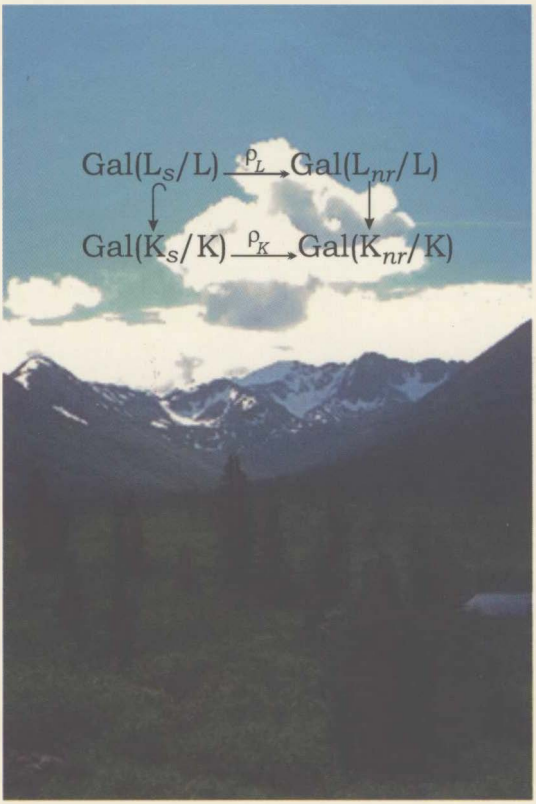
Campos Locales

Felipe Zaldívar



UNIVERSIDAD AUTONOMA METROPOLITANA
Casa abierta al tiempo
UNIDAD IZTAPALAPA

Campos locales

Campos locales

Felipe Zaldívar

Primera edición: 2001

Av. Michoacán y La Purísima
Iztapalapa, 09340, México D.F.

ISBN: 970-654-868-8

Impreso en México/*Printed in Mexico*

Índice

Prólogo

trattando l'ombre come cosa salda
Dante, Purg. 21.136.

Kurt Hensel introdujo los números p-ádicos como series de potencias con respecto al primo p, usando la analogía entre el anillo de enteros $\mathbb{Z}$ y su campo de cocientes $\mathbb{Q}$ y el anillo de polinomios $\mathbb{C}[x]$ y su campo de cocientes $\mathbb{C}(x)$, y donde los primos $p \in \mathbb{Z}$ corresponden a los polinomios irreducibles $(x - \alpha) \in \mathbb{C}[x]$; Hensel nota que dado cualquier polinomio $f(x) \in \mathbb{C}[x]$ y cualquier $\alpha \in \mathbb{C}$ fijo, es posible escribir (con $a_i \in \mathbb{C}$)

$$f(x) = \sum_{i=0}^{n} a_i (x - \alpha)^i, \tag{1}$$

por ejemplo usando la expansión de Taylor de $f(x)$. Lo mismo se puede hacer con enteros (digamos, positivos): dado $m \geq 1$ y un primo p fijo, se tiene que

$$m = \sum_{i=0}^{n} a_i p^i, \tag{2}$$

con $a_i \in \mathbb{Z}$ y $0 \leq a_i \leq p - 1$.

El paso siguiente es observar que en el campo $\mathbb{C}(x)$ cualquier función racional $f(x)$ tiene una expansión como (1), sólo que ahora usualmente es una serie

$$f(x) = \sum_{i \geq n_0}^{\infty} a_i (x - \alpha)^i \tag{3}$$

con $a_i \in \mathbb{C}$ y $n_0 \in \mathbb{Z}$, a saber, la expansión de Laurent de $f(x)$. La idea de Hensel es extender lo anterior, formalmente, a la expansión de un racional

$a \in \mathbb{Q}$ en una serie de la forma

$$a = \sum_{i \geq n_0}^{\infty} a_i p^i \tag{4}$$

con $a_i \in \mathbb{Z}$, $n_0 \in \mathbb{Z}$. Por supuesto que estas series de potencias no convergen con respecto al valor absoluto usual y así no representan números en el sentido usual del término, de tal forma que esta idea de Hensel y sus consecuencias aritméticas encontraron varios reparos al principio. En 1912 Josef Kürschák escribe un artículo donde aclara y fundamenta las ideas de Hensel introduciendo la noción de *valuación* en un campo (más precisamente, la noción de *valor absoluto generalizado*). Este artículo aparece en la revista de Crelle en 1913 y en él encontramos los axiomas ya familiares de un valor absoluto generalizado, i.e., una función $|\ |_K : K \to \mathbb{R}$ tal que $|a|_K \geq 0$ para todo $a \in K$, $|a|_K = 0$ si y sólo si $a = 0$, $|ab|_K = |a|_K |b|_K$ y la desigualdad del triángulo en la forma $|1 + a|_K \leq 1 + |a|_K$. Los axiomas de Kürschák son generalizaciones de las propiedades que Hensel había dado a los p-ádicos (con alguna pequeña corrección al reemplazar p con p^{-1}) en la definición del valor absoluto p-ádico. De esta forma, con el valor absoluto $|\ |_p$ en $\mathbb{Q}$, las series (4) convergen en la completación $\mathbb{Q}_p$ de $\mathbb{Q}$ con respecto a la nueva métrica. Kürschák escribe que este artículo fue inspirado por el libro de Hensel sobre números algebraicos y su motivación es dar un fundamento sólido a los números p-ádicos de Hensel en forma análoga a como ya se había fundamentado el análisis sobre $\mathbb{R}$ o $\mathbb{C}$. En lo que respecta a la extensión de una valuación a un campo más grande, varias demostraciones en el artículo de Kürschák se complicaban porque no tenía a la mano la clasificación de campos completos que obtendría Alexander Ostrowski en 1913, donde muestra que, en el caso arquimediano, los únicos campos completos son $\mathbb{R}$ y $\mathbb{C}$, y en estos casos la extensión de la valuación es fácil. En el caso no arquimediano, Kürschák observa que el método usado por Hensel en su libro se puede generalizar a lo que hoy llamamos el lema de Hensel, y usando este lema extiende la valuación de K a $L \supsetneq K$.

En 1918 Ostrowski determinó todas las valuaciones de los racionales, que son las que uno ya conocía, redondeando el trabajo de Hensel y Kürschák.

En 1920 H. Hasse, motivado por el libro de K. Hensel, se muda a Marburgo para estudiar con Hensel la nueva teoría de números p-ádicos que éste había desarrollado. En su tesis doctoral del año siguiente Hasse introduce el principio de local a global, demostrando su validez para el caso de formas cuadráticas, un

resultado que luego extendería a cualquier campo de números en una serie de artículos publicados en 1923 y 1924. El principio de local a global o *principio de Hasse* dice: si F es una afirmación acerca de objetos aritméticos o geométricos definidos sobre un campo de números K y F es verdadera cuando se interpreta en cada localización $K_{\mathfrak{p}}$ de K (para todo primo $\mathfrak{p}$ de K incluyendo al *primo* infinito ∞), entonces F es verdadera sobre K. En los casos cuando el principio de Hasse es verdadero, se tiene una simplificación del resultado buscado. El principio de Hasse no es válido en general; sin embargo, aun en los casos en que falla, sirve de guía de cómo proceder para analizar el problema en cuestión; un ejemplo de esto es el grupo de Shafarevich-Tate de puntos racionales de una curva elíptica que detecta la obstrucción al principio de Hasse en el caso de curvas elípticas. Después de estos artículos de Hasse, la teoría de números p-ádicos de Hensel se estableció firmemente como una herramienta poderosa en la teoría de números; hoy los campos locales y sus generalizaciones tienen un papel prominente en la teoría de números. Es de notarse que muchos de los resultados aritméticos de Hasse fueron inspirados por su estudio de la ley de reciprocidad cuadrática de Hilbert para campos de números y por la búsqueda de una interpretación del símbolo de Hilbert en términos del principio de local a global: siguiendo una idea de Hensel, Hasse interpreta el símbolo cuadrático de Hilbert $\left(\frac{a,b}{\mathfrak{p}}\right)$ de un campo de números K en términos de las completaciones $K_{\mathfrak{p}}$ de K y sus extensiones cuadráticas. Es necesario enfatizar que los artículos de Hasse son de una naturaleza totalmente diferente a la de los artículos fundacionales de Kürschák y Ostrowski: estos últimos estaban tratando de dar una fundamentación a la teoría de valuaciones; por su parte, Hasse toma esta fundamentación como dada y usa sus propiedades para obtener resultados aritméticos en la dirección mostrada por Hilbert hacia una teoría de las extensiones abelianas de campos de números. La teoría de campos de clases tiene sus orígenes en los trabajos de Gauss, Kummer, Kronecker y Weber (que acuñó el término *campo de clases*), y fue Hilbert en 1898 quien sugiere que la teoría de campos de clases es la teoría de las extensiones abelianas de campos de números. Hilbert mismo estudia el caso de las extensiones abelianas no ramificadas, sugiriendo en sus observaciones iniciales la posible generalización al caso ramificado. T. Takagi creó una sensación cuando en 1920-1922 completa el programa de Hilbert en toda su generalidad y lo aplica a leyes de reciprocidad en campos de números en su segundo gran artículo de 1922. Cuando estos resultados se conocieron en Europa, Emil Artin y Helmut Hasse, entre otros,

estaban preparados para asimilarlos rápidamente, y casi de inmediato Artin publica un par de artículos, uno sobre funciones zeta de campos y otro sobre las nuevas funciones L que ahora llevan su nombre, conjeturando en forma confiada lo que ahora se conoce como la ley de reciprocidad de Artin, cuya demostración él mismo publicaría en 1925 después de conocer el artículo de Chebotarev, [5], sobre la densidad de primos, traducido al alemán en en 1925. La ley de reciprocidad de Artin corona la teoría de campos de clases de Takagi obteniendo el isomorfismo abstracto de Takagi como un isomorfismo natural e incluye todas las leyes de reciprocidad superior conocidas hasta entonces. Poco después, Furtwängler demuestra el teorema de capitulación (todo ideal se vuelve principal en su campo de clases de Hilbert) que había sido conjeturado por Hilbert. Al mismo tiempo Helmut Hasse, inspirado por los trabajos de Takagi, nota la relevancia de estos resultados en su proyecto, en colaboración con Hensel, de estudiar las normas locales para extensiones abelianas que ya habían iniciado en un artículo conjunto donde describen el grupo de normas locales para extensiones cíclicas de grado primo ℓ, bajo la hipótesis de que las raíces ℓ-ésimas de la unidad estén en el campo base. La idea de Hasse era aplicar la teoría de Takagi al caso general quitando la hipótesis sobre las raíces de la unidad. Para aprender la nueva teoría de Takagi, Hasse ofreció un curso sobre la teoría de campos de clases de Takagi en 1923 y un curso sobre leyes de reciprocidad superiores en 1923-1924; las notas de estos cursos forman la base del reporte sobre la teoría de campos de clases, el Klassenkörperbericht de Hasse, que apareció en tres partes en 1926, 1927 y 1930. Este reporte, sugerido a Hasse por Hilbert como un seguimiento a su Zahlbericht de 1897, fue también comisionado y publicado por la Sociedad Matemática Alemana (DMV) y Hasse presentó un extracto de este reporte en una conferencia en Danzig en 1925. El impacto del reporte de Hasse fue grande; Hasse no sólo presenta los resultados de Takagi, sino que da una visión panorámica y sistemática de toda la teoría de campos de clases conocida en esa época, incluyendo no sólo simplificaciones en las demostraciones y resultados de otros matemáticos, tales como la ley de reciprocidad de Artin y el teorema de ideales principales de Furtwängler, sino también nuevos resultados debidos a Hasse mismo. Como consecuencia de este reporte la teoría de campos de clases se volvió fácilmente accesible, como Hilbert había deseado, de tal forma que sólo asumía como conocido lo que ya estaba incluido en el reporte de Hilbert sobre la teoría de números algebraicos; de hecho, como Hasse escribe en el prefacio a su reporte, explícitamente sólo

asume los capítulos 1 a 7 del reporte de Hilbert. Tal vez sea este un buen lugar para enfatizar que el Zahlbericht de Hilbert contiene, además de los resultados fundamentales de la teoría de números algebraicos que Hilbert presenta en el contexto diseñado por él, y a veces debidos a sus antecesores, principalmente Kummer, varios teoremas directamente relevantes en el contexto de la teoría de campos de clases, en especial el teorema 90 (del cual, el caso particular de extensiones de $\mathbb{Q}(\zeta_p)$ había sido descubierto por Kummer), que parece ser el resultado más famoso del Zahlbericht y ha sido generalizado en varios contextos en su variante descubierta por E. Noether: $H^1(\mathrm{Gal}(L/K), K^*) = 0$. Otro teorema sería el que lleva el número 92 y que hoy forma parte del teorema sobre el índice del grupo de normas de las unidades de un campo en el grupo de unidades del campo base (véase (1.69) en nuestro libro).También se puede pensar que el teorema 89, el cual afirma que el grupo de clases de ideales de un campo de números está generado por las clases de ideales primos de grado 1 (también debido a Kummer en el caso de campos ciclotómicos), es un caso especial de los teoremas de densidad en teoría de campos de clases del tipo de Chebotarev.

En 1930 Hasse descubre y analiza en [14][1] los principales resultados en la teoría de campos de clases local, para aquellos campos locales que aparecen como completaciones $K_\mathfrak{p}$ de campos de números, y en este artículo la teoría local la deriva de la teoría global, pero se da cuenta claramente de que el camino natural a la teoría de campos de clases debiera ser en la otra dirección: primero obtener la teoría local y luego, con algún principio de local a global, obtener la teoría global. Este programa fue completado por Hasse mismo y Chevalley en los años treinta, pero aquí quisiéramos observar que, con respecto a este programa, apareció la pregunta natural sobre la existencia de otros campos completos, además de los campos obtenidos al completar campos de números, para los cuales los resultados de la teoría de campos de clases local fueran ciertos. Ésta fue la motivación para el estudio de la estructura general de los campos valuados completos. Una primera pregunta que había que responder era si un campo podría ser completo con respecto a dos valuaciones no equivalentes. Esto fue resuelto por F. K. Schmidt en [31], donde prueba que esto no sucede en general a menos que el campo sea algebraicamente cerrado; en particular esto no ocurre si la valuación es discreta, que es el caso de interés en teoría de números. La estructura de los campos completos fue obtenida por Hasse y

[1]Las referencias incluídas en este prólogo aparecen al final de éste.

Schmidt en un artículo conjunto, donde prueban los resultados (1.16), (1.66) y (1.67) de nuestro libro, separando el caso de característica diferente y el caso de característica igual, donde el problema es esencialmente más complicado.

F. K. Schmidt, desde su tesis, había establecido los hechos básicos de la aritmética de campos de funciones con campo base finito y luego obtuvo otros resultados con el objetivo de trasladar la teoría de Takagi al caso de campos de funciones, obteniendo generalizaciones de resultados de Artin sobre funciones zeta en el caso de campos de funciones y de paso dando los antecedentes para la demostración, por Hasse en el caso de género 1 y por A. Weil en el caso general, de la hipótesis de Riemann en característica p. En su Habilitation, Schmidt obtiene la teoría de campos de clases para campos de funciones con campo de constantes finito, para extensiones (abelianas) de grado coprimo con la característica del campo residual p, en especial el isomorfismo de reciprocidad, el teorema de existencia y la ecuación funcional de la función L correspondiente. Poco después, Hasse publica un artículo donde, entre otras cosas, demuestra la ley de reciprocidad de Artin para el caso de extensiones cíclicas, usando la teoría de álgebras por primera vez, siguiendo ideas de E. Noether. Hasse observa que la ley de reciprocidad general se sigue del caso cíclico y dice que esto es inmediato y bien conocido. Aquí conviene aclarar que Hasse ya conocía los resultados de Herbrand sobre el conductor de una extensión abeliana y para esto refiere a la tesis de Chevalley, donde la transición del caso cíclico al caso abeliano general está desarrollado. De hecho, Chevalley, en su tesis, había desarrollado directamente la teoría de campos de clases local, sin usar argumentos globales.

Por otra parte, Witt, impresionado por las conferencias de Artin sobre teoría de campos de clases, se había propuesto también transferir la teoría de campos de clases al caso de campos de funciones, y en nuestro contexto las ideas desarrolladas son las siguientes: en el caso de campos de funciones, Hasse había dado una demostración de la ley de reciprocidad de Artin donde distinguía dos casos, a saber: cuando el grado n de la extensión L/K no es divisible por la característica p del campo residual y cuando $n = p$. En el primer caso Hasse observa que los argumentos son como para campos de números, pero en el caso $n = p$ tenía que usar teoría de Artin-Schreier, y sus cálculos en el caso de campos de funciones racionales lo llevaron a derivadas logarítmicas, para obtener una fórmula explícita de la ley de reciprocidad, análoga a las fórmulas de Kummer en el caso de campos de números. Hasse planteó a su estudiante

H. L. Schmid el problema de generalizar lo anterior al caso de campos de funciones no necesariamente racionales. Schmid obtuvo la fórmula explícita correspondiente, de donde se deduce inmediatamente el teorema de existencia. El problema de generalizar la fórmula de Schmid al caso de extensiones de grado p^m, con p la característica del campo residual, fue resuelto por Witt en un artículo donde introduce lo que ahora llamamos vectores de Witt.

La tendencia a algebrizar la teoría de campos de clases continuó y, de hecho, Chevalley ya había introducido métodos homológicos en la forma de productos cruzados, para después culminar con los métodos cohomológicos de Nakayama, Hochschild y Tate en los años cincuenta. En esos años no había una buena descripción del morfismo de reciprocidad local de Artin ni una forma explícita de construir la máxima extensión abeliana de un campo local excepto, por supuesto, para $\mathbb{Q}_p$. En 1950 B. Dwork obtuvo una descripción explícita del morfismo de reciprocidad local y en 1965 Lubin y Tate introdujeron grupos formales en la teoría de campos de clases local y dieron construcciones explícitas de la máxima extensión abeliana de un campo local arbitrario y del morfismo de reciprocidad local, suponiendo conocida su existencia.

La teoría de Lubin-Tate puede pensarse como una analogía con la teoría de multiplicación compleja para curvas elípticas. Recordemos que, en este contexto, si K es un campo de números cuadrático imaginario, entonces existe una única (salvo isogenia) curva elíptica E sobre K tal que su anillo de endomorfismos es el anillo de enteros $\mathcal{O}_K$ de K. Para cualquier entero $n \geq 1$ los puntos de n-torsión $E[n]$ de E forman un $\mathcal{O}_K$-módulo cíclico y se prueba que adjuntando las coordenadas de estos puntos se obtiene una extensión abeliana. La analogía para campos locales comienza reemplazando el grupo algebraico E por un análogo local, a saber un grupo formal; para esto debe buscarse un grupo formal cuyo anillo de endomorfismos sea tal que sus puntos de torsión formen un módulo cíclico. Aquí el candidato obvio es el anillo de valuación $\mathcal{O}_v$ del campo local (K, v). Es natural pedir que el grupo formal admita a π (un elemento primo de K) como endomorfismo; consideraciones sobre alturas y el deseo de que los puntos de torsión formen un módulo cíclico sugieren que el endomorfismo asociado a π esté dado por una serie de potencias que satisfaga la congruencia $f(x) \equiv x^q$ mód $\mathfrak{p}_K$, ($q = |K|$ la cardinalidad del campo residual de K). Más aún, como se quiere que el grupo formal $\mathcal{F}$ dependa de π (porque la extensión que se quiere construir debe depender de π), es natural pedir que $f(x) = \pi x + \cdots$. Esto lleva a la construcción del conjunto $\mathcal{F}_\pi$ y a la teoría que

naturalmente se sigue hasta culminar con la construcción explícita del morfismo de reciprocidad para extensiones de Lubin-Tate.

Existen varios enfoques para obtener las leyes de reciprocidad para las extensiones abelianas de campos locales, y acá hemos elegido el enfoque directo y elemental de Neukirch [28] desarrollando *ab initio* toda la herramienta que se necesita. Al enfocarnos sobre campos locales hemos disminuido el material de álgebra conmutativa necesario.

El capítulo 1 contiene los elementos básicos de la aritmética de campos valuados discretos completos. En el capítulo 2, siguiendo a Neukirch [28] se construye el morfismo de reciprocidad de Artin para campos locales, se obtienen sus propiedades más importantes, en particular el teorema de existencia, el teorema de Kronecker-Weber local y se construye la teoría de símbolos locales. Al obtener el símbolo de reciprocidad local para el caso de característica igual (el teorema de Schmid) hemos corregido un error en [34] basándonos en la demostración original de Schmid [30]. En el capítulo 3, siguiendo a Lubin-Tate [27] se introduce la teoría de grupos formales y se calcula el símbolo de Artin para las extensiones de Lubin-Tate construidas usando grupos formales, obteniéndose en particular una generalización del teorema de Kronecker-Weber. En el capítulo 4 se obtienen los resultados clásicos de Hasse-Arf y Herbrand sobre grupos de ramificación superiores, con la novedad de que se usan los resultados sobre extensiones de Lubin-Tate del capítulo previo.

Los capítulos 1 y 2 tienen unos *anexos* que se pueden leer independientemente del contenido del capítulo correspondiente, pero que contienen algunos resultados que se usan en el texto principal y a los cuales se hace referencia cuando corresponde.

Bibliografía

[1] Artin, E., *Über die Zetafunktionen gewisser algebraischen Zahlkörper*, Math. Annalen **89**, (1923), 147-156.

[2] Artin, E., *Über eine neue Art von L-Reihen*, Abh. Math. Sem. Hamburg **3**, (1923), 89-108.

[3] Artin, E., *Beweis des allgemeine Reziprozitätsgesetzes*, Abh. Math. Sem. Hamburg **5**, (1927), 353-363.

[4] Artin, E. und O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Hamburg **5**, (1927), 225-231.

[5] Chebotarev, N.G., *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welsche zu einer gegebenen Substitutionesklasse gehören.* Publicado en ruso en 1923 y traducido al alemán en: Math. Annalen **95** (1925), 191-228.

[6] Chevalley, C. *La théorie du symbole de restes normiques*, J. Reine Angew. Math. **169** (1933), 140-157.

[7] Chevalley, C. *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Univ. Tokyo Sect. I **2** (1933), 365-476.

[8] Dwork, B. *Norm residue symbol in local number fields.* Abh. Math. Sem. Univ. Hamburg **22** (1958), 180-190.

[9] Furtwängler, Ph., *Beweis des Hauptidealsatzes für Klassenkörper algebraischen Zahlkörper*, Abh. Math. Sem. Hamburg **7**, (1930), 14-36.

[10] Hasse, H. und K. Hensel, *Über die Normreste eines relativ-zyklischen Körpers vom Primzahl ℓ nach einem Primteiler $\mathfrak{l}$ von ℓ*, Math. Annalen **90** (1923), 162-278.

[11] Hasse, H., *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, I. *Klassenkörpertheorie*, Jahresbericht der DMV **35** (1926), 1-55.

[12] Hasse, H., *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Ia. *Beweise zu Teil I*, Jahresbericht der DMV **36** (1927), 233-311.

[13] Hasse, H., *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, II. *Reziprozitätsgesetze*, Jahresbericht der DMV Ergänzungsband **6** (1930), 1-204.

[14] Hasse, H., *Die Normenresttheorie relativ-abelscher Zahlkörper als Klassenkörpertheorie im Kleinem*, J. Reine Angew. Math. **170** (1933), 4-63.

[15] Hasse, H. und F.K. Schmidt, *Die Struktur diskret bewerteter Körper*, J. Reine Angew. Math. **162** (1930), 145-154.

[16] Hasse, H., *Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper*, J. Fac. Sci. Univ. Tokyo Sect. I **2** (1934), 477-498.

[17] Hasse, H. *Theorie der relativ-zyklischen algebraischen Funktionenkörper inbesondere bei endlichen Konstantenkörper.* Crelle's Journal **172** (1934), 37-54.

[18] Hasse, H., *Theorie der Differentiale in algebraischen Funktionenkörper mit vollkommenen Konstantenkörper.* Crelle's Journal **172** (1934), 55-64.

[19] Hasse, H., *History of Class-Field Theory*, in Cassels-Fröhlich: *Algebraic Number Theory*, Academic Press, London (1967), 266-279.

[20] Hensel, K., *Theorie der Algebraischen Zahlen*, Leipzig, 1908.

[21] Hazewinkel, M. *Abelian extensions of local fields.* Doctoral Dissertation, Universiteit van Amsterdam, Amsterdam (1969).

[22] Hazewinkel, M. *Local class-field theory is easy.* Adv. Math. **18** (1975), 148-181.

[23] Herbrand, J., *Sur la théorie des groupes de decomposition, d'inertie et de ramification.* J. Math. Pures et Appl. **10** (1931), 481-498.

[24] Hilbert, D., *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der DMV **4** (1897), reimpreso en *Gessamelte Abhandlungen* Vol. 1, Chelsea, New York (1970).

[25] Hilbert, D., *Über die Theorie der relativ-abelscher Zahlkörper*, Nachtr. der K. Ges. der Wiss. Göttingen (1897), 377-399.

[26] Kürschák, J. *Über Limesbildung und allgemeine Körpertheorie.* Crelle's Journal **142** (1913), 211-253.

[27] Lubin, J.; Tate, J. *Formal complex multiplication in local fields.* Ann. of Math. **81** (1965), 380-387.

[28] Neukirch, J. *Neubegründung der Klassenkörpertheorie*, Math. Zeit. **186** (1984), 557-574.

[29] Ostrowski, A. *Über einige Lösungen der Funktionalgleichung* $\varphi(x)\cdot\varphi(y) = \varphi(xy)$. Acta Math. **41** (1918), 271-284.

[30] Schmid, H. L. *Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichen Konstantkörper.* Math. Zeit. **40** (1936), 94-109.

[31] Schmidt, F.K. *Mehrfach perfekte Körper.* Math. Annalen **108** (1933), 1-25.

[32] Schmidt, F.K. *Zur Klassenkörpertheorie im Kleinem.* Crelle's J. **162** (1930), 155-168.

[33] Schmidt, F.K. *Die Theorie der Klassenkörpertheorie über einem Körper algebraischer Funktionem in einer Unbestimmeten und mit endlichen Koeffizientenbereich.* Sitz.-Ber. Phys. Med. Soz. **62** (1931), 267-284.

[34] Serre, J.-P. *Local Fields.* Springer-Verlag, Berlin (1979).

[35] Takagi, T. *Über eine Theorie des relativ abelschen Zahlkörpers*. J. College of Sci. Imp. Univ. of Tokyo **41** (1920), 1-133.
[36] Takagi, T. *Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper*. J. College of Sci. Imp. Univ. of Tokyo **44** (1922), 1-50.
[37] Tate, J. *The higher dimensional cohomology groups of class field theory*. Ann. of Math. **56** (1952), 294-297.
[38] Witt, E. *Der Existenzsatz für abelsche Funktionenkörper*, Crelle's J. **173** (1935), 43-51.

Capítulo 1

Campos locales

En la aritmética de campos, los campos finitos, los campos de números (extensiones finitas de $\mathbb{Q}$) y los campos de funciones aparecen tempranamente. Un lugar intermedio ocupan los *campos locales*, que son estructuralmente más complejos que los campos finitos y se obtienen *completando* campos de números o campos de funciones con campo de constantes finito.

En este capítulo introducimos los conceptos y resultados básicos sobre campos con una valuación no arquimediana, enfocándonos después al caso de campos con una valuación discreta y finalmente al caso de campos locales (campos con una valuación discreta completos y con campo residual finito), clasificándolos y obteniendo algunas de sus propiedades básicas. Otras propiedades importantes de esta clase de campos se demostrarán en los capítulos siguientes.

1.1 Valuaciones no arquimedianas

Si K es un campo, una *valuación no arquimediana* en K es una función

$$v : K \to \mathbb{R} \cup \{+\infty\}$$

(donde el símbolo $+\infty$ satisface las convenciones usuales) tal que:

(i) La restricción $v : K^* \to \mathbb{R}$ es un homomorfismo del grupo multiplicativo de K en el grupo aditivo de $\mathbb{R}$. Se define convencionalmente $v(0) := +\infty$.

(ii) $v(a+b) \geq \min\{v(a), v(b)\}$ para todo $a, b \in K$.

Ejemplo 1. Si K es cualquier campo, la función $v_0 : K \to \mathbb{R} \cup \{+\infty\}$ dada por

$$v_0(a) := \begin{cases} 0 & \text{si} \quad a \neq 0 \\ +\infty & \text{si} \quad a = 0 \end{cases}$$

es una valuación de K a la que se llama la *valuación trivial*.

Ejemplo 2. Si $K = \mathbb{Q}$ es el campo de los números racionales y $p \in \mathbb{Z} \subseteq \mathbb{Q}$ es un primo, cada número racional $x = a/b \neq 0$ se puede escribir de forma única como

$$x = \frac{a}{b} = p^r \frac{a}{b'}$$

con $r, a', b' \in \mathbb{Z}$ y $p \nmid a'b'$. Se define entonces $v_p(x) := r$ y $v_p(0) := +\infty$. Claramente v_p satisface la condición (i) y si $x = p^r a/b$ y $z = p^s c/d$ con $p \nmid abcd$, entonces

$$x + z = \frac{p^r ad + p^s bc}{bd}$$

donde $p \nmid bd$. Ahora, sea p^t la mayor potencia de p que divide al numerador. Entonces, $t \geq \min\{r, s\}$ y

$$v_p(x + z) = t \geq \min\{r, s\} \geq \min\{v_p(x), v_p(z)\}.$$

La valuación v_p anterior se llama la *valuación p-ádica* de $\mathbb{Q}$.

Ejemplo 3. Este ejemplo es formalmente análogo al anterior. Sea $K = F(X)$ el campo de funciones racionales en una indeterminada X con coeficientes en el campo F. Si $\pi(X) \in F[X]$ es un polinomio irreducible dado, entonces todo elemento $\alpha \neq 0$ de K se puede escribir de manera única como

$$\alpha = \pi(X)^r \frac{f(X)}{g(X)}$$

con $f(X), g(X) \in F[X]$, $\pi \nmid fg$ y $r \in \mathbb{Z}$. Se define entonces $v(\alpha) := r$ y $v(0) := \infty$. Ésta es una valuación en $K = F(X)$.

Ejemplo 4. Sea $K = F((T))$ el campo de series formales de Laurent en una variable T con coeficientes en el campo F. Los elementos de K son de la forma

$$\alpha = \sum_{n \geq n_0} a_n T^n$$

con $a_n \in F$ y $n, n_0 \in \mathbb{Z}$. Si $\alpha \neq 0$ en K está dado como arriba con $n_0 \neq 0$, se define entonces $v(\alpha) = n_0$ y $v(0) = +\infty$, y se verifica fácilmente que ésta es una valuación de $K = F((T))$.

Ejemplo 5. Si $\mathbb{F}_q$ es el campo finito de orden $q = p^n$, entonces la única valuación v de $\mathbb{F}_q$ es la trivial. Esto es porque todo elemento $a \neq 0$ de $\mathbb{F}_q$ satisface que $a^{q-1} = 1$ y así $(q-1)v(a) = v(a^{q-1}) = v(1) = 0$ y como $q - 1 \neq 0$ se sigue que $v(a) = 0$. En este ejemplo usamos la parte (1) del siguiente lema.

Si K es un campo con una valuación no arquimediana v, diremos que K es un *campo valuado*. Si v es una valuación en K, convencionalmente lo denotaremos por $v : K^* \to \mathbb{R}$, asumiendo tácitamente que $v(0) = +\infty$. A continuación listamos algunas propiedades básicas de una valuación.

Lema 1.1. *Sea K, v un campo valuado. Entonces:*

(1) $v(1) = 0$.

(2) $v(-a) = v(a)$ *para todo* $a \in K$.

(3) $v(a^{-1}) = -v(a)$ *para todo* $a \in K^*$.

(4) *Si* $v(a) \neq v(b)$, *entonces* $v(a+b) = \min\{v(a), v(b)\}$.

DEMOSTRACIÓN. Como $1 = 1 \cdot 1$, entonces $v(1) = v(1) + v(1)$ y así $v(1) = 0$. También, como $1 = (-1)(-1)$ entonces $0 = v(1) = v(-1) + v(-1)$ en $\mathbb{R}$ y así $v(-1) = 0$. Se sigue que $v(-a) = v((-1)a) = v(-1) + v(a) = v(a)$. Ahora, si $a \in K^*$, entonces $1 = aa^{-1}$ y así $0 = v(1) = v(a) + v(a^{-1})$, y por lo tanto $v(a^{-1}) = -v(a)$.

Para (4), supongamos que $v(a) < v(b)$; entonces $v(a+b) \geq \min\{v(a), v(b)\} = v(a)$ y como $a = (a+b) - b$, entonces $v(a) = v((a+b) - b) \geq \min\{v(a+b), v(b)\} = v(a+b)$ ya que no puede suceder que $\min\{v(a+b), v(b)\} = v(b)$ porque entonces se tendría que $v(a) \geq v(b)$, en contradicción con la hipótesis de que $v(a) \neq v(b)$. Se sigue que $v(a) \geq v(a+b) \geq v(a)$, i.e., $v(a) = v(a+b)$. □

Lema 1.2. *Si K, v es un campo valuado, entonces:*

(1) *El conjunto*

$$\mathcal{O}_K := \{a \in K \ : \ v(a) \geq 0\}$$

es un anillo local con ideal máximo $\mathfrak{p}_K$ dado por

$$\mathfrak{p}_K := \{a \in K \ : \ v(a) > 0\}.$$

(2) *El grupo de unidades del anillo $\mathcal{O}_K$ es*

$$U_K := \{a \in K \ : \ v(a) = 0\}.$$

DEMOSTRACIÓN. Claramente $1, 0 \in \mathcal{O}_K$. Ahora, si $a, b \in \mathcal{O}_K$ entonces $v(a \pm b) \geq \min\{v(a), v(b)\} \geq 0$ y así $a \pm b \in \mathcal{O}_K$. Similarmente, $v(ab) = v(a) + v(b) \geq 0$ y así $ab \in \mathcal{O}_K$. En forma análoga se prueba que $\mathfrak{p}_K$ es un ideal de $\mathcal{O}_K$ y para mostrar que es el único ideal máximo de $\mathcal{O}_K$, obsérvese que $\mathcal{O}_K - \mathfrak{p}_K = U_K$ y úsese (2), que se demuestra como sigue: si $\alpha \in U_K$, sea $\beta \in K^*$ tal que $\alpha\beta = 1$; entonces, $0 = v(1) = v(\alpha) + v(\beta) = v(\beta)$ ya que

$v(\alpha) = 0$. Se sigue que $\beta \in \mathcal{O}_K$ y así α es una unidad de $\mathcal{O}_K$, i.e., $U_K \subseteq \mathcal{O}_K^*$. Recíprocamente, si $a \in \mathcal{O}_K^*$ entonces $a^{-1} \in \mathcal{O}_K$ y así $v(a^{-1}) = -v(a)$ con ambos $v(a), v(a^{-1}) \geq 0$, por lo que $v(a) = 0 = v(a^{-1})$, i.e., $a \in U_K$ y así $\mathcal{O}_K^* \subseteq U_K$. □

Definición 1.3. Si K, v es un campo valuado (no arquimediano) , el anillo local $\mathcal{O}_K$ se llama el *anillo de la valuación v de K* y algunas veces lo denotaremos con $\mathcal{O}_v$. El ideal $\mathfrak{p}_K$ se llama el *ideal máximo* de la valuación v y algunas veces lo denotamos con $\mathfrak{p}_v$. El grupo $U_K = \mathcal{O}_K - \mathfrak{p}_K = \mathcal{O}_K^*$ se llama el *grupo de unidades* de la valuación. El campo cociente $K_v = k_v := \mathcal{O}_K/\mathfrak{p}_K$ se llama el *campo residual de la valuación*.

Observemos que el homomorfismo $v : K^* \to (\mathbb{R}, +)$ tiene núcleo U_K y así induce un isomorfismo $v : K^*/U_K \xrightarrow{\simeq} v(K^*) \subseteq \mathbb{R}$.

Ejemplo 6. Si $K = \mathbb{Q}$ y $v = v_p$ es la valuación p-ádica, se tiene que

$$\begin{aligned} \mathcal{O}_K &= \{\frac{a}{b} \in \mathbb{Q} \quad p \nmid b\} =: \mathbb{Z}_{(p)} \\ \mathfrak{p}_K &\quad \{\frac{a}{b} \in \mathbb{Q} \quad p \nmid b \text{ y } p|a\} = p\mathbb{Z}_{(p)} \\ U_K &\quad \{\frac{a}{b} \in \mathbb{Q} \quad p \nmid b \text{ y } p \nmid a\} \\ K &\quad \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p. \end{aligned}$$

Esto se sigue directamente de las definiciones y sólo verificaremos que $K = \mathbb{F}_p$. En efecto, la inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)}$ que manda $m \mapsto m/1$ es tal que manda al ideal $p\mathbb{Z}$ dentro del ideal $p\mathbb{Z}_{(p)}$ y así induce por paso al cociente el morfismo $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, el cual es fácil ver que es un isomorfismo.

