \supset k$, entonces la siguiente aplicación es un homomorfismo continuo de grupos topológicos inyectivo:

$$\begin{array}{ccc} G & \longrightarrow & G_1 \times G_2, \\ \sigma & \longmapsto & (\sigma_{|L_1}, \sigma_{|L_2}). \end{array}$$

Si $L_1 \cap L_2 = k$ entonces es un isomorfismos de grupos.

Demostración. 1. Ver [Lan02] *Teorema 1.12, Capítulo IV.*

2. Ver [Lan02] *Teorema 1.14, Capítulo IV.*

□

En particular, gracias al segundo apartado sabemos que la composición de dos extensiones abelianas de k (extensiones de Galois con grupo de Galois abeliano) de nuevo es abeliana.

4.3.1. Grupos de Weil

Por lo general, los grupos de Galois de extensiones infinitas son demasiado grandes y hay automorfismos de los que no podemos saber demasiado. Por ejemplo, si k es un cuerpo local no arquimediano y $k^{\mathtt{ur}}$ es su extensión no ramificada maximal, sabemos que la extensión $k^{\mathtt{ur}} \supset k$ es una extensión de Galois con grupo de Galois isomorfo a $\hat{\mathbb{Z}}$, siendo un generador topológico el elemento de Frobenius φ_k. No es fácil describir elementos de $\mathtt{Gal}(k^{\mathtt{ur}}|k) \setminus \langle \varphi_k \rangle$. En este caso aún podríamos razonar usando el isomorfismo $\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$ y describir elementos que no están en $\mathbb{Z}$. Si consideramos una extensión de Galois $L \supset k$, de modo que $L \supset k^{\mathtt{ur}}$, es aún más dificil describir los elementos del grupo de Galois. Por esta razón, a menudo nos concentramos en un subgrupo denso y que suele ser suficiente para obtener información del grupo de Galois. En esta subsección vamos a definir este subgrupo, el llamado *grupo de Weil*, y ver sus propiedades elementales.

Supongamos que tenemos $L \supset k$ una extensión de Galois, y sea $L_0 = L \cap k^{\mathtt{ur}}$ la extensión no ramificada maximal de k en L. Como k es un cuerpo local tenemos que $L_0 \supset k$ es una extensión de Galois. Consideremos la sobreyección

$$\mathtt{Gal}(L|k) \xrightarrow{\mathtt{res}} \mathtt{Gal}(L_0|k).$$

Si consideramos el elemento de Frobenius de k, denotado φ_k, tenemos que el grupo $\mathtt{Gal}(L_0|k)$ está generado topológicamente por $(\varphi_k)_{|L_0}$. Hacemos la siguiente definición:

Definición 4.3.4. Dada una extensión de Galois $L \supset k$ consideramos $L_0 = L \cap k^{\mathtt{ur}}$ la subextensión no ramificada maximal de k en L. Se define el **grupo de Weil** de la extensión $L \supset k$ como

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

Obviamente el grupo de Weil es un subgrupo del grupo de Galois pues es la preimagen por un homomorfismo de un subgrupo. Hagamos algunas observaciones más sobre esta definición:

a. El grupo de Weil $\mathtt{W}(L|k)$ es un subgrupo normal de $\mathtt{Gal}(L|k)$. En efecto, dado $\sigma \in \mathtt{W}(L|k)$ y $\tau \in \mathtt{Gal}(L|k)$ tenemos que $(\tau^{-1}\sigma\tau)_{|L_0} = \tau^{-1}_{|\sigma(\tau(L_0))}\sigma_{|\tau(L_0)}\tau_{|L_0} = \tau^{-1}_{|L_0}\sigma_{|L_0}\tau_{|L_0} \in \tau^{-1}_{|L_0}\langle(\varphi_k)_{|L_0}\rangle\tau_{|L_0}$ usando que la extensión $L_0 \supset k$ es normal. Como el grupo $\mathtt{Gal}(L_0|L)$ es procíclico, deducimos que es abeliano y por ello $\tau^{-1}_{|L_0}\langle(\varphi_k)_{|L_0}\rangle\tau_{|L_0} = \langle(\varphi_k)_{|L_0}\rangle$.

b. Si la extensión $L \supset k$ es finita, entonces $L_0 \supset k$ es una extensión no ramificada finita y en este caso $\mathtt{Gal}(L_0|k) = \langle\varphi_{|L_0}\rangle$ de modo que $\mathtt{W}(L|k) = \mathtt{Gal}(L|k)$. Para las extensiones finitas la definición del grupo de Weil es superflua.

c. Si $L = L_0 = k^{\mathtt{ur}}$ entonces $\mathtt{W}(k^{\mathtt{ur}}|k) = \langle\varphi_k\rangle$. Se ve que en este caso el grupo de Weil es denso en $\mathtt{Gal}(L|k)$. De forma más general, si la extensión $L = L_0 \supset k$ es no ramificada e infinita entonces $\mathtt{W}(L|k) = \langle(\varphi_k)_{|L}\rangle$, de nuevo subgrupo denso de $\mathtt{Gal}(L|k) = \overline{\langle(\varphi_k)_{|L}\rangle}$.

d. El grupo de Weil $\mathtt{W}(L|k)$ se puede ver dentro de la siguiente sucesión exacta de grupos:

$$\{\mathtt{id}\} \to \mathtt{Gal}(L|L_0) \to \mathtt{W}(L|k) \to \mathtt{W}(L_0|k) \to \{\mathtt{id}\}.$$

Observar que $\mathtt{W}(L_0|L) = \langle(\varphi_k)_{|L_0}\rangle$ y $\mathtt{Gal}(L|L_0)$ es el grupo de inercia de la extensión.

e. Nosotros no necesitaremos una topología en el grupo de Weil, será suficiente entenderlo como subgrupo. Cuando se "topologiza" se hace exigiendo que el grupo de inercia $\mathtt{Gal}(L|L_0)$, con la topología heredada de $\mathtt{Gal}(L|k)$, sea un subgrupo abierto de $\mathtt{W}(L|k)$. En este caso, si $\sigma_0 \in \mathtt{W}(L|k)$ es tal que $\sigma_{0|L_0} = (\varphi_k)_{|L_0}$, se prueba que la aplicación $\mathtt{Gal}(L|L_0) \times \mathtt{W}(L_0|L) \to \mathtt{W}(L|k)$ que lleva $(\alpha, (\varphi_k)^n_{|L_0}) \to \alpha\circ\sigma_0^n$ es un homeomorfismo y $\mathtt{W}(L|k)$ con esta topología es un espacio topológico de Hausdorff. Es importante resaltar que la topología de $\mathtt{W}(L|k)$ definida como antes no coincide con la topología inducida de $\mathtt{Gal}(L|k)$ a menos que $[L : k] < \infty$. Lo mejor que se tiene es que la aplicación $\mathtt{W}(L|k) \hookrightarrow \mathtt{Gal}(L|k)$ es continua y con imagen densa. Si hubiésemos dotado al grupo de Weil $\mathtt{W}(L|k)$ con la topología de subespacio entonces el grupo de inercia $\mathtt{Gal}(L|L_0) \subset \mathtt{W}(L|k)$ no sería abierto. En conclusión, sobre el grupo de Weil se define una topología más fina que la de ser subespacio. El grupo de Weil tiene algunas propiedades más (ver `http://virtualmath1.stanford.edu/~conrad/249BW09Page/handouts/profinite.pdf`). Nosotros nos quedaremos

con que es un subgrupo más sencillo que el grupo de Galois pero que lo aproxima en un sentido topológico. Una de esas otras propiedades es precisamente que esta noción de aproximación se tiene, no sólo desde un punto de vista topológico, si no estructural.

Como se ha dicho en el apartado **e.** de las observaciones anteriores, una propiedad que nos interesa del grupo de Weil es que es denso en $\mathtt{Gal}(L|k)$. Para demostrarlo necesitamos un lema sobre grupos topológicos:

Lema 4.3.5. Sea G un grupo topológico y H un subgrupo cerrado de G. Dotemos el conjunto de clases a izquierda G/H con la topología cociente. Entonces la aplicación canónica $p : G \to G/H$ es una aplicación cociente y además es abierta.

Demostración. La aplicación p es una aplicación cociente por definición de la topología cociente. Veamos que es abierta. Sea $U \subset G$ un abierto. Es suficiente probar que el conjunto $p^{-1}(p(U))$ es abierto. Para ello, observar

$$p^{-1}(p(U)) = \cup_{u\in U} uH = \{uh \mid u \in U, h \in H\} = \cup_{h\in H} Uh.$$

Como los conjuntos Uh son abiertos, pues son trasladados de un abierto, deducimos que $p^{-1}(p(U))$ es abierto y por ello $p(U)$ es abierto.

□

Proposición 4.3.6. El grupo de Weil $\mathtt{W}(L|k)$ es denso en $\mathtt{Gal}(L|k)$.

Demostración. Sea $\sigma \in \mathtt{Gal}(L|k)$ y sea $L \supset K \supset k$ una subextensión de Galois finita sobre k. Consideramos el entorno abierto de σ dado por $\sigma\mathtt{Gal}(L|K) := \sigma U$ Veamos que $\mathtt{W}(L|k)$ corta a σU. Sabemos que $\mathtt{Gal}(L_0|k) \simeq \mathtt{Gal}(L|k)/\mathtt{Gal}(L|L_0)$, este último grupo con la topología cociente, de modo que la aplicación canónica $\mathtt{res} : \mathtt{Gal}(L|k) \to \mathtt{Gal}(L_0|k)$ es un aplicación cociente y gracias a 4.3.5 también es una aplicación abierta. De este modo $\mathtt{res}(U)$ es un abierto del grupo procíclico $\mathtt{Gal}(L_0|k) = \overline{\langle(\varphi_k)_{|L_0}\rangle}$ y por densidad el conjunto $\sigma_{|L_0}\mathtt{res}(U) = \mathtt{res}(\sigma U)$ corta al subgrupo $\langle(\varphi_k)_{|L_0}\rangle$. Sea $m \in \mathbb{Z}$ de modo que $(\sigma u)_{|L_0} = (\varphi_k)^m_{|L_0}$ con $u \in U$. Por definición, $\sigma u \in \mathtt{res}^{-1}(\langle(\varphi_k)_{|L_0}\rangle) = \mathtt{W}(L|k)$.

□

El resultado anterior es equivalente a que para toda subextensión finita de Galois $L \supset F \supset k$ la imagen del grupo de Weil $\mathtt{W}(L|k)$ por la restricción $\mathtt{res} : \mathtt{Gal}(L|k) \to \mathtt{Gal}(F|k)$ es todo el grupo $\mathtt{Gal}(F|k)$. En efecto, $\mathtt{W}(L|k)$ es denso si y sólo si $\mathtt{W}(L|k) \cap \sigma\mathtt{Gal}(L|F) \neq \emptyset\ \forall F \supset k$ Galois, $\forall\sigma$, que equivale a decir que para toda extensión de Galois $F \supset k$ para todo elemento $\sigma \in \mathtt{Gal}(F|k)$ existe una preimagen en $\mathtt{W}(L|k)$ para la restricción.

Capítulo 5

Teoría de Cuerpos de Clase Local

5.1. Objetivos y Organigrama

La teoría de cuerpos de clase se preocupa 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: "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 preocupa, dicha información vendrá codificada por el grupo de unidades $k^\times$ y cierta familia de subgrupos, en definitiva, información intrínseca a k. 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 $\mathtt{Art}_k(\pi)_{|k^{\mathtt{ur}}}$ es el inverso del elemento de Frobenius de k.
   b. Si $k' \supset k$ es una extensión abeliana finita, entonces $\mathtt{Art}_k\left(\mathtt{N}_{k'|k}(k'^\times)\right)_{|k'} = \mathrm{id}\,.$

   Además, este homomorfismo es *inyectivo* y su imagen es el conjunto
   $$\mathtt{W}_k^{\mathtt{ab}} := \left\{\sigma \in \mathtt{Gal}(k^{\mathtt{ab}}|k) \ : \ \sigma_{|k^{\mathtt{ur}}} \in \mathtt{Frob}_k^{\mathbb{Z}}\right\}.$$
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, gracias al toerema de existencia sabemos que todos los subgrupos abiertos de índice finito proceden de alguna extensión abeliana finita.

Nuestro objetivo es demostrar estos dos resultados y dar los detalles necesarios para alcanzar una comprensión profunda de los numerosos conceptos involucrados, los cuales hemos ido desarrollando en los capítulos anteriores.

Nuestro enfoque será el de la teoría de Lubin-Tate, más concretamente, usaremos los grupos de Lubin-Tate relativos para obtener una teoría más flexible que nos permita demostrar con comodidad estos teoremas. Informalmente, lo que haremos es "categorificar" los conjuntos formados por los parámetros de uniformización de cada extensión finita no ramificada del cuerpo k y ver que para cada clase de isomorfía podemos obtener un invariante, las llamadas extensiones de Lubin-Tate. Posteriormente veremos cómo dichas clases de isomorfía evolucionan a medida que el grado de la extensión finita no ramificada aumenta. De esta forma obtendremos de manera canónica una única extensión bien definida y para la cual se verifican los teoremas anteriores de la teoría de cuerpos de clase local sin más que cambiar la extensión abeliana maximal de k por esta nueva extensión construida. El último paso será demostrar que esta extensión que hemos construido es realmente la extensión abeliana maximal de k, resultado que se conoce como *Teorema de Kronecker-Weber para cuerpos locales.*

5.2. Grupos Formales y Grupos de Lubin-Tate

5.2.1. Leyes de Grupo Formal

El primer paso es obtener una noción abstracta de "estructura" que podamos asociar a cada parámetro de uniformización con el objetivo de estudiar posteriormente los morfismos entre estas "estructuras". Es en este sentido como hemos de entender el término "categorificar" usado en la introducción. Estas estructuras las obtendremos gracias a la noción de *ley de grupo formal.*

Dado un anillo conmutativo con unidad no trivial A, 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 último 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 $F - G \in (X_1, \ldots, X_n)^d \subset A[[X_1, \ldots, X_n]]$.

Definimos qué es una *ley formal de grupo sobre A:*

Definición 5.2.1. 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. $F(X, Y) = F(Y, X)$.