Equivalencia de valuaciones. Si $v : K \to \mathbb{R} \cup \{+\infty\}$ es una valuación no arquimediana y $a > 0$ es un número real, entonces la función $av : K \to \mathbb{R} \cup \{+\infty\}$ dada por $(av)(x) := a \cdot v(x)$ es de nuevo una valuación (no arquimediana). Diremos que dos valuaciones v, w de K son equivalentes, denotado $v \sim w$, si existe un número real $a > 0$ tal que $v = aw$. Claramente ésta es una relación de equivalencia, y valuaciones equivalentes tienen los mismos anillos de valuación, ideales máximos, grupo de unidades y campos residuales.

El resultado siguiente clasifica las valuaciones no arquimedianas de $\mathbb{Q}$:

Proposición 1.4 (Ostrowski). *Si v es una valuación no arquimediana no trivial en $\mathbb{Q}$, entonces v es equivalente a una valuación p-ádica.*

DEMOSTRACIÓN. Como v es no arquimediana, entonces $v(n) \geq 0$ para todo $n \neq 0$ en $\mathbb{Z}$ ya que si $n \geq 1$, entonces $v(n) = v(1+\cdots+1) \geq \min\{v(1)\} = 0$. Y si $n \leq -1$, entonces $v(n) = v(-n(-1)) = v(-1-\cdots-1) \geq \min\{v(-1)\} = 0$.

Ahora, si sucediera que $v(n) = 0$ para todo $n \neq 0$ en $\mathbb{Z}$, entonces para todo $x = a/b \in \mathbb{Q} - \{0\}$ se tendría que $v(x) = v(a) - v(b) = 0$ y por lo tanto v sería la valuación trivial de $\mathbb{Q}$. Entonces, debe existir un $p > 1$ en $\mathbb{Z}$ tal que $v(p) > 0$. Escojamos un tal p mínimo con la propiedad de que $v(p) > 0$. Entonces p es un entero primo ya que si $p = ab$ en $\mathbb{Z}$ con $a, b > 1$, entonces $0 < v(p) = v(a) + v(b)$ y por lo tanto $v(a) > 0$ ó $v(b) > 0$ en contradicción con la minimalidad de p.

Entonces, si $c \in \mathbb{Z}$ es tal que $p \nmid c$, poniendo $c = pu + r$ con $0 < r < p$ por la minimalidad de p se tiene que $v(r) = 0$. Por otra parte $v(pu) = v(p) + v(u) > 0$ ya que $v(u) \geq 0$. Se sigue que

$$v(c) = v(pu + r) = \min\{v(pu), v(r)\} = 0. \tag{1}$$

Ahora, si $c \in \mathbb{Z}$ es tal que $p|c$, pongamos $c = p^r u$ con $p \nmid u$. Entonces

$$v(c) = v(p^r u) = rv(p) + v(u) = rv(p) \tag{2}$$

porque $p \nmid u$ y (1).

Poniendo $\alpha := v(p) \in \mathbb{R}$ se tiene que $\alpha > 0$ y resulta que v es equivalente a la valuación p-ádica v_p ya que si $c = p^r u$ como arriba, entonces $v(c) = rv(p) = r\alpha = \alpha v_p(c)$, y así para todo $x = a/b \in \mathbb{Q} - \{0\}$ se tiene que

$$v(x) = v(a) - v(b) = \alpha v_p(a) - \alpha v_p(b) = v_p(x),$$

i.e., $v = \alpha \cdot v_p$ y así $v \sim v_p$. □

El valor absoluto asociado a una valuación. Si K, v es un campo valuado no arquimediano y $a \in \mathbb{R}$ es tal que $0 < a < 1$, se define, para $x \in K^*$:

$$|x|_v := a^{v(x)}$$

y si $x = 0$, se define $|0|_v = 0$. La función

$$|\ |_v : K \to \mathbb{R}_{\geq 0}$$

satisface las propiedades siguientes (consecuencia de las propiedades correspondientes de v):

(i) $|xy|_v = |x|_v|y|_v$.

(ii) $|x + y|_v \leq \max\{|x|_v, |y|_v\}$.

(iii) $|x|_v = 0$ si y sólo si $x = 0$.

La desigualdad (ii) es más fuerte que la desigualdad del triángulo usual:

$$|x + y|_v \leq |x|_v + |y|_v.$$

Una función $|\ |_v$ que satisfaga las propiedades anteriores se llama un *valor absoluto ultramétrico* en el campo K. Así, en este lenguaje, toda valuación no arquimediana v en K induce un valor absoluto ultramétrico $|\ |_v$ en K. Recíprocamente, todo valor absoluto ultramétrico $|\ |_K$ en K induce una valuación no arquimediana en K mediante: $v_K : K \to \mathbb{R} \cup \{\infty\}$ dada por $v_K(0) := \infty$ y si $\alpha \in K^*$ se define $v_K(\alpha) := -\log_c |\alpha|_K$ con $c > 1$ un real fijo; se prueba fácilmente que v_K es en efecto una valuación no arquimediana de K. Observemos ahora que para $\alpha \neq 0$ en K, poniendo $\log_c |\alpha|_K = -v_K(\alpha)$ se tiene que $|\alpha|_K = c^{-v_K(\alpha)} = (c^{-1})^{v_K(\alpha)}$ con $a := c^{-1}$ que satisface $0 < a < 1$ en $\mathbb{R}$, y por lo tanto $|\alpha|_K$ es de la forma $|\alpha|_K = a^{v_K(\alpha)}$ con $0 < a < 1$. Nótese que usando el valor absoluto $|\ |_K$, el anillo de enteros, el ideal máximo y el grupo de unidades de K están dados por

$$\begin{aligned} \mathcal{O}_K &= \{\alpha \in K \quad |\alpha|_K \leq 1\} \\ \mathfrak{p}_K &= \{\alpha \in K \quad |\alpha|_K < 1\} \\ U_K &= \{u \in K \quad |u|_K = 1\}. \end{aligned}$$

Observemos ahora que, dado un campo valuado no arquimediano (K, v), considerando el valor absoluto ultramétrico $|\ |_v$ asociado a v se tiene una *métrica* en K, de tal forma que $(K, |\ |_v)$ es un espacio métrico. Nótese que como espacio topológico, la topología de K no depende de la elección del número real $0 < a < 1$ usado para definir la métrica dada por $|\ |_v$. Es fácil comprobar que, con la topología inducida por la valuación, resulta que K es un *campo topológico*, i.e., las operaciones suma y producto son continuas, lo mismo que las operaciones de tomar inversos aditivo o multiplicativo.

Éste es un buen lugar para aclarar el uso del término *no arquimediano*: recordemos que en $\mathbb{R}$ el axioma de Arquímedes dice que dado un real $a \neq 0$ y cualquier otro real b, para el valor absoluto usual $|\ |$ de $\mathbb{R}$ se tiene que $|na| > |b|$ para un número natural n suficientemente grande. Ahora, si K es un campo valuado no arquimediano y $|\ |_K$ es el valor absoluto ultramétrico asociado,

entonces para todo natural n se tiene que $n = 1 + \cdots + 1 \in K$ satisface que $|n|_K \leq \max\{|1|_K\} = 1$ y por lo tanto, para todo $a \in K^*$ y todo $n \in \mathbb{N}$:

$$|na|_K = |n|_K |a|_K \leq |a|_K$$

y así no se satisface el axioma de Arquímedes.

Definición 1.5. Un campo valuado no arquimediano K, v se dice que es *completo* si el espacio métrico asociado lo es, i.e., si toda sucesión de Cauchy en $(K, |\ |_v)$ converge a un elemento de K.

Sólo notamos que la definición de *sucesión de Cauchy* en K, v la podemos ver en términos del valor absoluto ultramétrico $|\ |_v$ en la forma usual o equivalentemente en términos de la valuación v, donde toma la forma siguiente: una sucesión $\{a_n\}_{n\geq 0}$ de K es de Cauchy si para todo número real $c \in \mathbb{R}$ existe un número natural n_0 tal que $v(a_m - a_n) \geq c$ para todo $m, n \geq n_0$.

Observación. Recordemos que si $|\ |_\infty$ es el valor absoluto usual de $\mathbb{R}$ y si $\{a_n\}$ es una sucesión de Cauchy de números reales, entonces $\lim_{n\to\infty} |a_{n+1} - a_n|_\infty = 0$. Sin embargo, el recíproco es falso. Por ejemplo, si $\{a_n\}$ es una sucesión de reales que converge a 0 y si ponemos $s_n := a_1 + \cdots + a_n$, entonces se tiene que $\lim_{n\to\infty} |s_{n+1} - s_n|_\infty = \lim_{n\to\infty} |a_n|_\infty = 0$; sin embargo puede suceder que la sucesión $\{s_n\}$ no sea de Cauchy, e incluso puede que no sea convergente; el ejemplo típico es el de la sucesión $\{a_n\} = \{1/n\}$. Sin embargo, si el campo K es no arquimediano, se tiene que:

Lema 1.6. *Sean K, v un campo valuado no arquimediano completo y $\{a_n\}$ una sucesión en K. Entonces, $\{a_n\}$ es de Cauchy si y sólo si $\lim_{n\to\infty} |a_{n+1} - a_n|_v = 0$.*

DEMOSTRACIÓN. Sólo necesitamos probar que si $\lim_{n\to\infty} |a_{n+1} - a_n|_v = 0$ entonces $\{a_n\}$ es de Cauchy. Para esto, notemos que como este límite es 0, entonces para todo $\varepsilon > 0$ existe un N tal que si $n > N$, entonces $|a_{n+1} - a_n|_v < \varepsilon$.

Escribamos $m = n + r > n$ y observemos que

$$\begin{aligned} |a_m - a_n|_v &= |a_{n+r} - a_{n+r-1} + a_{n+r-1} - a_{n+r-2} + \cdots + a_{n+1} - a_n|_v \\ &\leq \max\{|a_{n+r} - a_{n+r-1}|_v, |a_{n+r-1} - a_{n+r-2}|_v, \ldots, |a_{n+1} - a_n|_v\} \\ &< \varepsilon. \end{aligned}$$

□

En ocasiones, cuando involucramos la métrica inducida por una valuación, conviene por varias razones, no sólo psicológicas, considerar el valor absoluto $|\ |_v$ asociado a la valuación v en lugar de la valuación v propia; un ejemplo de esto es el resultado siguiente y su corolario: dada una sucesión de Cauchy $\{a_n\}$ en K, v se tiene la sucesión $\{|a_n|_v\}$ en $\mathbb{R}$ y resulta que ésta es también de Cauchy como consecuencia del lema siguiente:

Lema 1.7. *Si K, v es un campo valuado no arquimediano y si $|\ |_\infty$ es el valor absoluto usual de $\mathbb{R}$, entonces para todo $a, b \in K$:*

$$||a|_v - |b|_v|_\infty \leq |a - b|_v.$$

DEMOSTRACIÓN. Como $b = a + (b - a)$, entonces $|b|_v \leq |a|_v + |b - a|_v$ y así

$$-|a - b|_v \leq |a|_v - |b|_v.$$

Similarmente, $a = b + (a - b)$ implica $|a|_v \leq |b|_v + |a - b|_v$ y así

$$|a|_v - |b|_v \leq |a - b|_v.$$

□

Corolario 1.8. *Si $\{a_n\}$ es una sucesión de Cauchy en K, v entonces $\{|a_n|_v\}$ es una sucesión de Cauchy en $\mathbb{R}$ y como $\mathbb{R}$ es completo, entonces $\lim_{n\to\infty} \{|a_n|_v\}$ existe en $\mathbb{R}$.*

□

Extensión de valuaciones. Si L/K es una extensión de campos y v_L es una valuación de L, la *restricción* de v_L a K^* define una valuación de K. Ahora, si v_K es una valuación de K tal que existe una valuación w de L cuya restricción a K es v_K, diremos que w es una *extensión* de v_K a L y lo denotamos $w|v_K$. Una *extensión de campos valuados* es una extensión de campos L/K tales que $v_L|v_K$. Nótese que dada una valuación de L su restricción a K está bien definida; sin embargo, dada una valuación de K, *a priori* no se sabe si se puede extender a L o si en caso de existir una tal extensión ésta es única. Éste es un tema importante que trataremos en la sección §1.4. El resultado siguiente es fácil de probar:

Lema 1.9. *Si L/K es una extensión de campos valuados no arquimedianos, entonces:*

(1) $\mathcal{O}_K = \mathcal{O}_L \cap K$.

(2) $\mathfrak{p}_K = \mathfrak{p}_L \cap K = \mathfrak{p}_L \cap \mathcal{O}_K$.

(3) $U_K = U_L \cap K$.

(4) $L_{v_L} \supseteq K_{v_K}$, *i.e., se tiene una extensión de los campos residuales* L_{v_L}/K_{v_K}.

(5) $v_K(K^*) \subseteq v_L(L^*)$.

DEMOSTRACIÓN. Sólo probaremos (4):

$$K_{v_K} = \mathcal{O}_K/\mathfrak{p}_K = \mathcal{O}_K/(\mathfrak{p}_L \cap \mathcal{O}_K) \simeq (\mathcal{O}_K + \mathfrak{p}_L)/\mathfrak{p}_L \subseteq \mathcal{O}_L/\mathfrak{p}_L = L_{v_L}.$$

□

Dado un campo valuado K, v, como espacio métrico existe un espacio completo L que lo contiene y además K es denso en L. El resultado siguiente nos dice que de hecho K, v se puede incluir en forma densa en un campo completo esencialmente único.

Definición 1.10. Sea K, v un campo valuado. Una *completación* de K, v es un campo $\widehat{K}$ con una valuación $\widehat{v}$ tal que:

(i) $\widehat{K}, \widehat{v}$ es completo, $K \subseteq \widehat{K}$ y $\widehat{v}|v$.

(ii) K es denso en $\widehat{K}$ con respecto a la métrica inducida por $\widehat{v}$.

Recordemos que un subconjunto A de un espacio métrico X es *denso* en X si toda bola abierta $B(x, \varepsilon)$ con centro en un elemento $x \in X$ contiene un elemento de A, i.e., $B(x, \varepsilon) \cap A \neq \emptyset$.

Teorema 1.11. *Sea K, v un campo valuado. Entonces existe una completación $\widehat{K}, \widehat{v}$ de K, v, única salvo K-isomorfismo.*

DEMOSTRACIÓN. Sea A el conjunto de sucesiones de Cauchy $\{a_n\}_{n>0}$ en K. Claramente A es un anillo con la suma y producto de sucesiones definidos término a término. Sea M el subconjunto de sucesiones de A que convergen a 0. Entonces M es un ideal de A.

Más aún, M es un ideal *máximo* ya que si $\{a_n\} \in A - M$, entonces $\lim_{n\to\infty} \{a_n\} \neq 0$ y así existe un $n_0 \geq 0$ y un número real $c > 0$ tal que $|a_n|_v \geq c > 0$, en particular $a_n \neq 0$ para $n \geq n_0$. Definimos entonces

$$b_n := \begin{cases} 0 & \text{si} \quad n < n_0 \\ a_n^{-1} & \text{si} \quad n \geq n_0. \end{cases}$$

Claramente, $\{b_n\}$ es una sucesión de Cauchy en K ya que

$$|b_{n+1} - b_n|_v = \left|\frac{1}{a_{n+1}} - \frac{1}{a_n}\right|_v = \left|\frac{a_{n+1} - a_n}{a_n a_{n+1}}\right|_v \leq \frac{|a_{n+1} - a_n|_v}{c^2} \to 0,$$

la desigualdad es porque $|a_n|_v \geq c > 0$. Y como $\{a_n\}$ es de Cauchy, por (1.6) el límite arriba es cero, y de nuevo por (1.6) se sigue que $\{b_n\}$ es de Cauchy. Notamos ahora que $\{a_n\}\{b_n\} = \{1\} + \{c_n\}$, donde $\{1\}$ es la sucesión constante 1 y $\{c_n\} \in M$ está dada por

$$c_n = \begin{cases} -1 & \text{si} \quad n < n_0 \\ 0 & \text{si} \quad n \geq n_0. \end{cases}$$

Así, $\{a_n\}\{b_n\} = \{1\} + \{c_n\} \in \{1\} + M$, i.e., $\{a_n\}$ es una unidad del anillo A y por lo tanto M es máximo.

Entonces, el cociente $\widehat{K} := A/M$ es un campo y es una extensión de K ya que la función $K \to \widehat{K}$ que manda $\alpha \in K$ en la sucesión constante $\{\alpha\}$ mód M es un morfismo de campos y por lo tanto inyectiva.

En el campo $\widehat{K}$ se define la función $|\ |_{\widehat{v}}$ mediante

$$|\{a_n\} + M|_{\widehat{v}} := \lim_{n\to\infty} (|a_n|_v).$$

Entonces:

(1): Como $\{a_n\}$ es una sucesión de Cauchy en K, por el corolario (1.8) $\{|a_n|_v\}$ es una sucesión de Cauchy en la métrica usual de $\mathbb{R}$, y por lo tanto $\lim(|a_n|_v)$ existe. Ahora, si $\{a_n\} + M = \{b_n\} + M$, entonces $\{a_n - b_n\} \in M$ y así $\lim(a_n - b_n) = 0$; pero por (1.7) $||a_n|_v - |b_n|_v|_\infty \leq |a_n - b_n|_v$ y por lo tanto $\lim(|a_n|_v - |b_n|_v) = 0$, y como $\{|a_n|_v\}$ y $\{b_n|_v\}$ son sucesiones de Cauchy en $\mathbb{R}$ por (1.8), y por lo tanto convergen, se sigue que: $\lim(|a_n|_v) = \lim(|b_n|_v)$, i.e., $|\ |_{\widehat{v}}$ está bien definida en $\widehat{K}$.

(2): $|\ |_{\widehat{v}} : \widehat{K} \to \mathbb{R}$ es un valor absoluto ultramétrico ya que si $\{a_n\} = \{a_n\} + M$, entonces

$$\begin{aligned} |\overline{\{a_n\}\{b_n\}}|_{\widehat{v}} &= |\overline{\{a_n b_n\}}|_{\widehat{v}} = \lim_{n\to\infty} |a_n b_n|_v \\ &= \lim_{n\to\infty} |a_n|_v \cdot \lim_{n\to\infty} |b_n| \\ &= |\overline{\{a_n\}}|_{\widehat{v}} \cdot |\overline{\{b_n\}}|_{\widehat{v}}. \end{aligned}$$

y

$$\begin{aligned} |\{a_n\}+\{b_n\}|_{\widehat{v}} &= |\overline{\{a_n+b_n\}}|_{\widehat{v}} = \lim_{n\to\infty} |a_n+b_n|_v \\ &< \lim_{n\to\infty} \max\{|a_n|_v, |b_n|_v\} \\ &\leq \max\{\lim_{n\to\infty} |a_n|_v, \lim_{n\to\infty} |b_n|_v\} \\ &< \max\{|\{a_n\}|_{\widehat{v}}, |\{b_n\}|_{\widehat{v}}\}. \end{aligned}$$

Claramente $|\ |_{\widehat{v}}$ restringido a K es $|\ |_v$ y así $|\ |_{\widehat{v}}$ es un valor absoluto ultramétrico de $\widehat{K}$ que extiende al valor absoluto $|\ |_v$ de K.

(3): $\widehat{K}, \widehat{v}$ es *completo*. Sea $\{(a_{n,m})_{n\geq 0}\}_{m\geq 0}$ una sucesión de Cauchy en $\widehat{K}, \widehat{v}$; en esta notación, fijo el índice m, cada $\{a_{n,m}\}_{n\geq 0}$ es un elemento de $\widehat{K} = A/M$, i.e., es una sucesión de Cauchy en K, v módulo M y así, para todo $\varepsilon > 0$ existe un $N = n(m)$ (que depende del m fijo) tal que

$$|a_{r,m} - a_{s,m}|_v < \varepsilon \qquad \text{si} \quad r, s \geq n(m).$$

Nótese que si $m \geq m'$, entonces podemos elegir $n(m) \geq n(m')$ de tal forma que tenemos una sucesión creciente de enteros $n(0), n(1), \ldots, n(m), \ldots$ tal que para todo $\varepsilon > 0$ se tiene que $|a_{r,m} - a_{s,m}|_v < \varepsilon$ siempre que $r, s \geq n(m)$. Entonces, la sucesión $\{a_{n(m),m}\}_{m\geq 0}$ es una sucesión de Cauchy en K ya que para todo $\varepsilon > 0$ se tiene que

$$\begin{aligned} |a_{n(m),m} - a_{n(m'),m'}|_v &\quad |a_{n(m),m} - a_{n(m'),m} + a_{n(m'),m} - a_{n(m'),m'}|_v \\ &< |a_{n(m),m} - a_{n(m'),m}|_v + |a_{n(m'),m} - a_{n(m'),m'}|_v \\ &< \varepsilon/2 + \varepsilon/2 = \varepsilon \end{aligned}$$

ya que $\{a_{n(m),m}\}_{n(m)\geq 0}$ y $\{a_{n(m),m}\}_{m\geq 0}$ son sucesiones de Cauchy.

Se sigue que $\{a_{n(m),m}\}_{m\geq 0} \in \widehat{K}$. Finalmente, el límite con respecto a $\widehat{v}$ de la sucesión $\{(a_{n,m})_{n\geq 0}\}_{m\geq 0}$ es

$$\lim\{(a_{n,m})_{n\geq 0}\}_{m\geq 0} = \{a_{n(m),m}\}_{m\geq 0} \in \widehat{K}$$

y por lo tanto $\widehat{K}$ es completo.

(4): K es *denso* en $\widehat{K}$. Dado $\{a_n\}_{n\geq 0} \in \widehat{K}$, queremos mostrar que existe un elemento $a \in K$ tal que para todo $\varepsilon > 0$ se tenga que $|\{a_n\}_{n\geq 0} - a|_{\widehat{v}} < \varepsilon$. Para esto, sea $\{a_n\}_{n>0}$ una sucesión de Cauchy en K; entonces, para el $\varepsilon > 0$ dado existe un $n_0 \geq 0$ tal que $|a_n - a_m|_v < \varepsilon/2$ para todo $m, n \geq n_0$; en particular,

$|a_n - a_{n_0}|_v < \varepsilon/2$ para todo $n \geq n_0$. Ponemos $a = a_{n_0} \in K$ y observamos que para la sucesión constante $\{a\}$ se tiene que

$$|\{a_n\} - \{a\}|_{\widehat{v}} = \lim_{n\to\infty} |a_n - a|_v = 0,$$

la última igualdad porque $a = a_{n_0}$, y si $n \geq n_0$ se tiene que $|a_n - a_{n_0}|_v < \varepsilon/2$; se sigue que el límite $\lim_{n\to\infty} |a_n - a|_v \leq \varepsilon/2 < \varepsilon$.

(5): *Unicidad*. Si se tuvieran dos completaciones $\widehat{K_1}, \widehat{v_1}$ y $K_2, \widehat{v_2}$ de K, v, en el diagrama

$$\begin{array}{ccc} \widehat{K_1} & \overset{i_{1,2}}{\dashrightarrow} & \widehat{K_2} \\ | & & | \\ K & \xrightarrow[id]{} & K \end{array}$$

el morfismo identidad $id : K \to K$ se extendería por continuidad a un morfismo $i_{1,2} : \widehat{K_1} \to \widehat{K_2}$ ya que K es denso en K_1. Similarmente, invirtiendo las flechas se tendría un morfismo $i_{2,1} : \widehat{K_2} \to \widehat{K_1}$ y claramente uno es inverso del otro, y además $\widehat{v_2} \circ i_{1,2} = \widehat{v_1}$. □

Corolario 1.12. *Sea K, v un campo valuado no arquimediano y sea $\widehat{K}, \widehat{v}$ su completación. Entonces:*

(1) *El anillo $\mathcal{O}_K$ es denso en $\mathcal{O}_{\widehat{K}}$.*

(2) *El ideal $\mathfrak{p}_K$ es denso en $\mathfrak{p}_{\widehat{K}}$.*

(3) *El monomorfismo natural $K \rightarrowtail \widehat{K}$ entre sus campos residuales es un isomorfismo.*

(4) $v(K^*) = \widehat{v}(\widehat{K}^*)$.

DEMOSTRACIÓN. Las partes (1) y (2) se siguen de la demostración del teorema anterior.

Para (3), sólo falta probar que $K \rightarrowtail \widehat{K}$ es suprayectiva. Sea $\alpha \in \mathcal{O}_{\widehat{K}} \subseteq \widehat{K}$. Por definición de completación existe un $a \in K$ tal que $|\alpha - a|_v < 1$. Entonces,

$$|a|_v = |-a|_v = |(\alpha - a) - \alpha|_v \leq \max\{|\alpha - a|_v, |\alpha|_v\} \leq 1,$$

la última desigualdad es porque $|\alpha - a|_v < 1$ y $|\alpha|_v \leq 1$, ya que $\alpha \in \mathcal{O}_{\widehat{K}}$. Se sigue que $a \in \mathcal{O}_K \subseteq \mathcal{O}_{\widehat{K}}$ y como $|\alpha - a|_v < 1$, entonces $\alpha - a \in \mathfrak{p}_{\widehat{K}}$, i.e., $\overline{\alpha} = \overline{a}$ en $\widehat{K}$ con $\overline{a} \in K$ y por lo tanto el monomorfismo natural es suprayectivo.

En (4), ya sabemos que $v(K^*) \subseteq \widehat{v}(\widehat{K}^*)$. Para la otra inclusión, si $\widehat{v}(\alpha) \in \widehat{v}(\widehat{K}^*)$, como $\alpha = (a_n)$ es una sucesión de Cauchy con $a_n \in K$, entonces $\widehat{v}(\alpha) = \lim(v(a_n))$ y así, para toda $c \in \mathbb{R}$ existe un $n_0 \in \mathbb{N}$ tal que $v(a_n - \alpha) > c$ siempre que $n \geq n_0$. En particular, para $c = \widehat{v}(\alpha)$ existe un $N_0 \in \mathbb{N}$ tal que $v(a_n - \alpha) > \widehat{v}(\alpha)$ para todo $n \geq N_0$. Se sigue que

$$v(a_n) = \widehat{v}(a_n) = \widehat{v}((a_n - \alpha) + \alpha) = \min\{\widehat{v}(a_n - \alpha), \widehat{v}(\alpha)\} = \widehat{v}(\alpha)$$

y por lo tanto $\widehat{v}(\alpha) = v(a_n) \in v(K^*)$, i.e., $\widehat{v}(\widehat{K}^*) \subseteq v(K^*)$. □

En vista del resultado anterior, para estudiar un campo valuado K, v frecuentemente sumergimos K, v en su completación $\widehat{K}, \widehat{v}$ y estudiamos el campo valuado completo $\widehat{K}, \widehat{v}$ para deducir de éste propiedades del campo valuado dado.

Ejemplo 7. Sea p un primo de $\mathbb{Z} \subseteq \mathbb{Q}$ y consideremos la valuación p-ádica v_p de $\mathbb{Q}$. La completación de $\mathbb{Q}, v_p$ se denota $\mathbb{Q}_p$ y se llama el *campo de números p-ádicos.* A su valuación se le sigue denotando, por abuso de notación, como v_p. El *anillo de valuación* de $\mathbb{Q}_p$ se denota $\mathbb{Z}_p$ y se llama el *anillo de enteros p-ádicos.* Nótese que por el ejemplo 6 después de (1.3) y la parte (3) del corolario anterior, se tiene que el campo residual de $\mathbb{Q}_p$ es $\mathbb{F}_p$.

Ejemplo 8. Sean K un campo y x una indeterminada. Consideremos el *campo de funciones* $K(x)$ con la valuación v_x dada como sigue: si $f(x) \in K[x]$ es un polinomio, escribamos $f(x) = x^r h(x)$ donde $x \nmid h(x)$. Se define $v_x(f(x)) := r$ y para $f(x)/g(x) \in K(x)$ se define $v_x(f(x)/g(x)) := v_x(f(x)) - v_x(g(x))$. Ésta es una valuación no arquimediana tal que $v_x(x) = 1$ y la completación de $K(x), v_x$ es el *campo de series formales de Laurent* $K((x))$ con coeficientes en K cuyos elementos son de la forma

$$\sum_{n \gg -\infty}^{\infty} a_n x^n$$

con $n \in \mathbb{Z}$, $a_n \in K$ y $n \gg -\infty$ quiere decir que sólo hay un número finito de términos con exponente negativo.

El anillo de enteros de $K((x))$ es el anillo $K[[x]]$ de series de potencias formales de la forma

$$\sum_{n=0}^{\infty} a_n x^n$$

con $a_n \in K$.

El estudio de las series en campos no arquimedianos se facilita debido al resultado siguiente:

Lema 1.13. *Sea K, v un campo no arquimediano completo. Entonces, una serie $\sum_{n=0}^{\infty} a_n$ con $a_n \in K$ converge si y sólo si la sucesión $\{a_n\} \to 0$.*

DEMOSTRACIÓN. Supongamos que $\{a_n\} \to 0$; entonces, para todo $\varepsilon > 0$ existe un $n_0 \in \mathbb{N}$ tal que $|a_m|_v < \varepsilon$ para todo $m > n_0$. Sean $s_t := \sum_{j=0}^{t} a_j$ las sumas parciales de la serie dada. Entonces, si $m > n > n_0$ se tiene que

$$|s_m - s_n|_v = |a_{n+1} + \cdots + a_m|_v \leq \max_j\{|a_j|_v\} < \varepsilon$$

ya que $j \geq m > n_0$. Por lo tanto, la sucesión de sumas parciales $\{s_t\}$ es de Cauchy y como K es completo, entonces converge en K.

La otra implicación es válida en general. □

1.2 Valuaciones discretas

Una valuación (no arquimediana) $v : K^* \to \mathbb{R}$ se dice que es *discreta* si $v(K^*)$ es un subgrupo discreto del grupo aditivo de $\mathbb{R}$, esto es, si

$$v(K^*) = \mathbb{Z}\alpha := \{m\alpha \ : \ m \in \mathbb{Z}\}$$

para algún número real $\alpha \geq 0$. Nótese que cuando $\alpha = 0$ se tiene la valuación trivial v_0 de K. En el caso cuando $\alpha = 1$ se tiene que $v(K^*) = \mathbb{Z}$ y se dice que la valuación v es *normalizada*. Obsérvese también que *si $v : K^* \to \mathbb{R}$ es una valuación discreta no trivial, entonces v es equivalente a una valuación normalizada*. En efecto, como v es discreta entonces $v(K^*) = \mathbb{Z}\alpha$ para algún real $\alpha > 0$. Se define entonces la valuación $w : K^* \to \mathbb{R}$ mediante $w(x) := \alpha^{-1}v(x)$. Claramente, $w(K^*) = \mathbb{Z}$ y $v \sim w$. Un campo con una valuación discreta se llamará un *campo valuado discreto*.

Si K es un campo con una valuación discreta v_K y si $v_K(K^*) = \alpha\mathbb{Z}$ con $\alpha \geq 0$ un real, a cualquier elemento $\pi_K \in K^*$ tal que $v_K(\pi_K) = \alpha$ (el generador del grupo $v_K(K^*)$) se le llama un *elemento primo* de K. Nótese que cualesquiera dos elementos primos de K difieren sólo por una unidad.

Cuando $v : K^* \twoheadrightarrow \mathbb{Z}$ es una *valuación discreta normalizada*, un elemento primo es un $\pi_K \in K^*$ tal que $v(\pi_K) = 1 \in \mathbb{Z}$. Entonces, $\pi_K \in \mathcal{O}_K$ ya que

$v(\pi_K) = 1 > 0$ y, de hecho, $\pi_K \in \mathfrak{p}_K$. Más aún, $\mathfrak{p}_K$ es un ideal principal generado por $\pi = \pi_K$:

$$\mathfrak{p}_K = \langle \pi_K \rangle = \pi_K \mathcal{O}_K,$$

ya que si $a \in \mathfrak{p}_K$ sea $n = v(a) \in \mathbb{Z}$ y notemos que $v(a\pi^{-n}) = v(a) + v(\pi^{-n}) = n - n = 0$, y así $a\pi^{-n} \in U_K$, digamos $a\pi^{-n} = u \in U_K$ y por lo tanto $a = \pi^n u$ con $u \in U_K$. Se sigue que $a \in \langle \pi_K \rangle$ y así $\mathfrak{p}_K = \langle \pi_K \rangle$ es un ideal principal (de hecho, probaremos en (1.15) que $\mathcal{O}_K$ es un dominio de ideales principales). Al elemento π_K de $\mathcal{O}_K$ tal que $\mathfrak{p}_K = \langle \pi_K \rangle$ se le llama un *elemento primo* o *parámetro uniformizador* del campo valuado discreto K. De ahora en adelante, cuando tratemos de valuaciones discretas, a menos que explícitamente digamos lo contrario, se asumirá que son normalizadas. El lema siguiente recoge lo que hemos probado en estas observaciones:

Lema 1.14. *Sea K, v un campo valuado no arquimediano. Entonces:*

(1) *La valuación $v : K^* \to \mathbb{R}$ es discreta si y sólo si el ideal $\mathfrak{p}_K$ es principal.*

(2) *Si K, v es un campo valuado discreto y π es un elemento primo de K, entonces todo $\alpha \in K^*$ se puede escribir en forma única como*

$$\alpha = \pi^n u$$

con $n \in \mathbb{Z}$ y $u \in U_K$.

DEMOSTRACIÓN. (1): Sólo falta probar que si $\mathfrak{p}_K$ es principal, entonces la valuación v es discreta. Supongamos pues que $\mathfrak{p} = \langle \pi \rangle$. Queremos probar que existe un abierto U en $\mathbb{R}^*$ tal que $U \cap v(K^*) = \{0\}$. En efecto, para el número $v(\pi) \neq 0$ en $\mathbb{R}$, si $v(\pi) > 0$ ponemos $U := (-v(\pi), v(\pi))$ y si $v(\pi) < 0$ ponemos $U := (v(\pi), -v(\pi))$. En cualquier caso, ésta es una vecindad abierta del $0 \in \mathbb{R}$. Supongamos que $v(\pi) > 0$. Observemos que, dado cualquier $a \in K^*$, si $v(a) > 0$ entonces $a \in \mathfrak{p}_K = \langle \pi \rangle$ y por lo tanto $a = \pi b$ con $b \in \mathcal{O}_K$, y así $v(a) = v(\pi) + v(b) \geq v(\pi)$ ya que $v(b) \geq 0$.

Ahora, si $v(a) < 0$, entonces $a^{-1} \in \mathfrak{p}_K = \langle \pi \rangle$ y por lo tanto $a^{-1} = \pi b$ con $b \in \mathcal{O}_K$ y así $-v(a) = v(a^{-1}) = v(\pi) + v(b) \geq v(\pi)$, i.e., $v(a) \leq -v(\pi)$.

En cualquiera de los dos casos $a \notin U$ y así $U \cap v(K^*) = \{0\}$. El caso $v(\pi) < 0$ es similar. Se sigue que $v(K^*)$ es un subgrupo discreto de $\mathbb{R}$.

(2): Antes del enunciado del lema probamos que todo $\alpha \in K^*$ se puede escribir como $\alpha = \pi^n u$ con $u \in U_K$. Ahora, si sucediera que $\alpha = \pi^n u = \pi^m \varepsilon$ con $n, m \in \mathbb{Z}$ y $u, \varepsilon \in U_K$, entonces $n = v(\alpha) = v(\pi^m \varepsilon) = m$ y consecuentemente $\pi^n u = \pi^n \varepsilon$, por lo que $u = \varepsilon$. □

Ejemplo 9. El campo de los números p-ádicos es un campo valuado discreto y p es un elemento primo de la valuación ya que $v_p(p) = 1$. El ideal máximo es $p\mathbb{Z}_p$ y así, por el ejemplo 7 después de (1.12), su campo residual es $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, el campo finito con p elementos.

Ejemplo 10. El campo de series de Laurent $K((x))$ con la valuación v_x es un campo valuado discreto y x es un elemento primo. Así, el ideal máximo es $xK[[x]]$ y por lo tanto su campo residual es $K[[x]]/xK[[x]] \simeq K$, el campo de constantes K.

Proposición 1.15. *Sean K un campo valuado discreto, $\mathcal{O}_K$ su anillo de valuación, $\mathfrak{p}_K = \langle \pi \rangle$ su ideal máximo y π un elemento uniformizador. Entonces:*

(1) *El anillo $\mathcal{O}_K$ es un dominio de ideales principales y de hecho todo ideal propio $I \subsetneq \mathcal{O}_K$ es de la forma*

$$I = \mathfrak{p}_K^n = \pi^n \mathcal{O}_K$$

para algún entero $n \geq 1$. En particular, $\mathfrak{p}_K = \langle \pi \rangle = \pi \mathcal{O}_K$.

(2) *La intersección de todos los ideales propios de $\mathcal{O}_K$ es el ideal* 0.

(3) *La cadena de ideales*

$$\mathcal{O}_K \supseteq \mathfrak{p}_K \supseteq \mathfrak{p}_K^2 \supseteq \mathfrak{p}_K^3 \supseteq \cdots$$

forma una base de vecindades abiertas del elemento $0 \in K$.

DEMOSTRACIÓN. Sea $0 \neq I \subsetneq \mathcal{O}_K$ un ideal propio. Entonces, el conjunto $\{v(a) \ : \ a \in I, a \neq 0\} \subseteq \mathbb{N}$ tiene un elemento mínimo, digamos $n > 0$, $n = v(a)$ con $a \in I - \{0\}$. Usando el lema anterior escribamos $a = \pi^n u$ con $u \in U_K$ una unidad. Así, $\pi^n = au^{-1} \in I$ y por lo tanto $\langle \pi^n \rangle \subseteq I$. Ahora, si $\beta \in I$ es otro elemento entonces $v(\beta) \geq n$ por la elección de $n = v(a)$, y así $v(\beta) = n + t$ con $t \geq 0$ y por lo tanto $\beta = \pi^n \pi^t \varepsilon$ con $\varepsilon \in U_K$ y en consecuencia, $\beta \in \langle \pi^n \rangle$, i.e., $I \subseteq \langle \pi^n \rangle$. Esto prueba (1).

Para (2), si $a \in \bigcap_{n \geq 1} \mathfrak{p}_K^n$ entonces $a \in \langle \pi^n \rangle$ para toda $n \geq 1$ y así $a = \pi^n u_n$ con $u_n \in \mathcal{O}_K$ para todo $n \geq 1$ y por lo tanto $v(a) \geq n$ para toda $n \in \mathbb{N}$. Esto sólo es posible si $v(a) = +\infty$, i.e., si $a = 0$.

Para (3), observemos que si $|\alpha|_K = c^{-v_K(\alpha)}$ (con $c > 1$ un real fijo) es el valor absoluto asociado, entonces

$$\mathfrak{p}_K^n = \{\alpha \in K \quad |\alpha|_K < \frac{1}{c^{n-1}}\}.$$

□

Para los campos valuados discretos completos se tiene una descripción explícita de sus elementos:

Proposición 1.16. *Sean K un campo valuado discreto completo, $\mathcal{O}_K$ su anillo de valuación, $\mathfrak{p}_K = \langle \pi \rangle$ su ideal máximo, K su campo residual y $\mathcal{R}$ un conjunto completo de representantes de K en $\mathcal{O}_K$. Entonces,*

(1) *Todo elemento $\alpha \in \mathcal{O}_K$ se puede escribir como una serie convergente:*

$$\alpha = \sum_{n=0} a_n \pi^n \qquad \text{con} \quad a_n \in \mathcal{R}.$$

(2) *Similarmente, todo elemento $\beta \in K$ se puede escribir como*

$$\beta = \sum_{n \gg -\infty}^{\infty} a_n \pi^n \qquad \text{con} \quad a_n \in \mathcal{R},$$

donde $n \gg -\infty$ quiere decir que se tiene sólo un número finito de términos con exponente negativo.

DEMOSTRACIÓN. La segunda afirmación se sigue de la primera, ya que dado $\beta \in K$ existe un entero $t \in \mathbb{Z}$ tal que $\pi^t \beta \in \mathcal{O}_K$. Supongamos pues que $\alpha \in \mathcal{O}_K$. Considerando su reducción módulo π: $\overline{\alpha} \in K = \mathcal{O}_K/\langle \pi \rangle$, por definición de $\mathcal{R}$ existe un único $a_0 \in \mathcal{R}$ tal que $\alpha - a_0 \equiv 0$ mód π. Escribamos

$$\alpha = a_0 + \pi t_1 \qquad \text{con} \quad t_1 \in \mathcal{O}_K$$

y apliquemos el mismo procedimiento anterior a t_1. Entonces, existe un $a_1 \in \mathcal{R}$ tal que $t_1 = a_1 + \pi t_2$ con $t_2 \in \mathcal{O}_K$ y por lo tanto,

$$\alpha = a_0 + \pi(a_1 + \pi t_2) = a_0 + a_1 \pi + \pi^2 t_2.$$

El procedimiento es recursivo y así, para todo n

$$\alpha = a_0 + a_1 \pi + \cdots + a_n \pi^n + \pi^{n+1} t_{n+1},$$

con $a_j \in \mathcal{R}$ y $t_{n+1} \in \mathcal{O}_K$. Entonces, para la suma parcial $s_n := \sum_{i=0}^{n} a_i \pi^i$ se tiene que $\alpha - s_n = t_{n+1}\pi^{n+1} \to 0$ ya que $|t_{n+1}|_K \leq 1$ y $|\pi_K|_K < 1$, y por lo tanto

$$\alpha = \lim_{n\to\infty} \{s_n\} = \sum_{n=0}^{\infty} a_n \pi^n.$$

□

Ejemplo 11. Si $K = \mathbb{Q}_p$ entonces $\mathcal{O}_K = \mathbb{Z}_p$, $K = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ y se puede tomar como

$$\mathcal{R} = \{0, 1, 2, \ldots, p-1\}.$$

Pero también se puede escoger (véase el ejemplo 14 antes de (1.24), donde se muestra que $\mathbb{Q}_p$ contiene las raíces $(p-1)$-ésimas de la unidad):

$$\mathcal{R} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$$

donde ζ es una raíz primitiva $(p-1)$-ésima de la unidad.

Surge entonces la pregunta sobre si existirá alguna forma óptima de elegir al conjunto $\mathcal{R}$; por ejemplo, si $\mathcal{R} \subseteq K$ fuera un subcampo (necesariamente entonces isomorfo a K) entonces se debería tener que car (K) = car $(\mathcal{R})$ = car (K). La proposición siguiente nos dice en cuál caso es posible elegir a $\mathcal{R}$ con estas propiedades:

Proposición 1.17. *Sean K un campo valuado discreto completo, $\mathcal{O}_K$ su anillo de valuación y K su campo residual. Supongamos que* car $(K) = p \neq 0$ *y que K es perfecto. Entonces:*

(1) *Existe un único sistema de representantes $f : K \to \mathcal{O}_K$ que conmuta con p-potencias, i.e., tal que $f(\lambda^p) = f(\lambda)^p$.*

(2) *Sea $\mathcal{R} := f(K) \subseteq \mathcal{O}_K$. Entonces, un elemento α de $\mathcal{O}_K$ pertenece a $\mathcal{R}$ si y sólo si α es una p^n-potencia para todo $n \geq 0$.*

(3) *Este sistema de representantes es multiplicativo, i.e.,*

$$f(\alpha\beta) = f(\alpha)f(\beta)$$

para todo $\alpha, \beta \in K$.

(4) *Si además* $\operatorname{car}(K) = \operatorname{car}(K) = p > 0$, *entonces este sistema es aditivo, i.e.,*

$$f(\alpha + \beta) = f(\alpha) + f(\beta)$$

para todo $\alpha, \beta \in K$.

DEMOSTRACIÓN. Sea $\lambda \in K$; para definir $f(\lambda) \in \mathcal{O}_K$ observemos que como K es perfecto, el morfismo $x \mapsto x^p$ es un automorfismo de K y así cada $x \in K$ tiene una raíz p-ésima a la que denotamos con $x^{p^{-1}}$. Así, para cada $n \geq 0$, denotemos con $L_n(\lambda) \subseteq \mathcal{O}_K$ a la imagen inversa, bajo el epimorfismo canónico $\rho : \mathcal{O}_K \twoheadrightarrow K$, del elemento $\lambda^{p^{-n}}$ de K. Pongamos

$$V_n(\lambda) := \{x^{p^n} \ : \ x \in L_n(\lambda)\} \subseteq \mathcal{O}_K.$$

Nótese que $L_0(\lambda) = \{x \in \mathcal{O}_K \ : \ \bar{x} = \lambda^{p^0} = \lambda\}$ es la clase residual de λ en K. Se tiene además que los conjuntos $V_n(\lambda) \subseteq L_0(\lambda)$ ya que si $x \in L_n(\lambda)$, entonces $\bar{x} = \lambda^{p^{-n}} \in K$ y así $x^{p^n} \in L_n(\lambda)$ es tal que su clase es

$$\overline{(x^{p^n})} = \bar{x}^{p^n} = (\lambda^{p^{-n}})^{p^n} = \lambda^{p^0} = \lambda$$

y por lo tanto $V_n(\lambda) \subseteq L_0(\lambda)$. Más aún, los $V_n(\lambda)$ forman una sucesión decreciente, i.e., $V_{n+1}(\lambda) \subseteq V_n(\lambda)$ ya que si $x^{p^{n+1}} \in V_{n+1}(\lambda)$, i.e., si $x \in L_{n+1}(\lambda)$, entonces $x^p \in L_n(\lambda)$ ya que como $x \in L_{n+1}(\lambda)$ se tiene que $\bar{x} = \lambda^{p^{-n-1}}$ y por otra parte $\overline{(x^p)} = \bar{x}^p = (\lambda^{p^{-n-1}})^p = \lambda^{p^{-n}}$, y así $x^p \in L_n(\lambda)$; se sigue que si $x^{p^{n+1}} \in V_{n+1}(\lambda)$, entonces $x^{p^{n+1}} = (x^p)^{p^n} \in V_n(\lambda)$ ya que $x^p \in L_n(\lambda)$ y así $V_{n+1}(\lambda) \subseteq V_n(\lambda)$.

Mostraremos ahora que $\{V_n(\lambda)\}$ es base de un filtro de Cauchy de $\mathcal{O}_K$. En efecto, si $a = x^{p^n}$ y $b = y^{p^n}$ entonces $a \equiv b \mod \mathfrak{p}_K^{n+1}$; esto se demuestra por inducción sobre n: Para $n = 0$ se tiene que $a = x$ y $b = y$ son elementos de $V_0(\lambda) = L_0(\lambda) = \bar{\lambda}$ y así $a \equiv \lambda \equiv b \mod \mathfrak{p}_K$. El paso inductivo es consecuencia de la observación de que si $a \equiv b \mod \mathfrak{p}_K^n$ entonces $a^p \equiv b^p \mod \mathfrak{p}_K^{n+1}$, lo cual se sigue de la fórmula binomial y del hecho de $p \in \mathfrak{p}_K$ y por lo tanto $p \cdot \mathfrak{p}_K^n \subseteq \mathfrak{p}_K^{n+1}$.

Habiendo ya mostrado que $\{V_n(\lambda)\}$ es base de un filtro de Cauchy de $\mathcal{O}_K$, como $\mathcal{O}_K$ es completo podemos definir

$$f(\lambda) := \lim_{n \to \infty} V_n(\lambda) \in \mathcal{O}_K.$$

Esta fórmula define un conjunto de representantes $f : K \to \mathcal{O}_K$.

Observemos ahora que elevar a la p-potencia es una función de $V_n(\lambda)$ en $V_n(\lambda^p)$, de tal forma que pasando al límite se tiene que $\lim_{n\to\infty} V_n(\lambda)$ elevado a la p-potencia es $\lim_{n\to\infty} V_n(\lambda^p)$, es decir, $f(\lambda)^p = f(\lambda^p)$. Esto prueba la existencia de un sistema de representantes con la propiedad deseada en (1). Sólo falta probar su unicidad: supongamos que $g : K \to \mathcal{O}_K$ es otro sistema de representantes tal que $g(\lambda)^p = g(\lambda^p)$. Entonces, para todo n se tiene que $g(\lambda)^{p^n} = g(\lambda^{p^n})$ y por lo tanto $g(\lambda) \in V_n(\lambda)$ para todo n. Ahora, como los $V_n(\lambda)$ son un filtro de Cauchy, entonces $g(\lambda) = f(\lambda)$, lo cual muestra la unicidad de f y al mismo tiempo que

$$\bigcap_{n=0}^{\infty} V_n(\lambda) = \{f(\lambda)\}.$$

Esto prueba (1) y (2).

Para (3) observamos que si x y y son p^n-potencias para todo n, entonces xy también lo es.

Para (4), suponiendo además que $\operatorname{car}(K) = p = \operatorname{car}(K)$ y si x y y son p^n-potencias para todo n, entonces $x + y$ también lo es ya que $(a + b)^{p^n} = a^{p^n} + b^{p^n}$. □

Definición 1.18. Si K es un campo valuado discreto completo con campo residual K perfecto de característica $p > 0$, el sistema de representantes $\mathcal{R}$ de K de la proposición anterior se llama un *sistema de representantes multiplicativo* por la propiedad (3). Nótese que si además $\operatorname{car}(K) = \operatorname{car}(K) = p > 0$, entonces por (4), $\mathcal{R}$ es un campo isomorfo a K.

Ejemplo 12. Para el campo de números p-ádicos $K = \mathbb{Q}_p$, el sistema de representantes $\mathcal{R} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$, donde ζ es una raíz primitiva $(p-1)$-ésima de la unidad (véase el ejemplo 14 antes de (1.24) donde se muestra que $\mathbb{Q}_p$ contiene a las raíces $(p-1)$-ésimas de la unidad), es un sistema multiplicativo, pero no es aditivo ya que $\operatorname{car}(\mathbb{Q}_p) = 0$.

1.3 Polinomios sobre campos no arquimedianos

En esta sección estudiamos polinomios con coeficientes en un campo valuado no arquimediano, en particular resultados sobre irreducibilidad de estos polinomios y sobre sus raíces, incluyendo el *lema de Hensel*. Comenzamos con los resultados sobre irreducibilidad:

Lema 1.19 (Gauss). *Sean K, v un campo valuado no arquimediano, $\mathcal{O}_K$ su anillo de enteros y $f(x) \in \mathcal{O}_K[x]$ un polinomio. Entonces, $f(x)$ es irreducible en $K[x]$ si y sólo si $f(x)$ es irreducible en $\mathcal{O}_K[x]$.*

DEMOSTRACIÓN. Como $\mathcal{O}_K[x] \subseteq K[x]$, claramente si $f(x)$ es irreducible en $K[x]$ entonces lo es en $\mathcal{O}_K[x]$. Para probar la otra implicación, comenzamos extendiendo la valuación v de K al campo de cocientes $K(x)$ del anillo de polinomios $K[x]$ como sigue: si $f(x) = a_0 + a_1 x + \cdots + a_t x^t \in K[x]$ no es el polinomio 0, definimos

$$w(f) := \min_j \{v(a_j)\}$$

y si $\phi(x) = f(x)/g(x) \in K(x)$, con $f, g \in K[x]$, definimos

$$w(\phi) := w(f) - w(g)$$

(por supuesto, si $\phi \neq 0$, i.e., si $f \neq 0$). Se tiene que:

(1). Si $g, h \in K[x]$, entonces $w(g + h) \geq \min\{w(g), w(h)\}$.

(2). Si $g, h \in K[x] - \{0\}$, entonces $w(gh) = w(g) + w(h)$.

La primera afirmación es obvia y para la segunda observemos que si

$$g(x) = \sum_{i=0}^{m} b_i x^i \qquad \text{y} \qquad h(x) = \sum_{j=0}^{n} c_j x^j,$$

entonces

$$\begin{aligned} w(gh) &= \min\{v(\sum_{i+j} b_i c_j)\} \\ &> \min\{\min_{i,j}\{v(b_i) + v(c_j)\}\} = \min_{i,j}\{v(b_i) + v(c_j)\} \\ &> \min\{v(b_i)\} + \min\{v(c_j)\} = w(g) + w(h). \end{aligned}$$

Para la otra desigualdad, si $f(x) := g(x)h(x)$, con $g, h \in K[x]$, escribamos

$$g(x) = \sum_{i=0}^{m} b_i x^i, \quad h(x) = \sum_{i=0}^{n} c_i x^i, \quad f(x) = \sum_{i=0}^{m+n} a_i x^i.$$

Sean

$$\ell_1 := \min\{i \quad v(b_i) = \min\{v(b_j)\}\}$$

y

$$\ell_2 := \min\{i \quad v(c_i) = \min\{v(c_j)\}\}.$$

Entonces, como $a_i = \sum b_j c_{i-j}$, para el término

$$\begin{aligned} a_{\ell_1+\ell_2} \quad & \sum b_j c_{\ell_1+\ell_2-j} \\ = \quad & (b_0 c_{\ell_1+\ell_2} + \cdots + b_{\ell_1-1} c_{\ell_2+1}) + b_{\ell_1} c_{\ell_2} \\ & + (b_{\ell_1+1} c_{\ell_2-1} + \cdots + b_{\ell_1+\ell_2} c_0) \end{aligned}$$

se tiene que para los términos del primer paréntesis,

$$v(b_j c_{\ell_1+\ell_2-j}) > v(b_{\ell_1} c_{\ell_2})$$

ya que $j < \ell_1$, y similarmente para los términos del segundo paréntesis usando que $j < \ell_2$. Por lo tanto $v(a_{\ell_1+\ell_2}) = v(b_{\ell_1} c_{\ell_2}) = v(b_{\ell_1}) + v(c_{\ell_2})$ y así

$$w(f) = w(gh) := \min\{v(a_i)\} \leq v(a_{\ell_1+\ell_2}) = v(b_{\ell_1}) + v(c_{\ell_2}) = w(g) + w(h);$$

se sigue que $w(gh) = w(g) + w(h)$.

Finalmente notamos que la extensión de w de $K[x]$ a $K(x)$ está bien definida ya que si $f(x)/g(x) = \phi(x)/\psi(x)$, entonces $f\psi = g\phi$ en $K[x]$ y así $w(f) + w(\psi) = w(g) + w(\phi)$, i.e., $w(f/g) = w(\phi/\psi)$. Es claro que w extiende a v.

Ahora, para probar la implicación faltante en el lema, supongamos que $f(x)$ es irreducible en $\mathcal{O}_K[x]$ y que es reducible en $K[x]$, i.e., que

$$f(x) = g(x)h(x) \qquad \text{con} \qquad g, h \in K[x]$$

y consideremos la valuación w de $K(x)$. Como queremos una factorización de $f(x)$ en $\mathcal{O}_K[x]$, si sucediera que $w(g) \geq 0$ y $w(h) \geq 0$, entonces por definición de w, la factorización ya estaría. Supongamos entonces que una de estas valuaciones es negativa, digamos $w(g) = v(b_{\ell_1}) < 0$, con $b_{\ell_1} \in K - \{0\}$. Entonces pongamos

$$f(x) = \left(b_{\ell_1}^{-1} g(x)\right)\left(b_{\ell_1} h(x)\right)$$

y obsérvese que $b_{\ell_1}^{-1} g(x) \in \mathcal{O}_K[x]$ ya que

$$w(b_{\ell_1}^{-1} g(x)) = w(b_{\ell_1}^{-1}) + w(g(x)) = -v(b_{\ell_1}) + \min\{v(b_i)\} = -v(b_{\ell_1}) + v(b_{\ell_1}) = 0$$

y como $f(x) \in \mathcal{O}_K[x]$, entonces $w(f) \geq 0$ y de $(*)$ se sigue que

$$0 \leq w(f) = w(b_{\ell_1}^{-1} g b_{\ell_1} h) = w(b_{\ell_1}^{-1} g) + w(b_{\ell_1} h) = 0 + w(b_{\ell_1} h)$$

por lo que $w(b_{\ell_1} h) \geq 0$, i.e., $b_{\ell_1} h \in \mathcal{O}_K[x]$, i.e., $(*)$ es una factorización de $f(x)$ en $\mathcal{O}_K[x]$, una contradicción. □

Como una consecuencia importante tenemos el siguiente criterio, debido a G. Eisenstein, para la irreducibilidad de un polinomio con coeficientes en $\mathcal{O}_K$:

Teorema 1.20 (Eisenstein). *Sean K, v un campo valuado discreto, $\mathcal{O}_K$ su anillo de enteros y π un elemento primo de v. Supongamos que $f(x) = a_0 + a_1x + \cdots + a_nx^n$ es un polinomio con coeficientes en $\mathcal{O}_K$ tal que:*

(1) $v(a_n) = 0$.

(2) $v(a_j) \geq 1$ *para* $0 \leq j \leq n-1$.

(3) $v(a_0) = 1$.

Entonces, $f(x)$ es irreducible en $K[x]$.

DEMOSTRACIÓN. Por el lema de Gauss basta probar que $f(x)$ es irreducible en $\mathcal{O}_K[x]$. Supongamos entonces que

$$f(x) = g(x)h(x) \qquad \text{en} \quad \mathcal{O}_K[x],$$

donde $g(x) = b_0 + \cdots + b_rx^r$, $h(x) = c_0 + \cdots + c_sx^s$ y $r + s = n$. Al reducir (los coeficientes de) estos polinomios módulo el ideal máximo $\mathfrak{p}_K = \pi\mathcal{O}_K$ se obtiene

$$\overline{f}(x) = a_0 + a_1x + \cdots + a_n\dot{x}^n = a_n\dot{x}^n,$$

ya que $a_j \in \mathfrak{p}_K$ para $0 \leq j \leq n-1$. Ahora, como $f = gh$ en $\mathcal{O}_K[x]$, entonces $f = \overline{g}\overline{h}$ en $K_v = \mathcal{O}_K/\mathfrak{p}_K$ y por lo tanto

$$\overline{a_n}\dot{x}^n = \overline{f} = \overline{g}\overline{h} = \overline{b_r}\overline{c_s}x^{r+s},$$

y así $\overline{g}(x) = b_r\dot{x}^r$ y $\overline{h}(x) = c_s\dot{x}^s$. En particular $v(b_0) \geq 1$ y $v(c_0) \geq 1$, de tal forma que $v(a_0) = v(b_0c_0) = v(b_0) + v(c_0) \geq 2$, en contradicción con la hipótesis (3). □

Un polinomio que satisfaga el criterio de Eisenstein anterior se llama un *polinomio de Eisenstein*.

Ejemplo 13. Sea $K = \mathbb{Q}_p$. Entonces, el *polinomio ciclotómico*

$$\phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}_p[x]$$

es irreducible en $\mathbb{Q}_p[x]$.

En efecto, notamos primero que $\phi_p(x)$ es irreducible si y sólo si $\phi_p(x+1)$ lo es. Usando esto escribamos

$$\begin{aligned}\phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{1}{x}\left(x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x + 1 - 1\right) \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}\end{aligned}$$

y notemos que como $p|\binom{p}{i}$ para $1 \leq i \leq p-1$, entonces $|\binom{p}{i}|_p < 1$ para estos coeficientes; ahora, para el término de grado $|1|_p = 1$ y para el término independiente $\binom{p}{p-1} = p$, y así $|\binom{p}{p-1}|_p = |p|_p$.

El *lema de Hensel*, que probaremos a continuación en una de sus versiones, es un resultado análogo al método de Newton en $\mathbb{R}$, que infiere la existencia de una raíz de un polinomio de la existencia de una raíz aproximada del mismo.

Lema 1.21 (Hensel). *Sea K, v un campo valuado no arquimediano completo. Sean $f(x) \in \mathcal{O}_K[x]$ y $a_0 \in \mathcal{O}_K$ tales que*

$$(*) \qquad |f(a_0)|_v < |f'(a_0)|_v^2$$

donde $f'(x)$ es la derivada de $f(x)$. Entonces:

(1) *Existe un $a \in \mathcal{O}_K$ tal que $f(a) = 0$.*

(2) *Más aún, $|a - a_0|_v \leq \dfrac{|f(a_0)|_v}{|f'(a_0)|_v}$.*

(3) *De hecho, existe un único $a \in \mathcal{O}_K$ tal que $f(a) = 0$ y satisface* (2).

Demostración. Sean X, Y indeterminadas algebraicamente independientes sobre K. Substituyendo x por $X+Y$ en $f(x)$, expandiendo los binomios $(X+Y)^j$ y agrupando potencias de Y, podemos escribir

$$(1) \qquad f(X+Y) = f(X) + Yf_1(X) + Y^2 f_2(X) + \cdots,$$

donde cada $f_j(X) \in K[X]$ y, de hecho, como $f(x) \in \mathcal{O}_K[x]$, entonces $f_j(X) \in \mathcal{O}_K[X]$. Es claro que $f(X)$ aparece como el primer término en (1) y además $f_1(X) = f'(X)$.

Ahora, de la hipótesis (*) se sigue que $f'(a_0) \neq 0$ ya que de lo contrario por (*) se tendría que $|f(a_0)|_v < 0$, lo cual es absurdo. Podemos entonces definir

$$b_0 := -\frac{f(a_0)}{f_1(a_0)} = -\frac{f(a_0)}{f'(a_0)}$$

de tal forma que

$$|b_0|_v = \frac{|f(a_0)|_v}{|f'(a_0)|_v} = \frac{|f(a_0)|_v |f'(a_0)|_v}{|f'(a_0)|_v^2} < |f'(a_0)|_v \leq 1$$

(la penúltima desigualdad por (*) y la última desigualdad porque $a_0 \in \mathcal{O}_K$ y $f'(x) \in \mathcal{O}_K[x]$). Se sigue que

$$|b_0|_v < |f'(a_0)|_v \leq 1. \tag{2}$$

De la definición de b_0 se tiene que $f(a_0) + b_0 f_1(a_0) = 0$, y substituyendo X por a_0 y Y por b_0 en (1) obtenemos

$$\begin{aligned}
|f(a_0 + b_0)|_v &= |f(a_0) + b_0 f_1(a_0) + b_0^2 f_2(a_0) + \cdots + b_0^j f_j(a_0) + \cdots|_v \\
&= |b_0^2 f_2(a_0) + \cdots + b_0^j f_j(a_0) + \cdots|_v \\
&\leq \max_{j\geq 2}\{|b_0^j f_j(a_0)|_v\} = \max_{j\geq 2}\{|b_0^j|_v |f_j(a_0)|_v\} \\
&\leq \max_{j\geq 2}\{|b_0^j|_v\} \quad \text{ya que} \quad f_j(a_0) \in \mathcal{O}_K \\
&\leq |b_0|_v^2 \quad \text{ya que } |b_0|_v < 1, \text{ y así la mayor potencia es } |b_0|_v^2 \\
&= \left| \begin{matrix} f(a_0) \\ f_1(a_0) \end{matrix} \right|_v^2 \quad \text{por definición de } b_0 \\
&= \frac{|f(a_0)|_v}{|f_1(a_0)|^2} |f(a_0)|_v < |f(a_0)|_v, \quad \text{por (*)}.
\end{aligned}$$

Similarmente, si en lugar de $f(x)$ usamos el polinomio $f_1(x)$, substituimos x por $X + Y$ y luego X por a_0 y Y por b_0, obtenemos que

$$\begin{aligned}
|f_1(a_0 + b_0) - f_1(a_0)|_v &= |f_1(a_0) + b_0 f_{1,1}(a_0) + \cdots + b_0^n f_{1,n}(a_0) - f_1(a_0)|_v \\
&= |b_0 f_{1,1}(a_0) + b_0^2 f_{1,2}(a_0) + \cdots + b_0^n f_{1,n}(a_0)|_v \\
&\leq \max\{|b_0^j f_{1,j}(a_0)|_v\} \\
&\leq \max\{|b_0^j|_v\} \quad \text{ya que } f_{1,j}(a_0) \in \mathcal{O}_K \\
&\leq |b_0|_v < |f_1(a_0)|_v;
\end{aligned}$$

la penúltima desigualdad porque $|b_0|_v < 1$ y así $|b_0|_v^1$ es la mayor potencia, y la última desigualdad por (2). De esta desigualdad se sigue, ya que $|\ |_v$ es no arquimediana, que

$$\begin{aligned} |f_1(a_0+b_0)|_v &= |(f_1(a_0+b_0)-f_1(a_0))+f_1(a_0)|_v \\ &= \text{máx}\{|(f_1(a_0+b_0)-f_1(a_0))|_v, |f_1(a_0)|_v\} = |f_1(a_0)|_v. \end{aligned}$$

Poniendo $a_1 := a_0 + b_0 \in \mathcal{O}_K$, hemos mostrado que

$$|f_1(a_1)|_v = |f_1(a_0)|_v$$

y

$$|f(a_1)|_v < |f(a_0)|_v.$$

Repitiendo inductivamente el proceso se obtiene una sucesión de elementos $a_n = a_{n-1} + b_{n-1} \in \mathcal{O}_K$ con $f(a_n) + b_n f_1(a_n) = 0$ y tales que:

(i) $$|f_1(a_n)|_v = |f_1(a_0)|_v \quad \text{para toda } n$$

y

(ii) $$|f(a_{n+1})|_v \leq \frac{|f(a_n)|_v^2}{|f_1(a_n)|_v^2} < |f(a_n)|_v.$$

Se sigue que

(3) $$|f(a_{n+1})|_v < |f(a_n)|_v < |f(a_{n-1})|_v < \cdots < |f(a_0)|_v < |f'(a_0)|_v^2 \leq 1$$

y, por lo tanto,

$$\lim_{n\to\infty} \{f(a_n)\} = 0.$$

Más aún,

$$\begin{aligned} |a_{n+1}-a_n|_v \quad & |a_n+b_n-a_n|_v \quad \text{por definición de } a_{n+1} \\ & |b_n|_v \\ & \left|-\frac{f(a_n)}{f_1(a_n)}\right|_v \quad \text{ya que } f(a_n)+b_n f_1(a_n)=0 \\ & \frac{|f(a_n)|_v}{|f_1(a_0)|_v} \quad \text{por (i)} \end{aligned}$$

y así

$$|a_{n+1}-a_n|_v = \frac{|f(a_n)|_v}{|f_1(a_0)|_v} \longrightarrow 0$$

ya que $f(a_n) \to 0$. Se sigue que la sucesión $\{a_n\}$ es de Cauchy en K, que es completo, y por lo tanto converge a algún elemento $a \in K$. Además, como $|a_n|_v \leq 1$ para todo n ya que $a_n \in \mathcal{O}_K$, entonces

$$|a|_v := |\lim_{n\to\infty} a_n|_v \leq 1$$

y por lo tanto $a \in \mathcal{O}_K$. También,

$$|f(a)|_v = |f(\lim_{n\to\infty}(a_n))|_v = |\lim_{n\to\infty} f(a_n)|_v = 0,$$

lo que demuestra la parte (1).

Para la parte (2), como

$$\begin{aligned} a_1 &:= a_0 + b_0 \\ a_2 &:= a_1 + b_1 \end{aligned}$$

$$a_n := a_{n-1} + b_{n-1}$$

entonces

$$\begin{aligned} a_n - a_0 &= a_{n-1} + b_{n-1} - a_0 \\ &- a_{n-2} + b_{n-2} + b_{n-1} - a_0 \end{aligned}$$

$$\begin{aligned} &a_1 + b_1 + b_2 + \cdots + b_{n-2} + b_{n-1} - a_0 \\ &a_0 + b_0 + b_1 + \cdots + b_{n-1} - a_0 \\ &\sum_{j=0}^{n-1} b_j \end{aligned}$$

y por lo tanto

$$a - a_0 = \lim_{n\to\infty}(a_n - a_0) = \sum_{j=0} b_j.$$

También, como $f(a_n) + b_n f_1(a_n) = 0$ para toda n, entonces

$$b_n = -\frac{f(a_n)}{f_1(a_n)} = -\frac{f(a_n)}{f_1(a_0)},$$

(la última igualdad por (i)). Se sigue que

$$\begin{aligned} |a_n - a_0|_v &= \left| \sum_{j=0}^{\infty} b_j \right|_v = \sum_{j=0}^{\infty} - \frac{f(a_j)}{f_1(a_0)} \\ &< \text{máx} \left\{ \frac{|f(a_j)|_v}{|f_1(a_0)|_v} \right\} \\ &= \frac{|f(a_0)|_v}{|f_1(a_0)|_v} \quad \text{por (3)} \\ &= \frac{|f(a_0)|_v}{|f'(a_0)|_v}, \end{aligned}$$

lo cual demuestra la parte (2).

Para demostrar la parte (3) supongamos que existe un $\widetilde{a} \neq a$ tal que $\widetilde{a} \in \mathcal{O}_K$, $f(\widetilde{a}) = 0$ y $|\widetilde{a} - a_0|_v \leq \dfrac{|f(a_0)|_v}{|f'(a_0)|_v}$.

Pongamos $\widetilde{b} := \widetilde{a} - a \in \mathcal{O}_K$. Entonces

$$\begin{aligned} 0 \quad & f(\widetilde{a}) = f(a + b) \\ = \quad & f(a) + \widetilde{b} f_1(a) + \widetilde{b}^2 f_2(a) + \cdots \\ & \widetilde{b} f_1(a) + \widetilde{b}^2 f_2(a) + \cdots \quad \text{(ya que } f(a) = 0\text{)}. \end{aligned}$$

Por otra parte,

$$\begin{aligned} |\widetilde{b}|_v \quad & |\widetilde{a} - a|_v = |\widetilde{a} - a_0 + a_0 - a|_v \\ < \quad & \text{máx}\{|\widetilde{a} - a|_v, |a_0 - a|_v\} \\ < \quad & \frac{|f(a_0)|_v}{|f'(a_0)|_v} \quad \text{por la parte (2) aplicada a } a \text{ y } \widetilde{a} \\ & \frac{|f(a_0)|_v}{|f'(a_0)|_v^2} |f'(a_0)|_v \\ < \quad & |f'(a_0)|_v = |f'(a)|_v; \end{aligned}$$

la última desigualdad por la hipótesis (*) del lema y la última igualdad porque para todo n, $|f'(a_n)|_v = |f'(a_0)|_v$. Se sigue que

$$|\widetilde{b}|_v < |f'(a)|_v \leq 1.$$

Ahora, como para toda $j \geq 2$ se tiene que $|f_j(a)|_v \leq 1$, entonces

$$|\tilde{b}^j|_v |f_j(a)|_v \leq |\tilde{b}^j|_v < |\tilde{b}|_v^2 < |\tilde{b}|_v |f'(a)|_v$$

y por lo tanto

$$0 = |f(\tilde{a})|_v = |f(a+\tilde{b})|_v = |\tilde{b} f_1(a) + \tilde{b}^2 f_2(a) + \cdots|_v = |\tilde{b} f_1(a)|_v = |\tilde{b}|_v |f_1(a)|_v,$$

pero como $|f_1(a)|_v \neq 0$, entonces $|\tilde{b}|_v = 0$, i.e., $\tilde{b} = 0$, i.e., $\tilde{a} = a$, lo que demuestra la parte (3). □

La variación que veremos a continuación es un caso particular del lema de Hensel anterior y de la versión que veremos inmediatamente después:

Corolario 1.22. *Sea K, v un campo valuado no arquimediano completo y sean $f(x) \in \mathcal{O}_K[x]$ y $a_0 \in \mathcal{O}_K$. Consideremos sus reducciones $\overline{f}(x) \in K[x]$ y $\overline{a}_0 \in K$ y supongamos que se tiene que*

$$(\dagger) \qquad \overline{f}(\overline{a}_0) = 0 \qquad \textit{en} \quad K$$

y que además

$$(\dagger\dagger) \qquad \overline{f}'(\overline{a}_0) \neq 0,$$

i.e., $\overline{a}_0$ es raíz simple de $\overline{f}(x)$. Entonces, existe un $a \in \mathcal{O}_K$ tal que $\overline{a} = \overline{a}_0$ y $f(a) = 0$.