A partir de la definición deducimos las siguientes propiedades:

Lema 5.2.2. 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 $A[[X]]$.

Demostración. 1. Definimos $f(X) := F(X, 0) \in A[[X]]$. Sabemos que $f(X) = F(X, 0) \equiv X \pmod{\texttt{deg}2}$ de modo que el coeficiente de la X en la serie de potencias f es uno y existe una serie de potencias inversa de f para la composición, que denotaremos por f^{-1}. Como $F(F(X, 0), 0) = F(X, F(0, 0)) = F(X, 0)$ deducimos que $f \circ f = f$. Componiendo con f^{-1} obtenemos que $F(X, 0) = f(X) = X$. De manera análoga, $F(0, Y) = Y$. Las igualdades $F(X, 0) = X, F(0, Y) = Y$ nos dicen que F no tiene términos que contengan únicamente las variables X o Y aparte de los términos lineales $X + Y$.

2. Consideremos la serie de potencias $H(X,Y) = X - F(X,Y) \in A[[X,Y]]$. Si la vemos como una serie de potencias en la variable Y, es decir, como un elemento del anillo $(A[[X]])[[Y]]$, vemos que H no tiene término constante y el coeficiente de la variable Y es $-1 \in A[[X]]^\times$. Deducimos que existe una serie de potencias $G(X,Y) \in (A[[X]])[[Y]]$ de modo que $H(X, G(X,Y)) = Y$. Usando la definición de H llegamos a que existe una serie de potencias $G(X,Y) \in A[[X,Y]]$ tal que

$$F(X, G(X,Y)) = X - Y,$$

sustituyendo en esta igualdad $Y = X$ obtenemos que la serie $G(X,X) \in A[[X]]$ verifica las condiciones del enunciado.

La unicidad se comprueba como sigue: Si $G_1, G_2 \in A[[X]]$ verifican la condición del enunciado, entonces

$$\begin{aligned} G_1(X) &= F(G_1(X), 0) \\ &= F(G_1(X), F(X, G_2(X))) = F(F(G_1(X), X), G_2(X)) \\ &= F(0, G_2(X)) = G_2(X). \end{aligned}$$

□

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 ha convertido 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). Definimos la noción formal de homomorfismo:

Definición 5.2.3. 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 por medio de 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 5.2.4. 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.

Demostración. Veamos que $(\mathtt{Hom}_A(F,G),+_G)$ es un grupo abeliano. Dados $\varphi,\psi \in \mathtt{Hom}_A(F,G) \subset (X) \subset A[[X]]$, tenemos las siguientes igualdades:

$$\begin{aligned}
(\varphi +_G \psi)(F(X,Y)) &= G(\varphi(X),\psi(X))(F(X,Y)) \\
&= G\big(\varphi(F(X,Y)),\psi(F(X,Y))\big) \\
&= G\big(G(\varphi(X),\varphi(Y)),G(\psi(X),\psi(Y))\big) \\
&= G\Big(G\big(G(\varphi(X),\varphi(Y)),\psi(X)\big),\psi(Y)\Big) \\
&= G\Big(G\big(\varphi(X),G(\varphi(Y),\psi(X))\big),\psi(Y)\Big) \\
&= G\Big(G\big(G(\varphi(X),\psi(Y)),\varphi(Y)\big),\psi(Y)\Big) \\
&= G\big(G(\varphi(X),\psi(X)),G(\varphi(Y),\psi(Y))\big) \\
&= G((\varphi +_G \psi)(X),(\varphi +_G \psi)(Y)).
\end{aligned}$$

Estas igualdades prueban que la operación $+_G$ es una operación binaria e interna. Ahora veamos que $i_G \in \mathtt{Hom}_A(F,G)$:

$$\begin{aligned}
G \circ i_G &= G(G \circ i_G, 0) \\
&= G(G \circ i_G, G(G, i_G \circ G)) \\
&= G(G(G \circ i_g, G), i_g \circ G) \\
&= G(0, i_G \circ G) = i_G \circ G,
\end{aligned}$$

usando que

$$G(G(i_G(X),i_G(Y)),G(X,Y)) = G(G(i_G(X),X),G(i_G(Y),Y)) = G(0,0) = 0.$$

A partir de estas propiedades es sencillo probar que el conjunto anterior es un grupo. Para concluir la demostración veamos que $(\mathtt{End}_A(F),+_F,\circ)$ es un anillo. Para ello, es suficiente probar que el producto distribuye sobre la suma. Sean $\psi_1,\psi_2,\psi_3 \in \mathtt{End}_A(F)$:

$$\begin{aligned}
\psi_1 \circ (\psi_2 +_F \psi_3) &= \psi_1(F(\psi_2(X),\psi_3(X))) \\
&= F((\psi_1 \circ \psi_2)(X),(\psi_1 \circ \psi_3)(X)) \\
&= \psi_1 \circ \psi_2 +_F \psi_1 \circ \psi_3.
\end{aligned}$$

De manera análoga se demuestra que $(\psi_1 +_F \psi_2) \circ \psi_3 = \psi_1 \circ \psi_3 +_F \psi_2 \circ \psi_3$.

□

5.2.2. Grupos de Lubin-Tate Relativos

Visto como podemos construir leyes de grupo formal, volvemos a nuestro problema original: asociar a cada parámetro de uniformización una estructura que nos permita compararlos. Fijamos la configuración en la que vamos a trabajar. Denotamos por k al cuerpo local, su valoración normalizada por ν_k, su anillo de enteros 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 o bien L es una extensión no ramificada finita de k o L es la compleción de la extensión maximal no ramificada 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 (por continuidad) a L 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. $F(H_1, \ldots, H_n)^{\varphi^n} = F^{\varphi^n}(H_1^{\varphi^n}, \ldots, H_N^{\varphi^n})$,
3. Si F es una ley de grupo formal sobre $\mathcal{O}_L$ entonces F^{φ^n} también lo es.

Definición 5.2.5. Dado $u \in \mathcal{O}_L^\times$ definimos el conjunto

$$\Theta_u^L := \{\theta \in \mathcal{O}_L \ : \ \theta^\varphi = u\theta\}.$$

También definimos el conjunto $\Theta_u^{L,\times} := \Theta_u^L \cap \mathcal{O}_L^\times$.

Notar que 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 5.2.6. 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 condiciones siguientes:

1. $f(X) \equiv \pi X \pmod{\mathtt{deg2}}$,
2. $f(X) \equiv X^q \pmod{\mathcal{O}_\mathcal{L}[[X]]\mathfrak{p}_L}$.

El siguiente lema es esencial en la construcción que vamos a hacer de los grupos de Lubin-Tate:

Lema 5.2.7. 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 $\theta_1, \ldots, \theta_n \in \Theta_{\pi/\pi'}^L$. Entonces existe una única serie de potencias $F \in \mathcal{O}_L[[X_1, \ldots, X_n]]$ verificando las siguientes condiciones:

$$F \equiv \theta_1 X_1 + \cdots + \theta_n X_n \pmod{\mathtt{deg2}}, \qquad f' \circ F = F^\varphi \circ f.$$

Demostración. Ver [Yos08] *Lema 3.4.* □

Gracias a este resultado podemos asociar a cada serie de potencias de Frobenius de un parámetro de uniformización una ley de grupo formal. También nos permitirá interpretar los grupos Θ_u^L como ciertos homomorfismos entre leyes de grupo formal:

Proposición 5.2.8. 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:

$$[\theta]_{f,f'}(X) \equiv \theta X \quad (\text{mód } \mathtt{deg}2), \qquad f' \circ [\theta]_{f,f'} = [\theta]^\varphi_{f,f'} \circ f.$$

   Además tiene las siguientes propiedades: $[\theta]_{f,f'} +_{F_{f'}} [\theta']_{f,f'} = [\theta + \theta']_{f,f'}$ y $[\theta']_{f',f''} \circ [\theta]_{f,f'} = [\theta\theta']_{f,f''}$.

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

Demostración. 1. Aplicando 5.2.7 con $\pi = \pi', f = f', n = 2, \theta_1 = \theta_2 = 1$ obtenemos una única serie de potencias $F_f \in \mathcal{O}_L[[X, Y]]$ verificando $F_f \equiv X + Y$ (mód $\mathtt{deg}2$) y $f \circ F_f = F_f^\varphi \circ f$. Al ser $X + Y = Y + X$, $F_f(Y, X)$ tiene las mismas propiedades que $F_f(X, Y)$ y por la unicidad obtenemos que $F_f(X, Y) = F_f(Y, X)$. Análogamente, las series $F_f(F_f(X, Y), Z)$ y $F_f(X, F_f(Y, z))$ verifican que (mód $\mathtt{deg}2$) coinciden con $X + Y + Z$ y por ejemplo:

$$F \circ F_f(F_f, \mathrm{id}) = F_f^\varphi(f \circ F_f, f) = F_f^\varphi(F_f^\varphi \circ f, f) = (F_f(F_f, \mathrm{id}))^\varphi \circ f.$$

   De nuevo, gracias a la unicidad de 5.2.7, concluimos que $F_f(F_f, \mathrm{id}) = F_f(\mathrm{id}, F_f)$. Concluimos que F_f es una ley de grupo formal con $f \in \mathtt{Hom}_{\mathcal{O}_L}(F_f, F_f^\varphi)$.

2. Usando 5.2.7 con $t = 1$ obtenemos $[\theta]_{f,f'}$. Gracias a las igualdades

$$f' \circ ([\theta]_{f,f'} +_{F_{f'}} [\theta']_{f,f'}) = (f' \circ [\theta]_{f,f'}) +_{F_{f'}^\varphi} (f' \circ [\theta']_{f,f'}) = ([\theta]^\varphi_{f,f'} +_{F_{f'}^\varphi} [\theta']^\varphi_{f,f'}) \circ f = ([\theta]_{f,f'} +_{F_{f'}} [\theta']_{f,f'})^\varphi \circ f,$$

$$f'' \circ ([\theta']_{f',f''} \circ [\theta]_{f,f'}) = [\theta']^\varphi_{f',f''} \circ f' \circ [\theta]_{f,f'} = [\theta']^\varphi_{f',f''} \circ [\theta]^\varphi_{f,f'} \circ f = ([\theta']_{f',f''} \circ [\theta]_{f,f'})^\varphi \circ f,$$

   concluimos el resultado usando la unicidad que nos provee 5.2.7. La inyectividad es clara pues podemos recuperar θ a partir de $[\theta]_{f,f'}$ por ser el coeficiente que acompaña a la variable X.

3. De nuevo, las igualdades

$$f' \circ ([\theta]_{f,f'} \circ F_f) = [\theta]^{\varphi}_{f,f'} \circ f \circ F_f = ([\theta]^{\varphi}_{f,f'} \circ F_f^{\varphi}) \circ f = ([\theta]_{f,f'} \circ F_f)^{\varphi} \circ f,$$

$$f' \circ (F_{f'} \circ [\theta]_{f,f'}) = F_{f'}^{\varphi} \circ f' \circ [\theta]_{f,f'} = (F_{f'}^{\varphi} \circ [\theta]^{\varphi}_{f,f'}) \circ f = (F_{f'} \circ [\theta]_{f,f'})^{\varphi} \circ f,$$

demuestran que $[\theta]_{f,f'} \circ F_f = F_{f'} \circ [\theta]_{f,f'}$ usando la unicidad de 5.2.7 con $\pi = \pi', n = 2, \theta_1 = \theta_2 = \theta$.

□

Como corolario obtenemos:

Corolario 5.2.9. 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 $[\theta]^{-1}_{f,f'} = [\theta^{-1}]_{f',f}$.

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 ley de grupo formal y de esta forma conseguimos la categorificación comentada al principio. Observar que los grupos Θ_u^L pueden tener un comportamiento muy dispar, por ejemplo, $\Theta_u^k = \emptyset$ si $u \neq 1$ y si $u = 1$ sabemos que $\mathcal{O}_k \subset \Theta_1^k$. Conocer estos grupos es muy importante pues nos permitirá tener un buen control sobre ciertas extensiones de k. En las siguientes secciones alcanzaremos un conocimiento lo suficientemente satisfactorio como para obtener los resultados de la teoría de cuerpos de clase local.

Antes de pasar a la siguiente sección haremos unas últimas observaciones sobre las series de potencias construidas aquí:

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. En efecto, observar que $[\pi]_{f,f^{\varphi}}(X) \equiv \pi X \pmod{\mathtt{deg}2}$ y también $[\pi]_{f,f^{\varphi}} \circ F_f = F_f^{\varphi} \circ [\pi]_{f,f^{\varphi}}$. Smbas propiedades las cumple f, por unicidad concluimos que son iguales.

2. Se tiene que $F_f^{\varphi} = F_{f^{\varphi}}$ y $[\theta]^{\varphi}_{f,f'} = [\theta^{\varphi}]_{f^{\varphi},f'^{\varphi}}$. En efecto, $F_{f^{\varphi}}$ es la única ley de grupo formal verificando que $f^{\varphi} \circ F_{f^{\varphi}} = F^{\varphi}_{f^{\varphi}} \circ f^{\varphi}$. Pero $f^{\varphi} \circ F_f^{\varphi} = (f \circ F_f)^{\varphi} = (F_f^{\varphi} \circ f)^{\varphi} = (F_f^{\varphi})^{\varphi} \circ f^{\varphi}$ y gracias a la unicidad obtenemos la igualdad. Análogamente, las igualdades

$$f'^{\varphi} \circ [\theta]^{\varphi}_{f,f'} = (f' \circ [\theta]_{f,f'})^{\varphi} = ([\theta]^{\varphi}_{f,f'} \circ f)^{\varphi} = ([\theta]^{\varphi}_{f,f'})^{\varphi} \circ f^{\varphi}$$

prueban la igualdad $[\theta]^{\varphi}_{f,f'} = [\theta^{\varphi}]_{f^{\varphi},f'^{\varphi}}$.