DEMOSTRACIÓN. Como $f(a_0) \in \mathfrak{p}_K$ por $(\dagger)$ y $f'(a_0) \in \mathcal{O}_K - \mathfrak{p}_K$ por $(\dagger\dagger)$, entonces $|f(a_0)|_K < 1$ y $|f'(a_0)|_K = 1$, y así se satisfacen las hipótesis del lema de Hensel (1.21) y por lo tanto existe un $a \in \mathcal{O}_K$ tal que $f(a) = 0$ y por (1.21)(2) se tiene que $|a - a_0|_K \leq |f(a_0)|_K / |f'(a_0)|_K < 1$, por lo que $a - a_0 \in \mathfrak{p}_K$, i.e., $\overline{a} = \overline{a}_0$. □

Nótese que esta variación nos dice que si un polinomio $f(x) \in \mathcal{O}_K[x]$ al reducirlo mod $\mathfrak{p}_K$ se tiene que $\overline{f}(x) = (x - \overline{a}_0)\overline{g}(x)$ en $K[x]$, entonces existe un $a \in \mathcal{O}_K$ y un polinomio $\phi(x) \in \mathcal{O}_K[x]$ tal que $\overline{a} = \overline{a}_0$, $\overline{\phi}(x) = \overline{g}(x)$ y $f(x) = (x - a)\phi(x)$. Ésta es la forma en que se generalizará este corolario al considerar una factorización de $\overline{f}(x)$ en $K[x]$ bajo la condición correspondiente a la hipótesis de que $\overline{a}_0$ es una raíz simple, i.e., bajo la condición de que $(x - \overline{a}_0)$ es coprimo con $\overline{g}(x)$. La versión del lema de Hensel que veremos a continuación tiene, en cierta forma, alguna semejanza con el lema de Gauss que nos dice que si un polinomio se factoriza en $K[x]$, entonces se factoriza en $\mathcal{O}_K[x]$: esta versión del lema de Hensel nos dice que, bajo ciertas condiciones, una factorización en $K[x]$ se levanta a una factorización en $\mathcal{O}_K[x]$:

Teorema 1.23 (Lema de Hensel, segunda versión). *Sea K, v un campo valuado no arquimediano completo y sea $f(x) \in \mathcal{O}_K[x]$. Supongamos que existen polinomios $g_1(x)$, $h_1(x)$ en $\mathcal{O}_K[x]$ tales que:*

(1) *$g_1(x)$ es mónico.*

(2) *$\overline{g}_1(x)$ y $\overline{h}_1(x)$ son coprimos en $K[x]$.*

(3) *$\overline{f}(x) = \overline{g}_1(x)\overline{h}_1(x)$ en $K[x]$.*

Entonces, existen polinomios $g(x)$, $h(x)$ en $\mathcal{O}_K[x]$ tales que:

(1)' *$g(x)$ es mónico.*

(2)' *$\overline{g}(x) = \overline{g}_1(x)$ y $\overline{h}(x) = \overline{h}_1(x)$.*

(3)' *$f(x) = g(x)h(x)$ en $\mathcal{O}_K[x]$.*

DEMOSTRACIÓN. La idea de la demostración es similar a la demostración de la primera versión del lema de Hensel, aproximándonos a la factorización deseada por medio de factorizaciones módulo potencias π^k de un elemento $\pi \in \mathfrak{p}_K$, de tal forma que en el límite se tenga la factorización requerida. Nótese que como por hipótesis $g_1(x)$ es mónico y queremos que $g(x)$ sea mónico, entonces se debe tener que $\mathrm{gr}(g) = \mathrm{gr}(g_1)$. Pongamos entonces $n = \mathrm{gr}(f)$ y $m = \mathrm{gr}(g_1) = \mathrm{gr}(g)$. Como $\overline{f} = \overline{g}_1\overline{h}_1$ en $K[x]$, entonces $\mathrm{gr}(h_1) \leq n - m$ (puede ser menor si $\mathrm{gr}(\overline{f}) < \mathrm{gr}(f)$, lo cual puede suceder si al reducir coeficientes módulo $\mathfrak{p}_K$ se vuelve 0 el coeficiente de grado de $f(x)$). Queremos construir dos sucesiones de polinomios $g_i(x)$ y $h_i(x)$ con coeficientes en $\mathcal{O}_K[x]$ tales que:

(i) Cada g_i sea mónico de grado m;

(ii) $g_{i+1} \equiv g_i \bmod \pi^i$ y $h_{i+1} \equiv h_i \bmod \pi^i$;

(iii) $f(x) \equiv g_i(x)h_i(x) \bmod \pi^i$,

donde se entiende que las congruencias son coeficiente a coeficiente. Observemos que una vez construidas estas sucesiones ya habremos probado el teorema ya que definiendo $g(x)$ como el límite (coeficiente a coeficiente) de los $g_i(x)$, y $h(x)$ como el límite (coeficiente a coeficiente) de los $h_i(x)$, notando que estos límites existen por la condición (ii) de arriba y porque $|\pi|_K < 1$ y porque K es completo, se tendrá entonces que $g(x)$ y $h(x)$ están definidos y de hecho tienen coeficientes en $\mathcal{O}_K$. Más aún, como cada g_i es mónico de grado m, entonces $g(x)$ también es mónico de grado m, y la condición (ii) de arriba implica que $g(x) \equiv g_1(x) \bmod \mathfrak{p}_K$ y $h(x) \equiv h_1(x) \bmod \mathfrak{p}_K$, y, por (iii),

$f(x) \equiv g(x)h(x)$ mód π^j para toda $j \geq 1$ y por lo tanto $f(x) = g(x)h(x)$ como se quiere.

Resta entonces mostrar la existencia de las sucesiones de polinomios g_i y h_i con las propiedades (i), (ii) y (iii) anteriores. Para comenzar, observemos que por la hipótesis (3) del teorema la diferencia $f(x) - g_1(x)h_1(x)$ tiene coeficientes en $\mathfrak{p}_K$ y por la hipótesis (2) existen $a(x), b(x) \in \mathcal{O}_K[x]$ tales que

$$a(x)g_1(x) + b(x)h_1(x) \equiv 1 \text{ mód } \mathfrak{p}_K.$$

Entonces, entre los coeficientes de los polinomios $f(x) - g_1(x)h_1(x)$ y $a(x)g_1(x) + b(x)h_1(x) - 1$ (estos coeficientes están en $\mathfrak{p}_K$) escogemos uno que tenga mayor valor absoluto; éste es el elemento $\pi \in \mathfrak{p}_K$ que necesitamos. Si $\pi = 0$, $f(x) = g_1(x)h_1(x)$ es la factorización deseada. Si $\pi \neq 0$, construiremos la sucesión de polinomios deseada observando que ya tenemos g_1 y h_1 por las hipótesis del teorema. Para construir g_2 y h_2 notemos que como se debe tener que $g_2(x) \equiv g_1(x)$ mód π, entonces se debe tener que $g_2(x) = g_1(x) + \pi r_1(x)$ con $r_1(x) \in \mathcal{O}_K[x]$. Similarmente se debe tener que $h_2(x) = h_1(x) + \pi s_1(x)$ con $s_1(x) \in \mathcal{O}_K[x]$. Así, para mostrar la existencia de g_2 y h_2 debemos mostrar la existencia de r_1 y s_1 con las propiedades deseadas, i.e., debemos resolver

$$\begin{aligned} f(x) &- g_2(x)h_2(x) \text{ mód } \pi^2 \\ &- (g_1(x) + \pi r_1(x))(h_1(x) + \pi s_1(x)) \text{ mód } \pi^2 \\ &- g_1(x)h_1(x) + \pi r_1(x)h_1(x) + \pi s_1(x)g_1(x) + \pi^2 r_1(x)s_1(x) \text{ mód } \pi^2 \\ &- g_1(x)h_1(x) + \pi r_1(x)h_1(x) + \pi s_1(x)g_1(x) \text{ mód } \pi^2. \end{aligned}$$

Ahora, como $f(x) \equiv g_1(x)h_1(x)$ mód π, entonces $f(x) - g_1(x)h_1(x) = \pi t(x)$ con $t(x) \in \mathcal{O}_K[x]$ y así, substituyendo en la congruencia anterior debemos resolver

$$\pi t(x) \equiv \pi r_1(x)h_1(x) + \pi s_1(x)g_1(x) \text{ mód } \pi^2,$$

donde cada miembro $t(x)$, $r_1(x)h_1(x)$ y $s_1(x)g_1(x)$ tiene coeficientes en $\mathcal{O}_K$. Dividiendo la congruencia anterior entre π obtenemos

$$t(x) \equiv r_1(x)h_1(x) + s_1(x)g_1(x) \text{ mód } \pi$$

y ésta es la congruencia que debemos resolver para determinar r_1 y s_1.

Ahora, de la definición de π, si c_j son los coeficientes del polinomio $a(x)g_1(x) + b(x)h_1(x) - 1$, entonces $|c_j|_K \leq |\pi|_K < 1$, por lo que $c_j/\pi \in \mathcal{O}_K$

y así

$$a(x)g_1(x) + b(x)h_1(x) - 1 = \sum_j c_j x^j = \left(\sum (c_j/\pi)x^j\right)\pi \equiv 0 \text{ mód } \pi,$$

es decir, $a(x)g_1(x) + b(x)h_1(x) \equiv 1 \text{ mód } \pi$, y multiplicando ahora esta congruencia por $t(x)$ obtenemos

$$a(x)t(x)g_1(x) + b(x)t(x)h_1(x) \equiv t(x) \text{ mód } \pi$$

y esto resuelve la congruencia $(*)$ poniendo $\tilde{r}_1(x) := b(x)t(x)$ y $\tilde{s}_1(x) := a(x)t(x)$; sin embargo, tenemos el problema de que no se tiene control sobre el grado de $\tilde{r}_1(x)$ y por lo tanto no podemos garantizar que $g_1(x) + \pi\tilde{r}_1(x)$ sea mónico (y éste es el candidato para $g_2(x)$). Para remediar esto observemos que lo que necesitamos es un polinomio $\tilde{r}_1(x)$ que satisfaga que $\text{gr}(\tilde{r}_1) < \text{gr}(g_1)$. Ahora, dividiendo $\tilde{r}_1(x)$ por $g_1(x)$ obtenemos $\tilde{r}_1(x) = g_1(x)q(x) + r_1(x)$ con $\text{gr}(r_1) < \text{gr}(g_1)$ y poniendo $s_1 := \tilde{s}_1(x) + h_1(x)q(x)$ se sigue que

$$\begin{aligned} r_1h_1 + s_1g_1 &= (\tilde{r}_1 - g_1q)h_1 + (\tilde{s}_1 + h_1q)g_1 \\ &\quad \tilde{r}_1h_1 - g_1h_1q + \tilde{s}_1g_1 + g_1h_1q \\ &\quad \tilde{r}_1h_1 + \tilde{s}_1g_1 \\ &\quad t \text{ mód } \pi, \end{aligned}$$

la última congruencia porque $\tilde{r}_1$ y $\tilde{s}_1$ son soluciones de $(*)$; se sigue que los polinomios $r_1(x)$ y $s_1(x)$ de $\mathcal{O}_K[x]$ también son soluciones de la congruencia $(*)$ pero ahora con la condición de que $\text{gr}(r_1) < \text{gr}(g_1)$, por lo que $g_2(x) := g_1(x) + \pi r_1(x)$ es mónico y tiene grado $m = \text{gr}(g)$. Claramente, $g_2(x) \equiv g_1(x) \text{ mód } \pi$. Más aún, poniendo $h_2(x) := h_1(x) + \pi s_1(x)$ se tiene que $h_2(x) \equiv h_1(x) \text{ mód } \pi$ y

$$\begin{aligned} g_2h_2 &- (g_1 + \pi r_1)(h_1 + \pi s_1) = g_1h_1 + \pi g_1s_1 + \pi r_1h_1 + \pi^2 r_1s_1 \\ &\quad g_1h_1 \equiv f \text{ mód } \pi, \end{aligned}$$

como se requería.

Finalmente, obsérvese que como g_1 y h_1 son coprimos mód $\mathfrak{p}_K$, entonces g_2 y h_2 también son coprimos mód $\mathfrak{p}_K$. El argumento anterior se aplica recursivamente comenzando ahora con g_2 y h_2 para producir las sucesiones deseadas. □

Ejemplo 14. Sea p un primo y consideremos el campo $\mathbb{Q}_p$ y el polinomio $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$. Entonces, reduciendo coeficientes módulo $p\mathbb{Z}_p$ y

ya que $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$, se tiene que $\overline{f}(x) = x^{p-1} - 1 \in \mathbb{F}_p[x]$. Observamos que el polinomio $\overline{f}(x)$ se descompone en factores lineales sobre $\mathbb{F}_p$ y así, aplicando repetidamente el lema de Hensel anterior, tenemos que $f(x)$ se descompone en factores lineales sobre $\mathbb{Z}_p$. En otras palabras, $\mathbb{Z}_p$ contiene a las raíces $(p-1)$-ésimas de la unidad. Esto se usó en el ejemplo 11 después de (1.16) y en el ejemplo 12 después de (1.18).

El corolario siguiente nos dice que si un polinomio mónico en $K[x]$ es irreducible y tiene término independiente en $\mathcal{O}_K$, este polinomio de hecho está en $\mathcal{O}_K[x]$:

Corolario 1.24. *Sea K un campo valuado no arquimediano completo y sea $f(x) = a_0 + a_1x + \cdots + x^n \in K[x]$ un polinomio mónico irreducible tal que $a_0 \in \mathcal{O}_K$. Entonces $f(x) \in \mathcal{O}_K[x]$.*

DEMOSTRACIÓN. Si $f(x)$ no estuviera en $\mathcal{O}_K[x]$, entonces alguno de sus coeficientes a_i tendría valor absoluto $|a_i|_K > 1$; nótese que este coeficiente no puede ser el término de grado (ya que éste es 1) ni el término independiente. Sea N el menor de los índices i tales que $0 < i < n$ y $|a_N|_K > 1$ es el mayor de todos estos $|a_i|_K > 1$. Consideremos el polinomio $g(x) := (1/a_N)f(x)$ y observemos que $g(x) \in \mathcal{O}_K[x]$. Entonces

$$g(x) - \frac{a_0}{a_N} + \frac{a_1}{a_N}x + \cdots + \frac{a_{N-1}}{a_N}x^{N-1} + x^N + \frac{a_{N+1}}{a_N}x^{N+1} + \cdots + \frac{1}{a_N}x^n$$
$$(\frac{a_0}{a_N} + \cdots + \frac{a_{N-1}}{a_N}x^{N-1}) + x^N(1 + \frac{a_{N+1}}{a_N}x + \cdots + \frac{1}{a_N}x^{n-N})$$

y así en $K[x]$ se tiene que $\overline{g}(x) = x^N(1+\cdots+(1/a_N)x^{n-N})$, ya que el polinomio en el primer paréntesis anterior tiene coeficientes en $\mathfrak{p}_K$.

Por la segunda versión del lema de Hensel se sigue que $g(x) = \phi(x)\psi(x)$ en $K[x]$ con $\operatorname{gr}(\phi) = N$ y $\operatorname{gr}(\psi) = n - N$, i.e. $g(x) = (1/a_N)f(x) = \phi(x)\psi(x)$ es reducible y por lo tanto $f(x)$ también lo es; una contradicción. □

1.4 Extensiones finitas de campos completos

En esta sección estudiamos extensiones finitas de campos L/K, donde K es un campo no arquimediano completo, y probamos que su valuación v_K se puede extender en forma única a una valuación v_L de L de tal forma que L, v_L resulta un campo valuado no arquimediano completo también.

Recordemos primero que si L/K es una extensión finita de campos valuados, como L es un espacio vectorial sobre K, el valor absoluto $|\ |_L$ de L induce *normas* y *distancias* en L, donde recordamos que una *norma* de un K-espacio vectorial V de dimensión finita $n \geq 1$ es una función

$$\|\ \| : V \longrightarrow \mathbb{R}^+ \cup \{0\}$$

tal que:

(i) $\|a\| \geq 0$ para todo $a \in V$ y $\|a\| = 0$ si y sólo si $a = 0$.

(ii) $\|a + b\| \leq \|a\| + \|b\|$ para todo $a, b \in V$.

(iii) $\|\lambda a\| = |\lambda|_K \|a\|$ para toda $a \in V$ y todo $\lambda \in K$, donde $|\ |_K$ es la valuación de K.

Entonces, para probar la *unicidad* de la extensión del valor absoluto $|\ |_K$ de K al campo L debemos probar que si K es completo, entonces cualesquiera dos normas de L inducen la misma topología en L. El lema siguiente demuestra esto:

Lema 1.25. *Sea K, $|\ |_K$ un campo valuado completo y sea V un K-espacio vectorial de dimensión finita n. Entonces, cualesquiera dos normas $\|\ \|_1$ y $\|\ \|_2$ en V inducen la misma topología. Más aún, V es completo bajo la métrica inducida.*

DEMOSTRACIÓN. Por inducción sobre $n \geq 1$. Si $n = 1$ no hay nada que probar ya que en este caso $V \simeq K$ y si $\{w_1\}$ es una base de V y $\|\ \|$ es cualquier norma de V, entonces para todo $a \in V$, escribiendo $a = \lambda w_1$ con $\lambda \in K$, se tiene que

$$\|a\| = \|\lambda w_1\| = |\lambda|_K \|w_1\|$$

y poniendo $c := \|w_1\| > 0$ (ya que $w_1 \neq 0$), entonces $\|a\| = c|\lambda|_K$, por lo que $\|\ \|$ y $|\ |_K$ inducen la misma topología en V y claramente V es completo bajo esta métrica.

Supongamos ahora que $n > 1$ y que el resultado es válido para K-espacios vectoriales de dimensión $\leq n - 1$. Sea $w_1, \ldots, w_n$ una base de V y sea $\|\ \|$ una norma arbitraria en V. Compararemos a $\|\ \|$ con la *norma del máximo* $\|\ \|_0 : V \to \mathbb{R}$ dada como sigue: si $\beta = \lambda_1 w_1 + \cdots + \lambda_n w_n \in V$ se define $\|\beta\|_0 := \max_j |\lambda_j|_K$. Claramente, $\|\ \|_0$ es una norma de V y V es completo con respecto a esta norma.

Probaremos primero que la topología inducida por $\| \ \|_0$ es *más fina* que la topología inducida por $\| \ \|$. En efecto, sea $\alpha = \lambda_1 w_1 + \cdots + \lambda_n w_n \in V$ con los $\lambda_i \in K$. Entonces

$$\begin{aligned} \|\alpha\| &= \|\sum_j \lambda_j w_j\| \leq \sum_j |\lambda|_K \|w_j\| \\ &< \sum_j (\max_j |\lambda_j|_K)\|w_j\| = (\max_j |\lambda_j|_K) \sum_j \|w_j\| \\ &= \|\alpha\|_0 \cdot c_0 \quad \text{con } c_0 := \textstyle\sum_j \|w_j\| > 0 \text{ constante.} \end{aligned}$$

Se sigue que para toda $\varepsilon > 0$, poniendo $\delta = \varepsilon/c_0$ se tiene que $\|\alpha\|_0 < \delta$ implica que $\|\alpha\| \leq \|\alpha\|_0 c_0 < \delta c_0 = \varepsilon$, como se quería demostrar.

Mostraremos ahora que la topología inducida por $\| \ \|$ es *más fina* que la topología inducida por $\| \ \|_0$. En efecto, supongamos que ya probamos que *para todo* $\varepsilon > 0$ *existe un* $\delta > 0$ *tal que si* $\alpha = \sum_{i=1}^{n} \lambda_i w_i$ *y* $\|\alpha\| < \delta$, *entonces* $|\lambda_n|_K < \varepsilon$. Asumiendo esto, para todo $\varepsilon > 0$, si $\alpha = \sum_{i=1}^{n} \lambda_i w_i$, sea $\delta_n > 0$ tal que $\|\alpha\| < \delta_n$ implica $|\lambda_n|_K < \varepsilon$ por la afirmación anterior. Como la norma del máximo $\|\alpha\|_0$ es igual al mayor valor absoluto $|\lambda_j|_K$ de los coeficientes de $\alpha = \sum_j \lambda_j w_j$, permutando los vectores w_j, si hiciera falta, podemos suponer que $\|\alpha\|_0 = |\lambda_n|_K$ y por lo tanto si $\|\alpha\| < \delta_n$, entonces $|\lambda_n|_K < \varepsilon$, i.e., $\|\alpha\|_0 < \varepsilon$, que es lo que se quiere demostrar. Resta entonces demostrar la afirmación de arriba. Supongamos que la afirmación es falsa. Entonces existe un $\varepsilon > 0$ tal que para todo $\delta > 0$ existe un $\alpha = \sum \lambda_i w_i$ con $\|\alpha\| < \delta$ pero $|\lambda_n|_K \geq \varepsilon$. Pongamos

$$\beta := \frac{1}{\lambda_n}\alpha = \frac{\lambda_1}{\lambda_n} w_1 + \cdots + \frac{\lambda_{n-1}}{\lambda_n} w_{n-1} + w_n \in V.$$

Nótese que $\lambda_n \neq 0$ ya que $|\lambda_n|_K \geq \varepsilon$ por hipótesis. Se tiene entonces que

$$\|\beta\| = \frac{1}{|\lambda_n|_K} \|\alpha\| \leq \delta/\varepsilon$$

ya que $\|\alpha\| \leq \delta$ y $|\lambda_n|_K \geq \varepsilon$ y por lo tanto $1/|\lambda_n|_K \leq 1/\varepsilon$. Ahora, como esto sucede para todo $\delta > 0$, reemplazando δ por $\delta\varepsilon$ se tiene que para todo $\delta > 0$

existe un $\beta_\delta \in V$ de la forma

$$\beta_\delta = \gamma_1 w_1 + \cdots + \gamma_{n-1} w_{n-1} + w_n \in V$$

con $\|\beta_\delta\| < \delta$. En particular, para $\delta = 1/m$ con $m \in \mathbb{N}$, existe una sucesión de elementos

$$\beta_m = \gamma_1^{(m)} w_1 + \cdots + \gamma_{n-1}^{(m)} w_{n-1} + w_n \in V$$

tales que $\|\beta_m\| < 1/m$. Se sigue que

$$\beta_m - \beta_t = \sum_{i=1}^{n-1} \left(\gamma_i^{(m)} - \gamma_i^{(t)}\right) w_i$$

(se cancela el w_n) y además

$$\|\beta_m - \beta_t\| \leq \|\beta_m\| + \|\beta_t\| < \frac{1}{m} + \frac{1}{t}.$$

Ahora, por hipótesis de inducción la norma $\|\ \|$ de V restringida al subespacio W generado por $\{w_1, \ldots, w_{n-1}\}$ induce la misma topología que $\|\ \|_0$ y como $\beta_m - \beta_t \in W$ satisfacen que $\|\beta_m - \beta_t\| < 1/m + 1/t$, entonces si m, t son suficientemente grandes se tiene que $\|\beta_m - \beta_t\|$ es pequeño y por lo tanto $\|\beta_m - \beta_t\|_0 = \max |\gamma_i^{(m)} - \gamma_i^{(t)}|$ debe ser pequeño también, y por lo tanto los $|\gamma_i^{(m)} - \gamma_i^{(t)}|$ deben ser pequeños, i.e., $\{\gamma_i^{(m)}\}$ para $i = 1, \ldots, n-1$, son sucesiones de Cauchy en K, que es completo, y por lo tanto convergen a elementos $\tilde{\gamma}_i = \lim_{m\to\infty} \{\gamma_i^{(m)}\} \in K$ para $0 \leq i \leq n-1$. Pongamos ahora

$$\tilde{\gamma} := \tilde{\gamma}_1 w_1 + \cdots + \tilde{\gamma}_{n-1} w_{n-1} + w_n \in V.$$

Entonces,

$$\|\tilde{\gamma} - \beta_m\| = \| \sum_{j=1}^{n-1} \left(\tilde{\gamma}_j - \tilde{\gamma}_j^{(m)}\right) w_j \| \leq \sum_{j=1}^{n-1} |\tilde{\gamma}_j - \tilde{\gamma}_j^{(m)}|_K \|w_j\| < \varepsilon$$

la última desigualdad porque los $\|w_i\|$ son fijos y $\gamma_j^{(m)} \to \tilde{\gamma}_j$, por lo que los $|\tilde{\gamma}_j - \tilde{\gamma}_j^{(m)}|_K$ son pequeños para m suficientemente grande. Se sigue que

$$\|\tilde{\gamma}\| = \|\tilde{\gamma} - \beta_m + \beta_n\| \leq \|\tilde{\gamma} - \beta_m\| + \|\beta_m\| < \varepsilon + \frac{1}{m},$$

i.e., $\|\tilde{\gamma}\| = 0$ y así $\tilde{\gamma} = 0$, por lo que

$$0 = \tilde{\gamma} = \tilde{\gamma}_1 w_1 + \cdots + \tilde{\gamma}_{n-1} w_{n-1} + w_n$$

en contradicción con la independencia lineal de los w_i (ya que el coeficiente de w_n es 1). Se sigue que la afirmación inicial es verdadera, como se quería probar. □

Para la demostración de la *existencia* de la valuación usaremos el corolario (1.24) de la segunda versión del lema de Hensel. El resultado que buscamos es:

Teorema 1.26. *Sea K un campo no arquimediano completo y sea L/K una extensión finita de grado n. Entonces, existe una única extensión $|\ |_L$ del valor absoluto $|\ |_K$ de K, dada por*

$$|a|_L := |N_{L/K}(a)|_K^{1/n}$$

para $a \in L$, donde $N_{L/K} : L^* \to K^*$ es la norma (véase el anexo §1.10). *Más aún, L es completo con respecto a $|\ |_L$.*

En términos de valuaciones, la valuación v_L de L que extiende a la valuación v_K de K está dada por

$$v_L(a) := \frac{1}{n} v_K(N_{L/K}(a)).$$

Para las propiedades de la norma $N_{L/K}$ que usamos, véase el anexo §1.10.

DEMOSTRACIÓN. *Unicidad.* Si $|\ |_1$ y $|\ |_2$ son dos valuaciones de L que extienden a la valuación $|\ |_K$ de K, entonces las normas asociadas $\|\ \|_1$ y $\|\ \|_2$ inducen la misma topología por el lema (1.25), y por lo tanto las valuaciones son equivalentes $|\ |_1 \sim |\ |_2$. Más aún, por el mismo lema, si ya se tuviera una extensión $|\ |_L$ de $|\ |_K$ a L, entonces L sería completo con respecto a esa valuación.

Existencia. Definiendo la función $|\ |_L : L \to \mathbb{R}$ mediante $|a|_L := |N_{L/K}(a)|_K^{1/n}$, mostraremos que en efecto es una valuación de L. Primero, claramente extiende a la valuación de K ya que si $a \in K$ entonces $N_{L/K}(a) = a^n$ y por lo tanto $|a|_L := |N_{L/K}(a)|_K^{1/n} = |a^n|_K^{1/n} = |a|_K$. También es claro que $|a|_L \geq 0$ para todo $a \in L$ y además $|a|_L = |N_{L/K}|_K^{1/n} = 0$ si y sólo si $|N_{L/K}(a)|_K = 0$, y esto sucede si y sólo si $N_{L/K}(a) = 0$, i.e., si y sólo si $a = 0$. También, como $N_{L/K}$ es multiplicativa entonces

$$|ab|_L = |N_{L/K}(ab)|_K^{1/n} = |N_{L/K}(a)|_K^{1/n} |N_{L/K}(b)|_K^{1/n} = |a|_L |b|_L.$$

Mostraremos ahora que $|a|_L \leq 1$ implica que $|a+1|_L \leq 1$. Nótese que esto implica que $|\ |_L$ satisface la desigualdad ultramétrica ya que si $a, b \in L$ son arbitrarios y, digamos, $|a|_L \geq |b|_L$, entonces poniendo $c := b/a \in L$ se tiene que $|c|_L \leq 1$ y así $|1+c|_L \leq 1$, por lo que

$$|a+b|_L = |a(1+b/a)|_L = |a|_L|1+c|_L \leq |a|_L = \text{máx}\{|a|_L, |b|_L\}.$$

Resta entonces probar que $|N_{L/K}(a)|_K^{1/n} \leq 1$ implica que $|N_{L/K}(a+1)|_K^{1/n} \leq 1$, o lo que es lo mismo, que $|N_{L/K}(a)|_K \leq 1$ implica que $|N_{L/K}(a+1)|_K \leq 1$. Para esto, primero observamos que considerando el campo intermedio $K(a)$ en la torre de campos $K \subseteq K(a) \subseteq L$ y como la norma es multiplicativa, entonces

$$N_{L/K}(a) = N_{K(a)/K}N_{L/K(a)}(a) = N_{K(a)/K}(a)^{[L:K(a)]},$$

la última igualdad porque $a \in K(a)$. Se sigue entonces que debemos probar que

$$|N_{K(a)/K}(a)|_K \leq 1 \quad \text{implica} \quad |N_{K(a)/K}(1+a)|_K \leq 1.$$

Recordando (§1.10) que la norma $N_{K(a)/K}(a)$ está dada en términos del polinomio mínimo $f(x) = \text{Irr}(a, K) = x^r + \cdots + a_1 x + a_0$ como $N_{K(a)/K}(a) = \pm a_0$, entonces como $|a_0|_K = |N_{K(a)/K}(a)|_K \leq 1$ se sigue que $a_0 \in \mathcal{O}_K$ y como $f(x)$ es mónico irreducible, por el corolario (1.24) de la segunda versión del lema de Hensel se sigue que $f(x) \in \mathcal{O}_K[x]$. Finalmente, observando que $f(x-1) = \text{Irr}(a+1, K)$ y que el término independiente de $f(x-1)$ es $f(-1)$, y como $1 \in \mathcal{O}_K$ y $f(x) \in \mathcal{O}_K[x]$ implican que $f(-1) \in \mathcal{O}_K$, entonces $N_{K(a)/K}(a+1) = \pm f(-1) \in \mathcal{O}_K$ y por lo tanto $|N_{K(a)/K}(1+a)|_K \leq 1$, como se quería probar. □

Corolario 1.27. *Sea K, v un campo no arquimediano completo y sea L/K una extensión finita. Entonces:*

(1) *Si $a, b \in L$ son conjugados (i.e., raíces del mismo mónico irreducible en $K[x]$), entonces $|a|_K = |b|_K$.*

(2) *Si L/K es Galois y si v_L es la valuación de L que extiende a la valuación de K, entonces para todo $\sigma \in \text{Gal}(L/K)$ se tiene que $v_L \circ \sigma = v_L$.*

(3) *Si L/K es Galois, entonces para todo $\sigma \in \text{Gal}(L/K)$ se tiene $\sigma\mathcal{O}_L = \mathcal{O}_L$ y $\sigma\mathfrak{p}_L = \mathfrak{p}_L$. Se sigue que $\sigma \in \text{Gal}(L/K)$ induce, por restricción y paso al cociente, un automorfismo $\overline{\sigma} \in \text{Gal}(\overline{L}/K)$ de los campos residuales respectivos.*

DEMOSTRACIÓN. (1): Por hipótesis a y b tienen el mismo mónico irreducible $m(x) = \mathrm{Irr}(a, K) = \mathrm{Irr}(b, K) \in K[x]$, y por lo tanto tienen la misma norma por §1.10: $N_{L/K}(a) = N_{L/K}(b)$ y así, por el teorema anterior tienen la misma valuación. El inciso (2) es consecuencia directa de (1), ya que si $\alpha \in L$ y $\sigma \in \mathrm{Gal}(L/K)$, entonces α y $\sigma(\alpha)$ son conjugados. La parte (3) también se sigue de (1). □

Corolario 1.28. (1) *Sea L/K una extensión finita de campos valuados completos y supongamos que v_K es discreta. Entonces v_L es discreta también.*

(2) *Si L/K es una extensión finita de Galois de campos valuados discretos y si π es un elemento primo de L entonces para todo $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\pi)$ es un elemento primo de L.*

DEMOSTRACIÓN. (1): Si $n = [L : K]$, por el teorema (1.26) se tiene que

$$v_L(L^*) = (1/n)v_K(N_{L/K}(L^*)) \subseteq (1/n)v_K(K^*)$$

y así, como $v_K(K^*)$ es discreto, entonces también $v_L(L^*)$ lo es. La parte (2) se sigue del inciso (1) del corolario anterior. □

Observación. Si L/K es una extensión algebraica, no necesariamente finita, de un campo valuado no arquimediano completo K, entonces la valuación v_K de K se extiende de manera única a cualquier subcampo $M \subseteq L$ de grado finito sobre K y por lo tanto, usando el lema de Zorn, se extiende de manera única a L. Sin embargo, el campo L con esta valuación v_L no necesariamente es completo.

1.5 Ramificación

Dada una extensión L/K de campos valuados no arquimedianos completos, donde la valuación v_L de L extiende a la valuación v_K de K, denotado $v_L|v_K$, en esta sección estudiamos algunos invariantes asociados a L/K y $v_L|v_K$, en especial los grupos $v_K(K^*) \subseteq v_L(L^*)$ y la extensión $\overline{L}/K$ de sus campos residuales:

Definición 1.29. El índice $e = e(L/K) := [v_L(L^*) : v_K(K^*)]$ se llama el *índice de ramificación* de la extensión de campos valuados L/K.

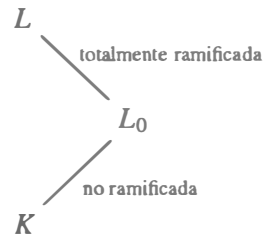
El grado $f = f(L/K) := [\overline{L} : K]$ de la extensión de campos residuales L/K se llama el *grado residual* de la extensión de campos valuados L/K.

Ambos invariantes son números enteros ≥ 1 ó $+\infty$.

Probaremos primero en (1.33) que si L/K es finita de grado n, entonces $ef \leq n$. Si además la valuación v_K es discreta (y por lo tanto v_L también es discreta por el corolario anterior), entonces mostraremos en (1.35) que $ef = n$.

Si $f = n$ se dice que L/K es *no ramificada* y si $f = 1$ se dice que L/K es *totalmente ramificada*. En el primer caso los grupos de valuación resultan ser iguales y se pueden describir en términos de la extensión de campos residuales $\overline{L}/K$. En el segundo caso, los campos residuales son iguales y se pueden describir en términos de polinomios de Eisenstein.

Al final, probaremos que si L/K es una extensión finita de campos valuados discretos completos, entonces existe un campo intermedio L_0 tal que



Los invariantes e_{v_L/v_K} y f_{v_L/v_K} son transitivos en el sentido siguiente:

Lema 1.30. *Sea $L \supseteq M \supseteq K$ una torre de campos valuados. Entonces:*

(1) $e_{v_L/v_K} = e_{v_L/v_M} e_{v_M/v_K}$.

(2) $f_{v_L/v_K} = f_{v_L/v_M} f_{v_M/v_K}$.

DEMOSTRACIÓN. Directa de las inclusiones $v_L(L^*) \supseteq v_M(M^*) \supseteq v_K(K^*)$ y $K \subseteq M \subseteq L$ respectivamente. □

Lema 1.31. *Sea L/K una extensión finita de campos valuados no arquimedianos. Sean $n = [L : K]$ y $f = f_{v_L/v_K}$. Entonces, $f \leq n$.*

DEMOSTRACIÓN. Mostraremos que cualesquiera $n + 1$ elementos $\overline{a}_1, \ldots, \overline{a}_{n+1}$ del campo residual $\overline{L}$ son linealmente dependientes sobre K. Sean $a_1, \ldots, a_{n+1}$ en $\mathcal{O}_L$ representantes de los $\overline{a}_i$. Como $\mathcal{O}_L \subseteq L$ y $[L : K] = n$, entonces los a_i son linealmente dependientes sobre K y así existen $\alpha_i \in K$ tales que

$$\sum_{i=1}^{n+1} \alpha_i a_i = 0 \quad \text{con algún } \alpha_i \neq 0.$$

Dividiendo por el coeficiente $\alpha_j \neq 0$ que tenga mayor valor $|\alpha_j|_{v_K}$ podemos suponer que $\max\{|\alpha_i|_{v_K}\} = 1$ y por lo tanto todos los coeficientes α_i en $(*)$

están en $\mathcal{O}_K$ y alguno de ellos tiene valor $|\alpha_j|_{v_K} = 1$ y por lo tanto no está en $\mathfrak{p}_K$, i.e., algún $\overline{\alpha}_j \neq 0$ en K. Reduciendo la igualdad $(*)$ módulo $\mathfrak{p}_L$ se obtiene

$$\sum_{i=1}^{n+1} \overline{\alpha}_i \overline{a}_i = 0 \quad \text{con algún } \overline{\alpha}_j \neq 0 \text{ en } K,$$

i.e., las $n+1$ clases $\overline{a}_i \in L$ son linealmente dependientes sobre K. □

Lema 1.32. *Sea L/K una extensión finita de campos valuados no arquimedianos. Sean $n = [L : K]$ y $e = e_{v_L/v_K}$. Entonces, $e \leq n$.*

DEMOSTRACIÓN. Sea $k \leq e_{v_L/v_K}$ cualquier número natural y supongamos que se tienen elementos $\alpha_1, \ldots, \alpha_k \in L^*$ tales que las clases laterales $v_L(\alpha_1)+v_K(K^*)$, $\ldots$, $v_L(\alpha_k)+v_K(K^*)$ son distintas en el grupo cociente $v_L(L^*)/v_K(K^*)$. Mostraremos que los elementos $\alpha_1, \ldots, \alpha_k \in L^*$ son linealmente independientes sobre K. En efecto, si

$$\sum_{i=1}^{k} c_i \alpha_i = 0 \quad \text{con } c_i \in K,$$

observamos que para cada par de términos $c_i\alpha_i$ y $c_j\alpha_j$ con $i \neq j$, si sucediera que $v_L(c_i\alpha_i) = v_L(c_j\alpha_j)$ entonces se tendría que

$$v_L(c_i) + v_L(\alpha_i) = v_L(c_i\alpha_i) = v_L(c_j\alpha_j) = v_L(c_j) + v_L(\alpha_j)$$

y por lo tanto $v_L(\alpha_i) - v_L(\alpha_j) = v_L(a_j) - v_L(a_i) \in v_K(K^*)$, es decir, las clases laterales $v_L(\alpha_i)+v_K(K^*) = v_L(\alpha_j)+v_K(K^*)$, lo cual es una contradicción con la suposición inicial sobre estas clases. Se sigue que $v_L(c_i\alpha_i) \neq v_L(c_j\alpha_j)$ si $i \neq j$. Entonces, por (1.1) se tiene la última igualdad en

$$+\infty = v_L(0) = v_L\left(\sum_{i=1}^{k} c_i\alpha_i\right) = \min\{v_L(c_i\alpha_i)\},$$

y por lo tanto $v_L(c_i\alpha_i) = +\infty$ para toda i, es decir, $c_i\alpha_i = 0$ para toda i, y así $c_i = 0$ para toda i ya que los $\alpha_i \neq 0$. Se sigue que los $\alpha_i \in L^*$ son linealmente independientes sobre K para todo $k \leq e_{v_L/v_K}$ y consecuentemente $e_{v_L/v_K} \leq [L : K] = n$. □

El resultado principal combina el grado n de la extensión finita L/K, el índice de ramificación e y el grado residual f de $v_L|v_K$:

Teorema 1.33. *Sea L/K una extensión finita de campos valuados no arquimedianos tales que $v_L|v_K$. Sean $n = [L : K]$, $e = e(v_L/v_k)$, $f = f(v_L/v_k)$. Entonces $ef \leq n$.*

DEMOSTRACIÓN. Usando los dos lemas anteriores, sean $\alpha_1, \ldots, \alpha_f$ elementos de $\mathcal{O}_L$ tales que sus clases residuales $\overline{\alpha}_j$ formen una base de L sobre K. Y sean $\beta_1, \ldots, \beta_e$ elementos de L^* tales que sus valuaciones $v_L(\beta_j)$ sean representantes de clases laterales distintas en el cociente $v_L(L^*)/v_K(K^*)$. Probaremos que los ef elementos $\alpha_i\beta_j \in L$ son linealmente independientes sobre K. Supongamos entonces que

$$\sum_{i,j} c_{ij}\alpha_i\beta_j = 0 \qquad \text{con los } c_{ij} \in K.$$

Multiplicando los coeficientes c_{ij} por el inverso multiplicativo del coeficiente que tenga la menor valuación $v_K(c_{ij})$, podemos suponer que todos los coeficientes $c_{ij} \in \mathcal{O}_K$ pero *no* todos están en $\mathfrak{p}_K$.

Observemos ahora que si para toda j se tuviera que $\sum_i c_{ij}\alpha_i \in \mathfrak{p}_L$, entonces $\sum_i \overline{c}_{ij}\overline{\alpha}_i = 0$ en L y como los $\overline{\alpha}_i$ son linealmente independientes sobre K, entonces se tendría que todas las $c_{ij} \in \mathfrak{p}_K$, en contradicción con el párrafo anterior. Se sigue que debe existir un índice j tal que $\sum_i c_{ij}\alpha_i \in \mathcal{O}_L - \mathfrak{p}_L = U_L$ y así

$$v_L\left(\sum_i c_{ij}\alpha_i\right) = 0. \tag{1}$$

Ahora, consideremos la igualdad

$$0 = \sum_{i,j} c_{ij}\alpha_i\beta_j = \sum_j \beta_j \sum c_{ij}\alpha_i$$

y observemos que para cada j, dividiendo el sumando $\sum_i c_{ij}\alpha_i$ entre el coeficiente $c_{i_0 j}$ dado por $v_L(c_{i_0 j}) := \min_i\{v_L(c_{ij})\}$, se tiene que

$$\begin{aligned} v_L\left(\sum_i c_{ij}\alpha_i\right) &= v_L\left(c_{i_0 j}\sum_i \frac{c_{ij}}{c_{i_0 j}}\alpha_i\right) \\ &= v_L(c_{i_0 j}) + v_L\left(\sum_i \frac{c_{ij}}{c_{i_0 j}}\alpha_i\right) \\ &\quad v_L(c_{i_0 j}) \qquad \text{por (1)} \\ &\quad \min_i\{v_L(c_{ij})\}. \end{aligned}$$

Entonces, para cada j el sumando correspondiente de $(*)$ satisface que

$$v_L\left(\beta_j \sum_i c_{ij}\alpha_i\right) = v_L(\beta_j) + \min_i\{v_L(c_{ij})\}$$

/ estos números son distintos entre sí porque los $v_L(\beta_j)$ representan clases aterales distintas en $v_L(L^*)/v_K(K^*)$. Aplicando (1.1)(4) a $(*)$ se sigue que

$$\begin{aligned} +\infty = v_L(0) &= v_L\left(\sum_j \beta_j \sum_i c_{ij}\alpha_i\right) \\ &- \min_j\left\{v_L\left(\beta_j \sum_i c_{ij}\alpha_i\right)\right\} \\ &\min_j\left\{v_L(\beta_j) + \min_i\{v_L(c_{ij})\}\right\} \\ &= \min_j\left\{\min_i\{v_L(\beta_j c_{ij})\}\right\} \\ &= \min_{i,j}\{v_L(\beta_j c_{ij})\} \end{aligned}$$

y por lo tanto todos los $\beta_j c_{ij} = 0$, pero como los $\beta_j \neq 0$, entonces todos los $c_{ij} = 0$. □

Observación. En general no se tiene la igualdad $ef = n$. Por ejemplo, si K no es completo y $\widehat{K}$ es su completación, entonces $[\widehat{K} : K] \neq 1$ pero $e(\widehat{K}/K) = 1 = f(\widehat{K}/K)$ por (1.12) (3) y (4). De hecho, aun si L/K es una extensión finita de campos completos, pero no discretos, la igualdad puede falar, como lo muestra el ejemplo siguiente:

Ejemplo 15. En la literatura de campos valuados este ejemplo no ha sido tratado en detalle; por su importancia ofrecemos los detalles del mismo:

Sean $K_0 = \mathbb{Q}_2$, $K_1 = K_0(\zeta_1)$ con $\zeta_1^2 = 2$, y recursivamente se define $K_n = K_{n-1}(\zeta_n)$ donde $\zeta_n^2 = \zeta_{n-1}$. Entonces $K = \bigcup_{n\geq 0} K_n$, y claramente $K/\mathbb{Q}_2$ es una extensión algebraica; así, la valuación 2-ádica v de $\mathbb{Q}_2$ se extiende en forma única a una valuación v de K. Observemos ahora que $v(K_n) = (1/2^n)\mathbb{Z}$ para toda $n \geq 0$. En efecto, $v(K_0) = v(\mathbb{Q}_2) = \mathbb{Z} = (1/2^0)\mathbb{Z}$, y si suponemos,

por hipótesis de inducción, que $v(\zeta_{n-1}) = 1/2^{n-1}$, como $\zeta_n^2 = \zeta_{n-1}$, entonces $v(\zeta_n) = 1/2^n$ por lo que $\zeta_n \notin K_{n-1}$ y por lo tanto

$$2 = [K_n : K_{n-1}] \geq [v(K_n) : v(K_{n-1})] \geq 2;$$

se sigue que $v(K_n) = (1/2^n)\mathbb{Z}$. Como consecuencia de esto se tiene que

$$v(K) = \bigcup_{n=0}^{\infty} (1/2^n)\mathbb{Z}.$$

De esta igualdad se sigue que si $v(K) \subseteq H$, con H un subgrupo de $\mathbb{R}^*$ y $[H : v(K)] \leq 2$, entonces $v(K) = H$.

Mostraremos ahora que el campo residual K_v de (K, v) es $\mathbb{F}_2$. En efecto, sea v_n la restricción de v a K_n. La torre de extensiones $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots$ induce la torre de campos residuales $K_{0,v_0} \subseteq K_{1,v_1} \subseteq \cdots \subseteq K_{n,v_n} \subseteq \cdots$, por lo que $K_v = \bigcup_{n=0}^{\infty} K_{n,v_n}$.

De la desigualdad del teorema (1.33)

$$2 = [K_n : K_{n-1}] \geq [v_n(K_n) : v_{n-1}(K_{n-1})] \cdot [K_{n,v_n} : K_{n-1,v_{n-1}}]$$

y de la igualdad obvia

$$[v_n(K_n) : v_{n-1}(K_{n-1})] = [(1/2^n)\mathbb{Z} : (1/2^{n-1})\mathbb{Z}] = 2$$

se sigue que $[K_{n,v_n} : K_{n-1,v_{n-1}}] = 1$, i.e., $K_{n,v_n} = K_{n-1,v_{n-1}}$ para toda $n \geq 1$, y por lo tanto

$$K_v = \mathbb{Q}_2 = \mathbb{F}_2.$$

Como es usual, denotemos por $\sqrt{-1} = i$ (una raíz de $x^2 + 1 \in K[x]$), y sea $\widetilde{K} = K(i)$. Mostraremos que $[\widetilde{K} : K] = 2$, i.e., mostraremos que el polinomio $\phi(x) = x^2 + 1$ es irreducible en $K[x]$. En efecto, si no lo fuera tendría una raíz en K y por lo tanto en algún K_n. Sea $n \geq 0$ el menor índice tal que $i \in K_n$. Obsérvese que $n > 0$ ya que, con el cambio de variable $x \leftrightarrow x + 1$, es evidente que el polinomio

$$\phi(x + 1) = (x + 1)^2 + 1 = x^2 + 2x + 2$$

es irreducible sobre $K_0 = \mathbb{Q}_2$, por el criterio de irreducibilidad de Eisenstein. Se sigue que $n \geq 1$ y así, $i \in K_n$ es de la forma $i = c + d\zeta_n$ con $c, d \in K_{n-1}$. Elevando al cuadrado esta igualdad se obtiene

$$-1 = i^2 = (c + d\zeta_n)^2 = c^2 + d^2\zeta_{n-1} + 2cd\zeta_n,$$

y comparando coeficientes se tiene que $cd = 0$ por lo que $c = 0$ ó $d = 0$. Si $c = 0$, entonces $-1 = d^2\zeta_{n-1}$ y por lo tanto

$$0 = v(-1) = v(d^2) + v(\zeta_{n-1}) = 2v(d) + 1/2^{n-1},$$

y así $v(d) = -1/2^n$, una contradicción ya que $d \in K_{n-1}$. Si $d = 0$, entonces $i = c \in K_{n-1}$, lo cual contradice la elección de n. Se sigue que $x^2 + 1$ es irreducible sobre K y por lo tanto $\widetilde{K} = K(i)$ es de grado 2 sobre K. De manera similar, para $\widetilde{K}_n := K_n(i)$ se tiene que $[\widetilde{K}_n : K_n] = 2$ para toda $n \geq 0$.

Sea $\tilde{v}$ la (única) extensión de la valuación v de K a $\widetilde{K}$. Entonces, $[\tilde{v}(\widetilde{K}) : v(K)] \leq 2$, y así, por una observación previa se tiene que $\tilde{v}(\widetilde{K}) = v(K)$, por lo que $e(\widetilde{K}/K) = 1$. Mostraremos ahora que $f(\widetilde{K}/K) = 1$, es decir, mostraremos que los campos residuales $\widetilde{K}_{\tilde{v}} = K_v$ son iguales. Para esto necesitaremos el cálculo siguiente: para cada $n \geq 1$ sea

$$s_n := 1 + 2\left(\frac{1}{\zeta_1} + \frac{1}{\zeta_2} + \cdots + \frac{1}{\zeta_n}\right).$$

Mostraremos que $\tilde{v}(s_n - i) \geq 1 - 1/2^{n+1}$ para $i = \sqrt{-1}$. En efecto,

$$\begin{aligned}
s_n^2 + 1 &= [1 + (s_n - 1)]^2 + 1 = 2 + 2(s_n - 1) + (s_n - 1)^2 \\
&= 2 + 4\left(\frac{1}{\zeta_1} + \cdots + \frac{1}{\zeta_n}\right) + 4\left(\frac{1}{\zeta_1} + \cdots + \frac{1}{\zeta_n}\right)^2 \\
&= 2 + 4\left(\frac{1}{\zeta_1} + \cdots + \frac{1}{\zeta_n}\right) + 4\left(\frac{1}{2} + \frac{1}{\zeta_1} + \cdots + \frac{1}{\zeta_{n-1}} + 2\sum_{k \neq j} \frac{1}{\zeta_j \zeta_k}\right) \\
&= 4\left(1 + \frac{2}{\zeta_1} + \cdots + \frac{2}{\zeta_{n-1}}\right) + \frac{4}{\zeta_n} + 8\sum_{k \neq j} \frac{1}{\zeta_j \zeta_k} \\
&= 4s_{n-1} + \frac{4}{\zeta_n} + 8\sum_{k \neq j} \frac{1}{\zeta_j \zeta_k},
\end{aligned}$$

y notamos que $\tilde{v}(s_{n-1}) = 0$, por lo que $\tilde{v}(4s_{n-1}) = \tilde{v}(4) = v(4) = 2$. En forma similar

$$\tilde{v}\left(\frac{4}{\zeta_n}\right) = \tilde{v}(4) - \tilde{v}(\zeta_n) = 2 - \frac{1}{2^n},$$

y

$$\begin{aligned}\widetilde{v}\left(8\sum_{k\neq j}\frac{1}{\zeta_j\zeta_k}\right) &= \widetilde{v}(8)+\widetilde{v}\left(\sum_{k\neq j}\frac{1}{\zeta_j\zeta_k}\right)\\ &= 3+\sum_{k\neq j}\left(\widetilde{v}\left(\frac{1}{\zeta_j}\right)+\widetilde{v}\left(\frac{1}{\zeta_k}\right)\right)\\ &= 3-\sum_{k\neq j}\left(\frac{1}{2^j}+\frac{1}{2^k}\right)\\ &= 3-\frac{1}{2}-\frac{1}{4}=\frac{9}{4}.\end{aligned}$$

Se sigue que

$$\widetilde{v}(s_n^2+1)=\min\{2,\,2-\frac{1}{2^n},\,\frac{9}{4}\}=2-\frac{1}{2^n}.$$

Ahora, como $s_n^2+1=(s_n+i)(s_n-i)$ y estos dos factores son conjugados en $\widetilde{K}/K$, y $\widetilde{v}$ es la (única) extensión de v a $\widetilde{K}$, entonces $\widetilde{v}(s_n+i)=\widetilde{v}(s_n-i)$, por lo que

$$2-\frac{1}{2^n}=\widetilde{v}(s_n^2+1)=\widetilde{v}(s_n+i)+\widetilde{v}(s_n-i)=2\widetilde{v}(s_n-i),$$

y así $\widetilde{v}(s_n-i)=1-1/2^{n+1}$. Se sigue que si $n<m$, entonces

$$\widetilde{v}(s_n-i)<\widetilde{v}(s_m-i).$$

Usando este cálculo mostraremos que $\widetilde{K}_{\widetilde{v}}=K_v$. En efecto, sea $a+bi\in\mathcal{O}_{\widetilde{v}}$ cualquier elemento. Entonces su conjugado $a-bi\in\mathcal{O}_{\widetilde{v}}$, y por lo tanto (sumando y restando) $2a, 2bi\in\mathcal{O}_{\widetilde{v}}$, por lo que $v(2a)\geq 0$ y $v(2bi)\geq 0$, y así $v(a)\geq -1$ y $v(b)\geq -1$ (ya que $i^2=-1$ implica que $v(i)=0$).

Sea $n\geq 0$ tal que $a+bi\in\widetilde{K}_n$, y consecuentemente $a+bi\in\mathcal{O}_{\widetilde{v}_n}$.

(i) Si $\widetilde{K}_{n,\widetilde{v}_n}=K_{n,v_n}$, entonces existe un $c\in K_n\cap\mathcal{O}_v$ tal que $a+bi-c\in\mathfrak{p}_{\widetilde{v}}$ y por lo tanto $\widetilde{K}_{\widetilde{v}}\subseteq K_v$, como se quería.

(ii) Si $\widetilde{K}_{n,\widetilde{v}_n}\neq K_{n,v_n}$, entonces $[\widetilde{K}_{n,\widetilde{v}_n}:K_{n,v_n}]=2$, y como $ef\leq 2$, entonces $\widetilde{v}(\widetilde{K}_n)=v(K_n)$. Ahora, como

$$\begin{aligned}\widetilde{v}[(a+bi)-(a+bs_n)]=\widetilde{v}[b(i-s_n)]&=\widetilde{v}(b)+\widetilde{v}(i-s_n)\\ &\geq -1+1-1/2^{n+1}=-1/2^{n+1},\end{aligned}$$

de la igualdad $\widetilde{v}(\widetilde{K}_n) = v(K_n) = (1/2^n)\mathbb{Z}$ se sigue que $\widetilde{v}[(a+bi)-(a+bs_n)] \geq 0$. Si $m > n$, se tiene que

$$\begin{aligned}\widetilde{v}[(a+bi)-(a+bs_m)] &= \widetilde{v}(b) + \widetilde{v}(i-s_m)\\ &> \widetilde{v}(b) + \widetilde{v}(i-s_n)\\ &= \widetilde{v}[(a+bi)-(a+bs_n)] \geq 0.\end{aligned}$$

Con $c := a + bs_m \in \mathcal{O}_v$ se tiene que $(a+bi) - c \in \mathfrak{p}_{\widetilde{v}}$, como se quería.

Finalmente, si K' es la completación de K, entonces $L = K'(i)$ es la completación de $K(i) = \widetilde{K}$, y se tiene que $[L : K'] = 2$, con $e(L/K') = e(\widetilde{K}/K) = 1$ y $f(L/K') = f(\widetilde{K}/K) = 1$.

Sin embargo, en el caso cuando las valuaciones de K y L son discretas y los campos son completos, se tiene la igualdad $ef = n$ como probaremos en el siguiente teorema. Necesitaremos el lema siguiente:

Lema 1.34. *Sea L/K una extensión finita de campos valuados discretos y sean π_K y π_L primos de las valuaciones v_K y v_L respectivamente. Sea $e = e(v_L/v_K) \leq [L : K]$. Entonces $\pi_L^e = \pi_K u$, con $u \in U_L$ una unidad.*

DEMOSTRACIÓN. Como $e = \text{card}\ (v_L(L^*)/v_K(K^*))$, $v_L(\pi_L)$ es el generador de $v_L(L^*)$ y $v_K(\pi_K)$ es el generador de $v_K(K^*)$, entonces $ev_L(\pi_L) = v_K(\pi_K)$. □

El resultado principal es:

Teorema 1.35. (1) *Si L/K es una extensión de campos valuados discretos completos tal que $e = e(L/K) < \infty$ y $f = f(L/K) < \infty$, entonces L/K es finita de grado $[L : K] \leq ef$.*

(2) *En particular, si L/K es una extensión finita de campos valuados discretos completos de grado $n = [L : K]$ y si $e = e(v_L/v_K)$ y $f = f(v_L/v_K)$, entonces $ef = n$.*

DEMOSTRACIÓN. Para la parte (1) pongamos $\mathfrak{p}_L = \langle \pi_L \rangle$ y $\mathfrak{p}_K = \langle \pi_K \rangle$. Sean $\alpha_i \in \mathcal{O}_K$, $1 \leq i \leq f$ tales que sus clases residuales $\overline{\alpha}_i \in L$ son una base de L sobre K. Entonces, todo elemento $\overline{a} \in \overline{L}$ se puede representar por un elemento de la forma $a = a_1\alpha_1 + \cdots + a_f\alpha_f$, con $a_i \in \mathcal{O}_K$.

Ahora, por (1.16) todo elemento $\alpha \in L^*$ se puede escribir como una serie

$$\alpha = \sum_{k \gg -\infty}^{\infty}$$

con los $a_k \in \mathcal{R}_L \subseteq \mathcal{O}_L$ (un conjunto completo de representantes de L que contiene al 0). También, por el lema anterior, como $\pi_L^e = \pi_K u$ con $u \in U_L$ una unidad, para las potencias π_L^k, escribiendo $k = es + j$ con $0 \leq j \leq e-1$, se tiene que $\pi_L^k = \pi_K^s \pi_L^j u_s$ con $0 \leq j \leq e-1$, $s \in \mathbb{Z}$ y $u_s \in U_L$ una unidad. Entonces, escribiendo el k-ésimo término de $(*)$ como $a_k \pi_L^k = (a_k u_s)\pi_K^s \pi_L^j$, donde $a_k u_s \in \mathcal{O}_L$ de tal forma que usando el párrafo anterior podemos representar a su clase residual $\overline{a}_k \overline{u}_s \in \overline{L}$ como $a_k u_s = a_{1ks}\alpha_1 + \cdots + a_{fks}\alpha_f$ con $a_{iks} \in \mathcal{O}_K$. Entonces, la serie $(*)$ queda:

$$\begin{aligned}
\alpha &= \sum_{k \gg -\infty}^{\infty} a_k \pi_L^k = \sum_{k \gg -\infty}^{\infty} (a_k u_s)\pi_K^s \pi_L^j \\
&= \sum_{k \gg -\infty}^{\infty} \left(\sum_{i=1}^{f} a_{iks} \alpha_i \pi_K^s \pi_L^j \right) \\
&= \sum_{j=1}^{f} \left(\sum_{i,s} a_{ijs} \alpha_i \pi_K^s \pi_L^j \right) \\
&\quad \sum_{i,j,s} a_{ijs} \alpha_i \pi_K^s \pi_L^j \\
&= \sum_{j=0}^{e-1} \sum_{i=1}^{f} \left(\sum_{s}^{\infty} a_{ijs} \pi_K^s \right) \alpha_i \pi_L^j,
\end{aligned}$$

donde $a_{ijs} \in \mathcal{O}_K \subseteq K$ y así $\sum_s^{\infty} a_{ijs}\pi_K^s \in K^*$. Hemos mostrado así que todo α en L^* se puede expresar como una combinación lineal, con coeficientes $\sum_s^{\infty} a_{ijs}\pi_K^s$ en K^*, de los ef elementos $\{\alpha_i \pi_L^j\}_{1 \leq i \leq f,\, 0 \leq j \leq e-1}$, y por lo tanto este conjunto genera a L sobre K, i.e., $[L : K] \leq ef$.

La parte (2) se sigue de la desigualdad $ef \leq n = [L : K]$ del teorema (1.33) y de la desigualdad de la parte (1) de este teorema. □

Corolario 1.36. *Sea L/K una extensión finita de campos valuados discretos completos de grado $[L : K] = n$. Entonces:*

(1) *L/K es no ramificada (i.e., $f = n$) si y sólo si $e = 1$.*

(2) *L/K es totalmente ramificada (i.e., $f = 1$) si y sólo si $e = n$.*

(3) *Si L/K es no ramificada y π_K es un primo de K, entonces también es primo de L.*

DEMOSTRACIÓN. (1) y (2) se siguen de las definiciones y del teorema anterior. Para (3), como $e = 1$, por (1.34), $\pi_K = \pi_L u$, con π_L un primo de L y $u \in U_L$. □

Otra consecuencia de la demostración del teorema anterior es la existencia de bases de los anillos de valuación de los campos involucrados:

Lema 1.37. *Sea K un campo valuado no arquimediano, no necesariamente completo, y sea $\mathcal{O}_K$ su anillo de valuación. Entonces, todo $\mathcal{O}_K$-módulo M finitamente generado y libre de torsión tiene una $\mathcal{O}_K$-base.*

DEMOSTRACIÓN. Sea $e_1, \ldots, e_n$ un conjunto de generadores de M. Si no forman una $\mathcal{O}_K$-base, entonces existen $a_1, \ldots, a_n \in \mathcal{O}_K$ no todos cero tales que

$$a_1 e_1 + \cdots + a_n e_n = 0. \tag{1}$$

Sin perder generalidad, podemos suponer que $|a_n|_v = \max\{|a_j|_v\}$ y así $a_n \neq 0$ y por lo tanto $b_j := a_j/a_n \in \mathcal{O}_K$. De (1) se obtiene

$$a_n(b_1 e_1 + \cdots + b_{n-1} e_{n-1} + e_n) = 0 \tag{2}$$

con $a_n \neq 0$ y así, como M es libre de torsión, se sigue que

$$b_1 e_1 + \cdots + b_{n-1} e_{n-1} + e_n = 0$$

i.e., $e_n \quad -b_1 e_1 - \cdots - b_{n-1} e_{n-1}$ y así $\{e_1, \ldots, e_{n-1}\}$ es un conjunto de $\mathcal{O}_K$-generadores de M. Si es una base ya acabamos y si no lo es, se repite el proceso. □

Proposición 1.38. *Sea L/K una extensión finita de campos discretos completos. Sean $\mathcal{O}_K$ y $\mathcal{O}_L$ sus anillos de valuación y $\mathfrak{p}_K = \langle \pi_K \rangle$ y $\mathfrak{p}_L = \langle \pi_L \rangle$ sus ideales máximos. Sean $f = f(L/K)$, $e = e(L/K)$ y $ef = n = [L : K]$. Sea $\overline{\alpha}_1, \ldots, \overline{\alpha}_f$ una base de la extensión de campos residuales $\overline{L}/K$. Entonces, los ef elementos $\alpha_i \pi_L^j$, $1 \leq i \leq f$, $0 \leq j \leq e-1$, son una $\mathcal{O}_K$-base de $\mathcal{O}_L$.*

DEMOSTRACIÓN. Claramente $\mathcal{O}_L$ es un $\mathcal{O}_K$-módulo libre de torsión ya que está metido en un campo. De la demostración del teorema (1.35) anterior se tiene

que el conjunto $\{\alpha_i \pi_L^j\}$ es una base de L/K. Sea $\alpha \in \mathcal{O}_L \subset L$; entonces existen $a_{ij} \in K$ tales que

$$\alpha = \sum_{i,j} a_{ij} \alpha_i \pi_L^j; \tag{1}$$

mostraremos que los $a_{ij} \in \mathcal{O}_K$. En efecto, por (1.16)(1) se tiene que

$$\alpha = \sum_{k=0}^{\infty} a_k \pi_L^k \qquad \text{con} \qquad a_k \in R_L \subseteq \mathcal{O}_L$$

y así, como en la demostración de (1.35) la expresión anterior para α queda

$$\alpha = \sum_{j=0}^{e-1} \sum_{i=1}^{f} \left(\sum_{s=0}^{\infty} a_{ijs} \pi_K^s \right) \alpha_i \pi_L^j \tag{2}$$

donde, como en este caso $s \geq 0$, se tiene que $\sum_{s=0}^{\infty} a_{ijs} \pi_K^s \in \mathcal{O}_K$. Por la unicidad de la expresión de α en (1) y (2) se sigue que los $a_{ij} = \sum_{s=0}^{\infty} a_{ijs} \pi_K^s \in \mathcal{O}_K$, como se quería. □

Corolario 1.39. *Sea L/K una extensión finita de campos valuados discretos completos y supongamos que la extensión correspondiente de sus campos residuales $\overline{L}/K$ es separable. Sean π_L un elemento primo de L y $\alpha \in \mathcal{O}_L$ un representante de un elemento primitivo $\overline{\alpha}$ de $\overline{L}/K$, i.e., tal que $L = K(\overline{\alpha})$. Sean $e = e(L/K)$ y $f = f(L/K)$. Entonces:*

(1) *Los productos $\alpha^i \pi_L^j \in \mathcal{O}_L$, $0 \leq i < f$, $0 \leq j < e$, forman una base del $\mathcal{O}_K$-módulo $\mathcal{O}_L$.*

(2) *El elemento $\alpha \in \mathcal{O}_L$ se puede elegir de tal forma que existe un polinomio mónico $\psi(x) \in \mathcal{O}_K[x]$ de grado f tal que $\psi(\alpha)$ es un elemento primo de L.*

DEMOSTRACIÓN. (1): Directo de la proposición anterior ya que $L = K(\overline{\alpha})$ es de grado f sobre K y los f elementos $1, \overline{\alpha}, \ldots, \overline{\alpha}^{f-1}$ son una base de $\overline{L}/K$.

(2): Escojamos un $\alpha \in \mathcal{O}_L$ tal que $L = K(\overline{\alpha})$ y sea $\psi(x) \in \mathcal{O}_K[x]$ un polinomio mónico cuya reducción mod $\mathfrak{p}_K$ es el mónico irreducible de $\overline{\alpha}$, i.e., tal que $\overline{\psi}(x) = \mathrm{Irr}(\overline{\alpha}, K)$. Entonces, para la valuación v_L de L se tiene que $v_L(\psi(\alpha)) \geq 1$ ya que $\psi(\alpha) = \overline{\psi}(\overline{\alpha}) = 0$ en K, i.e., $\psi(\alpha) \in \mathfrak{p}_K$, i.e., $v_L(\psi(\alpha)) > 0$. Ahora,

si se diera la igualdad $v_L(\psi(\alpha)) = 1$, entonces $\psi(\alpha)$ sería un elemento primo de L y ya acabamos. Si sucediera que $v_L(\psi(\alpha)) \geq 2$, sea $\beta \in \mathcal{O}_L$ cualquier elemento primo, i.e., tal que $v_L(\beta) = 1$, y apliquemos la fórmula de Taylor:

$$\psi(\alpha + \beta) = \psi(\alpha) + \beta\psi'(\alpha) + \beta^2 b$$

con $b \in \mathcal{O}_L$. Observemos que como $\overline{L}/K$ es separable, entonces $\psi'(\overline{\alpha}) \neq 0$ y así $\psi'(\alpha) \in U_K$ y por lo tanto el término $\beta\psi'(\alpha)$ tiene valuación 1, y como los otros términos de $\psi(\alpha + \beta)$ tienen valuación ≥ 2, entonces

$$v_L(\psi(\alpha + \beta)) = \min\{v_L(\psi(\alpha)), v_L(\beta\psi'(\alpha)), v_L(\beta^2 b)\} = v_L(\psi(\alpha)) = 1$$

y consecuentemente $\alpha + \beta \in \mathcal{O}_L$ es el elemento que necesitamos, ya que $\alpha + \beta = \overline{\alpha}$ porque $\beta \in \mathfrak{p}_L$. □

El corolario siguiente tendrá varias aplicaciones importantes más adelante:

Corolario 1.40. *Sea L/K una extensión finita de campos valuados discretos completos de grado n y supongamos que L/K es separable. Entonces, $\mathcal{O}_L$ tiene una base sobre $\mathcal{O}_K$ de la forma $1, \alpha, \ldots, \alpha^{n-1}$, i.e., $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.*

DEMOSTRACIÓN. Sean $e = e(L/K)$, $f = f(L/K)$ y $n = ef = [L : K]$. Escojamos un $\alpha \in \mathcal{O}_L$ como en la parte (2) del corolario previo y sea $\pi_L = \psi(\alpha) \in \mathcal{O}_L$. Por la parte (1) del corolario anterior se tiene que los productos $\alpha^i \pi_L^j$, $0 \leq i < f$, $0 \leq j < e$, forman una base de $\mathcal{O}_L$ sobre $\mathcal{O}_K$ y como, por la parte (2) del corolario previo, $\pi_L = \psi(\alpha) = \alpha^f + a_{f-1}\alpha^{f-1} + \cdots + a_1\alpha + a_0$, con los $a_i \in \mathcal{O}_K$, entonces los $\alpha_i \pi_L^j$ son combinaciones lineales, con coeficientes en $\mathcal{O}_K$, de las potencias α^k, con $0 \leq k \leq n-1$, i.e., $1, \alpha, \cdots, \alpha^{n-1}$ generan $\mathcal{O}_L$ sobre $\mathcal{O}_K$ y por lo tanto forman una base ya que $ef = n$ y por la parte (1) del corolario previo. □

Extensión de valuaciones normalizadas. Si L/K es una extensión finita de campos con K un campo valuado discreto completo y además v_K es normalizada, por (1.26) v_K se puede extender a L de tal forma que L, v_L es completo y por (1.28) v_L es discreta; sin embargo, v_L no necesariamente es normalizada. Sea pues v_L' la normalización de v_L; entonces $v_L' \sim v_L$ y por lo tanto existe un número real $a > 0$ tal que $v_L' = av_L$ y como v_L es discreta, entonces v_L' también lo es. Observemos ahora que como $v_L|_K = v_K$, entonces $v_L'|_K = av_K$ y por lo tanto

$$v_L'|_K(K^*) = av_K(K^*) = a\mathbb{Z},$$

la última igualdad porque v_K es normalizada. Se sigue que

$$e = e(L/K) := [v'_L(L^*) : v'_L|_K(K^*)] = [\mathbb{Z} : a\mathbb{Z}] = a,$$

la penúltima igualdad porque v'_L es normalizada. Se sigue que $a = e$ y por lo tanto $v'_L = e \cdot v_L$ y $v'_L|_K = e \cdot v_K$. Entonces, para todo $\alpha \in L$ se tiene que

$$\begin{aligned} v'_L(\alpha) &= e \cdot v_L(\alpha) \\ &= e \cdot \frac{1}{n} v_K(N_{L/K}\alpha) \quad \text{por (1.26)} \\ &= \frac{e}{ef} v_K(N_{L/K}\alpha) \quad \text{por (1.35)} \\ &= \frac{1}{f} v_K(N_{L/K}\alpha). \end{aligned}$$

Hemos así probado:

Proposición 1.41. *Si L/K es una extensión finita y K, v_K es un campo valuado discreto completo con v_K normalizada, entonces v_K se extiende a una valuación discreta normalizada v_L en L tal que L, v_L es completo y de hecho v_L está dada por*

$$v_L(\alpha) = \frac{1}{f} v_K(N_{L/K}\alpha),$$

donde $f = f(L/K)$ es el grado residual de L/K.

□

1.5.1 Extensiones no ramificadas

En esta sección clasificamos y obtenemos varias propiedades importantes de las extensiones L/K no ramificadas en términos del discriminante

$$D(\alpha_1, \ldots, \alpha_n) := \det[\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)]_{n\times n} \in K$$

de una base $\alpha_1, \ldots, \alpha_n$ de L/K (véase el Anexo 2), donde, para el caso de campos valuados discretos completos, toma la forma siguiente: por la proposición (1.38) el anillo $\mathcal{O}_L$ tiene una $\mathcal{O}_K$-base, digamos $\alpha_1, \ldots, \alpha_n$. Supongamos que $\beta_1, \ldots, \beta_n$ es otra tal base; entonces, la matriz $A = (a_{ij})$ de cambio de base tiene ahora entradas $a_{ij} \in \mathcal{O}_K$ y por lo tanto su determinante $\det(A) \in \mathcal{O}_K$ también. Es claro que A^{-1} también tiene coeficientes en $\mathcal{O}_K$ y por lo tanto también $\det(A^{-1}) \in \mathcal{O}_K$ y consecuentemente $\det(A)$ es una unidad de $\mathcal{O}_K$. De la proposición (1.99) en el Anexo 2 se sigue que:

Lema 1.42. *Sea L/K una extensión finita separable de campos valuados discretos completos. Sea $n = [L : K]$. Entonces, para cualquier $\mathcal{O}_K$-base $\alpha_1, \ldots, \alpha_n$ de $\mathcal{O}_L$ se tiene que:*

(1) $D(\alpha_1, \ldots, \alpha_n) \neq 0$.

(2) *Sus clases laterales $D(\alpha_1, \ldots, \alpha_n) \in \mathcal{O}_K^*/(\mathcal{O}_K^*)^2$ son iguales en el grupo cociente y por lo tanto sus valuaciones $|D(\alpha_1, \ldots, \alpha_n)|_v$ son iguales.*

□

Definición 1.43. Sea L/K una extensión finita separable de campos valuados discretos completos. Sea $n = [L : K]$. A la clase lateral en $\mathcal{O}_K/(\mathcal{O}_K^*)^2$ del discriminante de cualquier $\mathcal{O}_K$-base de $\mathcal{O}_L$ se le llama el *discriminante* de L/K y se denota por $\Delta_{L/K}$.

Regresando ahora al caso de una extensión finita no ramificada de campos valuados discretos completos L/K, recordemos, para comenzar, que por (1.36)(3), un elemento primo π_K de K también es un elemento primo de L.