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

$$f_m = [\pi^{\varphi^{m-1}}]_{f^{\varphi^{m-1}}, f^{\varphi^m}} \circ \cdots \circ [\pi^{\varphi}]_{f^{\varphi}, f^{\varphi^2}} \circ [\pi]_{f, f^{\varphi}} = [\pi_m]_{f, f^{\varphi^m}},$$

con $\pi_m \in \mathcal{O}_L$ definido por

$$\pi_m := \prod_{t=0}^{m-1} \pi^{\varphi^t}, \ \pi_0 = 1.$$

5.3. Extensiones de Lubin-Tate y Aplicaciones de Artin

5.3.1. Extensiones de Lubin-Tate

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

Definición 5.3.1. 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

$$\mu_{f,m} := \{\alpha \in L_f^m \ : \ f_m(\alpha) = 0\},$$

$$\mu_{f,m}^{\times} := \mu_{f,m} \setminus \mu_{f,m-1}.$$

Observar que, al suponer que el polinomio f es mónico y que 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 $n \neq 1, q$ elementos del ideal $\mathfrak{p}_L$. En particular, cada uno de estos polinomios es $\mathfrak{p}_L$-Eisenstein luego irreducible y separable sobre L. El más sencillo de todos estos polinomios es $\pi X + X^q$. Por último, 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. Nosotros 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 caracterísitca del cuerpo es no nula, una demostración de la separabilidad de f_m se puede encontrar en [Yos08] *Apéndice II.*

Lema 5.3.2. 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 $\alpha \in \mathfrak{p}_{L^{\text{sep}}}$:

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

Demostración. 1. Como hemos comentado antes, los polinomios f_m son separables y por ello las extensiones $L_f^m \supset L$ son separables. Además, como $f_m \in \mathcal{O}_L[X]$ son polinomios mónicos sabemos que sus raíces son elementos integrales de L_f^m y por ello $\mu_{f,m} \subset \mathcal{O}_{L_f^m}$. Si $\alpha \in \mathcal{O}_{L_f^m}^\times$ entonces $f_m(\alpha) \equiv \alpha^{q^m} \pmod{\mathfrak{p}_{L_f^m}}$ de modo que $f_m(\mathcal{O}_{L_f^m}^\times) \subset \mathcal{O}_{L_f^m}^\times$. Esto implica que $\mu_{f,m} \subset \mathfrak{p}_{L_f^m}$.

2. Tenemos que $[x]_f = [x/\pi_m]_{f^{\varphi^m},f} \circ f_m$. Al ser x/π_m invertible obtenemos la primera equivalencia. La segunda equivalencia es clara pues x genera al ideal $\mathfrak{p}_L^m$ al ser la extensión $L \supset k$ no ramificada.

□

Vamos a estudiar con detalle los conjuntos $\mu_{f,m}$:

Proposición 5.3.3. 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:

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

Demostración. 1. Sean $\alpha, \beta \in \mu_{f,m}$ y $\lambda \in \mathcal{O}_k$. Dado $a \in \mathfrak{p}_L^m$ tenemos que

$$[a]_f([\lambda]_f(\alpha)) = [a\lambda]_f(\alpha) = 0$$

aplicando 5.3.2 pues $a\lambda \in \mathfrak{p}_L^m$ y $\alpha \in \mu_{f,m}$. Así mismo,

$$[a]_f(\alpha +_{F_f} \beta) = [a]_f(\alpha) +_{F_f} [a]_f(\beta) = 0 +_F 0$$

usando de nuevo 5.3.2. Concluimos que $[\lambda]_f(\alpha), \alpha +_{F_f} \beta \in \mu_{f,m}$. Podemos considerar el homomorfismo de $\mathcal{O}_k$-módulos $h : \mathcal{O}_k \to \mu_{f,m}$ de modo que $a \mapsto [a]_f(\alpha)$. Gracias a 5.3.2 sabemos que $\mathfrak{p}_k^m \subset \ker(h)$. Así mismo, como $\alpha \notin \mu_{f,m-1}$ sabemos que existe $a \in \mathfrak{p}_k^{m-1}$ de modo que $[a]_f(\alpha) \neq 0$. Recordando que $\mathcal{O}_k$ es un dominio de valoración discreta, concluimos que $\ker(h) = \mathfrak{p}_k^m$. Gracias al primer teorema de isomorfía, obtenemos una inyección de $\mathcal{O}_k/\mathfrak{p}_k^m$ en $\mu_{f,m}$ de modo que $q^m = \deg(f_m) \geq |\mu_{f,m}| \geq |\mathcal{O}_k/\mathfrak{p}_k^m| = q^m$. Deducimos que dicha aplicación es en realidad sobreyectiva y obtenemos el resultado del enunciado. Observar que también obtenemos la igualdad $|\mu_{f,m}^\times| = |\mu_{f,m}| - |\mu_{f,m-1}^\times| = q^{m-1}(q-1)$.

2. Como las series de potencias $[a]_f$ tienen coeficientes en $\mathcal{O}_L$ y el cuerpo L es completo, deducimos que

$$\mu_{f,m} = \{[a]_f(\alpha) \mid a \in \mathcal{O}_k\} \subset L(\alpha).$$

Por tanto, $L_f^m = L(\mu_{f,m}) \subset L(\alpha) \subset L_f^m$ y tenemos la igualdad. En particular, $L_f^m \supset L$ es una extensión de Galois. El coeficiente de grado 0 de f_m/f_{m-1} podemos escribirlo como $\pi^{\varphi^{m-1}} = \prod_{\alpha \in \mu_{f,m}^\times}(-\alpha)$. Si miramos la imagen por la valoración normalizada $\nu_{L_f^m}$ de la igualdad anterior obtenemos

$$e(L_f^m|L) = \nu_{L_f^m}\left(\pi^{\varphi^{m-1}}\right) = \sum_{\alpha \in \mu_{f,m}^\times} \nu_{L_f^m}(-\alpha) \geq |\mu_{f,m}^\times|$$

pues $\mu_{f,m} \subset \mathfrak{p}_{L_f^m}$. Como

$$|\mu_{f,m}^\times| = \deg(f_m/f_{m-1}) \geq [L_f^m : L] = e(L_f^m|L) f(L_f^m|L) \geq e(L_f^m|L),$$

obtenemos que todo son igualdades. En particular, la extensión $L_f^m \supset L$ es totalmente ramificada, el polinomio f_m/f_{m-1} es irreducible y α es un parámetro de uniformización de L_f^m.

3. Como las series de potencias $F_f, [\cdot]_f$ tienen coeficientes en $\mathcal{O}_L$, para todo $\sigma \in \mathtt{Gal}(L_f^m|L)$ se verifica que

$$\sigma(\alpha +_{F_f} \alpha') = \sigma(\alpha) +_{F_f} \sigma(\alpha'),\ \sigma([a]_f(\alpha)) = [a]_f(\sigma(\alpha)).$$

De esta forma, podemos definir $\rho_{f,m} : \mathtt{Gal}(L_f^m|L) \to \mathtt{Aut}_{\mathcal{O}_k}(\mu_{f,m})$ como $\rho_{f,m}(\sigma) = \sigma_{|\mu_{f,m}}$. Esta aplicación es inyectiva pues $L_f^m = L(\alpha)$ y σ está determinado de manera única por su imagen $\sigma(\alpha) \in \mu_{f,m}^\times$. Así mismo, como $\mu_{f,m} \sim \mathcal{O}_k/\mathfrak{p}_k^m$ sabemos que $\mathtt{Aut}_{\mathcal{O}_k}(\mu_{f,m}) \simeq (\mathcal{O}_k/\mathfrak{p}_k^m)^\times \simeq \mathcal{O}_k^\times/(1+\mathfrak{p}_k^m)$. Concluimos que $\rho_{f,m}$ también es sobreyectivo pues

$$|\mathtt{Gal}(L_f^m|L)| = [L_f^m : L] = |\mu_{f,m}^\times| = q^{m-1}(q-1) = |\mathcal{O}_k^\times/(1+p_k^m)|.$$

□

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 5.3.2.2 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 $\nu_k(a) = m - t$.

5.3.2. Homomorfismo de Artin

Vamos a extender la definición de $\pi_j \in L^{\times}$ para valores de $j \in \mathbb{Z}$ negativos. 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 $\pi_j = (\pi_{-j}^{-1})^{\varphi^j}$. Notar que si $m+n \geq 0$ entonces $\pi_{m+n} = \pi_{n+m}$ y gracias a la definición de π_j para $j < 0$ es inmediato que 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 $\pi_{j+j'} = \pi_{j'}{}^{\varphi^j} \pi_j$. Para demostrarlo, antes observar que $\pi_j = \prod_{t=j}^{-1} (\pi^{-1})^{\varphi^t}$ para $j < 0$. La identidad anterior es inmediata si $j, j' \geq 0$ y por simetría también cierta si $j, j' < 0$. La demostración no es trivial con $j > 0, j' < 0$ o $j < 0, j' > 0$. Es suficiente probar sólo uno de estos, supondremos que $j > 0, j' < 0$:

$$\begin{aligned} \pi_{j'}^{\varphi^j} \pi_j &= \prod_{t=j'}^{-1} (\pi^{-1})^{\varphi^{t+j}} \cdot \prod_{t=0}^{j-1} \pi^{\varphi^t} \\ &= \prod_{t=j'+j}^{j-1} (\pi^{-1})^{\varphi^t} \cdot \prod_{t=0}^{j-1} \pi^{\varphi^t}. \end{aligned}$$

Hay dos posibles casos, que sea $0 < j + j' \leq j - 1$ o $j + j' < 0 \leq j - 1$. En el primer caso obtendremos como resultado el producto $\prod_{t=0}^{j'+j-1} \pi^{\varphi^t}$ y en el segundo $\prod_{t=j+j'}^{-1} (\pi^{-1})^{\varphi^t}$. En ambos casos el resultado es $\pi_{j+j'}$.

Tenemos el siguiente resultado:

Lema 5.3.4. Sean π, π' parámetros de uniformización de L. Si $\theta \in \Theta^L_{\pi'/\pi}$, entonces $\theta^{\varphi^j}/\theta = \pi'_j/\pi_j$ para todo $j \in \mathbb{Z}$. Además, $\pi_j \in \Theta^L_{\pi^{\varphi^j}/\pi}$.

Demostración. Es suficiente comprobar el resultado para $j \geq 0$. En efecto, si es $j < 0$ sabemos que $\theta^{\varphi^{-j}} \pi_{-j} = \theta \pi'_{-j}$. Como $\pi_{-j} = \left(\pi_j^{-1}\right)^{\varphi^{-j}}$ obtenemos la igualdad:

$$\left(\theta \pi_j^{-1}\right)^{\varphi^{-j}} = \theta \left(\pi'^{-1}_j\right)^{\varphi^{-j}} = \left(\theta^{\varphi^j} \pi'^{-1}_j\right)^{\varphi^{-j}}.$$

Aplicando φ^j obtenemos la igualdad buscada. Veamos el resultado para $j \geq 0$. Por inducción, el lema es obvio para $j = 0$. Supongamos que hemos deducido la igualdad para un valor j, veamos que es cierto para $j+1$: Es $\pi_{j+1} = \pi^{\varphi^j}\pi_j, \pi'_{j+1} = \pi'^{\varphi^j}\pi'_j, \theta^{\varphi^j}\pi_j = \pi'_j\theta$ y $\theta^{\varphi}\pi = \theta\pi'$. Concluimos que

$$\theta^{\varphi^{j+1}}\pi_{j+1} = (\theta^{\varphi}\pi)^{\varphi^j}\pi_j = \theta^{\varphi^j}\pi'^{\varphi^j}\pi_j = \theta\pi'^{\varphi^j}\pi'_j = \theta\pi'_{j+1}.$$

Para la segunda parte, de nuevo es suficiente probar el caso $j \geq 0$. Si $j < 0$ entonces $\pi_{-j}^{\varphi}\pi = \pi^{\varphi^{-j}}\pi_{-j}$ con $\pi_{-j} = (\pi_j^{-1})^{\varphi^{-j}}$. Por tanto, $(\pi_j^{-1})^{\varphi^{-j+1}}\pi = (\pi\pi_j^{-1})^{\varphi^{-j}}$ de modo que $(\pi_j^{-1})^{\varphi}\pi^{\varphi^j} = \pi\pi_j^{-1}$. Para $j \geq 0$, es claro que $\pi_j^{\varphi}\pi = \pi_{j+1} = \pi^{\varphi^j}\pi_j$.

□

El siguiente resultado será esencial para nosotros pues nos va a permitir asociar a cada clase de isomorfía de leyes de grupos formales un conjunto de invariantes que será la cadena de extensiones de Lubin-Tate:

Lema 5.3.5. Sean $f, f' \in \mathcal{O}_L[X]$ polinomios de Frobenius para parámetros de uniformización π, π' de L. Si $\theta \in \Theta^{L,\times}_{\pi'/\pi}$ 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 $L_f^m = L_{f'}^m$.

Demostración. Tenemos las siguientes igualdades:

$$f'_m \circ [\theta]_{f,f'} = [\pi'_m]_{f',f'^{\varphi^m}} \circ [\theta]_{f,f'} = [\theta\pi'_m]_{f,f'^{\varphi^m}} \overset{5.3.4}{=} [\theta^{\varphi^m}\pi_m]_{f,f'^{\varphi^m}} = [\theta^{\varphi^m}]_{f^{\varphi^m},f'^{\varphi^m}} \circ [\pi_m]_{f,f^{\varphi^m}} = [\theta]_{f,f'^{\varphi^m}} \circ f_m.$$

Vemos que $[\theta]_{f,f'}(\mu_{f,m}) \subset \mu_{f',m}$ y la aplicación $[\theta]_{f,f'} : \mu_{f,m} \to \mu_{f',m}$ está bien definida. Gracias a 5.2.8.2 y 5.2.8.3 sabemos que $[\theta]_{f,f'}$ es un homomorfismo de $\mathcal{O}_k$-módulos. Concluimos que es un isomorfismo pues su inversa viene dada por $[\theta^{-1}]_{f',f}$. Por último, como $[\theta]_{f,f'}, [\theta^{-1}]_{f',f} \in \mathcal{O}_L[[X]]$ y los cuerpos $L_f^m, L_{f'}^m$ son completos deducimos que:

$$\mu_{f',m} = [\theta]_{f,f'}(\mu_{f,m}) \subset L_f^m, \ \mu_{f,m} = [\theta^{-1}]_{f',f}(\mu_{f',m}) \subset L_{f'}^m.$$

Llegamos a que $L_f^m = L_{f'}^m$.

□

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

Proposición 5.3.6. 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 5.3.3.3 podemos extenderlos a los siguientes isomorfismos:

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

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 $\rho_f : \mathtt{W}\left((\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}} | k\right) \to k^\times$.

Nota: Los grupos de Weil que aparecen en el segundo apartado son respecto a la extensión continua del elemento de Frobenius a $\hat{k}^{\mathtt{ur}}$.

Demostración. 1. Observar que la llegada de la aplicación se define como la unión disjunta de los conjuntos $\mu_{f^{\varphi^j},m}^\times$, pudiendo aparecer varias copias de un mismo conjunto $\mu_{f^{\varphi^j},m}^\times$. Un ejemplo en el que aparecen varias copias del conjunto $\mu_{f,m}^\times$ es cuando la extensión $L \supset k$ es finita de grado de n. En este caso, $\mu_{f,m} = \mu_{f^{\varphi^{kn}},m}$ para todo $k \in \mathbb{Z}$. Por otro lado, la condición de extensibilidad de los k-automorfismos $\langle \varphi_{|L} \rangle$ se puede deducir directamente de que las extensiones $L_f^m \supset k$ son de Galois cuando $[L : k] < \infty$.

Dicho esto, sea $x(1+\mathfrak{p}_k^m)$ con $\nu_k(x) = -j$. Entonces $x\pi_j \in \Theta_{\pi^{\varphi^j}/\pi}^{L,\times}$ pues x es invariante bajo la acción de φ y $\pi_j \in \Theta_{\pi^{\varphi^j}/\pi}^{L,\times}$ gracias a 5.3.4 con $\nu_L(\pi_j) = j$. Vemos entonces que $[x\pi_j]_{f,f^{\varphi^j}} : \mu_{f,m} \to \mu_{f^{\varphi^j},m}$ es un isomorfismo de $\mathcal{O}_k$-módulos, usando 5.2.9.2 y 5.3.5. En particular, $[x\pi_j]_{f,f^{\varphi^j}}(\alpha) \in \mu_{f^{\varphi^j},m}^\times$.

Veamos que la aplicación restringida a $\nu_k^{-1}(-j)/(1+\mathfrak{p}_k^m)$ es una biyección con $\mu_{f^{\varphi^j},m}^\times$.

En efecto, para la **inyectividad**, supongamos que $[x\pi_j]_{f,f^{\varphi^j}}(\alpha) = [y\pi_j]_{f,f^{\varphi^j}}(\alpha)$ con $x(1+\mathfrak{p}_k^m), y(1+\mathfrak{p}_k^m) \in \nu_k^{-1}(-j)/(1+\mathfrak{p}_k^m)$. Tenemos entonces que $[xy^{-1}]_f(\alpha) = \alpha$. Ahora bien, como $\alpha \in \mu_{f,m}^\times$, sabemos que dado $\beta \in \mu_{f,m}$ entonces existe $a \in \mathcal{O}_k$ tal que $[a]_f(\alpha) = \beta$. Obtenemos entonces que $[xy^{-1}]_f(\beta) = ([a]_f \circ [xy^{-1}]_f)(\alpha) = [a]_f(\alpha) = \beta$. Concluimos que $[xy^{-1}]_f$ actúa como la identidad sobre $\mu_{f,m}$. Gracias a 5.3.3.3 concluimos que $xy^{-1} \in 1+\mathfrak{p}_k^m$, es decir, $x(1+\mathfrak{p}_k^m) = y(1+\mathfrak{p}_k^m)$.

Para la **sobreyectivad,** dado $\gamma \in \mu_{f^{\varphi^j},m}^\times$, para cualquier $x(1+\mathfrak{p}_k^m) \in \nu_k^{-1}(-j)$ tenemos que existe $\alpha' \in \mu_{f,m}^\times$ con $[x\pi_j]_{f,f^{\varphi^j}}(\alpha') = \gamma$, pues $[x\pi_j]_{f,f^{\varphi^j}} : \mu_{f,m} \to \mu_{f^{\varphi^j},m}$ es un isomorfismo.

Ahora bien, como $\alpha \in \mu_{f,m}^{\times}$, existe $a \in \mathcal{O}_k$ tal que $[a]_f(\alpha) = \alpha'$. De hecho, como $[a]_f(\alpha) \in \mu_{f,m}^{\times}$ sabemos que tiene que ser $0 \leq \nu_k(a) \leq m - m = 0$ y por ello $a \in \mathcal{O}_k^{\times}$. Concluimos que $\gamma = [ax\pi_j]_{f,f^{\varphi^j}}(\alpha)$ con $\nu_k(ax) = \nu_k(a) + \nu_k(x) = \nu_k(x)$.

Por último, si tenemos $\varphi_{|L}^j \in \langle \varphi_{|L} \rangle$, recordando que $L(\alpha) = L_f^m = L_{f^{\varphi^j}}^m$ gracias a 5.3.3.2 y 5.3.5, cualquier extensión σ de $\varphi_{|L}^j$ a L_f^m debe verificar que $\sigma(\alpha)$ es una raíz de $(f_m)^{\sigma}/(f_{m-1})^{\sigma} = (f_m)^{\varphi_{|L}^j}/(f_{m-1})^{\varphi_{|L}^j} = (f^{\varphi_{|L}^j})_m/(f^{\varphi_{|L}^j})_{m-1}$, i.e., $\sigma(\alpha) \in \mu_{f^{\varphi^j},m}^{\times}$. Ahora bien, probada la biyección anterior, sabemos que será $\sigma(\alpha) = [x\pi_j]_{f,f^{\varphi^j}}(\alpha)$ para un único $x(1+\mathfrak{p}_k^m) \in \nu_k^{-1}(-j)/(1+\mathfrak{p}_k^m)$. Cada una de las posibles extensiones anteriores dan una extensión válida de $\varphi_{|L}^j$, y por ello hay $|\mu_{f,m}^{\times}| = q^{m-1}(q-1) = [L_f^m : L]$ posibles extensiones.

2. Consideramos $\sigma \in \mathtt{W}\left((\hat{k}^{\mathtt{ur}})_f^m | k\right)$ con $\sigma_{|\hat{k}^{\mathtt{ur}}} = \varphi^j$. Como hemos visto antes, si $\alpha \in \mu_{f,m}^{\times}$ entonces $\sigma(\alpha) \in \mu_{f^{\varphi^j},m}^{\times}$ y por ello $\sigma(\alpha) = [x\pi_j]_{f,f^{\varphi^j}}(\alpha)$ para un único $x(1+\mathfrak{p}_k^m)$ con $\nu_k(x) = -j$. En realidad será $\sigma(\beta) = [x\pi_j]_{f,f^{\varphi^j}}(\beta)$ para todo $\beta \in \mu_{f,m}$ pues si $\beta = [a]_f(\alpha)$ con $a \in \mathcal{O}_k$, entonces

$$\sigma(\beta) = [a]_f^{\varphi^j}(\sigma(\alpha)) = ([a]_{f^{\varphi^j}} \circ [x\pi_j]_{f,f^{\varphi^j}})(\alpha) = [x\pi_j]_{f,f^{\varphi^j}}(\beta).$$

En particular, esto demuestra que las aplicaciones $\rho_{f,m} : \mathtt{W}\left((\hat{k}^{\mathtt{ur}})_f^m | k\right) \to k^{\times}/(1+\mathfrak{p}_k^m)$ forman un sistema proyectivo.

$\rho_{f,m}$ es un homomorfismo de grupos ya que si $\tau(\alpha) = [y\pi_{j'}]_{f,f^{\varphi^{j'}}}(\alpha)$ entonces:

$$(\sigma\tau)(\alpha) = \sigma([y\pi_{j'}]_{f,f^{\varphi^{j'}}}(\alpha)) = ([y\pi_{j'}]_{f,f^{\varphi^{j'}}}^{\varphi^j} \circ [x\pi_j]_{f,f^{\varphi^j}})(\alpha) = [y\pi_{j'}^{\varphi^j} x\pi_j]_{f,f^{\varphi^{j+j'}}}(\alpha) = [xy\pi_{j+j'}]_{f,f^{\varphi^{j+j'}}}(\alpha).$$

Para ver que $\rho_{f,m}$ es un isomorfismo, consideramos el siguiente diagrama commutativo:

$$\begin{array}{ccccccccc}
\{\mathtt{id}\} & \longrightarrow & \mathtt{Gal}\left((\hat{k}^{\mathtt{ur}})_f^m | \hat{k}^{\mathtt{ur}}\right) & \longrightarrow & \mathtt{W}\left((\hat{k}^{\mathtt{ur}})_f^m | k\right) & \longrightarrow & \mathtt{W}\left(\hat{k}^{\mathtt{ur}} | k\right) & \longrightarrow & \{\mathtt{id}\} \\
 & & \downarrow{\scriptstyle \rho_{f,m}} & & \downarrow{\scriptstyle \rho_{f,m}} & & \downarrow{\scriptstyle \nu} & & \\
\{1\} & \longrightarrow & \mathcal{O}_k^{\times}/(1+\mathfrak{p}_k^m) & \longrightarrow & k^{\times}/(1+\mathfrak{p}_k^m) & \xrightarrow{-\nu_k} & \mathbb{Z} & \longrightarrow & \{1\}.
\end{array}$$

Usando el lema de los cinco concluimos que $\rho_{f,m}$ es un isomorfismo.

□

Lema 5.3.7. El homomorfismo $\psi : \hat{\mathcal{O}}_k^{\times} \to \hat{\mathcal{O}}_k^{\times}$ 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 $\Theta_{\pi'/\pi}^{\hat{k}^{\mathtt{ur}},\times} \neq \emptyset$.

Demostración. Sabemos que $\hat{\mathcal{O}}_k \simeq \varprojlim \mathcal{O}_k/\mathfrak{p}_k^m$ y claramente $\psi(1+\hat{\mathfrak{p}}_k^m) \subset 1+\hat{\mathfrak{p}}_k^m$, de modo que es suficiente probar que para todo $u \in \hat{\mathcal{O}}_k^{\times}$ y para todo $m \geq 1$, existe $\theta_m \in \hat{\mathcal{O}}_k^{\times}$ con $\psi(\theta_m)+\hat{\mathfrak{p}}_k^m = u+\hat{\mathfrak{p}}_k^m$ y $\theta_{m+1}+\hat{\mathfrak{p}}_k^m = \theta_m+\hat{\mathfrak{p}}_k^m$. Para $m=1$, observar que $\psi(\theta)+\hat{\mathfrak{p}}_k = \theta^{q-1}+\hat{\mathfrak{p}}_k$, y como $(\hat{\mathcal{O}}_k/\hat{\mathfrak{p}}_k)^{\times}) \simeq \overline{\mathbb{F}}_q^{\times}$,

el grupo de unidades de un cuerpo algebraicamente cerrado, concluimos que existe θ_1 verificando nuestras condiciones. Obtenido θ_m, vamos a ver como obtener θ_{m+1} de modo que

$$\theta_{m+1}+\hat{\mathfrak{p}}_k^m=\theta_m+\hat{\mathfrak{p}}_k^m,\ \psi(\theta_{m+1})+\hat{\mathfrak{p}}_k^{m+1}=u+\hat{\mathfrak{p}}_k^{m+1}.$$

Escribimos $u/\psi(\theta_m)=1+\alpha\pi^m$ para cierto parámetro de uniformizaciónπ de k. Como la aplicación $\beta+\hat{\mathfrak{p}}_k\mapsto(\beta^\varphi-\beta)+\hat{\mathfrak{p}}_k=(\beta^q-\beta)+\hat{\mathfrak{p}}_k\in\hat{\mathcal{O}}_k/\hat{\mathfrak{p}}_k\simeq\overline{\mathbb{F}}_q$ es sobreyectiva, deducimos que existe $\beta\in\hat{\mathcal{O}}_k$ con $(\beta^\varphi-\beta)+\hat{\mathfrak{p}}_k=\alpha+\hat{\mathfrak{p}}_k$. Definimos $\theta_{m+1}=\theta_m(1+\beta\pi^m)$. Veamos que θ_{m+1} verifica las condicones. Observar que $\theta_{m+1}^{-1}=\theta_m^{-1}(1+\beta\pi^m)=\theta_m^{-1}(\sum_{k=0}^{\infty}(-\beta\pi^m)^k)$, y como $\beta^\varphi-\beta=\alpha+\lambda\pi$, con $\lambda\in\hat{\mathcal{O}}_k$, entonces $(\beta^\varphi-\beta)\pi_m+\hat{\mathfrak{p}}_k^{m+1}=\alpha\pi^m+\lambda\pi^{m+1}+\hat{\mathfrak{p}}_k^{m+1}=\alpha\pi^m+\hat{\mathfrak{p}}_k^{m+1}$.

Por tanto,

$$\begin{aligned}\psi(\theta_{m+1})+\hat{\mathfrak{p}}_k^{m+1}&=\psi(\theta_m)(1+\beta\pi^m)^\varphi(1-\beta\pi^m)+\hat{\mathfrak{p}}_k^{m+1}\\&=\psi(\theta_m)(1+\beta^\varphi\pi^m)(1-\beta\pi^m)+\hat{\mathfrak{p}}_k^{m+1}\\&=\psi(\theta_m)(1+(\beta^\varphi-\beta)\pi^m)+\hat{\mathfrak{p}}_k^{m+1}\\&=\psi(\theta_m)(1+\alpha\pi^m)+\hat{\mathfrak{p}}_k^{m+1}\\&=u+\hat{\mathfrak{p}}_k^{m+1}.\end{aligned}$$

Trivialmente se cumple la condición de compatibilidad.

□

Obtenemos el siguiente corolario, que entre otras cosas nos permite suprimir el subíndice f :

Corolario 5.3.8. Las extensiones $(\hat{k}^{\mathtt{ur}})_f^m$ y los homomorfismos $\rho_{f,m}$ de 5.3.6.2 no dependen de f. En particular, $(\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}},\rho_f$ tampoco dependen de f.