Teorema 1.44. *Sea L/K una extensión finita de campos valuados discretos completos de grado $n = [L : K]$. Supongamos que L/K y L/K son extensiones separables. Entonces, L/K es no ramificada si y sólo si $|\Delta_{L/K}|_K = 1$.*

DEMOSTRACIÓN. Supongamos que $|\Delta_{L/K}|_K = 1$ y que L/K es ramificada, i.e., $e = e(L/K) > 1$; entonces se tiene una base $\{\alpha_i \pi_L^j\}$, $1 \leq i \leq f < n$, $0 \leq j \leq e-1 \leq n$, de $\mathcal{O}_L$ sobre $\mathcal{O}_K$. Sea N/K una extensión finita normal que contiene a L. Sean $\sigma_k : L \rightarrowtail N$ las n K-inmersiones correspondientes; así, como L/K es separable recordamos que $L = K(\gamma)$ y los σ_i están dados mandando γ a γ_i (las n raíces distintas en N del polinomio $\mathrm{Irr}(\gamma, K)$). Observamos que para todo $a \in N$ se tiene que $|\sigma_k(a)|_N = |a|_N$, ya que $\sigma_k(a)$ y a son raíces del mismo mónico irreducible $\mathrm{Irr}(a, K)$ y por lo tanto tienen la misma norma por §1.10 y consecuentemente la misma valuación por (1.27). En particular, para $\alpha_i \pi_L^j \in L \subseteq N$ se tiene que

$$|\sigma_k(\alpha_i \pi_L^j)|_N = |\alpha_i \pi_L^j|_N = |\alpha_i|_N |\pi_L|_N^j = |\pi_L|_N^j,$$

la última igualdad ya que $|\alpha_i|_N = |\alpha_i|_L = 1$ porque $\alpha_i \in \mathcal{O}_L - \mathfrak{p}_L = U_L$ (sus clases laterales forman una base de los campos residuales). Ahora, como $e - 1 > 0$ existe un $j_0 > 0$ y para este índice se tiene que

$$|\sigma_k(\alpha_i \pi_L^{j_0})|_N = |\pi_L|_N^{j_0} < 1,$$

y así, fijando a este j_0 en la columna de la matriz $[\sigma_k(\alpha_i \pi_L^j)]$ que define al discriminante de L/K se tiene que cada entrada en esta columna tiene valuación < 1, y como claramente todas las entradas de la matriz tienen valuación (valor absoluto) ≤ 1 (la igualdad se da para $j = 0$), entonces

$$|\Delta_{L/K}|_K := |D(\alpha_i \pi_L^j)|_K = |\det(\sigma_k(\alpha_i \pi_L^j))|_K^2 < 1,$$

lo cual contradice la hipótesis.

Recíprocamente, supongamos que L/K es no ramificada. Entonces $f = n$ y así sean $\alpha_1, \ldots, \alpha_n$ en $\mathcal{O}_L$ representantes de una base de $\overline{L}/K$ y también son una base de L/K. Ahora, como ambas extensiones son separables, entonces podemos calcular los discriminantes de ambas bases y usando el hecho de que para todo $a \in \mathcal{O}_L$ se tiene que

$$\overline{\mathrm{Tr}_{L/K}(a)} = \mathrm{Tr}_{\overline{L}/\overline{K}}(\overline{a}),$$

lo cual probaremos en el lema siguiente, obtenemos

$$\begin{aligned} D_{L/K}(\alpha_1, \ldots, \alpha_n) \quad & \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right) \\ - \quad & \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right) \\ & \det\left(\mathrm{Tr}_{\overline{L}/\overline{K}}(\alpha_i \alpha_j)\right) \qquad \text{por } (*) \\ & D_{\overline{L}/\overline{K}}(\alpha_1, \ldots, \alpha_n) \\ \neq \quad & 0 \qquad \text{por (1.42);} \end{aligned}$$

aquí observamos que $D_{L/K}(\alpha_1, \ldots, \alpha_n) \in \mathcal{O}_L$ ya que los $\alpha_i \in \mathcal{O}_L$ y como hemos mostrado que su reducción módulo $\mathfrak{p}_L$ es $\neq 0$, entonces $D_{L/K}(\alpha_1, \ldots, \alpha_n) \in U_L$ y por lo tanto su valuación (valor absoluto) es 1 como se quería probar. □

Resta probar la afirmación $(*)$. Recordando de §1.10 que la traza de un elemento a es uno de los coeficientes del polinomio característico de a, esta afirmación es consecuencia del lema siguiente:

Lema 1.45. *Si L/K es no ramificada, entonces para todo $a \in \mathcal{O}_L$ el polinomio característico de $\overline{a} \in L$ se obtiene del polinomio característico de a reduciendo sus coeficientes módulo $\mathfrak{p}_L$.*

DEMOSTRACIÓN. Como L/K es no ramificada de grado n, entonces $f = n$ y así con la notación anterior tenemos una base $\alpha_1, \ldots, \alpha_n$ de $\mathcal{O}_L$ sobre $\mathcal{O}_K$ que es base de L/K y cuyas reducciones módulo $\mathfrak{p}_L$ son base de la extensión de campos residuales. Entonces, para $a \in \mathcal{O}_L$ considerando la transformación K-lineal $a : L \to L$ y usando la base α_i, el polinomio característico de a es

$$f(t) := \det(ta - I_n)$$

donde I_n es la matriz identidad $n \times n$. Recordamos también que la matriz asociada a la transformación a se obtiene al calcular

$$a\alpha_i = \sum_j a_{ij}\alpha_j \tag{1}$$

con los $a_{ij} \in K$ en general, pero como en nuestro caso $a \in \mathcal{O}_L$ entonces los $a_{ij} \in \mathcal{O}_K$. Se sigue que

$$f(t) = \det(t(a_{ij}) - I_n) \qquad \text{con } a_{ij} \in \mathcal{O}_K. \tag{2}$$

Similarmente, para el elemento $\bar{a} \in \overline{L}$ su matriz asociada se obtiene al reducir mod $\mathfrak{p}_L$ la igualdad (1) y así su polinomio característico es

$$\det(t(a_{ij}) - I_n),$$

el cual es precisamente la reducción mod $\mathfrak{p}_L$ de (2). □

A continuación obtenemos algunas propiedades de las extensiones no ramificadas.

Lema 1.46. *Sea L/K una extensión finita de campos valuados discretos completos.*

(1) *Si $\alpha \in \mathcal{O}_L$ y $f(x) = \mathrm{Irr}(\alpha, K)$ es el mónico irreducible de α sobre K, entonces $f(x) \in \mathcal{O}_K[x]$.*

(2) *Recíprocamente, si $f(x) \in \mathcal{O}_K[x]$ es mónico y $\alpha \in L$ es una de sus raíces, entonces $\alpha \in \mathcal{O}_L$.*

DEMOSTRACIÓN. Sea $p = \mathrm{car}\,(K)$. Si $p = 0$, entonces $\alpha \in L$ es separable sobre K. Si $p > 0$, existe un entero $m \geq 0$ tal que $\alpha^{p^m} \in L$ es separable sobre K (véase, por ejemplo, Lang [26], (6.1), p. 247). En cualquier caso existe un entero $m \geq 0$ tal que $\beta = \alpha^{p^m} \in L$ es separable sobre K. Sea M cualquier campo intermedio de L/K tal que $\beta \in M$ y tal que M/K es Galois. Como

$\alpha \in \mathcal{O}_L$, entonces $\beta \in \mathcal{O}_L$ y así $\beta \in \mathcal{O}_L \cap M = \mathcal{O}_M$. Sea $g(x) = \mathrm{Irr}(\beta, K)$. Entonces

$$g(x) = \prod_{i=1}^{r}(x - \sigma_i(\beta))$$

con $\sigma_i \in \mathrm{Gal}(M/K)$ y $\sigma_1 = id$. Como $\beta \in \mathcal{O}_M$, entonces $\sigma_i(\beta) \in \mathcal{O}_M$ y así $g(x) \in \mathcal{O}_M[x]$. También, como $\beta = \alpha^{p^m}$ y $f(x) = \mathrm{Irr}(\alpha, K)$ entonces $f(x) = g(x^{p^m}) \in \mathcal{O}_M[x] \cap K = \mathcal{O}_K[x]$, lo cual prueba (1).

Recíprocamente, si $\alpha \in L$ es una raíz de un mónico

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathcal{O}_K[x]$$

y si sucediera que $\alpha \notin \mathcal{O}_L$, entonces $\alpha^{-1} \in \mathcal{O}_L$ (de hecho en $\mathfrak{p}_L$) y substituyendo α en $f(x)$ se obtiene

$$0 = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$$

con los $a_i \in \mathcal{O}_K$. Y como $\alpha^{-1} \in \mathcal{O}_L$ entonces $\alpha^{-n} \in \mathcal{O}_L$ y así, multiplicando por α^{-n} la igualdad anterior, se obtiene

$$0 = 1 + a_{n-1}\alpha^{-1} + \cdots + a_1\alpha^{-n+1} + a_0\alpha^{-n}$$

con los $a_i \in \mathcal{O}_K \subseteq \mathcal{O}_L$ y los $\alpha^{-j} \in \mathfrak{p}_L$ para $j \geq 1$. Se sigue que

$$1 = -a_{n-1}\alpha^{-1} - \cdots - a_0\alpha^{-n} \in \mathfrak{p}_L,$$

lo cual es una contradicción. Se sigue que $\alpha \in \mathcal{O}_L$. □

Proposición 1.47. *Sea L/K una extensión finita de campos valuados discretos completos tal que la extensión de campos residuales $\overline{L}/K$ es separable.*

(1) *Si L/K es no ramificada y $\overline{L} = K(\theta)$ para algún $\theta \in \overline{L}$, sea $\alpha \in \mathcal{O}_L$ tal que $\overline{\alpha} = \theta$. Entonces $L = K(\alpha)$ y L/K es separable. Más aún, $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ y si $f(x) = \mathrm{Irr}(\alpha, K)$, entonces θ es una raíz simple del polinomio $\overline{f}(x)$ que es irreducible sobre K.*

(2) *Sea $f(x) \in \mathcal{O}_K[x]$ un polinomio mónico tal que su reducción $\overline{f}(x)$ es un polinomio mónico separable sobre K. Sea $\alpha \in K^{al}$ una raíz de $f(x)$ y sea $L = K(\alpha)$. Entonces L/K es no ramificada y $L = K(\overline{\alpha})$.*

Demostración. (1): Por el lema anterior $f(x) \in \mathcal{O}_K[x]$. Claramente $\mathrm{gr}(f) = \mathrm{gr}(\overline{f})$ y como $f(\alpha) = 0$, entonces $\overline{f}(\overline{\alpha}) = 0$. Más aún,

$$[L : K] \geq [K(\alpha) : K] = \mathrm{gr}(f) = \mathrm{gr}(\overline{f}) \geq [K(\theta) : K] = [\overline{L} : K] = [L : K]$$

y por lo tanto todas las desigualdades son igualdades, en particular $[K(\alpha) : K] = [L : K]$ y como $K(\alpha) \subseteq L$, entonces $L = K(\alpha)$. También, $\mathrm{gr}(\overline{f}) = [K(\theta) : K]$ y consecuentemente θ es una raíz simple del polinomio irreducible $\overline{f}(x)$. Se sigue que su derivada $\overline{f}'(\theta) \neq 0$ y por lo tanto también $f'(\alpha) \neq 0$, i.e., α es separable sobre K y así $L = K(\alpha)$ es separable sobre K. Finalmente, como L/K es no ramificada, $e = e(L/K) = 1$ y así, por la proposición (1.38), $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

(2): Sea

$$f(x) = \prod_{i=1}^{n} f_i(x)$$

la descomposición de $f(x)$ en irreducibles mónicos en $K[x]$. Por el lema de Gauss, $f_i(x) \in \mathcal{O}_K[x]$. Ahora, supongamos que $\alpha \in K^{al}$ es una raíz de $f_1(x)$; entonces $f_1(x)$ es un polinomio mónico separable sobre K y por el lema de Hensel para K, $f_1(x)$ es irreducible sobre K. Se sigue que $\alpha \in \mathcal{O}_L$ por el lema anterior. Y como $\theta = \overline{\alpha} \in \overline{L}$, entonces $\overline{L} \supseteq K(\theta)$ y

$$\mathrm{gr}(f_1) = [L : K] \geq [\overline{L} : K] \geq [K(\theta) : K] = \mathrm{gr}(f_1) = \mathrm{gr}(f_1)$$

y así todas las desigualdades son igualdades y por lo tanto $L = K(\theta)$ y también $[L : K] = [\overline{L} : K]$, i.e., L/K es no ramificada. □

El resultado siguiente estudia el comportamiento de la no ramificación con respecto a torres de campos:

Corolario 1.48. *Sea L/K una extensión finita de campos valuados discretos completos y supongamos que la extensión de campos residuales es separable. Entonces:*

(1) *Si $L \supseteq F \supseteq K$, entonces L/K es no ramificada si y sólo si L/F y F/K son no ramificadas.*

(2) *Si L/K es no ramificada y M/K es finita, entonces LM/M es no ramificada.*

(3) *Si L_1/K y L_2/K son finitas no ramificadas, entonces L_1L_2/K es no ramificada.*

DEMOSTRACIÓN. (1) se sigue de $e(L/K) = e(L/F)e(F/K)$. Para (2) observemos que por la proposición anterior L/K es separable y de hecho, como $L = K(\overline{\theta})$, existe $\alpha \in \mathcal{O}_L$ tal que $\overline{\alpha} = \overline{\theta}$ y $L = K(\alpha)$.

Ahora, la extensión LM/M también es simple; de hecho $LM = M(\alpha)$ y notemos que $\alpha \in \mathcal{O}_{LM}$ ya que $\alpha \in \mathcal{O}_L \subseteq \mathcal{O}_{LM}$.

Sea $\phi = \mathrm{Irr}(\alpha, M)$ y sea $\overline{\phi}$ su reducción mod $\mathfrak{p}_M$. Entonces $\overline{\phi}$ no tiene raíces múltiples por el lema de Hensel y por el lema (1.46) $\overline{\phi}$ es irreducible (y mónico). Y como $\overline{\phi}(\overline{\alpha}) = 0$, entonces $\overline{\phi} = \mathrm{Irr}(\overline{\alpha}, M)$. También, como $\mathrm{gr}(\overline{\phi}) = \mathrm{gr}(\phi)$ entonces en la desigualdad

$$\mathrm{gr}(\overline{\phi}) = [M(\overline{\alpha}) : M] \leq [LM : M] \leq [LM : M] = [M(\alpha) : M] = \mathrm{gr}(\phi),$$

como los extremos son iguales, entonces todos los grados de las extensiones involucradas son iguales, en particular

$$[LM : M] = [LM : M],$$

y por lo tanto LM/M es no ramificada.

La parte (3) se sigue de (1) y (2). □

En el caso cuando la extensión L/K es no ramificada y Galois, veremos a continuación que su grupo de Galois es isomorfo al grupo de Galois de L/K:

Teorema 1.49. *Sea L/K una extensión finita no ramificada de campos valuados discretos y sea $\overline{L}/K$ la extensión correspondiente de sus campos residuales a la cual supondremos separable. Entonces, L/K es Galois si y sólo si L/K lo es. Más aún, se tiene un isomorfismo*

$$\phi : \mathrm{Gal}(L/K) \xrightarrow{\simeq} \mathrm{Gal}(L/K)$$

dado por: $\sigma \mapsto \overline{\sigma}$, donde $\overline{\sigma}(\overline{\alpha}) := \sigma(\alpha)$ para $\alpha \in \mathcal{O}_L$ un representante de $\overline{\alpha} \in L$.

Demostración. Supongamos que $\overline{L}/K$ es Galois. Como $\overline{L}/K$ es separable, entonces $\overline{L} = K(\overline{\theta})$ para algún $\overline{\theta} \in \overline{L}$ por el teorema del elemento primitivo. Sea $f(x) = \mathrm{Irr}(\overline{\theta}, K)$ el mónico irreducible de $\overline{\theta}$. Como L/K es normal, entonces $f(x)$ se descompone en $\overline{L}$:

$$f(x) = \prod_{i=1}^{n} (x - \overline{\theta}_i)$$

con $\overline{\theta}_i \in \overline{L}$ y, digamos, $\overline{\theta}_1 = \overline{\theta}$. Sea $g(x) \in \mathcal{O}_K[x]$ un polinomio mónico del mismo grado que f y tal que su reducción mod $\mathfrak{p}_K$ es $f(x)$. Por el lema de

Hensel,

$$g(x) = \prod_{i=1}^{n}(x - \alpha_i),$$

donde los $\alpha_i \in \mathcal{O}_L$ son representantes de $\overline{\theta}_i \in \overline{L}$.

Por la proposición anterior, $L = K(\alpha_1)$ y es separable sobre K. Además, L es campo de descomposición del polinomio separable $g(x)$ y así L/K es Galois, como se quería.

Supongamos ahora que L/K es Galois. De nuevo, como $\overline{L}/K$ es separable por hipótesis, existe $\overline{\theta} \in \overline{L}$ tal que $L = K(\overline{\theta})$. Sea $\alpha \in \mathcal{O}_L$ tal que $\overline{\alpha} = \overline{\theta}$ y sea $f(x) = \mathrm{Irr}(\alpha, K)$. Por el lema (1.46) se tiene que $f(x) \in \mathcal{O}_K[x]$ y por la proposición anterior $L = K(\alpha)$ y $\overline{f}(x) = \mathrm{Irr}(\overline{\theta}, K)$. Ahora, como L/K es Galois, entonces $f(x)$ se descompone en L y por el lema (1.46) todas estas raíces están en $\mathcal{O}_L$ y por lo tanto todas las raíces de $\overline{f}$ están en $L = K(\overline{\theta})$ y consecuentemente, L/K es Galois.

Finalmente, notemos que si $\sigma \in \mathrm{Gal}(L/K)$, la función $\overline{\sigma} : L \to L$ está bien definida ya que si $\beta \in \mathcal{O}_L$ es tal que $\overline{\beta} = \overline{\alpha}$, entonces $\alpha - \beta \in \mathfrak{p}_L$ y así, para todo $\sigma \in \mathrm{Gal}(L/K)$ se tiene que $\sigma(\alpha - \beta) \in \mathfrak{p}_L$, i.e., $\sigma(\alpha) = \sigma(\beta)$. Claramente la función $\phi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(\overline{L}/K)$ dada por $\sigma \mapsto \overline{\sigma}$ es un homomorfismo de grupos y es suprayectivo, ya que como $\overline{L} = K(\overline{\theta})$ y $L = K(\alpha)$ con $\alpha \in \mathcal{O}_L$ tal que $\overline{\alpha} = \overline{\theta}$, entonces los automorfismos de $\mathrm{Gal}(\overline{L}/K)$ están determinados por la igualdad $\overline{\sigma}\overline{\theta} = \overline{\theta}_i$ con $\overline{\theta}_i$ una raíz de $\overline{f}(x)$. Entonces, si $\overline{\sigma} \in \mathrm{Gal}(\overline{L}/K)$ es tal que $\sigma(\overline{\theta}) = \overline{\theta}_i$, sean α, $\alpha_i \in \mathcal{O}_L$ tales que $\overline{\alpha} = \overline{\theta}$ y $\overline{\alpha}_i = \overline{\theta}_i$; el automorfismo $\sigma \in \mathrm{Gal}(L/K)$ dado por $\sigma(\alpha) = \alpha_i$ es tal que $\phi(\sigma) = \overline{\sigma}$. Finalmente, como

$$|\mathrm{Gal}(L/K)| = [L : K] = \mathrm{gr}(f(x)) = \mathrm{gr}(\overline{f}(x)) = [\overline{L}/K] = \left|\mathrm{Gal}(\overline{L}/K)\right|,$$

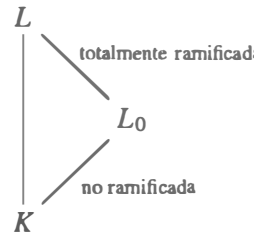
entonces ϕ es un isomorfismo ya que es suprayectivo y ambos grupos finitos tienen el mismo orden. □

Corolario 1.50. *Sea L/K una extensión finita de campos valuados discretos completos tal que la extensión de campos residuales $\overline{L}/K$ es separable. Entonces:*

(1) *Para cada $\overline{\alpha} \in \overline{L}$ existe un $a \in \overline{\alpha}$ tal que $K(a)/K$ es no ramificada, i.e., $[K(a) : K] = [K(\overline{\alpha}) : K]$. Más aún, el campo $K(a)$ depende sólo de $\overline{\alpha}$.*

(2) *Existe una biyección entre las subextensiones $L \supseteq M \supseteq K$ tales que M/K es no ramificada y los campos intermedios de L/K.*

(3) *Existe un campo intermedio L_0 de L/K tal que L_0/K es no ramificada y tal que para todo campo intermedio M de L/K con M/K no ramificada, se tiene que $M \subseteq L_0$. Más aún, L/L_0 es totalmente ramificada y el campo residual es $\overline{L}_0 = \overline{L}$:*



Así, L_0 es la máxima extensión no ramificada de K contenida en L.

(4) *Si L/K es normal y L_0 es como arriba, entonces L_0/K es normal y es el campo fijo del grupo*

$$G_0 := \{\sigma \in \mathrm{Gal}(L/K) \ : \ v_L(\sigma x - x) > 0 \quad \text{para todo} \quad x \in \mathcal{O}_L\}.$$

El subgrupo $G_0 \subseteq \mathrm{Gal}(L/K)$ se llama el *grupo de inercia* de la extensión L/K y el campo intermedio L_0 se llama el *campo de inercia* correspondiente. Nótese que

$$\mathrm{Gal}(L/L_0) \simeq G_0.$$

DEMOSTRACIÓN. (1): Sea $\overline{\phi}(x) = \mathrm{Irr}(\overline{\alpha}, K) \in K[x]$ el mónico irreducible de $\overline{\alpha}$ y sea $\Phi(x) \in \mathcal{O}_K[x]$ cualquier levantamiento de $\overline{\phi}(x)$. Por la proposición (1.49)(2) anterior existe $a \in \overline{\alpha}$ tal que satisface la primera parte de (1); para la segunda parte, si $b \in \overline{\alpha}$ es cualquier otro representante, entonces $|\Phi(b)|_L < 1$ y $|\Phi'(b)|_L = 1$ (esta última igualdad porque $\phi'(\overline{\alpha}) \neq 0$ por la separabilidad de $\overline{\alpha} \in L$). Entonces, aplicando el lema de Hensel usando como campo base a $K(b)$, existe un elemento $c \in K(b) \subseteq L$ tal que $\Phi(c) = 0$ y $|c - b|_L < 1$. Se sigue que $c \in \overline{\alpha}$ y además

$$[K(c) : K] = [K(\overline{\alpha}) : K].$$

Entonces, como $c \in K(b)$ implica que $K(c) \subseteq K(b)$, la igualdad

$$[K(c) : K] = [K(\overline{\alpha}) : K] = [K(b) : K]$$

implica que $K(b) = K(c)$.

(2): Como L/K es separable, toda subextensión M' lo es también y así, por el teorema del elemento primitivo, es de la forma $M' = K(\theta)$ para algún $\theta \in \overline{L}$.

Por la parte (1) existe un representante $a \in \theta$ tal que $K(a)/K$ es no ramificada y $[K(a) : K] = [K(\theta) : K]$ y el campo $K(a)$ sólo depende de la clase θ.

(3): En el inciso anterior pongamos $M' = \overline{L}$.

(4): Para todo $\sigma \in \mathrm{Gal}(L/K)$ la extensión $\sigma(L_0)/K$ es no ramificada, ya que para todo $a \in L$ se tiene que $|\sigma(a)|_L = |a|_L$. Se sigue que $\sigma(L_0) = L_0$, i.e., L_0/K es una extensión normal. Por el teorema anterior

$$\mathrm{Gal}(L_0/K) \simeq \mathrm{Gal}(L_0/K),$$

donde por el inciso (3) se tiene que $\overline{L}_0 = L$.

Notemos ahora que $\sigma \in G_0$ si y sólo si σ induce la identidad en el campo residual $L_0 = L$ y por lo tanto

$$\mathrm{Gal}(L_0/K) \simeq \mathrm{Gal}(L/K)/G_0 \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_0)$$

consecuentemente $\mathrm{Gal}(L/L_0) \simeq G_0$, i.e., $L_0 = L^{G_0}$ es el campo fijo de G_0. □

Observemos ahora que la parte (3) del corolario (1.48) nos dice que la composición de cualesquiera dos subextensiones finitas no ramificadas de K contenidas en un cerradura algebraica fija K^{al} de K también es no ramificada. Denotemos por K_{nr} a la composición de todas las subextensiones finitas no ramificadas de K contenidas en K^{al} y notemos que por la observación después de (1.28), la valuación de K se extiende a K_{nr} pero en general este campo no es completo. Diremos que K_{nr} es la *máxima extensión no ramificada* de K. Su maximalidad implica que para toda $\sigma \in \mathrm{Gal}(K_{sep}/K)$, donde K_{sep} es una cerradura separable de K, se tiene que $\sigma K_{nr} = K_{nr}$ y por lo tanto la extensión K_{nr}/K es Galois. Cuando una extensión algebraica L/K es la unión de subextensiones finitas no ramificadas, diremos que la extensión es no ramificada. Con este lenguaje, K_{nr}/K es no ramificada y tiene sentido el nombre de máxima extensión no ramificada de K. Nótese que el corolario (1.48) se extiende a extensiones algebraicas no ramificadas.

Corolario 1.51. *Sea K un campo valuado discreto y sea K_{nr} la máxima extensión no ramificada de K en una cerradura algebraica K^{al} de K. Entonces, el campo residual de K_{nr} es la cerradura separable del campo residual K de K y además*

$$\mathrm{Gal}(K_{nr}/K) \simeq \mathrm{Gal}(K_{sep}/K).$$

DEMOSTRACIÓN. Como $K_{nr} \subseteq \overline{K}^{sep}$, sólo necesitamos probar la otra inclusión. Sean $\bar{a} \in K^{sep}$ y $\overline{f}(x) = \mathrm{Irr}(\bar{a}, K)$. Sea $f(x) \in \mathcal{O}_K[x]$ un mónico tal que su reducción mod $\mathfrak{p}_K$ es $\overline{f}(x)$ como en la demostración del teorema previo. Sean α_i todas las raíces de $f(x)$ y pongamos $L = K(\{\alpha_i\})$. Por la proposición (1.47)(2) anterior, L/K es no ramificada y así $L \subseteq K_{nr}$ y $\bar{a} = \alpha_i$ para alguna α_i. Ahora, como $\alpha_i \in \mathcal{O}_L$ por el lema (1.46), entonces $\bar{a} = \alpha_i \in \overline{L} \subseteq K_{nr}$ (porque $L \subseteq K_{nr}$) y por lo tanto $\bar{a} \in \overline{K_{nr}}$, i.e., $\overline{K}^{sep} \subseteq \overline{K_{nr}}$. □

Proposición 1.52. *Sea L/K una extensión algebraica de campos valuados discretos completos. Entonces:*

(1) $L_{nr} = LK_{nr}$.

(2) $L_0 := L \cap K_{nr}$ *es la máxima extensión no ramificada de K contenida en L.*

(3) *Si $\overline{L}/K$ es separable, entonces L/L_0 y L_{nr}/K_{nr} son totalmente ramificadas y $[L : L_0] = [L_{nr} : K_{nr}]$.*

(4) $\mathrm{Gal}(L_{nr}/K_{nr}) \simeq \mathrm{Gal}(L/L_0)$ *y* $\mathrm{Gal}(L_{nr}/L) \simeq \mathrm{Gal}(K_{nr}/L_0)$.

DEMOSTRACIÓN. (1): Como $L \subseteq L_{nr}$ y $K_{nr} \subseteq L_{nr}$, entonces $LK_{nr} \subseteq L_{nr}$. Para la otra inclusión, como el campo residual LK_{nr} contiene a la composición $L\ K_{nr}$ y como $K_{nr} = K_{sep}$ y además $\overline{L}_{sep} = K_{sep}$ ya que L/K es separable, esto implica que $K_{nr} = K_{sep} = \overline{L}_{sep} = L_{nr}$, por lo que $\overline{LK_{nr}} \supseteq \overline{L}\ L_{sep} = L_{sep} = \overline{L}_{nr}$ y así $LK_{nr} \supseteq L_{nr}$, lo cual termina la demostración de (1).

(2): Primero, L_0/K es no ramificada ya que $L_0 \subseteq K_{nr}$. Ahora, si M/K es una subextensión no ramificada de L/K, entonces $M \subseteq K_{nr}$ y como $M \subseteq L$, entonces $M \subseteq L \cap K_{nr} = L_0$. Se sigue que L_0 es la máxima extensión no ramificada de K contenida en L.

(3): Sea L'/L una extensión finita no ramificada y sea $K' = L' \cap K_{nr}$. Entonces, K'/K es finita no ramificada. Ahora, por (1.50)(3) y la parte (2) de arriba, L/L_0 es totalmente ramificada y así $e(L/L_0) = [L : L_0]$.

Se tiene ahora que $e(L'/L_0) = e(L'/L)e(L/L_0) = e(L/L_0)$, ya que L'/L es no ramificada. Se sigue que

$$[L : L_0] = e(L/L_0) = e(L'/L_0) = e(L'/K')e(K'/L_0) = e(L'/K')$$

(la última igualdad porque L_0 es un campo intermedio de la extensión no ramificada K'/K y por lo tanto K'/L_0 es no ramificada por (1.48)(1)). Se

sigue que

$$[L : L_0] \leq [L' : K'].$$

Por otra parte, es claro que $[L : L_0] \geq [L' : K']$ y por lo tanto $[L : L_0] = [L' : K']$ y además

$$e(L'/K') = [L : L_0] = [L' : K'],$$

y consecuentemente $f(L'/K') = 1$, i.e., L'/K' es totalmente ramificada. Pasando al límite directo se sigue el resultado deseado.

(4): $\mathrm{Gal}(L_{nr}/K_{nr}) \simeq \mathrm{Gal}(LK_{nr}/K_{nr}) \simeq \mathrm{Gal}(L/L \cap K_{nr}) \simeq \mathrm{Gal}(L/L_0)$
y

$$\mathrm{Gal}(L_{nr}/L) \simeq \mathrm{Gal}(LK_{nr}/L) \simeq \mathrm{Gal}(K_{nr}/L \cap K_{nr}) \simeq \mathrm{Gal}(K_{nr}/L_0).$$

□

Corolario 1.53. *Sea L/K una extensión finita de Galois totalmente ramificada de campos valuados discretos completos. Entonces:*

(1) $L_{nr} = LK_{nr}$ *(composición de campos).*

(2) $L \cap K_{nr} = K$.

(3) L_{nr}/K_{nr} *es Galois totalmente ramificada con grupo de Galois*

$$\mathrm{Gal}(L_{nr}/K_{nr}) \simeq \mathrm{Gal}(L/K).$$

(4) *Similarmente:*

$$\mathrm{Gal}(L_{nr}/L) \simeq \mathrm{Gal}(K_{nr}/K).$$

DEMOSTRACIÓN. (1), (3) y (4) son directos de la proposición previa.

Para (2), por la proposición anterior $L \cap K_{nr} = L_0$ es la máxima extensión no ramificada de K contenida en L, pero como L/K es totalmente ramificada entonces se debe tener que $L_0 = K$. □

1.5.2 Extensiones totalmente ramificadas

En esta sección obtenemos una caracterización de las extensiones totalmente ramificadas de campos valuados discretos completos en términos de polinomios que satisfacen las condiciones del criterio de irreducibilidad de Eisenstein (1.20), a los cuales llamamos *polinomios de Eisenstein.*

Teorema 1.54. *Sea K un campo valuado discreto completo.*

(1) *Si $f(x) \in K[x]$ es un polinomio de Eisenstein de grado n y π es una raíz de $f(x)$, entonces $K(\pi)/K$ es una extensión totalmente ramificada de grado n, π es un elemento primo de $K(\pi)$ y $\mathcal{O}_{K(\pi)} = \mathcal{O}_K[\pi]$.*

(2) *Si L/K es una extensión finita totalmente ramificada de grado n, entonces $L = K(\pi)$ donde π es raíz de un polinomio de Eisenstein $f(x) \in K[x]$ de grado n y π es un elemento primo de L.*

DEMOSTRACIÓN. (1): Supongamos que $L = K(\pi)$ con π una raíz de un polinomio de Eisenstein $f(x) \in K[x]$ y sea $e = e(L/K)$. Entonces

$$0 = f(\pi) = a_0 + a_1\pi + \cdots + a_n\pi^n$$

y así $|-a_0|_v = |a_1\pi + \cdots + a_n\pi^n|_v$ con $|a_j|_v < 1$ para $j < n$, $|a_n|_v = 1$ y $|a_0|_v = |\pi|_v$. Claramente el polinomio

$$m(x) := \frac{1}{a_n} f(x) = \frac{a_0}{a_n} + \frac{a_1}{a_n}x + \cdots + x^n \in K[x]$$

es irreducible y mónico y además π es una de sus raíces. Como $L = K(\pi)$ se sigue que $N_{L/K}(\pi) = \pm a_0/a_n$ y por lo tanto

$$|\pi|_L := |N_{L/K}(\pi)|_K^{1/n} = |a_0/a_n|_K^{1/n} = |a_0|_K^{1/n}$$

ya que $|a_n|_K = 1$. Se sigue que

$$|\pi|_L^n = |a_0|_K = |\pi_K|_K \in v_K(K^*),$$

con π_K un elemento primo de K (por definición de polinomio de Eisenstein); y como por definición $e = e(L/K) = [v_L(L^*) : v_K(K^*)]$, entonces $|\pi|_L^e \in v_K(K^*)$, y así $|\pi|_L^e = |\pi_K|_K^m$ para algún $m \in \mathbb{Z}$. Pero como L y K son discretos, entonces $n = ef$ y así

$$|\pi_K|_K = |\pi|_L^n = |\pi|_L^{ef} = \left(|\pi|_L^e\right)^f = \left(|\pi_K|_K^m\right)^f = |\pi_K|_K^{mf}$$

y por lo tanto $mf = 1$, por lo que $f = 1$, i.e., L/K es totalmente ramificada. Más aún, como $m = 1$ entonces $|\pi|_L^e = |\pi_K|_K^m = |\pi_K|_K$ y por lo tanto π es un elemento primo de L.

(2): Supongamos ahora que $[L : K] = n$ y que L/K es totalmente ramificada, i.e., que $e = n$ y $f = 1$. Pongamos $\mathfrak{p}_L = \langle \pi_L \rangle$ y $\mathfrak{p}_K = \langle \pi_K \rangle$. Entonces, $\{1, \pi_L, \ldots, \pi_L^{n-1}\}$ es una base de $\mathcal{O}_L$ sobre $\mathcal{O}_K$ por (1.38) ya que $e = n$ y

$f = 1$. Se sigue que π_L^n se puede expresar como combinación lineal, sobre $\mathcal{O}_K$, de $1, \ldots, \pi_L^{n-1}$:

$$\pi_L^n + a_{n-1}\pi_L^{n-1} + \cdots + a_1\pi_L + a_0 = 0$$

con $a_j \in \mathcal{O}_K$ no todos cero. Obsérvese ahora que el polinomio

$$f(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathcal{O}_K[x]$$

es irreducible ya que si no lo fuera se tendría una relación como (*) con el exponente mayor $< n$, en contradicción con el hecho de que $1, \ldots, \pi_L^{n-1}$ es base. Obsérvese que $L = K(\pi_L)$ ya que $\{1, \pi_L, \ldots, \pi_L^{n-1}\}$ es base de L/K.