Demostración. Sean f,f' polinomios de Frobenius para ciertos parámteros de uniformización π,π' de $\hat{k}^{\mathtt{ur}}$. Usando 5.3.7, sea $\theta\in\Theta_{\pi'/\pi}^{\hat{k}^{\mathtt{ur}},\times}$ y el isomorfismo asociado $[\theta]_{f,f'}:\mu_{f,m}\to\mu_{f',m}$. Usando 5.3.5 sabemos que $(\hat{k}^{\mathtt{ur}})_f^m=(\hat{k}^{\mathtt{ur}})_{f'}^m$. Así mismo, dado $\sigma\in\mathtt{W}\left((\hat{k}^{\mathtt{ur}})_f^m|k\right)$ con $\sigma(\alpha)=[x\pi_j]_{f,f^{\varphi^j}}(\alpha)$, entonces

$$\begin{aligned}\sigma([\theta]_{f,f'}(\alpha))&=([\theta^{\varphi^j}]_{f^{\varphi^j},f'^{\varphi^j}}\circ[x\pi_j]_{f,f^{\varphi^j}})(\alpha)\\&=[\theta^{\varphi^j}x\pi_j]_{f,f'^{\varphi^j}}(\alpha)\\&\overset{5.3.4}{=}[x\pi_j'\theta]_{f,f'^{\varphi^j}}(\alpha)\\&=[x\pi_j']_{f',f'^{\varphi^j}}([\theta]_{f,f'}(\alpha)),\end{aligned}$$

de modo que $\rho_{f,m}=\rho_{f',m}$.

□

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

Lema 5.3.9. 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 $E \cap \widehat{F} = F$.

Demostración. 1. La extensión $E\widehat{F} \supset \widehat{F}$ es finita, luego la valoración de $\widehat{F}$ se extiende de manera única a $E\widehat{F}$ y $E\widehat{F}$ es completo respecto a dicha valoración. Claramente, dicha extensión de la valoración de $\widehat{F}$ coincide con la restricción a $E\widehat{F}$ de la valoración de $\widehat{E}$, deducimos que $E\widehat{F}$ es cerrado en $\widehat{E}$. Por otro lado, tenemos que $E \subset E\widehat{F} \subset \widehat{E}$, de modo que $E\widehat{F}$ es denso en $\widehat{E}$ y concluimos que se tiene la igualdad $E\widehat{F} = \widehat{E}$.

2. Por la primera parte del lema, $\widehat{E} = E\widehat{F}$ por tanto $\widehat{E} \supset \widehat{F}$ es una extensión de Galois y
$$[\widehat{E} : \widehat{F}] = [E\widehat{F} : \widehat{F}] = [E : E \cap \widehat{F}] \leq [E : F],$$
gracias a 4.3.3.1. Sabemos que todo elemento $\sigma \in \mathtt{Gal}(\widehat{E}|\widehat{F})$, cuando se restringe a E es una inmersión de E en $\widehat{E}$ que es la identidad sobre F. Como la extensión $E \supset F$ es normal, tenemos que la imagen de esta restricción debe ser E. Vemos así que la aplicación $\mathtt{Gal}(\widehat{E}|\widehat{F}) \to \mathtt{Gal}(E|F)$ está bien definida y es un homomorfismo. Además, esta aplicación es inyectiva pues todo elemento de $\mathtt{Gal}(\widehat{E}|\widehat{F})$ actúa de manera continua sobre $\widehat{E}$ y por ello está determinado por su restricción al subcuerpo denso E. La sobreyectividad se debe a que todo elemento de $\mathtt{Gal}(E|F)$ se extiende por continuidad a un elemento de $\mathtt{Gal}(\widehat{E}|\widehat{F})$. Con esto concluimos que la restricción es un isomorfismo y además $[\widehat{E} : \widehat{F}] = [E : F]$ de modo que $[E \cap \widehat{F} : F] = 1$, es decir, $E \cap \widehat{F} = F$.

3. Gracias a la segunda parte, el resultado es cierto para extensiones de Galois finitas. Veamos que este caso es suficiente. Primero observar que si la extensión $E \supset F$ es infinita, entonces $E \cap \widehat{F} = F$ si y sólo si para toda subextensión finita $E \supset E' \supset F$ se verifica que $E' \cap \widehat{F} = F$. Segundo, dada una extensión finita separable $E \supset F$, consideramos su clausura normal $N \supset$

$E \supset F$ de modo que $N \supset F$ es una extensión de Galois finita. Gracias al apartado anterior, se tiene la igualdad

$$F \subset E \cap \widehat{F} \subset N \cap \widehat{F} = F$$

y se obtiene el enunciado.

□

Usando el resultado 5.3.9 podemos hacer la siguiente definición:

Definición 5.3.10. 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 $\mathtt{W}(k_f^{\mathtt{LT}}|k) \simeq \mathtt{W}\left((\hat{k}^{\mathtt{ur}})_f^{\mathtt{LT}}|k\right)$. Diremos que toda extensión finita de k contenida en $k_f^{\mathtt{LT}}$ es una **extensión 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 hemos llamado "categorificar". 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, si no 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 estos y obtener los llamados *módulos de Lubin-Tate* $\mu_{f,m}$. Observar que nuestra categoría es más pequeña en cuanto objetos y morfismos que la categoría completa de las series de Frobenius y todos los homomorfismos entre sus leyes de grupo formal.

El último paso ha sido adjuntar estas raíces al cuerpo L y obtener las *cuerpos 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). En este punto es esencial haber disminuido el número de morfismos, ya que los morfismos que proceden de los grupos abelianos Θ_u^L inducen isomorfismos entre los módulos de Lubin-Tate y como son series de potencias concluimos que las extensiones de Frobenius son un *invariante de la clase de isomorfía de* f.

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 nuestra candidata para la teoría de cuerpos de clase.

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

5.4.1. Grupos de Galois

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

Lema 5.4.1. 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 $\nu_k^{-1}(\mathbb{Z}n) \subset k^\times$.

Demostración. 1. Veamos que k_n es el cuerpo fijo de φ^n en $k^{\mathtt{ur}}$. Sabemos que $\mathtt{Gal}(k^{\mathtt{ur}}|k)$ es isomorfo a $\hat{\mathbb{Z}}$, un grupo pro-cíclico. Por otro lado, si es F el cuerpo fijo de φ^n en $k^{\mathtt{ur}}$, por teoría de Galois tenemos que $\mathtt{Gal}(k^{\mathtt{ur}}|F) = \overline{\langle \varphi^n \rangle}$, de modo que $\mathtt{Gal}(k^{\mathtt{ur}}|F)$ es un subgrupo abierto de $\mathtt{Gal}(k^{\mathtt{ur}}|k)$ con índice n. Por otro lado, tenemos que $k_n \subset F$ pues k_n es el cuerpo de descomposición de $X^{q^n} - X$ sobre k, con $q = |\overline{k}|$, y el elemento de Frobenius φ actúa sobre las raíces de la unidad $X^{q^n-1} - 1$ igual que elevar a q. Concluimos que $\mathtt{Gal}(k^{\mathtt{ur}}|F) \subset \mathtt{Gal}(k^{\mathtt{ur}}|k_n)$ y usando que ambos tiene índice n obtenemos la igualdad.

Gracias a lo anterior y a la subsección 3.1.1 podemos terminar la demostración del resultado. Usaremos la notación de 3.1.1. Sea $\pi \in k$ un parámetro de uniformización de modo que π

también es un parámetro de uniformización de $\hat{k}^{\mathtt{ur}}$. Sea $a \in \hat{k}^{\mathtt{ur}}$ que podemos expresar de forma única como $a = \sum_{j=m}^{\infty} \alpha_j \pi^j, \alpha_j \in \cup_{n\geq 0}\mu_{q^n-1}, m \in \mathbb{Z}$. Entonces $a^{\varphi^n} = \sum_{j=m}^{\infty} \alpha_j^{\varphi^n} \pi^j$. Como esta expresión es única, tenemos que $a^{\varphi^n} = a$ si y sólo si $\alpha_j = \alpha_j^{\varphi^n}$ para todo j. Por la primera parte y teniendo en cuenta que $\cup_{n\geq 0}\mu_{q^n-1} \subset k^{\mathtt{ur}}$, vemos que la última condición se cumple si y sólo si $\alpha_j \in k_n$ para todo j. Deducimos que $\alpha_j \in (\mu_{q^n-1} \cup \{0\}) \cap k_n = \mu_{q^n-1} \cup \{0\}$ para todo j y por ello $a \in \overline{k_n} = k_n$ pues k_n es completo y $\mu_{q^n-1} \cup \{0\}$ es un sistema de representantes de $\mathcal{O}_{k_n}$.

2. Si π es un parámetro de uniformización de k, tenemos que $\nu_k^{-1}(\mathbb{Z}n) = \mathcal{O}_k^{\times} \times \langle \pi^n \rangle$ con $\mathtt{N}_{k_n|k}(\pi) = \pi^n$, luego es suficiente probar que $\mathtt{N}_{k_n|k} : \mathcal{O}_{k_n}^{\times} \to \mathcal{O}_k^{\times}$ es sobreyectiva. Sabemos que $\mathcal{O}_k^{\times} \simeq \varprojlim \mathcal{O}_k^{\times}/(1+\mathfrak{p}_k^m)$, $\mathcal{O}_{k_n}^{\times} \simeq \varprojlim \mathcal{O}_L^{\times}/(1+\mathfrak{p}_L^m)$ y $\mathtt{N}_{k_n|k}(1+\mathfrak{p}_L^m) \subset (1+\mathfrak{p}_L^m) \cap \mathcal{O}_k = 1+\mathfrak{p}_k^m$. Con estas observaciones podemos reducirnos a probar que para todo $x \in \mathcal{O}_k^{\times}$ y para todo $m \geq 1$ existe $u_m \in \mathcal{O}_L^{\times}$ verificándose:

$$\mathtt{N}_{k_n|k}(u_m) + \mathfrak{p}_k^m = x + \mathfrak{p}_k^m,$$

$$u_m + 1 + \mathfrak{p}_L^m = u_m + \mathfrak{p}_L^m.$$

Para $m = 1$, como $\overline{k} \subset \overline{k_n}$ es una extensión finita de cuerpos finitos, la norma es sobreyectiva. Supuesto que hemos obtenido u_m verificando las condiciones anteriores veamos como obtener u_{m+1}. Sea $x/\mathtt{N}_{k_n|k}(u_m) = 1 + \alpha\pi^m$. De nuevo, usando que la traza de extensiones finitas de cuerpos finitos es sobreyectiva, deducimos que existe $\beta \in \mathcal{O}_L$ tal que $\mathtt{Tr}_{k_n|k}(\beta) + \mathfrak{p}_k = \alpha + \mathfrak{p}_k$. Definimos $u_{m+1} := u_m(1+\beta\pi^m)$. Claramente $u_{m+1} + \mathfrak{p}_L^m = u_m + \mathfrak{p}_L^m$. Para la otra condición, observar que

$$\mathtt{N}_{k_n|k}(1+\beta\pi^m) + \mathfrak{p}_k^{m+1} = \prod_{k=0}^{n-1}(1+\beta^{\varphi^k}\pi^m) + \mathfrak{p}_k^{m+1} = (1 + \mathtt{Tr}_{k_n|k}(\beta)\pi^m) + \mathfrak{p}_k^{m+1},$$

$$\mathtt{Tr}_{k_n|k}(\beta)\pi^m + \mathfrak{p}_k^{m+1} = \alpha\pi^m + \mathfrak{p}_k^{m+1},$$

de modo que

$$\mathtt{N}_{k_n|k}(u_{m+1}) + \mathfrak{p}_k^{m+1} = \mathtt{N}_{k_n|k}(u_m) \cdot (1 + \mathtt{Tr}_{k_n|k}(\beta)\pi^m) + \mathfrak{p}_k^m = \mathtt{N}_{k_n|k}(u_m) \cdot (1+\alpha\pi^m) + \mathfrak{p}_k^{m+1} = x + \mathfrak{p}_k^{m+1}.$$

□

El siguiente resultado nos dice cuando dos grupos de Lubin-Tate son isomorfismos sobre k_n :

Proposición 5.4.2. Sean π, π' parámetros de uniformización de k_n y $\theta \in \Theta_{\pi'/\pi}^{\hat{k}^{\mathtt{ur}},\times}$. Entonces $\theta \in \Theta_{\pi'/\pi}^{k_n,\times}$ si y sólo si $\mathtt{N}_{k_n|k}(\pi) = \mathtt{N}_{k_n|k}(\pi')$.

Demostración. Usamos 5.3.4 con $j = n$ de modo que $\theta^{\varphi^n}\mathtt{N}_{k_n|k}(\pi') = \theta^{\varphi^n}\pi'_n = \pi_n\theta = \mathtt{N}_{k_n|k}(\pi)\cdot\theta$. El resultado es inmediato usando esta igualdad.

□

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 $(k_n)_f^m$ sólo dependen de los conjuntos (no vacíos por 5.4.1.2) $\{\pi \in k_n \mid \nu_{k_n}(\pi) = 1 \text{ y } \mathtt{N}_{k_n|k}(\pi) = x\}$, pues para un mismo parámetro de uniformización considerar distintos polinomios de Frobenius da lugar a leyes de grupo formal isomorfas y gracias a 5.4.2 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.

Tenemos la siguiente caracterización del homomorfismo de Artin para elementos que proceden de la norma:

Proposición 5.4.3. 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 $\sigma := \mathtt{Art}_k\left(\mathtt{N}_{k_n|k}(\pi)\right) \in \mathtt{W}\left(k_f^{\mathtt{LT}}|k\right)$ se caracteriza por las siguientes condiciones:

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

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

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

Demostración. Como $\nu \circ \mathtt{Art}_k = -\nu_k$ sabemos que $\sigma_{k^{\mathtt{ur}}} = \varphi^{-n}$ y por ello σ actúa sobre k_n como $\varphi^{-n}_{|k_n} = \mathtt{id}$. Así mismo, sabemos que $x = \mathtt{N}_{k_n|k}(\pi) = \pi_n$ y $\pi_{-n} = (\pi_n^{-1})^{\varphi^{-n}} = \pi_n^{-1}$ luego

$$[x\pi_{-n}]_{f,f^{\varphi^{-n}}} \overset{f\in\mathcal{O}_{k_n}[X]}{=} [1]_{f,f} = \mathtt{id}.$$

Concluimos que $\sigma_{(k_n)_f^m} = \mathtt{id}$ para todo $m \geq 1$. Por último, estas condiciones caracterizan a σ pues

$$k_f^{\mathtt{LT}} = \bigcup_{m\geq 1} k^{\mathtt{ur}}(k_n)_f^m = k^{\mathtt{ur}}\left(\bigcup_{m\geq 1}(k_n)_f^m\right)$$

con $k^{\mathtt{ur}} \cap \cup_m (k_n)_f^m = k_n$ ya que $\cup_m (k_n)_f^m \supset k_n$ es una extensión totalmente ramificada, es decir, lo caracterizamos gracias al isomorfismo de la teoría de Galois

$$\mathtt{Gal}\left(k_f^{\mathtt{LT}}|k^{\mathtt{ur}}\right) \xrightarrow{\simeq} \mathtt{Gal}\left(\cup_m (k_n)_f^m|k_n\right).$$

Para la última parte del enunciado razonamos como sigue. Consideramos la composición:

$$k^\times \xrightarrow{\mathtt{Art}_k} \mathtt{W}\left(k_f^{\mathtt{LT}}|k\right) \longrightarrow \mathtt{Gal}(\left(k_n\right)_f^m|k)\,,$$

donde la segunda flecha es la restricción. Dicha restricción es un homomorfismo sobreyectivo pues $\mathtt{W}\left(k_f^{\mathtt{LT}}|k\right)$ es subgrupo denso en $\mathtt{Gal}\left(k_f^{\mathtt{LT}}|k\right)$ y $(k_n)_f^m \supset k$ es una extensión de Galois finita. Vamos a estudiar el núcleo de la composición. Supongamos que $y \in k^\times$ tal que $\mathtt{Art}_k(y)_{|(k_n)_f^m} = \mathtt{id}$. En particular, será $\mathtt{Art}_k(y)_{|k_n} = \mathtt{id}$ y por ello $v := \nu_k(y) = tn,\ t \in \mathbb{Z}$. Sea $\pi \in k_n$ un parámetro de uniformización arbitrario y sea $f \in \mathcal{O}_{k_n}[X]$ un polinomio de Frobenius asociado a π. Tenemos que

$$\pi_{-v} = \pi_{-tn} = \pi_{-(t+1)n+n} = \pi_{-(t+1)n}\pi_n = \cdots = \pi_n^{-t}$$

y $f^{\varphi^{-v}} = f^{\varphi^{-tn}} = f$ de modo que

$$\mathtt{id} = \mathtt{Art}_k(y)_{|\mu_{f,m}} = [y\pi_{-v}]_{f,f}|\mu_{f,m} = \left[y\mathtt{N}_{k_n|k}(\pi)^{-t}\right]_{f,f}|\mu_{f,m}.$$

Deducimos que $y\mathtt{N}_{k_n|k}(\pi)^{-t} \in (1+\mathfrak{p}_k^m)$, es decir, $y \in (1+\mathfrak{p}_k^m) \times \langle \mathtt{N}_{k_n|k}(\pi)\rangle$. La otra inclusión es inmediata. Usando el primer teorema de isomorfía obtenemos el resultado del enunciado.

□

5.4.2. 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, $f \in \mathcal{O}_L[X]$ polinomio de Frobenius para π. Para la construcción de dicho operador hace falta el siguiente lema sobre series de potencias:

Lema 5.4.4. 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 $h \in \mathcal{O}_{k_n}[[X]]$.

Demostración. Ver [Yos08] *Lema 5.5.3.*

□

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 $\mathtt{Gal}\left((k_n)_f^1|k_n\right)$ a dichos coeficientes.

Notar que dicho producto verifica las condiciones de 5.4.4 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 $\mathtt{N}_f(g_1 g_2) = \mathtt{N}_f(g_1)\mathtt{N}_f(g_2)$. 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 del operador norma, así definidas, no es muy clara. En realidad, tenemos que

$$\mathtt{N}_f^m = \mathtt{N}_{f^{\varphi^{m-1}}} \circ \mathtt{N}_f^{m-1} = \cdots = \mathtt{N}_{f^{\varphi^{m-1}}} \circ \cdots \circ \mathtt{N}_{f^{\varphi}} \circ \mathtt{N}_f.$$

En efecto, esta identidad podemos demostrarla por inducción. Supongamos el resultado cierto para m, es decir, $\mathtt{N}_f^m = \mathtt{N}_{f^{\varphi^{m-1}}} \circ \mathtt{N}_f^{m-1}$. Se cumple la siguiente igualdad:

$$\begin{aligned}\left(\mathtt{N}_f^m(\mathtt{N}_f(g)^{\varphi^{-1}}) \circ f^{\varphi^{m-1}}\right)(X) &= \left(\mathtt{N}_{f^{\varphi^{m-1}}}(\mathtt{N}_f^{m-1}(\mathtt{N}_f(g)^{\varphi^{-1}})) \circ f^{\varphi^{m-1}}\right)(X) \\ &= \left(\mathtt{N}_{f^{\varphi^{m-1}}}(\mathtt{N}_f^m(g)^{\varphi^{-1}}) \circ f^{\varphi^{m-1}}\right)(X) \\ &= \prod_{\alpha \in \mu_{f^{\varphi^{m-1}},1}} \mathtt{N}_f^m(g)^{\varphi^{-1}}(X +_{F_{f^{\varphi^{m-1}}}} \alpha).\end{aligned}$$

Si $\tilde{\varphi}$ es una extensión arbitraria de φ a $(k_n)_f^1$, aplicando $\tilde{\varphi}$ a todos los coeficientes obtenemos la igualdad:

$$\begin{aligned}(\mathtt{N}_f^{m+1}(g) \circ f^{\varphi^m})(X) &= \prod_{\alpha \in \mu_{f^{\varphi^m},1}} \mathtt{N}_f^m(g)(X +_{F_{f^{\varphi^m}}} \alpha^{\tilde{\varphi}}) \\ &\overset{*}{=} \prod_{\alpha \in \mu_{f^{\varphi^m},1}} \mathtt{N}_f^m(g)(X +_{F_{f^{\varphi^m}}} \alpha) \\ &= (\mathtt{N}_{f^{\varphi^m}}(\mathtt{N}_f^m(g)) \circ f^{\varphi^m})(X),\end{aligned}$$

usando en $*$ que al ser $\tilde{\varphi}$ un automorfismo el producto no se ve afectado salvo un cambio en el orden de los factores. Usando la unicidad de 5.4.4 concluimos que

$$\mathtt{N}_f^{m+1} = \mathtt{N}_{f^{\varphi^m}} \circ \mathtt{N}_f^m.$$

La siguientes propiedades serán muy útiles en lo que sigue:

Lema 5.4.5. 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 $\mathtt{N}_f^m(g)/\mathtt{N}_f^{m-1}(g)^{\varphi} \equiv 1 \pmod{\mathfrak{p}_L^m}$.

Demostración. Ver [Yos08] *Proposiciones 5.7 y 5.8.*

□

Grupos de Normas

En la siguiente proposición utilizaremos de forma esencial el operador norma antes construido:

Proposición 5.4.6. 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, $\mathtt{N}_{(k_n)_f^m|k}\left((k_n)_f^{m\times}\right) = (1+\mathfrak{p}_k^m) \times \langle \mathtt{N}_{k_n|k}(\pi)\rangle$ para todo $m \geq 1$.

Demostración. Sea $\alpha \in \mu_{f,m}^\times$. Gracias a 5.3.3.2 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 5.3.3.2, 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 que $\mathtt{N}_{k_n(\alpha)|k}(\mathcal{O}_{k_n(\alpha)}^\times) = 1+\mathfrak{p}_k^m$.

$\mathtt{N}_{k_n(\alpha)|k}(\mathcal{O}_{k_n(\alpha)}^\times) \subset 1+\mathfrak{p}_k^m$: Gracias a 3.2.1 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. Para $i \geq 0$ definimos $u_i := \mathtt{N}_f^i(g)(0)$. Gracias a 5.4.6.1 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 5.4.6.4 $u_m/u_{m-1}^{\varphi} \in 1+\mathfrak{p}_{k_n}^m$. Concluimos que

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

$\mathtt{N}_{k_n(\alpha)|k}(\mathcal{O}^\times_{k_n(\alpha)}) \supset \mathbf{1}+\mathfrak{p}_k^m$ **:** Gracias a 5.4.3 tenemos el isomorfismo

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

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 $x'/x \in 1+\mathfrak{p}_k^m$ entonces $(1+\mathfrak{p}_k^m)\times\langle x\rangle = (1+\mathfrak{p}_k^m)\times\langle x'\rangle$ de modo que ambos subgrupos tienen el mismo cuerpo fijo, en particular, al ser x la norma de un elemento de $(k_n)_f^m$ deducimos que también lo es x'. 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 $u = (ux)/x \in \mathtt{N}_{(k_n)_f^m|k}\left((k_n)_f^{m\times}\right)$ y llegamos a la inclusión $1+\mathfrak{p}_k^m \subset \mathtt{N}_{(k_n)_f^m|k}\left((k_n)_f^{m\times}\right)$, es decir, $1+\mathfrak{p}_k^m \subset \mathtt{N}_{(k_n)_f^m|k}\left((k_n)_f^{m\times}\right)\cap\mathcal{O}_k^\times = \mathtt{N}_{(k_n)_f^m|k}\left(\mathcal{O}^\times_{(k_n)_f^m}\right)$.

□

Probaremos un último resultado sobre subgrupos de normas. Necesitaremos algunos lemas:

Lema 5.4.7. 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 $K^\times$.

Demostración. Sabemos que la norma $\mathtt{N}_{L|K} : L \to K$ es continua y $\mathcal{O}_K^\times$ es compacto en $K^\times$. Deducimos que $\mathtt{N}_{L|K}(\mathcal{O}_L^\times)$ es un subconjunto compacto del espacio de Hausdorff $L^\times$ de modo que también es cerrado en $L^\times$. Ahora bien, si denotamos por ν_L la única extensión normalizada de ν_K a L, sabemos que $\nu_L = (1/f)\cdot\nu_k\circ\mathtt{N}_{L|K}$ con f el grado residual de la extensión $L \supset K$. Entonces $\mathtt{N}_{L|K}(\mathcal{O}_L^\times) = \mathtt{N}_{L|K}(L^\times)\cap\mathcal{O}_K^\times \subset \mathcal{O}_K^\times$. Como $\mathcal{O}_K$ es un abierto de $K^\times$ deducimos que $\mathtt{N}_{L|K}(\mathcal{O}_L^\times)$ es abierto en $\mathtt{N}_{L|K}(L^\times)$ de modo que el cociente $\mathtt{N}_{L|K}(L^\times)/\mathtt{N}_{L|K}(\mathcal{O}_L^\times)$ es un subgrupo discreto $K^\times/\mathtt{N}_{L|K}(\mathcal{O}_L^\times)$. De aquí se deduce que $\mathtt{N}_{L|K}(L^\times)$ es un cerrado de $K^\times$.

□

Lema 5.4.8. Sea $E \supset K$ una extensión algebraica totalmente ramificada. Se verifica:

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

Demostración. El conjunto $\nu_K^{-1}(1) = \pi\mathcal{O}_K^\times$ es compacto en K. Cada intersección $\pi\mathcal{O}_K^\times\cap\mathtt{N}_{F|K}(F^\times)$, con $K\subset F\subset E$ y $K\subset F$ finita, es un subconjunto cerrado de $\pi\mathcal{O}_K^\times$ gracias a 5.4.7. Usando la caracterización de los conjuntos compactos por medio de la propiedad de intersección finita, para nosotros es suficiente probar que las intersecciones finitas $\pi\mathcal{O}_K^\times\cap\mathtt{N}_{F_1|K}(F_1^\times)\cap\cdots\cap\mathtt{N}_{F_r|K}(F_r^\times)$ son no vacías. Pero la intersección de un número finito de subgrupos de normas $\mathtt{N}_{F_j|K}(F_j^\times)$ contiene al subgrupo de normas $\mathtt{N}_{F|K}(F^\times)$ con $F = F_1\cdots F_r$. Como la extensión $F\supset K$ es totalmente ramificada (subextensión finita de una extensión totalmente ramificada) sabemos que $\pi\mathcal{O}_K^\times\cap\mathtt{N}_{F|K}(F^\times)$

contiene la norma de un elemento primo de $\mathcal{O}_F$ y gracias a 3.2.1 dicha norma es un elemento primo de $\mathcal{O}_K$.

□

Probamos el resultado que nos interesa:

Proposición 5.4.9. 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

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

Demostración. Usando la igualdad $\bigcap_m (1+\mathfrak{p}_k^m) = \{1\}$ obtenemos la inclusión siguiente:

$$\bigcap_{\substack{k\subset F\subset E\\ k\subset F \text{ finita}}} \mathtt{N}_{F|k}(F^\times) \subset \bigcap_{\substack{k\subset F\subset \bigcup_m (k_n)_f^m\\ k\subset F \text{ finita}}} \mathtt{N}_{F|k}(F^\times)$$

$$\subset \bigcap_{m\geq 1} \mathtt{N}_{(k_n)_f^m|k}\left((k_n)_f^{m\times}\right) \overset{5.4.6}{=} \left(\bigcap_{m\geq 1} 1+\mathfrak{p}_k^m\right) \times \langle x\rangle = \langle x\rangle.$$

Ahora bien, al ser la extensión $E \supset k_n$ totalmente ramificada, gracias a 5.4.8, existe $\pi \in k_n$ parámetro de uniformización tal que $\pi \in \bigcap_{\substack{k_n\subset L\subset E\\ k_n\subset L \text{ finita}}} \mathtt{N}_{L|k_n}(L^\times)$. Además sabemos que

$$\nu_{k_n} = (1/n)\cdot \nu_k \circ \mathtt{N}_{k_n|k},$$

siendo ν_{k_n} la valoración normalizada de k_n. Concluimos que $\mathtt{N}_{k_n|k}(\pi) \in \bigcap_{\substack{k\subset F\subset E\\ k\subset F \text{ finita}}} \mathtt{N}_{F|k}(F^\times)$ con $\nu_k(\mathtt{N}_{k_n|k}(\pi)) = n$.