También, el polinomio $f(x)$ es de Eisenstein ya que el coeficiente de x^n es $a_n = 1$ y así $|a_n|_K = |1|_K = 1$; como $f(x) = \mathrm{Irr}(\pi_L, K)$ y $L = K(\pi_L)$ entonces $N_{L/K}(\pi_K) = \pm a_0$ y por lo tanto

$$|a_0|_K = |\pm a_0|_K = |N_{L/K}(\pi_L)|_K = |\pi_L|^n = |\pi_L|_K^e = |\pi_K|_K$$

(la penúltima igualdad porque $n = e$). Ahora, para $0 \leq j < n$ se tiene que $a_j \in \mathcal{O}_K$ y por lo tanto $|a_j|_K \leq 1$ y si sucediera que algún j_0 es tal que $|a_{j_0}|_K = 1$, escojamos el menor índice para el cual $|a_{j_0}|_K = 1$. Entonces, como $|\pi_K|_K = |\pi_L|_L^e = |\pi_L|_L^n$ (porque $e = n$) y por la minimalidad de j_0, se tiene que

$$|a_0 + a_1\pi_L + \cdots + a_{j_0-1}\pi_L^{j_0-1}|_L \leq |\pi|_K = |\pi_L|_K^n,$$

$$|a_{j_0}\pi_K^{j_0}|_L = |\pi_L|_L^{j_0}$$

y

$$|a_{j_0+1}\pi_L^{j_0+1} + \cdots + a_{n-1}\pi_L^{n-1}|_L \leq |\pi_L|_L^{j_0+1}.$$

Se sigue que

$$\begin{aligned} |\pi_L|_L^n &= |a_{n-1}\pi_L^{n-1} + \cdots + a_1\pi_L + a_0|_L \\ &= |(a_{n-1}\pi_L^{n-1} + \cdots + a_{j_0+1}\pi_L^{j_0+1}) + a_{j_0} + (a_{j_0-1}\pi_L^{j_0-1} + \cdots + a_0)|_L \\ &\leq |\pi_L|_L^{j_0}, \end{aligned}$$

i.e., $|\pi_L|^n \leq |\pi_L|_L^{j_0}$, lo cual es una contradicción ya que $j_0 < n$. □

Corolario 1.55. *Sea K un campo valuado discreto completo. Entonces, para todo entero $e \geq 1$ existe una extensión L/K totalmente ramificada de grado $e = [L : K]$.*

DEMOSTRACIÓN. Sea $\pi \in K$ un elemento primo y pongamos

$$E(x) := x^e - \pi x - \pi \in K[x];$$

entonces $E(x)$ es Eisenstein de grado e. □

1.5.3 Extensiones mansamente ramificadas

De las extensiones ramificadas hay una clase que es más manejable porque no hay ramificación superior (véase (1.79) en la sección §1.8). Se dice que estas extensiones tienen ramificación mansa: una extensión finita L/K de campos valuados completos es *mansamente ramificada* si L/K es separable y $p \nmid e(L/K)$ donde $p = \text{car}\,(K)$. Nótese que si L/K es no ramificada, entonces $e(L/K) = 1$ y por lo tanto es mansa. Si L/K es totalmente ramificada, entonces $e(L/K) = [L : K] = n$ y por lo tanto es mansa si $p \nmid n$. En este caso se dice que L/K es mansa totalmente ramificada.

Proposición 1.56. *Sea K un campo valuado discreto completo, con campo residual K perfecto de característica p.*

(1) *Si L/K es una extensión finita mansa y si L_0/K es la mayor subextensión de L tal que L_0/K es no ramificada, entonces $L = L_0(\pi_L)$ y $\mathcal{O}_L = \mathcal{O}_{L_0}[\pi_L]$, donde π_L es un primo de L que es raíz de la ecuación $x^e - \pi_0$ para algún primo π_0 de L_0 y $e = e(L/K)$.*

(2) *Recíprocamente, si L_0/K es finita no ramificada y $L = L_0(\beta)$ donde $\beta^e = b \in L_0$ y si $p \nmid e$ donde $p = \text{car}\,(K) > 0$, entonces L/K es separable y mansa.*

DEMOSTRACIÓN. (1): Sea π_1 un elemento primo de L_0. Entonces, por (1.34), $\pi_1 = \pi_L^e u$ para un elemento primo π_L de L y una unidad $u \in U_L$. Ahora, como L/L_0 es totalmente ramificada, entonces $L = L_0$ y así existe un $u_0 \in U_{L_0}$ tal que $\overline{u}_0 = \overline{u}$. Se sigue que $\pi_1 u_0^{-1} = \pi_L^e w$ con $w = u u_0^{-1} \in U_L$.

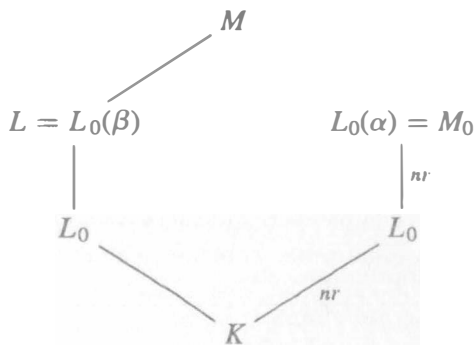
Ahora, para el polinomio $f(x) = x^e - w \in \mathfrak{o}_L[x]$ se tiene que $f(1) = 1 - w \in \mathfrak{p}_L$ y $f'(1) = e$. Por el lema de Hensel existe un elemento $\alpha \in \mathcal{O}_L$ tal que $\alpha^e = w$ y $\overline{\alpha} = 1$, por lo que α es una unidad de L. Por lo tanto, para el primo $\pi_0 := \pi_1 u_0^{-1} \in L_0$ y para el primo $\pi := \pi_L \alpha \in L$ se tiene que

$$\begin{aligned} \pi^e - \pi_0 \qquad & (\pi_L \alpha)^e - \pi_1 u_0^{-1} = \pi_L^e \alpha^e - \pi_L^e w \\ = \; & \pi_L^e w - \pi_L^e w = 0. \end{aligned}$$

Finalmente, como L/L_0 es totalmente ramificada y como el polinomio $x^e - \pi_0 \in L_0[x]$ es de Eisenstein, entonces por (1.54) $L = L_0(\pi)$ y $\mathcal{O}_L = \mathcal{O}_{L_0}[\pi]$.

(2): Como L_0/K es finita no ramificada y $L = L_0(\beta)$ con β una raíz del polinomio $x^e - b \in L_0[x]$, escribamos $b = \pi_1^a u$ con $a \in \mathbb{Z}$, π_1 un primo de L_0 y $u \in U_{L_0}$. El polinomio $g(x) = x^e - \overline{u}$ es separable en $\overline{L}_0[x]$ ya que $p \nmid e$. Nótese que para el polinomio $f(x) = x^e - u \in \mathcal{O}_{L_0}[x]$ su reducción $\overline{f}(x) = g(x)$ y así, por (1.47), si $\alpha \in K^{sep}$ es una raíz de $f(x)$, entonces $L_0(\alpha)/L_0$ es no ramificada y $L_0(\alpha) = L_0(\overline{\alpha})$.

Ahora, sean $M \quad L(\alpha) = L_0(\alpha, \beta)$ y $M_0 = L_0(\alpha)$. Entonces, en el diagrama



se tiene que

$$e(M/K) = e(M/M_0)e(M_0/L_0)e(L_0/K) = e(M/M_0)$$

ya que L_0/K es no ramificada por hipótesis y M_0/L_0 es no ramificada, como vimos anteriormente. Entonces, para probar que L/K es mansa basta probar que M/M_0 lo es, ya que si $p \nmid e(M/M_0) = e(M/K)$, entonces $p \nmid e(L/K)$ porque $e(L/K)|e(M/K)$.

Para probar que M/M_0 es mansa, observemos que

$$M = L(\alpha) = L_0(\alpha, \beta) = L_0(\alpha)(\beta\alpha^{-1}) = M_0(\beta_1),$$

con $\beta_1 := \beta\alpha^{-1}$. Notamos también que

$$\beta_1^e = \beta^e \alpha^{-e} = bu^{-1} = \pi_1^a u u^{-1} = \pi_1^a,$$

ya que $\beta^e = b = \pi_1^a u$ y $\alpha^e = u$.

Sea $d = \text{mcd}(e, a)$. Entonces

$$M = M_0(\beta_1) \subseteq M_0(\alpha_2, \zeta),$$

donde $\alpha_2^{e/d} = \pi_1^{a/d}$ y ζ es una raíz e-ésima primitiva de la unidad.

Con el mismo argumento que usamos para probar que $L_0(\alpha)/L_0$ es no ramificada, se prueba que $M_0(\zeta)/M_0$ es no ramificada, y como π_1 es primo de L_0, entonces π_1 también es primo de $L_0(\alpha) = M_0$ y por lo tanto también es primo de $M_0(\zeta)$ por (1.36)(3).

Sea v la valuación (discreta) de $M_0(\alpha_2, \zeta)$. Entonces

$$\left(\frac{a}{d}\right) v(\pi_1) = \left(\frac{e}{d}\right) v(\alpha_2) \in \left(\frac{e}{d}\right) \mathbb{Z}$$

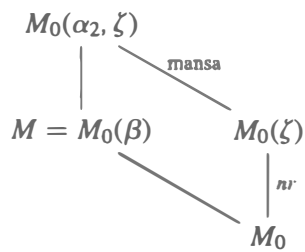
y como $\text{mcd}(a/d, e/d) = 1$, entonces $v(\pi_1) \in (e/d)\mathbb{Z}$. Se sigue que

$$e(M_0(\alpha_2, \zeta)/M_0(\zeta)) \geq e/d.$$

Sin embargo, como $\alpha_2^{e/d} = \pi_1^{a/d} \in M_0(\zeta)$ entonces $[M_0(\alpha_2, \zeta) : M_0(\zeta)] < e/d$. Se sigue entonces que

$$e(M_0(\alpha_2, \zeta)/M_0(\zeta)) = \frac{e}{d} = [M_0(\alpha_2, \zeta) : M_0(\zeta)]$$

y así $M_0(\alpha_2, \zeta)/M_0(\zeta)$ es totalmente ramificada y como $p \nmid e$, entonces $p \nmid (e/d)$ y así es mansa también. Finalmente, como se tiene el diagrama



entonces claramente $M_0(\alpha_2, \zeta)/M_0$ es mansa y por lo tanto M/M_0 también lo es. □

Ejemplo 16. Si K es un campo valuado discreto completo tal que su campo residual K es finito de característica $p > 0$, sean $n \geq 1$ un entero tal que $p \nmid n$ y μ_n el grupo de raíces n-ésimas de la unidad en una cerradura separable de K. Sea $L = K(\mu_n)$. Entonces L/K es mansamente ramificada. Esto se sigue de la parte (2) de la proposición anterior con $L_0 = K$ y $e = n$.

Corolario 1.57. *Sea K un campo valuado discreto completo, con campo residual K perfecto de característica p.*

(1) *Si L/K es mansa y totalmente ramificada y $[L : K] = e$, entonces L es de la forma $L = K(\alpha)$, donde α es una raíz de la ecuación $x^e - \pi_K = 0$, con π_K un primo de K.*

(2) *Más aún, L/K es Galois de grado $e = [L : K]$ si y sólo si K contiene a todas las raíces e-ésimas de la unidad.*

DEMOSTRACIÓN. La primera afirmación es directa de la parte (1) de la proposición anterior. La segunda afirmación se sigue de la primera. □

Corolario 1.58. *Sea K un campo valuado discreto completo, con campo residual perfecto de característica p.*

(1) *Si $L \supseteq M \supseteq K$ es una torre de extensiones finitas con L/M y M/K mansas, entonces L/K también lo es.*

(2) *Si L/K es mansa y M/K es finita, entonces LM/M es mansa.*

(3) *Si L_1/K y L_2/K son mansas, entonces L_1L_2/K es mansa.*

DEMOSTRACIÓN. Similar a la del corolario (1.48). □

1.6 Campos locales

Un *campo local* K es un campo valuado discreto completo con campo residual finito. En esta sección clasificamos los campos locales y probamos algunas de sus propiedades importantes. El nombre de campo local lo justifica la proposición siguiente, pero antes necesitamos un lema, válido en general para campos valuados discretos completos:

Lema 1.59. *Sea K, v un campo valuado discreto completo y sean $\mathcal{O}_K$ su anillo local y π_K un elemento primo. Entonces, el morfismo natural $f : \mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi_K^n\mathcal{O}_K$ dado por $\alpha \mapsto (\alpha \bmod \mathfrak{p}_K^n)$ induce un isomorfismo (y homeomorfismo):*

$$\mathcal{O}_K \simeq \varprojlim_n \mathcal{O}_K/\pi_K^n\mathcal{O}_K,$$

donde $\mathcal{O}_K/\pi_K^n\mathcal{O}_K$ tiene la topología discreta.

DEMOSTRACIÓN. Los morfismos naturales

$$\mathcal{O}_K/\mathfrak{p}_K \leftarrow \mathcal{O}_K/\mathfrak{p}_K^2 \leftarrow \mathcal{O}_K/\mathfrak{p}_K^3 \leftarrow \cdots$$

inducidos por las inclusiones $0 \subseteq \cdots \subseteq \mathfrak{p}_K^{n+1} \subseteq \mathfrak{p}_K^n \subseteq \cdots \subseteq \mathfrak{p}_K^2 \subseteq \mathfrak{p}_K \subseteq \mathcal{O}_K$ inducen el morfismo

$$f : \mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi_K^n \mathcal{O}_K,$$

el cual es inyectivo porque su núcleo es $\bigcap_{n=1}^{\infty} \mathfrak{p}_K^n = \{0\}$, la última igualdad por (1.15)(2).

Para probar que f es suprayectivo, sea $\mathcal{R} \subseteq \mathcal{O}_K$ un conjunto completo de representantes de $K = \mathcal{O}_K/\mathfrak{p}_K$ tal que $0 \in \mathcal{R}$. En la demostración de (1.16)(1) vimos que, para todo $\alpha \in \mathcal{O}_K$ y todo $n \geq 1$, las clases residuales α mód $\mathfrak{p}_K^n \in \mathcal{O}_K/\mathfrak{p}_K^n$ se pueden escribir, en forma única, como

$$\alpha \equiv a_0 + a_1\pi_K + \cdots + a_{n-1}\pi_K^{n-1} \text{ mód } \mathfrak{p}_K^n$$

con los $a_j \in \mathcal{R}$. Se sigue que cada elemento $\theta \in \varprojlim_n \mathcal{O}_K/\mathfrak{p}_K^n$ está dado por representantes (para cada $n \geq 1$): $\theta_n = a_0 + a_1\pi_K + \cdots + a_{n-1}\pi_K^{n-1}$ con coeficientes fijos $a_j \in \mathcal{R}$ y por lo tanto θ es la imagen, bajo f, del elemento

$$\vartheta := \lim_{n\to\infty} \theta_n = \sum_{j=0}^{\infty} a_j \pi_K^j \in \mathcal{O}_K.$$

Finalmente, que f es un homeomorfismo se demuestra como en (1.86)(1) ya que los conjuntos

$$V_n := \prod_{j>n} \mathcal{O}_K/\mathfrak{p}_K^j$$

forman una base de vecindades abiertas del 0 del producto directo $\prod_{j=1}^{\infty} \mathcal{O}_K/\mathfrak{p}_K^j$ y las intersecciones $V_n \cap \varprojlim_j \mathcal{O}_K/\mathfrak{p}_K^j$ forman una base de vecindades abiertas del 0 del límite $\varprojlim_j \mathcal{O}_K/\mathfrak{p}_K^j$, de tal forma que

$$f^{-1}(V_n \cap \varprojlim_j \mathcal{O}_K/\mathfrak{p}_K^j) = \mathfrak{p}_K^n,$$

donde los $\mathfrak{p}_K^n$ forman una base del 0 de $\mathcal{O}_K$ por (1.15)(3). □

Ejemplo 17. Si $K = \mathbb{Q}_p$ entonces $\mathcal{O}_K = \mathbb{Z}_p$, $\pi_K = p$ y como, por el ejemplo 7 después de (1.12), $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$, entonces

$$\mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Proposición 1.60. *Sea K, v un campo valuado discreto. Entonces, K es un campo local (i.e., K es completo y su campo residual K_v es finito) si y sólo si K es localmente compacto.*

En particular, el anillo de valuación $\mathcal{O}_K$ es compacto y por lo tanto el grupo de unidades U_K también es compacto.

DEMOSTRACIÓN. Si K es localmente compacto, entonces es completo. Ahora, como v es discreta, sea π un parámetro uniformizador. Entonces los ideales $\langle \pi^n \rangle$ forman un sistema de vecindades cerradas del $0 \in \mathcal{O}_K$ y por lo tanto al menos una de ellas es compacta y así, multiplicándola por π^{-n}, se sigue que $\mathcal{O}_K$ es compacto y por lo tanto el campo residual $K_v = \mathcal{O}_K/\pi\mathcal{O}_K$ también es compacto y como es discreto, entonces es finito.

Recíprocamente, si K es completo y K_v es finito, entonces de los epimorfismos $K_v = \mathcal{O}_K/\pi\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/\pi^n\mathcal{O}_K$ se sigue que los cocientes $\mathcal{O}_K/\pi^n\mathcal{O}_K$ también son finitos. Y como por el lema anterior

$$\mathcal{O}_K = \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K,$$

entonces $\mathcal{O}_K$ es el límite inverso de compactos y por lo tanto es compacto. Se sigue que K es localmente compacto.

Finalmente, como $U_K \subseteq \mathcal{O}_K$ es cerrado ya que es la imagen inversa del $\{0\} \subseteq \mathbb{R}$ bajo la función $v_K : K^* \to \mathbb{R}$ y como $\mathcal{O}_K$ es compacto, entonces U_K también es compacto. □

Cuando K, v es un campo local, el valor absoluto ultramétrico $|\ |_v$ asociado a la valuación v se puede elegir canónicamente tomando $a := q^{-1}$, donde $q = |K_v|$ es la cardinalidad del campo residual de K. En este caso se dice que el valor absoluto ultramétrico $|\ |_v$ está normalizado: $|x|_v = q^{-v(x)}$.

Ejemplo 18. El campo $\mathbb{Q}_p$ es un campo local con campo residual $\mathbb{F}_p$. Si $x = p^n a/b$ con $n, a, b \in \mathbb{Z}$ y $p \nmid ab$, entonces $v(x) = n$ y su valor absoluto ultramétrico normalizado es: $|x|_v = p^{-v(x)} = p^{-n}$.

Ejemplo 19. Si $K = \mathbb{F}_q((T))$ es el campo de series formales de Laurent en la variable T con coeficientes en el campo finito $\mathbb{F}_q$, entonces K es un campo local con campo residual $\mathbb{F}_q$.

De hecho, estos dos ejemplos y sus extensiones finitas son todos los campos locales como veremos a continuación, pero primero probamos que, con respecto a la característica, sólo hay dos clases de campos locales:

Proposición 1.61. *Sean K, v un campo local, K_v su campo residual y $p = \text{car}\,(K_v) \neq 0$. Entonces:*

(1) $\text{car}\,(K) = 0$
o
(2) $\text{car}\,(K) = p = \text{car}\,(K_v)$.

DEMOSTRACIÓN. Si $\text{car}\,(K) \neq 0$, sea $q = \text{car}\,(K) > 0$. Entonces $q = 0$ en el subanillo generado por el $1 \in K$ y por lo tanto $q = 0$ en $\mathcal{O}_K$; consecuentemente, $q = 0$ en $K_v = \mathcal{O}_K/\mathfrak{p}_K$, y como q es primo, entonces $q = p$. □

Para clasificar los campos locales, tenemos entonces dos casos a considerar, a saber: cuando K y su campo residual K tienen característica diferente y cuando tienen característica igual:

El caso de característica diferente. En este caso, por la proposición anterior, K tiene característica 0 y su campo residual K tiene característica $p > 0$. Como $\text{car}\,(K) = 0$, entonces $\mathbb{Q} \subseteq K$ y si v_K es la valuación de K, al restringirla a $\mathbb{Q}$ induce una valuación discreta en $\mathbb{Q}$, i.e., una valuación p-ádica v_p en $\mathbb{Q}$. Más aún, como K es completo, la completación $\mathbb{Q}_p$ de $\mathbb{Q} \subseteq K$ también está contenida en K y así K es una extensión de $\mathbb{Q}_p$. Entonces, se tiene la extensión $K/\mathbb{F}_p$ de los campos residuales correspondientes donde K es un campo finito y por lo tanto es de la forma $K = \mathbb{F}_q$ con $q = p^f$ y $f = [K : \mathbb{F}_p] < \infty$. Observemos ahora que el elemento $p \in \mathbb{Z} \subseteq \mathcal{O}_K$ va a dar al $\bar{0} \in K$, de tal forma que $p \in \mathfrak{p}_K$ y así $v_K(p) \geq 1$. El entero $e := v_K(p) \geq 1$ se llama *el índice de ramificación absoluto* de la extensión $K/\mathbb{Q}_p$. Esta terminología se justifica observando que, como podemos suponer que v_K es normalizada, entonces $v_K(K^*) = \mathbb{Z}$ y como $v_K|_{\mathbb{Q}_p}$ es discreta y $p \in \mathbb{Q}_p$ es un elemento primo, se tiene que $e := v_K(p)$ *genera* al grupo discreto $v_K|_{\mathbb{Q}_p}(\mathbb{Q}_p^*)$, es decir, $v_K|_{\mathbb{Q}_p}(\mathbb{Q}_p^*) = e\mathbb{Z}$ y por lo tanto

$$e(K/\mathbb{Q}_p) := [v_K(K^*) : v_K|_{\mathbb{Q}_p}(\mathbb{Q}_p^*)] = [\mathbb{Z} : e\mathbb{Z}] = e = v_K(p),$$

por lo que el entero $e = v_K(p)$ es el índice de ramificación de la extensión $K/\mathbb{Q}_p$. Entonces, la extensión $K/\mathbb{Q}_p$ satisface las hipótesis de la primera parte de (1.35) y consecuentemente $K/\mathbb{Q}_p$ es una extensión finita de grado $[K : \mathbb{Q}_p] = ef$. Hemos así probado el teorema siguiente:

Teorema 1.62. *Si K es un campo local de característica 0, entonces K es una extensión finita del campo $\mathbb{Q}_p$.*

□

El caso de característica igual. En este caso se tiene que car $(K) =$ car $(K) = p \neq 0$, y así la proposición (1.17) (3) y (4) nos dice que podemos elegir un conjunto $\mathcal{R} \subseteq \mathcal{O}_K$ de representantes de K que es un *campo*, de hecho isomorfo a K. Entonces, dados $\alpha = \sum_{n \gg -\infty}^{\infty} a_n \pi^n$ y $\beta = \sum_{n \gg -\infty}^{\infty} b_n \pi^n$, se tendría que

$$\alpha + \beta = \sum_{n \gg -\infty}^{\infty} a_n \pi^n + \sum_{n \gg -\infty}^{\infty} b_n \pi^n = \sum_{n \gg -\infty}^{\infty} (a_n + b_n)\pi^n$$

con $a_n + b_n \in \mathcal{R} \simeq K$, y similarmente para el producto $\alpha\beta$. Como consecuencia de esto tenemos:

Teorema 1.63. *Sea K un campo local de característica $p =$ car $(K) \neq 0$ y sea π un elemento primo de K; entonces:*

(1) $\mathcal{O}_K = K[[\pi]]$ *es el anillo de series formales en π con coeficientes en K.*

(2) $K = K((\pi))$ *es el campo de series formales de Laurent en π con coeficientes en K.*

DEMOSTRACIÓN. Para la parte (1) se usa la expansión (1.16)(1) de todo elemento $\alpha \in \mathcal{O}_K$ como una serie convergente:

$$\alpha = \sum_{n=0}^{\infty} a_n \pi^n \qquad \text{con} \qquad a_n \in \mathcal{R} \simeq K,$$

y la parte (2) es similar usando (1.16)(2) que todo elemento $\alpha \in K$ se puede escribir como una serie convergente:

$$\alpha = \sum_{n \gg -\infty}^{\infty} a_n \pi^n \qquad \text{con} \qquad a_n \in \mathcal{R} \simeq K.$$

□

La máxima extensión no ramificada de un campo local. Si L/K es una extensión finita de campos locales y si L/K es no ramificada, por (1.49) $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\overline{L}/\overline{K})$ y como $K = \mathbb{F}_q$ es un campo finito, digamos con q elementos, entonces $\mathrm{Gal}(\overline{L}/K)$ es un grupo cíclico generado por el *automorfismo de Frobenius* $\mathrm{Fr}_{\overline{K}} : \alpha \mapsto \alpha^q$; sea $\mathrm{Fr}_K \in \mathrm{Gal}(L/K)$ el elemento correspondiente a $\mathrm{Fr}_{\overline{K}}$. Entonces, Fr_K está caracterizado por la propiedad:

$$\mathrm{Fr}_K(a) \equiv a^q \text{ mód } \mathfrak{p}_K \quad \text{para todo} \quad a \in \mathcal{O}_L$$

y se llama el *Frobenius* de la extensión no ramificada L/K. Por definición es un generador del grupo cíclico $\mathrm{Gal}(L/K)$ y su orden es

$$f(L/K) = [L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Gal}(\overline{L}/K)| = [\overline{L} : K].$$

Similarmente, si K es un campo local con campo residual $K = \mathbb{F}_q$ y K_{nr} es la máxima extensión no ramificada de K en una cerradura algebraica K^{al} de K, entonces en este contexto el corolario (1.51) nos dice que

$$\mathrm{Gal}(K_{nr}/K) \simeq \mathrm{Gal}(\mathbb{F}_q^{sep}/\mathbb{F}_q)$$

donde por la observación del párrafo anterior y pasando al límite se tiene que el grupo $\mathrm{Gal}(\mathbb{F}_q^{sep}/\mathbb{F}_q)$ es el límite inverso de los grupos cíclicos finitos $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. (Véase el ejemplo 24 al final de la sección §1.9, donde probamos que este límite es la completación $\widehat{\mathbb{Z}}$ de $\mathbb{Z}$).

Dado un campo local K con campo residual $K = \mathbb{F}_q$, tenemos la siguiente descripción explícita de la máxima extensión no ramificada K_{nr} de K:

Proposición 1.64. *Sea K un campo local con campo residual $K = \mathbb{F}_q$ el campo finito de orden $q = p^f$. Dado un entero n coprimo con p, sean $K_n := K(\mu_n)$ y $K_n := K(\mu_n)$ los campos obtenidos adjuntando las raíces n-ésimas de la unidad a los campos base respectivos. Entonces:*

(1) *K_n/K es una extensión no ramificada y el campo residual de K_n es K_n.*

(2) *El grado $[K_n : K]$ es el menor entero $f' \geq 1$ tal que $q^{f'} \equiv 1$ (mód n).*

(3) *La máxima extensión no ramificada K_{nr} de K se obtiene adjuntando a K todas las raíces de la unidad de orden coprimo con p, i.e.,*

$$K_{nr} = \bigcup_{p \nmid n} K(\mu_n).$$

(4) *La extensión K_{nr}/K es Galois, y además el grupo de Galois*

$$\mathrm{Gal}(K_{nr}/K) \simeq \varprojlim_n \mathrm{Gal}(\mathbb{F}_q^n/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}}$$

está topológicamente generado por el automorfismo Fr_K, *llamado el* automorfismo de Frobenius, *que satisface*

$$\mathrm{Fr}_K(\alpha) \equiv \alpha^q \text{ mód } \mathfrak{p}_{K_{nr}} \qquad \text{para todo } \alpha \in \mathcal{O}_{K_{nr}}.$$

El isomorfismo $\widehat{\mathbb{Z}} \simeq \mathrm{Gal}(K_{nr}/K)$ *está dado, para* $\nu \in \widehat{\mathbb{Z}}$, *mediante:* $\nu \mapsto \mathrm{Fr}_K^{\nu}$.

DEMOSTRACIÓN. (1): El campo $K_n = K(\mu_n)$ es el campo de descomposición del polinomio $x^n - 1$ sobre $K = \mathbb{F}_q$. Ahora, si $f = [K(\mu_n) : K]$, entonces $|K(\mu_n)| = q^f$ para un $f \geq 1$; se sigue que $K(\mu_n)$ es el campo de descomposición del polinomio $x^{q^f} - x = x(x^{q^f-1} - 1)$ sobre $K = \mathbb{F}_q$, i.e., $K(\mu_n) = K(\mu_{q^f-1})$. Nótese que $f \geq 1$ es el menor entero tal que $q^f \equiv 1$ (mód n). Por (1.47)(2) y (1.50)(1), sea $K_{nr,f}$ la extensión no ramificada de K de grado f con campo residual $K_n = \mathbb{F}_{q^f}$. Ahora, para el polinomio $f(x) = x^{q^f-1} - 1$ sobre K se tiene que para todo $a \in \mathcal{O}_{K_{nr,f}}$:

$$|f'(a)|_{K_{nr,f}} = |(q^f - 1)a^{q^f-2}|_{K_{nr,f}} = 1$$

y así, por el lema de Hensel para todo $\alpha \in \mathbb{F}_{q^f}$ existe un $a \in \alpha \subseteq \mathcal{O}_{K_{nr,f}}$ tal que $f(a) = 0$. Y como $f(x)$ se descompone en $\mathbb{F}_{q^f}$, entonces $f(x)$ se descompone en $K_{nr,f}$. Además, el campo de descomposición de $f(x)$ sobre K no puede ser menor que $K_{nr,f}$ ya que su campo residual debe contener al menos q^f elementos. Se sigue que el campo de descomposición de $f(x)$ sobre K es $K_{nr,f}$, i.e., $K_n = K_{nr,f}$. Esto prueba (1).

(2): Se sigue de la demostración anterior. Nótese que f' es el menor entero tal que $\mathrm{Fr}_{K_n/K}^{f'} = 1$.

(3): Se sigue de (1) pasando al límite una vez que notamos que la unión de los campos K_n es la cerradura algebraica de K.

(4): K_{nr}/K es Galois por la observación previa a (1.51) y el grupo de Galois está calculado en (1.51). Finalmente, $\mathrm{Gal}(\mathbb{F}_q^{sep}/\mathbb{F}_q)$ es topológicamente generado por un automorfismo ϕ_q tal que $\phi_q : \alpha \mapsto \alpha^q$, para $\alpha \in \mathbb{F}_q^{sep}$. □

1.7 Filtraciones del grupo de unidades

Dado cualquier campo local K, consideremos la filtración siguiente del grupo de unidades U_K de K:

$$U_K =: U_K^{(0)} \supseteq U_K^{(1)} \supseteq U_K^{(2)} \supseteq \cdots$$

donde los $U_K^{(i)}$ se definen para $i \geq 1$ como

$$U_K^{(i)} := \{x \in U_K \ : \ v(x-1) \geq i\}.$$

Nótese que si $\pi \in K$ es un elemento primo, entonces $\mathfrak{p}_K = \pi \mathcal{O}_K$ y por lo tanto, para $i \geq 1$

$$U_K^{(i)} = 1 + \mathfrak{p}_K^i = 1 + \pi^i \mathcal{O}_K;$$

más aún, cada $U_K^{(i)}$ es un subgrupo abierto de U_K (en la topología de U_K inducida como subconjunto de K^*); de hecho, los grupos $U_K^{(i)}$ forman una base de abiertos del $1 \in K$, ya que si $|\alpha|_K = c^{-v_K(\alpha)}$ es el valor absoluto asociado a v_K, con $c > 1$ un real fijo, como en la demostración de (1.15)(3) se tiene que

$$U_K^{(n)} = 1 + \mathfrak{p}_K^n = \{\alpha \in K^* \ : \ |1-\alpha|_K < \frac{1}{c^{n-1}}\}.$$

Observe que los $U_K^{(n)}$ son, en efecto, subgrupos de U_K ya que claramente son cerrados bajo productos y si $u \in U_K^{(n)}$, entonces $u^{-1} \in U_K^{(n)}$ ya que

$$|1-u^{-1}|_K = |u|_K^{-1}|u-1|_K = |1-u|_K,$$

la última igualdad porque $u \in U_K$. Los grupos $U_K^{(n)}$, $n \geq 1$, se llaman los *grupos de unidades superiores*; el grupo $U_K^{(1)}$ se llama el *grupo de unidades principales* de K. De (1.15)(2) se sigue que $\bigcap_i U_K^{(i)} = 1$ y de (1.59) se deduce que

$$U_K \simeq \varprojlim_i U_K/U_K^{(i)},$$

donde los cocientes $U_K/U_K^{(i)}$ son finitos por la parte (3) del lema siguiente, y por lo tanto U_K es un grupo profinito (Hausdorff, completo y compacto, véase (1.60)). En forma totalmente análoga se tiene que

$$U_K^{(n)} \simeq \varprojlim_i U_K^{(n)}/U_K^{(n+i)},$$

donde los cocientes $U_K^{(n)}/U_K^{(n+i)}$ son finitos por la parte (2) del lema siguiente.

Lema 1.65. *Sea K un campo local, $\mathcal{O}_K$ su anillo de enteros, $\mathfrak{p}_K$ su ideal máximo y K su campo residual. Entonces:*

(1) *El epimorfismo canónico $\mathcal{O}_K \to K$ induce un isomorfismo*

$$\lambda_{0,K} : U_K/U_K^{(1)} \simeq \overline{K}^* \qquad \text{(el grupo multiplicativo).}$$

(2) *Para cada $i \geq 1$, la aplicación $u \mapsto u - 1$ induce un isomorfismo*

$$\lambda_{i,K} : U_K^{(i)}/U_K^{(i+1)} \simeq \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \simeq K^+ \qquad \text{(el grupo aditivo).}$$

(3) *Para cada $i \geq 1$, los cocientes $U_K/U_K^{(i)}$ son finitos.*

(4) *Más aún, si K_n/K es una extensión no ramificada y K_n es el campo residual de K_n, entonces los isomorfismos anteriores (para el grupo de unidades $U_n = U_{K_n}$ de K_n) son isomorfismos de* $\mathrm{Gal}(K_n/K)$*-módulos.*

DEMOSTRACIÓN. (1): El homomorfismo $\rho : U_K \to K^*$, $u \mapsto \overline{u}$ tiene núcleo

$$\mathrm{Ker}\,(\rho) = \{u \in U_K \,;\, \overline{u} = u + \mathfrak{p}_K = 1 + \mathfrak{p}_K\},$$

que es claramente igual a $U_K^{(1)} = 1 + \mathfrak{p}_K$. Más aún, todo $u \in \mathcal{O}_K - \mathfrak{p}_K$ es una unidad, i.e, $u \in U_K$, y por lo tanto la aplicación ρ es suprayectiva.

(2): El isomorfismo $U_K^{(i)}/U_K^{(i+1)} \simeq \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}$ está dado como sigue: si $u \in U_K^{(i)} = 1 + \mathfrak{p}_K^i$, entonces $u = 1 + t$ con $t \in \mathfrak{p}_K^i$, y se define la aplicación $u = 1 + t \mapsto u - 1 = t$ mód $(\mathfrak{p}_K^{i+1})$ de $U_K^{(i)} \to \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}$. Esta aplicación es un homomorfismo ya que si $u, u' \in U_K^{(i)}$ entonces $u = 1 + t$, $u' = 1 + t'$, y

$$uu' - 1 = (1 + t)(1 + t') - 1 = t + t' + tt' \equiv t + t' \text{ mód } (\mathfrak{p}_K^{i+1}).$$

Claramente, es suprayectiva y su núcleo es $1 + \mathfrak{p}_K^{i+1} = U_K^{(i+1)}$.

El isomorfismo de grupos aditivos $\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \simeq K^+$ está dado como sigue: ya que $\mathfrak{p}_K^i \neq \mathfrak{p}_K^{i+1}$, entonces existe un $a \in \mathfrak{p}_K^i - \mathfrak{p}_K^{i+1}$; la aplicación $x \mapsto xa$, para $x \in \mathcal{O}_K$, nos da isomorfismos

$$\mathcal{O}_K \simeq a\mathcal{O}_K \qquad \text{y} \qquad \mathfrak{p}_K \simeq a\mathfrak{p}_K,$$

y por lo tanto induce un isomorfismo

(i) $$\overline{K} = \mathcal{O}_K/\mathfrak{p}_K \simeq a\mathcal{O}_K/a\mathfrak{p}_K.$$

Pero como $a \in \mathfrak{p}_K^i - \mathfrak{p}_K^{i+1}$, entonces el ideal (a) se puede factorizar como

$$(a) = \mathfrak{p}_K^i \mathfrak{a}$$

con $\mathfrak{a}$ un ideal coprimo con $\mathfrak{p}_K$ y se tiene entonces un isomorfismo

(ii) $$a\mathcal{O}_K/a\mathfrak{p}_K \simeq \mathfrak{a}\mathfrak{p}_K^i/\mathfrak{a}\mathfrak{p}_K^{i+1}.$$

Se tiene además que

$$\mathfrak{a}\mathfrak{p}_K^i + \mathfrak{p}_K^{i+1} = \mathfrak{p}_K^i \qquad \text{y} \qquad \mathfrak{a}\mathfrak{p}_K^i \cap \mathfrak{p}_K^{i+1} = \mathfrak{a}\mathfrak{p}_K^{i+1},$$

y así la aplicación $x \mapsto x + \mathfrak{p}_K^{i+1}$, para $x \in \mathfrak{a}\mathfrak{p}_K^i$, induce un isomorfismo

(iii) $$\mathfrak{a}\mathfrak{p}_K^i/\mathfrak{a}\mathfrak{p}_K^{i+1} \simeq \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}.$$

Los isomorfismos (i), (ii), (iii) dan el resultado deseado.

(3): Por inducción sobre i considerando la sucesión exacta corta:

$$0 \to U_K/U_K^{(i)} \to U_K/U_K^{(i+1)} \to U_K^{(i)}/U_K^{(i+1)} \to 0,$$

donde los extremos son finitos por hipótesis de inducción y la parte (2) respectivamente.