□

5.4.3. 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.

La siguiente proposición pone de manifiesto que los cuerpos de Lubin-Tate que hemos construido y los resultados probados sobre sus grupos de normas son suficientemente fuertes como para poder obtener algo de información de $k^{\mathtt{sep}}$:

Proposición 5.4.10. 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

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

Demostración. Como $\sigma \in \mathtt{W}(k^{\mathtt{sep}}|k)$ sabemos que $\sigma_{|k^{\mathtt{ur}}} \in \langle\varphi\rangle$, de modo que $(\sigma_{|k^{\mathtt{LT}}})_{|k^{\mathtt{ur}}} = \sigma_{|k^{\mathtt{ur}}} \in \langle\varphi\rangle$ y $\sigma_{|k^{\mathtt{LT}}} \in \mathtt{W}(k^{\mathtt{LT}}|k)$. Podemos considerar $x := \mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}}) \in k^\times$ con $\nu_k(x) = n$. Sea $\pi \in k_n$ 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. Gracias a 5.4.3 tenemos que $\sigma_{|(k_n)_f^m} = \mathtt{id}$ para todo $m \geq 1$ de modo que $\cup_m (k_n)_f^m \subset (k^{\mathtt{sep}})^\sigma$. También por 5.4.3 tenemos que $(k^{\mathtt{sep}})^\sigma \cap k^{\mathtt{ur}} = (k^{\mathtt{ur}})^{\sigma_{|k^{\mathtt{ur}}}} = k_n$. Aplicando 5.4.9 obtenemos el enunciado.

□

Ahora podemos demostrar cómodamente el **teorema del cambio de base:**

Teorema 5.4.11. 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:

$$\begin{aligned}
\langle \mathtt{N}_{k'|k}(x') \rangle &= \mathtt{N}_{k'|k}(\langle x' \rangle) \\
&= \mathtt{N}_{k'|k}(\langle \mathtt{Art}_{k'}^{-1}(\sigma_{|k'^{\mathtt{LT}}}) \rangle) \\
&\overset{5.4.10}{=} \mathtt{N}_{k'|k}\left(\bigcap_{\substack{k' \subset F' \subset (k^{\mathtt{sep}})^{\sigma} \\ k' \subset F' \text{ finita}}} \mathtt{N}_{F'|k'}(F'^{\times}) \right) \\
&\subset \bigcap_{\substack{k \subset F \subset (k^{\mathtt{sep}})^{\sigma} \\ k \subset F \text{ finita}}} \mathtt{N}_{F|k}(F^{\times}) \\
&\overset{5.4.10}{=} \langle \mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}}) \rangle.
\end{aligned}$$

Para obtener la igualdad, observar que en $\langle \mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}}) \rangle$ hay un único elemento con valoración igual $\nu_k(\mathtt{Art}_k^{-1}(\sigma_{|k^{\mathtt{LT}}})) = -\nu(\sigma_{|k^{\mathtt{LT}}})$, por lo que es suficiente probar que en $\langle \mathtt{N}_{k'|k}(x') \rangle$ también hay un elemento con dicha valoración. Ahora bien, esto es inmediato por las siguientes igualdades:

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

donde $*$ se tiene gracias a que $\sigma_{|k^{\mathtt{ur}}} = \varphi_k^{-\nu_{k'}(x')f(k'|k)}$. De hecho, la igualdad entre las valoraciones prueba que $\nu(\sigma_{k^{\mathtt{LT}}})$ es no nulo pues $x' \in \mathfrak{p}_{k'}$, de modo que el razonamiento es válido.

Más aún, gracias 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, $\tau_{|k^{\mathtt{LT}}} = \mathtt{id}$. Deducimos que $k^{\mathtt{LT}} \subset (k^{\mathtt{sep}})^{\mathtt{Gal}(k^{\mathtt{sep}}|k'^{\mathtt{LT}})} = k'^{\mathtt{LT}}$. 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 para k^{LT} no es más que un corolario:

Corolario 5.4.12. (Teoría de Cuerpos de Clase para k^{LT})

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

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

   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 $\mathtt{W}(k^{\mathrm{LT}}|k)$.

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

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

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 5.4.11. Recíprocamente, sea $\mathcal{F}$ un homomorfismo verificando (a) y (b). Sea π es un parámetro de uniformización de k y $f \in \mathcal{O}_k[X]$ un polinomio de Frobenius para π. Gracias a 5.3.3.2 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 $k_f^{\mathrm{LT}} = k^{\mathtt{ur}} \cdot \cup_m (k_1)_f^m = \cup_m k_f^m$, usando el isomorfismo de la teoría de Galois $\mathtt{Gal}(k_f^{\mathrm{LT}}|k) \longrightarrow \mathtt{Gal}(k^{\mathtt{ur}}|k) \times \mathtt{Gal}(\cup_m (k_1)_f^m|k)$ (es isomorfismo pues $k^{\mathtt{ur}} \cap \cup_m (k_1)_f^m = k_1 = k$) (ver 4.3.3.2) deducimos que $\mathcal{F}(\pi)$ está caracterizado por las condiciones $\mathcal{F}(\pi)_{k^{\mathrm{ur}}} = \varphi^{-1}, \mathcal{F}(\pi)_{|\cup_m (k_1)_f^m} = \mathtt{id}$ 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 5.4.11. 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:

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

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 sigue 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:

$$\begin{array}{ccccc} & & & & \{\mathtt{id}\} \\ & & & & \downarrow \\ \mathtt{Gal}(k'^{\mathtt{LT}}|k') & \xrightarrow{\mathtt{res}} & \mathtt{Gal}(k^{\mathtt{LT}}k'|k') & \xrightarrow{\simeq} & \mathtt{Gal}(k^{\mathtt{LT}}|(k' \cap k^{\mathtt{LT}})) \\ & \searrow^{\mathtt{res}} & & & \downarrow \\ & & & & \mathtt{Gal}(k^{\mathtt{LT}}|k) \\ & & & & \downarrow{\scriptstyle \mathtt{res}} \\ & & & & \mathtt{Gal}((k' \cap k^{\mathtt{LT}})|k) \\ & & & & \downarrow \\ & & & & \{\mathtt{id}\} \end{array}$$

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. Para ello probaremos algunos resultados más de la teoría de cuerpos de clase local que nos simplificarán la tarea.

Corolario 5.4.13. 1. **Teorema de Limitación:** Sea $k' \supset k$ una extensión separable finita arbitraria. Entonces

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

teniéndose 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 $\mathtt{N}_{k'|k}(k'^{\times})/\mathtt{N}_{k''|k}(k''^{\times}) \to \mathtt{Gal}(k''|k')$.

Demostración. 1. Aplicamos 5.4.12.2. Tenemos el diagrama conmutativo siguiente

$$\begin{array}{ccccc} & & \mathtt{Gal}((k' \cap k^{\mathtt{LT}})|k) & & \\ & \nearrow^{\mathtt{Art}_{k'|k}} & & \nwarrow_{\mathtt{Art}_{(k' \cap k^{\mathtt{LT}})|k}} & \\ \dfrac{k^{\times}}{\mathtt{N}_{k'|k}(k'^{\times})} & & \longrightarrow & & \dfrac{k^{\times}}{\mathtt{N}_{(k' \cap k^{\mathtt{LT}})|k}((k' \cap k^{\mathtt{LT}})^{\times})} \end{array}$$

siendo el homomorfismo inferior el homomorfismo inducido por la inclusión $\mathtt{N}_{k'|k}(k'^{\times}) \subset \mathtt{N}_{(k' \cap k^{\mathtt{LT}})|k}((k' \cap k^{\mathtt{LT}})^{\times})$. Sabemos que $\mathtt{Art}_{k'|k}$ y $\mathtt{Art}_{(k' \cap k^{\mathtt{LT}})|k}$ son isomorfismos, de modo que $(k^{\times} : \mathtt{N}_{(k' \cap k^{\mathtt{LT}})|k}((k' \cap k^{\mathtt{LT}})^{\times})) = (k^{\times} : \mathtt{N}_{k'|k}(k'^{\times}))$. Como uno está incluido en el otro, deben ser iguales.

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

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

Concluimos que $(k^{\times} : \mathtt{N}_{k'|k}(k'^{\times})) = [k' : k]$ si y sólo si $k' = k' \cap k^{\mathtt{LT}}$.

2. Al ser $k'' \supset k$ una extensión de Lubin-Tate, sabemos que $k'' \subset k'$ si y sólo si $k'' \subset k' \cap k^{\mathtt{LT}}$. Esto último es equivalente a $\mathtt{Gal}(k^{\mathtt{LT}}|(k' \cap k^{\mathtt{LT}})) \subset \mathtt{Gal}(k^{\mathtt{LT}}|k'')$, que a su vez, gracias a 5.4.12.2, equivale a

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

3. Las siguientes igualdades son inmediatas:

$$\begin{aligned} \mathtt{Art}_{k''|k}(x\mathtt{N}_{k''|k}(k''^{\times}))_{|k'} &= (\mathtt{Art}_k(x)_{|k''})_{|k'} \\ &= \mathtt{Art}_k(x)_{|k'} \\ &= \mathtt{Art}_{k'|k}(x\mathtt{N}_{k'|k}(k'^{\times})). \end{aligned}$$

□

Teorema 5.4.14. (Teorema de Existencia para k^{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 $\pi^n \in H$. Es $H \cap \mathcal{O}_k^\times$ 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 5.4.6 (con $x = \pi^m$) sabemos que $(1 + \mathfrak{p}_k^m) \times \langle \pi^m \rangle = \mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\times})$ para algún polinomio de Frobenius $f \in \mathcal{O}_{k_n}[X]$ asociado a π. Gracias a 5.4.12.2 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 $H/\mathtt{N}_{(k_n)_f^m|k}((k_n)_f^{m\times})$, es decir, 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 5.4.13.3, 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 5.4.13.2.

□

Si combinamos 5.4.7 con 5.4.13.1 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 5.4.14. Además es conocido 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 equivalencia:

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

Esta equivalencia invierte las inclusiones (anti-isomorfismo) debido a 5.4.13.2. 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.

5.5. 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 enunciados de la Sección 4 del Capítulo 3 dedicada a los grupos de ramificación y usaremos la notación introducida allí.

Comenzamos estudiando brevemente los grupos de ramificación *relativos* de las extensiones de Galois introducidas en las secciones anteriores:

Proposición 5.5.1. 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 $m \geq 1$.

Demostración. Sea $\alpha \in \mu_{f,m}^\times$ de modo que $(k_n)_f^m = k_n(\alpha)$. Como α es un parámetro de uniformización de $(k_n)_f^m$ basta que estudiemos el valor de $\nu_{(k_n)_f^m}(\sigma\alpha - \alpha)$ para $\sigma \in \mathtt{Gal}((k_n)_f^m|k_n) \setminus \{\mathtt{id}\}$. Usando el isomorfismo de 5.3.3.3, supongamos que $\rho_{f,m}(\sigma) = [u]_f \in (\mathcal{O}_k/\mathfrak{p}_k^m)^\times$ de modo que $\sigma(\alpha) = [u]_f(\alpha)$. Con $\sigma \neq \mathtt{id}$ definimos $\beta := [u-1]_f(\alpha)$. Supongamos que $\nu_k(u-1) = i$ con $0 \leq i < m$ de modo que $\beta \in \mu_{f,m-i}^\times$ gracias a la observación que se hizo tras 5.3.3. Obtenemos que β es un parámetro de uniformización de $(k_n)_f^{m-i}$ de nuevo gracias a 5.3.3.2 lo que demuestra que $\nu_{(k_n)_f^m}(\beta) = \nu_{(k_n)_f^{m-i}}(\mathtt{N}_{(k_n)_f^m|(k_n)_f^{m-i}}(\beta)) = q^i$. Como

$$\sigma(\alpha) = [u]_f(\alpha) = \alpha +_{F_f} \beta = \alpha + \beta + \sum_{i>1,j>1} a_{ij}\alpha^i\beta^j$$

para ciertos $a_{ij} \in k_n$, deducimos que $\nu_{(k_n)_f^m}(\sigma\alpha - \alpha) = q^i$.

Gracias a lo anterior tenemos para todo $1 \leq i \leq m$ la igualdad

$$|G_n| = |\rho_{f,m}^{-1}((1+\mathfrak{p}_k^i)/(1+\mathfrak{p}_k^m))| = q^{m-i}, \quad \text{para } q^{i-1} - 1 < n \leq q^i - 1.$$

Llegamos a que

$$\phi(q^m-1) = \frac{1}{|G|}\sum_{i=1}^{q^m-1}|G_i| = \frac{1}{(q-1)q^{m-1}}\sum_{i=1}^{m}(q^i - q^{i-1})q^{m-i} = \frac{1}{(q-1)q^{m-1}}\sum_{i=1}^{m}(q-1)q^{m-1} = m.$$

En definitiva,

$$\mathtt{Gal}((k_n)_f^m|k_n)^m = \mathtt{Gal}((k_n)_f^m|k_m)_{q^m-1} = \{\mathtt{id}\}.$$

□

Ya podemos demostrar el teorema de Kronecker-Weber Local:

Teorema 5.5.2. (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 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, tenemos que $\mathtt{Gal}(k^{\mathtt{ab}}|(k^{\mathtt{ab}})^{\sigma}) = \overline{\langle\sigma\rangle} \simeq \hat{\mathbb{Z}}$, con el isomorfismo definido por $\sigma \mapsto 1$. Por otro lado, de nuevo 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

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

de forma que $k^{\mathtt{ab}} = k^{\mathtt{ur}}(k^{\mathtt{ab}})^{\sigma}$.

Ahora fijemos $\pi = \mathtt{Art}_k^{-1}(\varphi^{-1})$, que es un parámetro de uniformización de k. Como vimos en la prueba de 5.4.3 sabemos que $\cup_{m\geq 1}(k_1)_f^m \subset (k^{\mathtt{ab}})^{\sigma}$ para cierto polinomio de Frobenius f asociado a π. Como $k^{\mathtt{LT}} = k^{\mathtt{ur}} \cup_{m\geq 1} (k_n)_f^m$ es suficiente probar que $(k^{\mathtt{ur}})^{\sigma} \subset \cup_{m\geq 1}(k_n)_f^m$. Sea $k' \supset k$ una extensión finita de Galois contenida en el cuerpo $(k^{\mathtt{ab}})^{\sigma}$. Como $(k^{\mathtt{ab}})^{\sigma} \supset k$ es 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 5.5.1, usando 3.4.6.1 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 3.4.6.2. Concluimos que $k'(k_1)_f^m \subset (k_1)_f^m$, es decir, $k' \subset \cup_{m\geq 1}(k_1)_f^m$.

□

5.5.1. Teoría de Lubin-Tate para $\mathbb{Q}_p$. Teorema de Kronecker-Weber Local

Para ejemplificar la teoría desarrollada en este capítulo vamos a particularizar nuestros resultados en el caso en $k = \mathbb{Q}_p$. Vamos a ver que podemos escoger adecuadamente los polinomios de Frobenius y obtener los grupos de raíces de la unidad como módulos de Lubin-Tate. Una peculiaridad de $\mathbb{Q}_p$ es que para el parámetro de uniformización $p \in \mathbb{Q}_p$ podemos considerar el siguiente polinomio de Frobenius:

$$f(X) = (1+X)^p - 1 \in \mathbb{Z}_p[X].$$

Claramente es un polinomio de Frobenius pues usando el *binomio de Newton* llegamos a $f = pX + \binom{p}{2}X^2 + \cdots + pX^{p-1} + X^p$. De hecho, si consideramos la ley de grupo formal $F_{\mathtt{mult}} = X + Y + XY \in \mathbb{Z}_p[[X,Y]]$ tenemos que f es un endomorfismo de $F_{\mathtt{mult}}$ pues $F_{\mathtt{mul}}(X,Y) = (1+X)(1+Y) - 1$ de modo que

$$F_{\mathtt{mult}}(f(X), f(Y)) = (1+X)^p(1+Y)^p - 1 = f(F_{\mathtt{mul}}(X,Y)).$$

Observar que gracias a la unicidad de 5.2.8.1 deducimos que la ley de grupo formal de Lubin-Tate asociada a f tiene que ser $F_{\mathtt{mult}}$. De hecho, si consideramos el ideal maximal de $\mathbb{Z}_p$ generado por p y definimos la operación de grupo usando $F_{\mathtt{mult}}$, es decir, dados $\alpha, \beta \in \mathbb{Z}_p p$ definimos $\alpha * \beta := \alpha +_{F_{\mathtt{mult}}} \beta = \alpha + \beta + \alpha\beta$, entonces el grupo abeliano $(\mathbb{Z}_p, +_{F_{\mathtt{mult}}})$ es isomorfo al grupo de unidades principales $1 + \mathbb{Z}_p p = U^{(1)}_{\mathbb{Q}_p}$ de $\mathbb{Z}_p$ vía el isomorfismo $a \in \mathbb{Z}_p \mapsto 1 + a \in U^{(1)}_{\mathbb{Q}_p}$. En efecto, la aplicación obviamente es biyectiva y es suficiente comprobar que respeta las operaciones pero esto es inmediato pues $1 + \alpha + \beta + \alpha\beta = (1+\alpha)(1+\beta)$.

Observar que como $f \in \mathbb{Z}_p[X]$ el automorfismo de Frobenius actúa trivialmente sobre los coeficientes y por ello $f_m = \underset{m-\text{veces}}{f \circ \cdot \circ f} = (1+X)^{p^m} - 1$. Veamos cómo es la acción de $\mathbb{Z}_p$ sobre $\mu_{f,m}$ para cada m. Para ello, dado $a \in \mathbb{Z}_p$ definimos

$$(1+X)^a := \sum_{m \geq 0} \binom{a}{m} X^m$$

donde se definen los números combinatorios como sigue:

$$\binom{a}{m} := \frac{a(a-1)\cdots(a-m+1)}{m(m-1)\cdots 1}, \quad a \in \mathbb{Z}_p.$$

Claramente cuando $a \in \mathbb{Z}$ las definiciones anteriores coinciden con las usuales y si $a = \lim_{n\to\infty} a_n$ con $a_n \in \mathbb{Z}$, entonces $\binom{a_n}{m} \to \binom{a}{m}$ cuando $n \to \infty$. En efecto, en los números combinatorios sólo intervienen las operaciones de grupo de $\mathbb{Z}_p$ que son continuas por ser un grupo topológico. Deducimos que $\binom{a}{m} \in \mathbb{Z}_p$ para $a \in \mathbb{Z}_p$. Vamos a probar que $[a]_f(X) = (1+X)^a - 1$. En efecto, como $\binom{a}{0} = 1$ y $\binom{a}{1} = a$ tenemos que $(1+X)^a - 1 = aX + \cdots$ y además para todo $a \in \mathbb{Z}$ se tiene

$$f((1+X)^a - 1) = ((1+X)^a - 1 + 1)^p - 1 = (1+X)^{ap} - 1 = (1 + (1+X)^p - 1)^a - 1 = (1 + f(X))^a - 1$$

y por continuidad se tiene para todo $a \in \mathbb{Z}_p$. Bajo el isomorfismo $(\mathbb{Z}_p p, +_{F_{\mathtt{mult}}}) \overset{a\mapsto 1+a}{\longrightarrow} U^{(1)}_{\mathbb{Q}_p}$ la acción de $\mathbb{Z}_p$ se corresponde con la acción clásica de $\mathbb{Z}_p$ sobre $U^{(1)}_{\mathbb{Q}_p}$ definida por exponenciación. De hecho, bajo este isomorfismo, el conjunto $\mu_{f,m} = \{\alpha \in \mathbb{Q}_p^{\mathtt{sep}} \ : \ (1-\alpha)^{p^m} = 1\}$ se corresponde con el conjunto de las raíces de la unidad p^m-ésimas μ_{p^m}. Se obtiene, como sabíamos por 5.3.3.1, que $\mu_{f,m} \sim \mathbb{Z}/\mathbb{Z}p^m \simeq \mathbb{Z}_p/\mathbb{Z}_p p^m$, donde el primer isomorfismo depende de la raíz $\alpha \in \mu^{\times}_{f,m}$ elegida o equivalentemente depende de la raíz p^n-ésima primitiva de la unidad elegida. Observar que el

isomorfismo de 5.3.3.3 $\mathtt{Gal}(\mathbb{Q}_p(\alpha)|\mathbb{Q}_p) \simeq (\mathbb{Z}_p/\mathbb{Z}_p p^m)^\times$ se corresponde con el isomorfismo estándar $\mu_{p^m}^\times \to (\mathbb{Z}/\mathbb{Z}p^m)^\times$.

Ahora tenemos que las extensiones de Lubin-Tate $(\mathbb{Q}_p)_f^m = \mathbb{Q}_p(\mu_{f,m}) = \mathbb{Q}_p(\mu_{p^m})$ gracias al isomorfismo $\mu_{f,m} \simeq \mu_{p^n}$ pues $1 \in \mathbb{Q}_p$. Es decir, las extensiones de Lubin-Tate de $\mathbb{Q}_p$ no son más que las extensiones ciclotómicas obtenidas a partir de añadir raíces de la unidad de exponente una potencia de p. En este caso, llegamos a que $\cup_{m\geq 1}(\mathbb{Q}_p)_f^m = \mathbb{Q}_p(\cup_{m\geq 1}\mu_{p^m})$. Esto contrasta con las extensiones no ramificadas de $\mathbb{Q}_p$ pues sabemos que se obtienen al añadir raíces de la unidad de exponente un número coprimo con p, es decir, $\mathbb{Q}_p^{\mathtt{ur}} = \mathbb{Q}_p(\cup_{(m,p)=1}\mu_m)$. Teniendo en cuenta estas descripciones y el teorema de Kronecker-Weber Local 5.5.2 obtenemos:

Corolario 5.5.3. Se tiene la igualdad

$$\mathbb{Q}_p^{\mathtt{ab}} = \mathbb{Q}_p(\cup_{m\geq 1}\mu_m).$$

Equivalentemente, toda extensión abeliana de $\mathbb{Q}_p$ está contenida en una extensión ciclotómica.

Con este resultado queda resuelto el **problema número 12 de Hilbert** para los cuerpos de números p-ádicos $\mathbb{Q}_p$, pues podemos describir las extensiones abelianas de $\mathbb{Q}_p$ usando raíces de la unidad. Curiosamente, a partir de este resultado es sencillo probar que se cumple el teorema de Kronecker-Weber para $\mathbb{Q}$ y es lo que probaremos en la siguiente subsección:

5.5.2. Teorema de Kronecker-Weber. Algunos Comentarios Generales

El enunciado de este resultado es, como cabe esperar, el siguiente:

Teorema 5.5.4. (Teorema de Kronecker-Weber)
Toda extensión abeliana de $\mathbb{Q}$ está contenida en una extensión ciclotómica.

Para la demostración haremos uso del siguiente lema. En [Š51] aparece con el nombre de **Monodromía Aritmética:**

Lema 5.5.5. 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 $k \supset \mathbb{Q}$.

Demostración. Denotamos por H al subgrupo de G generado por los subgrupos de inercia. Recordar que si un primo $\mathfrak{p}$ de k no está ramificado entonces su grupo de inercia es trivial. Sea F el cuerpo fijo de H. Si denotamos al grupo de inercia de $\mathfrak{p} \in k$ por $\mathtt{I}(\mathfrak{p})$ entonces $k^{\mathtt{I}(\mathfrak{p})} \supset F$ para todo ideal primo $\mathfrak{p}$ de k y por ello $\mathfrak{p} \cap F$ es un primo no ramificado en la extensión $F \supset \mathbb{Q}$. Deducimos que F

es una extensión no ramificada de $\mathbb{Q}$ y tiene que ser $F = \mathbb{Q}$ pues la única extensión no ramificada de $\mathbb{Q}$ es el propio $\mathbb{Q}$ (Ver [Rib01] *9.2.D*).

□

Demostración de 5.5.4: 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 depende del primo p). Gracias al teorema de Kronecker-Weber para $\mathbb{Q}_p$ sabemos que existen número 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. Para n_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).

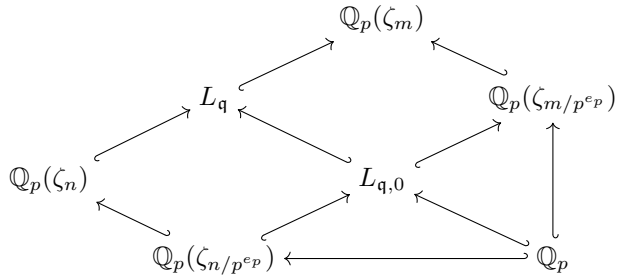
Consideramos la extensión $L = k(\zeta_n)$. Queremos demostrar que $L = \mathbb{Q}(\zeta_n)$. La extensión $L \supset \mathbb{Q}$ es abeliana por ser composición de extensiones abelianas. Esta vez tenemos (sin hacer uso directo del teorema de Kronecker-Weber para $\mathbb{Q}_p$) que $L_{\mathfrak{q}} = k_{\mathfrak{p}}\mathbb{Q}_p(\zeta_n) \subset \mathbb{Q}_p(\zeta_{n_p})\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{\mathtt{mcm}(n_p,n)})$, 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:

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

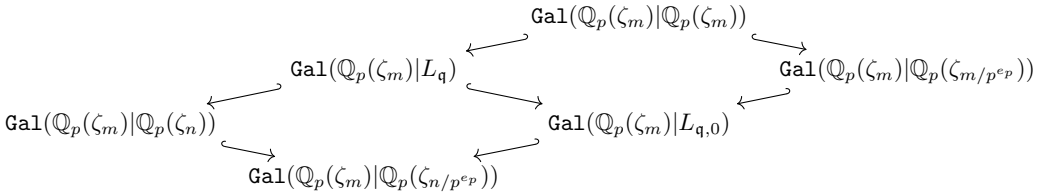
con $\nu_p(n) = \nu_p(m) = e_p$.

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 $\mathbb{Q}_p(\zeta_m)$)

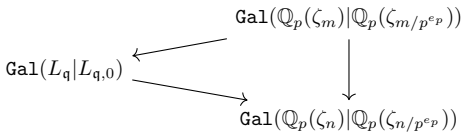
es la extensión $\mathbb{Q}_p(\zeta_{n/p^{e_p}})$ (resp. $\mathbb{Q}_p(\zeta_{m/p^{e_p}})$). Tenemos el siguiente retículo de extensiones:



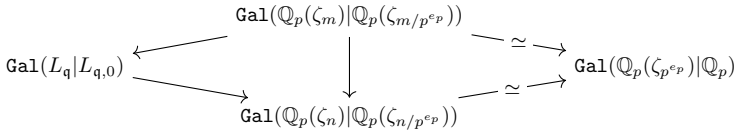
Si consideramos los correspondientes grupos de Galois respecto a $\mathbb{Q}_p$ obtenemos el siguiente retículo de subgrupos:



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. De modo que 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 5.5.5 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

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

Llegamos a que $k \subset L = \mathbb{Q}(\zeta_n)$ 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 $\mathbb{Q}$.

Aunque el teorema de Kronecker-Weber no es cierto en general sí que se puede estudiar y comprender la extensión abeliana maximal de estos cuerpos y desarrollar la Teoría de Cuerpos de Clase. En ese sentido, sí que se puede usar el *principio local a global* para obtener la definición del homomorfismo de Artin a partir de los correspondientes homomorfismos locales como los que hemos estudiado en este trabajo. Sin embargo, son necesarios nuevos métodos para obtener los resultados de la Teoría de Cuerpos de Clase ya sean de naturaleza analítica como las series L o algebraica como la cohomología de grupos. En cualquier caso, la descripción que se obtiene del homomorfismo de Artin no es tan explícita como la que hemos conseguido nosotros en el contexto local usando la teoría de Lubin-Tate, razón por la que no es tan sencillo obtener una descripción tan nítida de la extensiones abelianas como la que hemos conseguido con el teorema de Kronecker-Weber Local (demostrado gracias a un conocimiento profundo y detallado de las extensiones de Lubin-Tate).

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.

[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: `http://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.

[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: `https://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.