(4): Finalmente, que todos estos isomorfismos son de Galois se sigue del hecho de que como K_n/K es no ramificada, un primo π_K de K es también un primo de K_n, y así los morfismos de (i) y (ii) son $\mathrm{Gal}(K_n/K)$-morfismos, i.e., para toda $\sigma \in \mathrm{Gal}(K_n/K)$ se tiene

$$\sigma(u) = \sigma(1 + \pi^i\beta) = 1 + \pi^i\sigma(\beta).$$

□

Proposición 1.66. *Sea K un campo local. Entonces, el grupo K^* tiene la descomposición*

$$K^* = (\pi) \times U_K = (\pi) \times \mu_{q-1} \times U_K^{(1)},$$

donde $(\pi) = \{\pi^n \ : \ n \in \mathbb{Z}\} \subseteq K^*$ es el subgrupo cíclico infinito generado por el elemento primo $\pi = \pi_K$ de K, μ_{q-1} es el grupo de raíces $(q-1)$-ésimas de la unidad y q es la cardinalidad del campo residual de K.

DEMOSTRACIÓN. Todo elemento $a \in K^*$ tiene una descomposición única

$$a = \pi^{v_K(a)} \cdot u$$

con $u \in U_K$, lo cual muestra que

$$K^* = (\pi) \times U_K.$$

Más aún, el grupo U_K contiene al subgrupo μ_{q-1} ya que la ecuación $x^{q-1} - 1 = 0$ se descompone en factores lineales en el campo residual K_v de K (aquí q es la cardinalidad de K_v), y por el lema de Hensel cada una de estas raíces $\overline{\alpha} \in K_v$ se levanta a una raíz $\alpha \in K$ y así $x^{q-1} - 1$ se factoriza en K.

Ahora, el epimorfismo canónico $\rho : \mathcal{O}_K \to K_v = \mathcal{O}_K/\mathfrak{p}_K$ restringido a U_K manda $\mu_{q-1} \subseteq U_K$ suprayectivamente a K_v con núcleo $U_K^{(1)}$. Esto muestra que

$$U_K = \mu_{q-1} \times U_K^{(1)}.$$

□

Proposición 1.67. *Sea K un campo local y n un entero coprimo con* car (K). *Entonces, para todo entero $i \geq v_K(n) + 1$, la aplicación $a \mapsto a^n$ es un isomorfismo de $U_K^{(i)}$ en $U_K^{(i+v_K(n))}$, en particular*

$$(U_K^{(i)})^n = U_K^{(i+v_K(n))}$$

para todo $i \geq v_K(n) + 1$.

DEMOSTRACIÓN. Como $U_K^{(i)} = 1 + \mathfrak{p}_K^i = 1 + \pi_K^i \mathcal{O}_K$, entonces

$$\left(U_K^{(i)}\right)^n \subseteq U_K^{(i+v_K(n))}$$

ya que si $\alpha = 1 + a\pi_K^i \in U_K^{(i)}$, entonces

$$\begin{aligned} \alpha^n = (1 + a\pi_K^i)^n &= 1 + na\pi_K^i \text{ mód } \pi_K^{2i} \\ &= 1 + na\pi_K^i \text{ mód } (n\pi_K^{i+1}) \end{aligned}$$

ya que $v_K(n\pi_K^{i+1}) = v_K(n) + i + 1 \leq 2i$ porque $v_K(n) + 1 \leq i$ por hipótesis. Se sigue que $\alpha^n - 1 = na\pi_K^i + bn\pi_K^{i+1}$ con $a, b \in \mathcal{O}_K$ y por lo tanto

$$\begin{aligned} v_K(\alpha^n - 1) &\geq \min\{v_K(na\pi_K^i), v_K(bn\pi_K^{i+1})\} \\ &\geq v_K(n) + i \end{aligned}$$

ya que $v_K(na\pi_K^i) = v_K(n) + i + v_K(a)$ y $v_K(bn\pi_K^{i+1}) = v_K(n) + i + 1 + v_K(b)$ con $v_K(a) \geq 0$ y $v_K(b) \geq 0$.

Ahora, el núcleo de $U_K^{(i)} \longrightarrow \left(U_K^{(i)}\right)^n$ es el conjunto de raíces n-ésimas de 1 contenidas en $U_K^{(i)}$. Sea $\xi = 1 + a\pi_K^i$ una de estas raíces; entonces $\xi^2 \equiv 1 \bmod \mathfrak{p}_K^i$. En general, $\xi^r \equiv 1 \bmod \mathfrak{p}_K^i$. Ahora, si $\xi \neq 1$, entonces substituyendo $\xi^r \equiv 1 \bmod \mathfrak{p}_K^i$ en

$$\xi^{n-1} + \cdots + \xi + 1 = 0$$

se obtiene que $n = 1 + \cdots + 1 \equiv 0 \bmod \mathfrak{p}_K^i$ y por lo tanto $n \in \mathfrak{p}_K^i$ y así $v_K(n) \geq i > v_K(n)$, una contradicción a menos que $\xi = 1$. Se sigue que el núcleo del morfismo anterior es trivial, i.e., es un monomorfismo.

Finalmente, si $\alpha \in U_K^{(i+v_K(n))}$ consideremos la ecuación

$$f(x) = x^n - \alpha = 0.$$

Para aplicar el lema de Hensel a esta ecuación, con $\alpha_0 = 1$ en $\mathcal{O}_K$, se observa que $f(\alpha_0) = 1 - \alpha$ y $f'(\alpha_0) = n$, de tal forma que

$$\begin{aligned} v_K\left(\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right) &= v_K\left(\frac{1-\alpha}{n^2}\right) = v_K(1-\alpha) - v_K(n^2) \\ &= i + v_K(n) - 2v_K(n) = i - v_K(n) > 0, \end{aligned}$$

es decir, se satisfacen las hipótesis del lema de Hensel y consecuentemente existe un $a \in \mathcal{O}_K$ tal que $f(a) = 0$, i.e., tal que $a^n = \alpha$. Más aún, por la parte (2) del lema de Hensel (1.21):

$$v_K(a - \alpha_0) = v_K(a-1) \geq v_K\left(\frac{f(\alpha_0)}{f'(\alpha_0)}\right) = i + v_K(n) - v_K(n) = i$$

y por lo tanto $a \in U_K^{(i)}$ y es tal que $a^n = \alpha$, como se quería. □

Como una consecuencia de esta proposición probaremos que si K es un campo local, entonces para todo $m \geq 1$ coprimo con car (K) (arbitrario si car $(K) = 0$) se tiene que K^{*m} tiene índice finito en K^*; para esto necesitaremos el lema siguiente, de la teoría de grupos:

Lema 1.68. *Si $f : G \to G'$ es un homomorfismo de grupos y $H \lhd G$ es un subgrupo normal, entonces*

$$[G : H] = [f(G) : f(H)][\mathrm{Ker}\,(f) : \mathrm{Ker}\,(f|_H)].$$

DEMOSTRACIÓN. El morfismo f induce el isomorfismo $G/\mathrm{Ker}\,(f) \simeq f(G)$ y como $f(\mathrm{Ker}\,(f)H) = f(H)$, donde notamos que $\mathrm{Ker}\,(f)H$ es un subgrupo

normal de G, entonces f induce el isomorfismo $G/\mathrm{Ker}\,(f)H \simeq f(G)/f(H)$ y así $[G : \mathrm{Ker}\,(f)H :] = [f(G) : f(H)]$, por lo que

$$\begin{aligned}[G : H] \qquad & [G : \mathrm{Ker}\,(f)H][\mathrm{Ker}\,(f)H : H] \\ & [f(G) : f(H)][\mathrm{Ker}\,(f) : \mathrm{Ker}\,(f) \cap H] \\ & [f(G) : f(H)][\mathrm{Ker}\,(f) : \mathrm{Ker}\,(f|_H)].\end{aligned}$$

□

Corolario 1.69. *Si K es un campo local de característica $p \geq 0$ y $m \geq 1$ es un entero coprimo con p (arbitrario si $p = 0$), entonces K^{*m} tiene índice finito en K^*. De hecho, U_K^m tiene índice finito en U_K y más aún*

$$[K^* : K^{*m}] = m[U_K : U_K^m].$$

DEMOSTRACIÓN. Usando el lema anterior con el homomorfismo $v_K : K^* \twoheadrightarrow \mathbb{Z}$ y con $H := K^{*m} \subseteq K^* =: G$, observando que $\mathrm{Ker}\,(v_K) = U_K$ y $\mathrm{Ker}\,(v_K|_H) = H \cap U_K = U_K^m$, se tiene que

$$\begin{aligned}[K^* : K^{*m}] \qquad & [v_K(K^*) : v_K(K^{*m})][U_K : U_K^m] \\ & [\mathbb{Z} : m\mathbb{Z}][U_K : U_K^m] = m[U_K : U_K^m],\end{aligned}$$

y así basta probar que el índice $[U_K : U_K^m]$ es finito. Ahora, por la proposición (1.67) anterior, para i suficientemente grande se tiene que $(U_K^{(i)})^m = U_K^{(i+v_K(m))}$ y de hecho podemos elegir i suficientemente grande de tal forma que ningún elemento $\zeta \neq 1$ de $\mu_m(K)$ esté en $U_K^{(i)}$. Consideremos entonces el homomorfismo $f : U_K \to U_K^m$ dado por $u \mapsto u^m$ y apliquemos el lema previo con $H := U_K^{(i)} \subseteq U_K =: G$ notando que $\mathrm{Ker}\,(f) = \mu_m(K)$; se tiene entonces

$$\begin{aligned}[U_K : U_K^{(i)}] \qquad & [U_K^m : (U_K^{(i)})^m][\mu_m(K) : \mu_m(K) \cap U_K^{(i)}] \\ & [U_K^m : U_K^{(i+v_K(m))}][\mu_m(K) : 1] \\ = \quad & \frac{[U_K : U_K^{(i+v_K(m))}]}{[U_K : U_K^m]}\,|\mu_m(K)|,\end{aligned}$$

la última igualdad por el tercer isomorfismo de Noether. Se sigue que

$$[U_K : U_K^m] = \frac{[U_K : U_K^{(i+v_K(m))}]}{[U_K : U_K^{(i)}]}\,|\mu_m(K)|$$

y como los índices $[U_K : U_K^{(i)}]$ son finitos por (1.65)(3), entonces $[U_K : U_K^m]$ también es finito y consecuentemente $[K^* : K^{*m}] = m[U_K : U_K^m]$ también lo es. □

Si K es un campo local y $p = \text{car}(K)$, consideremos el homomorfismo $\phi_p : K^* \to K^*$ dado por $\alpha \mapsto \alpha^p$ y a continuación estudiaremos su acción en los subgrupos $U_K^{(i)} \subseteq K^*$. Como la característica del campo local K es 0 ó p, tenemos dos casos a considerar, el caso de característica igual siendo el más simple:

Proposición 1.70. *Si K es un campo local de característica* $\text{car}(K) = p = \text{car}(K)$, *entonces el homomorfismo $\phi_p : K^* \to K^*$ manda inyectivamente $U_K^{(i)}$ en $U_K^{(pi)}$ para toda $i \geq 1$, y se tienen diagramas conmutativos para toda $i \geq 1$:*

$$\begin{array}{ccc} U_K^{(i)}/U_K^{(i+1)} & \xrightarrow{\phi_p} & U_K^{(pi)}/U_K^{(pi+1)} \\ \downarrow{\scriptstyle \lambda_{i,K}} & & \downarrow{\scriptstyle \lambda_{pi,K}} \\ K & \xrightarrow[\text{Fr}_p]{} & K \end{array}$$

donde $\lambda_{j,K} : U_K^{(j)}/U_K^{(j+1)} \to K$ son los isomorfismos de (1.65) *y Fr_p es el automorfismo de Frobenius. Más aún, los morfismos ϕ_p son isomorfismos para toda $i \geq 1$.*

DEMOSTRACIÓN. Sea $\pi = \pi_K$ un elemento primo de K. Si $\alpha = 1 + \varepsilon\pi^i \in U_K^{(i)}$ entonces

$$\phi_p(\alpha) = (1 + \varepsilon\pi^i)^p = 1 + \varepsilon^p\pi^{pi}$$

(la última igualdad porque $\text{car}(K) = p$) y claramente $1 + \varepsilon^p\pi^{pi} \in U_K^{(pi)}$. Más aún, ϕ_p es inyectiva porque no hay p-torsión no trivial en K^*. Esto prueba la primera afirmación. Para la conmutatividad de los diagramas, recordemos de (1.65) que los morfismos $\lambda_{i,K}$ están dados para $\alpha = 1 + \varepsilon\pi^i \in U_K^{(i)}$ como: $\lambda_i(\alpha) = \bar{\varepsilon}$. Se tiene entonces que

$$\text{Fr}_p \circ \lambda_i(\alpha) = \text{Fr}_p(\bar{\varepsilon}) = \bar{\varepsilon}^p$$

y

$$\lambda_{pi} \circ \phi_p(\alpha) = \lambda_{pi}(\alpha^p) = \lambda_{pi}(1 + \varepsilon^p\pi^{pi}) = \varepsilon^p = \bar{\varepsilon}^p,$$

i.e., los diagramas conmutan.

Finalmente, como car $(K) = p$ y K es finito, entonces el Frobenius $\mathrm{Fr}_p : K \to K$ es un isomorfismo y como los λ_j son isomorfismos por (1.65), entonces $\phi_p : U_K^{(i)}/U_K^{(i+1)} \to U_K^{(pi)}/U_K^{(pi+1)}$ es un isomorfismo para toda $i \geq 1$. □

Consideraremos ahora el caso de característica diferente, i.e., car $(K) = 0$ y $p = \mathrm{car}\,(K)$. Nótese para comenzar que para $p = p \cdot 1 \in K$ se tiene que $p = 0$ en $K = \mathcal{O}_K/\mathfrak{p}_K$, de tal forma que $p \in \mathfrak{p}_K$ y por lo tanto $v_K(p) = e > 1$. Sea $\pi = \pi_K$ un elemento primo de K y sea $\mathcal{R} \subseteq \mathcal{O}_K$ un conjunto completo de representantes de K. Escribiendo al elemento $p \in K$ como

$$p = \sum \theta_i \pi^i \qquad \text{con } \theta_i \in \mathcal{R}$$

y $v_K(p) = \min\{i \quad \theta_i \neq 0\}$, como $v_K(p) = e > 1$ sea $\theta_0 \in \mathcal{R}$ el coeficiente de π^e en $(*)$. Entonces $p - \theta_0\pi^e \in \pi^{e+1}\mathcal{O}_K$ y $\overline{\theta}_0 \in K$ está unívocamente determinado por las condiciones anteriores.

Proposición 1.71. *Sea K un campo local de característica 0 y sea p* car (K). *Entonces:*

(1) *Para $i \leq e/(p-1)$, el homomorfismo ϕ_p manda $U_K^{(i)}$ en $U_K^{(pi)}$.*

(2) *Para $i > e/(p-1)$, ϕ_p manda $U_K^{(i)}$ en $U_K^{(i+e)}$.*

(3) *Los diagramas siguientes conmutan (donde los $\lambda_{j,K}$ son los isomorfismos de* (1.65)*):*

(i) *Para $i < e/(p-1)$:*

$$\begin{array}{ccc} U_K^{(i)}/U_K^{(i+1)} & \xrightarrow{\phi_p} & U_K^{(pi)}/U_K^{(pi+1)} \\ \downarrow{\scriptstyle \lambda_{i,K}} & & \downarrow{\scriptstyle \lambda_{pi,K}} \\ K & \xrightarrow[\mathrm{Fr}_p]{} & K \end{array}$$

(ii) *Para $i > e/(p-1)$:*

$$\begin{array}{ccc} U_K^{(i)}/U_K^{(i+1)} & \xrightarrow{\phi_p} & U_K^{(i+e)}/U_K^{(i+e+1)} \\ \downarrow{\scriptstyle \lambda_{i,K}} & & \downarrow{\scriptstyle \lambda_{i+e,K}} \\ K & \xrightarrow[\bar{\varepsilon} \mapsto \overline{\theta}_0\bar{\varepsilon}]{} & K \end{array}$$

(iii) *Si se tiene que* $i = e/(p-1) \in \mathbb{Z}$*:*

$$\begin{array}{ccc} U_K^{(i)}/U_K^{(i+1)} & \xrightarrow{\phi_p} & U_K^{(pi)}/U_K^{(pi+1)} \\ \downarrow{\scriptstyle \lambda_{i,K}} & & \downarrow{\scriptstyle \lambda_{pi,K}} \\ K & & K \\ \bar{\varepsilon} & \mapsto & \bar{\varepsilon}^p + \bar{\theta}_0 \bar{\varepsilon} \end{array}$$

Más aún, si $1 \leq i < e/(p-1)$*, entonces* ϕ_p *es un isomorfismo en* (i) *y si* $i > e/(p-1)$*, entonces* ϕ_p *es un isomorfismo en* (ii).

DEMOSTRACIÓN. Sea $1 + \alpha \in U_K^{(i)}$. Desarrollando el binomio

$$(1+\alpha)^p = 1 + p\alpha + \frac{p(p-1)}{2}\alpha^2 + \cdots + p\alpha^{p-1} + \alpha^p$$

observamos que las valuaciones de sus términos son

$$\begin{array}{rcll} v(p\alpha) & = & v(p) + v(\alpha) & = e + i \\ v((p(p-1)/2)\alpha^2) & & v(p(p-1)/2) + v(\alpha^2) & = e + 2i \end{array}$$

$$\begin{array}{rcll} v(p\alpha^{p-1}) & & v(p) + v(\alpha^{p-1}) & - e + (p-1)i \\ v(\alpha^p) & = & pv(\alpha) & = pi, \end{array}$$

de donde se sigue que

$$\begin{array}{rcll} v((1+\alpha)^p - 1) & - & v(p\alpha + \alpha^p) & \text{si} \quad v(p\alpha) \neq v(\alpha^p) \\ v((1+\alpha)^p - 1) & > & v(p\alpha + \alpha^p) & \text{si} \quad v(p\alpha) = v(\alpha^p). \end{array}$$

Nótese que

$$v(\alpha^p) \leq v(p\alpha) \Leftrightarrow pi \leq e + i \Leftrightarrow i \leq e/(p-1),$$

de tal forma que

$$\begin{array}{rcll} v(\alpha^p) & < & v(p\alpha) & \Leftrightarrow \quad i < e/(p-1) \\ v(\alpha^p) & > & v(p\alpha) & \Leftrightarrow \quad i > e/(p-1) \\ v(\alpha^p) & = & v(p\alpha) & \Leftrightarrow \quad i = e/(p-1) \in \mathbb{Z}. \end{array}$$

Se sigue entonces que para $\alpha = 1 + \varepsilon\pi^i \in U_K^{(i)}$:

$$\begin{array}{rcll} v((1+\varepsilon\pi^i)^p - 1) & = & v(\varepsilon^p \pi^{pi}) & \text{si} \quad i < e/(p-1) \\ v((1+\varepsilon\pi^i)^p - 1) & = & v(p\varepsilon\pi^i) & \text{si} \quad i > e/(p-1) \\ v((1+\varepsilon\pi^i)^p - 1) & = & v(\varepsilon^p \pi^{pi} + p\varepsilon\pi^i) & \text{si} \quad i = e/(p-1) \in \mathbb{Z}, \end{array}$$

es decir,

$$\begin{array}{lcll}(1+\varepsilon\pi^i)^p & = & 1+\varepsilon^p\pi^{pi} \text{ (mód } \pi^{pi+1}) & \text{si } i < e/(p-1)\\ (1+\varepsilon\pi^i)^p & & 1+\theta_0\varepsilon\pi^{i+e} \text{ (mód } \pi^{i+e+1}) & \text{si } i > e/(p-1)\\ (1+\varepsilon\pi^i)^p & = & 1+(\varepsilon^p+\theta_0\varepsilon)\pi^{i+e} \text{ (mód } \pi^{pi+1}) & \text{si } i = e/(p-1)\in\mathbb{Z}\end{array}$$

ya que la primera congruencia es consecuencia de la primera igualdad de las tres igualdades previas. La segunda congruencia es porque $\theta_0 \in \mathcal{R}$ es el coeficiente de π^e en la expansión de p en $(*)$, de tal forma que $p - \theta_0\pi^e \in \pi^{e+1}\mathcal{O}_K$. La última congruencia es porque $pi = e + i$ y así, usando de nuevo que $p - \theta_0\pi^e \in \pi^{e+1}\mathcal{O}_K$, se tiene que

$$\varepsilon^p\pi^{pi} + p\varepsilon\pi^i \equiv \varepsilon^p\pi^{pi} + \theta_0\pi^e\varepsilon\pi^i \equiv (\varepsilon^p + \theta_0\varepsilon)\pi^{i+e} \text{ mód } \pi^{i+e+1}.$$

La conmutatividad de los diagramas de la proposición se sigue de las tres congruencias anteriores.

Finalmente, si $1 \leq i < e/(p-1)$, en el primer diagrama λ_i y λ_{pi} son isomorfismos y $\mathrm{Fr}_p : K \to K$ es el isomorfismo de Frobenius (K es finito). Se sigue que $\phi_p : U_K^{(i)}/U_K^{(i+1)} \to U_K^{(pi)}/U_K^{(pi+1)}$ es un isomorfismo en este caso. También, si $i > e/(p-1)$, los morfismos λ_i y λ_{i+e} son isomorfismos en el segundo diagrama y la aplicación $\overline{\varepsilon} \mapsto \overline{\theta}_0\overline{\varepsilon}$ es un isomorfismo de K en K ya que $\theta_0 \neq 0$. Se sigue que ϕ_p también es un isomorfismo. □

Corolario 1.72. *Sean K un campo local y $p = \mathrm{car}\,(K)$.*

(1) *Si $n \geq 1$ es un entero coprimo con p, entonces para todo $i \geq 1$ los grupos $U_K^{(i)}$ son unívocamente n-divisibles.*

(2) *Si* car $(K) = 0$, *entonces para toda $n \geq 1$ el grupo $(K^*)^n$ es abierto de índice finito en K^*.*

(3) *Si* car $(K) = p =$ car (K), *entonces el grupo $(K^*)^n$ es abierto de índice finito en K^* si y sólo si $p \nmid n$.*

DEMOSTRACIÓN. (1): Si $\alpha = 1 + \varepsilon\pi^i \in U_K^{(i)}$ y si $\alpha^n = 1$, como la clase lateral de α^n en $U_K^{(i)}/U_K^{(i+1)} \simeq K$ es

$$\begin{aligned}1 = \alpha^n = (1+\varepsilon\pi^i)^n &= 1 + n\varepsilon\pi^i + \text{ términos en } \pi^j \text{ con } j \geq i+1\\ &\equiv 1 + n\varepsilon\pi^i \text{ mód } \mathfrak{p}_K^{i+1},\end{aligned}$$

entonces $1 \equiv 1 + n\varepsilon\pi^i$ mód $\mathfrak{p}_K^{i+1}$, i.e., $n\varepsilon\pi^i \in \mathfrak{p}_K^{i+1}$. Pero como K es unívocamente n-divisible y $p = \mathrm{car}\,(K) \nmid n$, entonces la única posibilidad para que se dé la igualdad anterior es que $n = 0$.

(2): Si car $(K) = 0$, entonces $(K^*)^n$ tiene índice finito en K^* por (1.69). Tenemos ahora dos subcasos:

(i). Si $p \nmid n$. Entonces $U_K^{(1)} \subseteq (K^*)^n$ por la parte (1), y así $(K^*)^n$ es abierto en K^*.

(ii). Si $p|n$, escribamos $n = p^t m$ con $p \nmid m$. Escojamos un entero i tal que $i \geq v_K(p^t) + 1 = t + 1$. Por (1.67) se tiene que

$$U_K^{(i+v_K(p^t))} = \left(U_K^{(i)}\right)^{p^t} \subseteq (K^*)^{p^t},$$

y por lo tanto $(K^*)^{p^t}$ es abierto.

(3): Si car $(K) = p =$ car (K), de nuevo consideramos dos subcasos:

(i). Si $p \nmid n$, de nuevo por la parte (1), $U_K^{(1)} \subseteq (K^*)^n$ y así $(K^*)^n$ es abierto. Y es de índice finito por (1.69).

(ii) Si $p|n$, escribamos $n = p^t m$ con $p \nmid m$ y notemos que si $p \nmid i$, entonces $U_K^{(i)} \not\subseteq (K^*)^p$ ya que si sucediera lo contrario, i.e., si $1 + \pi^i \in (K^*)^p$ con $1 + \pi^i \in U_K^{(i)}$, entonces existiría un $\alpha \in K^*$ tal que $\alpha^p = 1 + \pi^i$ y como estamos en característica $p > 0$, esto implica que $(\alpha - 1)^p = \alpha^p - 1 = \pi^i$, por lo que $pv_K(\alpha - 1) = i$, i.e., $p|i$, una contradicción ya que $\alpha \neq 0$.

Se sigue que $(K^*)^p$ no contiene a ningún $U_K^{(i)}$ con $p \nmid i$ y por lo tanto no contiene a ningún $U_K^{(j)}$, ya que por (1.70) el morfismo $\phi_p : U_K^{(j)} \rightarrowtail U_K^{(pj)}$ es inyectivo. Por lo tanto, $(K^*)^p$ no es abierto en K^*. □

La proposición anterior muestra que en característica 0 las propiedades topológicas y las algebraicas de un campo local K están estrechamente relacionadas. Esto no es así en el caso de característica igual.

1.8 Grupos de ramificación

En esta sección introducimos los grupos de ramificación de una extensión finita de Galois de campos locales y finalizamos probando que el grupo de Galois de una tal extensión es soluble. Será hasta el capítulo 4 cuando estudiaremos más a profundidad estos grupos de ramificación. En esta sección sólo estudiaremos las propiedades básicas que nos serán útiles inmediatamente.

Definición 1.73. Sea L/K una extensión finita de campos locales con grupo de Galois $G = \mathrm{Gal}(L/K)$. Para cada número real $s \geq -1$ se define el *s-ésimo grupo de ramificación* de L/K mediante

$$G_s = G_s(L/K) := \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(a)-a) \geq s+1 \text{ para todo } a \in \mathcal{O}_L\}.$$

El grupo $G_0 = \{\sigma \in \mathrm{Gal}(L/K) \ : \ v_L(\sigma(a) - a) \geq 1\}$ es el *grupo de inercia* (véase (1.50)(4)) de L/K y $G_{-1} = G = \mathrm{Gal}(L/K)$. El grupo G_1 se llama el *grupo de ramificación* de L/K y los grupos G_i, para $i \geq 2$ se llaman los *grupos de ramificación superior* de L/K.

Observemos que como $v_L : L^* \twoheadrightarrow \mathbb{Z}$ tiene valores enteros, entonces para todo número real $s \geq -1$ se tiene que

$$G_s = G_{j(s)},$$

donde $j(s)$ es el menor entero $\geq s$. En efecto, si $\sigma \in G_{j(s)}$, entonces para todo $a \in \mathcal{O}_L$ se tiene que

$$v_L(\sigma a - a) \geq j(s) + 1 \geq s + 1$$

ya que $j(s) \geq s$. Se sigue que $\sigma \in G_s$. Recíprocamente, si $\sigma \in G_s$ entonces $v_L(\sigma a - a) \geq s + 1$ para todo $a \in \mathcal{O}_L$. Pero como $v_L(\sigma a - a) \in \mathbb{Z}$, entonces el entero $v_L(\sigma a - a) - 1$ es $\geq s$ y como $j(s)$ es el menor entero con esta propiedad, entonces $j(s) \leq v_L(\sigma a - a) - 1$, i.e., $v_L(\sigma a - a) \geq j(s) + 1$ y por consiguiente $\sigma \in G_{j(s)}$.

Que los $G_i \subseteq G$ son, en efecto, subgrupos de G es porque si $\sigma \in G_i$, entonces para todo $a \in \mathcal{O}_K$ se tiene que $\sigma(a) - a \in \mathfrak{p}_K^{i+1}$ y por lo tanto

$$a - \sigma^{-1}(a) = \sigma^{-1}(\sigma(a) - a) \in \mathfrak{p}_K^{i+1},$$

por (1.27)(3), i.e., $\sigma^{-1} \in G_i$. Similarmente, si $\sigma, \tau \in G_i$ y $a \in \mathcal{O}_K$, entonces, de nuevo por (1.27)(3)

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

y por lo tanto $\sigma\tau \in G_i$.

Nótese que se tiene una cadena de subgrupos

$$\cdots \subseteq G_i \subseteq \cdots G_1 \subseteq G_0 \subseteq G.$$

Lema 1.74. *Sea L/K una extensión finita de Galois de campos locales. Entonces, los grupos G_s son subgrupos normales de $G = \mathrm{Gal}(L/K)$ y además $G_s = \{1\}$ para s suficientemente grande.*

DEMOSTRACIÓN. Si $\sigma \in G_s$ y $\tau \in G$, entonces como $v_L(\theta(a)) = v_L(a)$ para todo $\theta \in G$, se tiene que para $\theta = \tau^{-1}$:

$$v_L(\tau^{-1}\sigma\tau(x) - x) = v_L(\tau^{-1}(\sigma\tau x) - \tau^{-1}(\tau x)) = v_L(\sigma\tau x - \tau x) \geq s + 1,$$

la última desigualdad porque $\sigma \in G_s$ y $\tau x \in \mathcal{O}_L$; se sigue que $\tau^{-1}\sigma\tau \in G_s$.

Para la segunda afirmación, sea $\sigma \neq 1$; entonces existe un $a \in \mathcal{O}_L$ tal que $\sigma a \neq a$. Se sigue que si $s \geq v_L(\sigma a - a)$ entonces $\sigma \notin G_s$, i.e., G_s no contiene elementos $\sigma \neq 1$, i.e., $G_s = \{1\}$. Tomando entonces

$$s_0 := \max\{v_L(\sigma a - a) \ : \ \sigma \in G, \sigma \neq 1\}$$

(G es finito) se sigue que G_s es trivial para $s \geq s_0$. □

Lema 1.75. *Sea L/K una extensión finita de Galois de campos locales con grupo de Galois $G = \mathrm{Gal}(L/K)$.*

(1) *Si $j \geq -1$ es un entero, entonces*

$$G_j = \{\sigma \in G \ : \ \sigma \text{ actúa trivialmente en } \mathcal{O}_L/\mathfrak{p}_L^{j+1}\}.$$

(2) *Usando* (1.40) *escribamos $\mathcal{O}_L = \mathcal{O}_K[x]$ para algún $x \in \mathcal{O}_L$. Entonces*

$$G_s = \{\sigma \in G \ : \ v_L(\sigma(x) - x) \geq s + 1\}.$$

DEMOSTRACIÓN. (1): Si $\sigma \in G_j$, entonces para toda $a \in \mathcal{O}_L$ se tiene que $v_L(\sigma a - a) \geq j + 1$ y por lo tanto $\sigma a - a \in \mathfrak{p}_L^{j+1}$, i.e., $\sigma a = a$ en el cociente $\mathcal{O}_L/\mathfrak{p}_L^{j+1}$. La otra inclusión es similar.

(2): Por la observación después de la definición basta suponer que s es un entero ≥ -1. Pongamos

$$G_{s,x} := \{\sigma \in G \ : \ v_L(\sigma x - x) \geq s + 1\}.$$

Claramente, $G_s \subseteq G_{s,x}$. Recíprocamente, si $\sigma \in G_{s,x}$ y $a \in \mathcal{O}_L$ es cualquier elemento, entonces por (1.40) $a = \sum_{i \geq 0} a_i x^i$ con $a_i \in \mathcal{O}_K$ y por lo tanto

$$(*) \quad v_L(\sigma a - a) = v_L\left(\sum_{i \geq 0} a_i \sigma(x)^i - \sum_{i \geq 0} a_i x^i\right) = v_L\left(\sum_{i \geq 0} a_i(\sigma(x^i) - x^i)\right)$$

(la segunda igualdad porque $\sigma(a_i) = a_i$ ya que $a_i \in K$). Observemos ahora que si $\sigma \in G_{s,x}$, entonces $v_L(\sigma x - x) \geq s+1$ y así como

$$\sigma(x^2) - x^2 = \sigma(x)\sigma(x) - xx = \sigma(x)(\sigma x - x) + x(\sigma x - x)$$

donde $x, \sigma(x) \in \mathcal{O}_L$ se sigue que

$$\begin{aligned} v_L(\sigma x^2 - x^2) \quad & v_L(\sigma(x)(\sigma x - x) + x(\sigma x - x)) \\ \geq \quad & \min\{v_L(\sigma x(\sigma x - x)), v_L(x(\sigma x - x))\} \\ \geq \quad & v_L(\sigma x - x) \geq s+1. \end{aligned}$$

Recursivamente se prueba que

$$v_L(\sigma x^i - x^i) \geq s+1$$

y por lo tanto

$$v_L(\sigma a - a) = v_L\left(\sum_{i\geq 0} a_i(\sigma(x^i) - x^i)\right) \geq s+1,$$

i.e., $\sigma \in G_s$. □

Proposición 1.76. *Si L/K es una extensión finita normal de campos locales con campos residuales $L \supseteq K$ respectivamente y pongamos $G = \mathrm{Gal}(L/K)$; entonces:*

(1) $\mathrm{Gal}(L/K) \simeq G/G_0$.

(2) *El campo fijo de G_0 es la máxima extensión no ramificada L_0 de K contenida en L.*

(3) *Si π_K es un elemento primo de K (y por lo tanto es primo de L_0 ya que L_0/K es no ramificada), entonces para $j \geq 1$ se tiene que*

$$G_j = \{\sigma \in G_0 \ : \ v_{L_0}(\sigma\pi_K - \pi_K) \geq j+1\},$$

i.e., para $j \geq 1$ los grupos de ramificación de $G = \mathrm{Gal}(L/K)$ coinciden con los grupos de ramificación de su grupo de inercia $G_0 = \mathrm{Gal}(L/L_0)$.

DEMOSTRACIÓN. En (1.50) vimos que si L_0 es la máxima extensión no ramificada de K contenida en L se tiene que

$$\mathrm{Gal}(L/L_0) \simeq G_0$$

es el grupo de inercia de L/K. Esto es precisamente (2).

Para (1), en la torre de extensiones $L \supseteq L_0 \supseteq K$ se tiene que

$$G/G_0 \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_0) \simeq \mathrm{Gal}(L_0/K) \simeq \mathrm{Gal}(L/K),$$

el último isomorfismo porque L_0/K es no ramificada.

Finalmente, pongamos $G_{j,0} := \{\sigma \in G_0 \ : \ v_{L_0}(\sigma\pi_K - \pi_K) \geq j+1\}$. Claramente $G_{j,0} \subseteq G_j$. Recíprocamente, como $j \geq 1$ entonces $G_j \subseteq G_0$ y así, si $\sigma \in G_j$ entonces $\sigma \in G_0$ y por lo tanto $G_j \subseteq G_{j,0}$. □

Si L/K es una extensión finita de Galois de campos locales con grupo de Galois $G = \mathrm{Gal}(L/K)$ y grupos de ramificación G_i, sea π_L un elemento primo de L; como por la proposición anterior $G_0 = \mathrm{Gal}(L/L_0)$, entonces para todo $\sigma \in G_0$, $\sigma(\pi_L)$ sigue siendo un elemento primo de L y por lo tanto $\sigma\pi_L = u_\sigma \pi_L$ para algún $u_\sigma \in U_L$. Definimos entonces las funciones

$$\psi_{0,L} : G_0 \to \overline{L}^* \qquad \text{y} \qquad \psi_{i,L} : G_i \to L \quad (i \geq 1)$$

mediante

$$\psi_{i,L}(\sigma) := \lambda_{i,L}(\sigma\pi_L/\pi_L) = \lambda_{i,L}(u_\sigma),$$

donde

$$\lambda_{0,L} : U_L \to \overline{L}^* \qquad \text{y} \qquad \lambda_{i,L} : U_L^{(i)} \to L \quad (i \geq 1)$$

son los epimorfismos (véase la demostración de (1.65)) que inducen los isomorfismos de (1.65).

Corolario 1.77. *Sea L/K una extensión finita de Galois de campos locales con grupo de Galois $G = \mathrm{Gal}(L/K)$ y grupos de ramificación G_i. Entonces, las funciones $\psi_{i,L}$ son morfismos con núcleo G_{i+1}. Se sigue que:*

(1) *El grupo G_0/G_1 es isomorfo a un subgrupo de $\overline{L}^*$ (y por lo tanto es cíclico de orden coprimo con $p = \mathrm{car}\,(L)$).*

(2) *Para $i \geq 1$ los cocientes G_i/G_{i+1} son isomorfos a subgrupos del grupo aditivo L (y por lo tanto son abelianos).*

(3) *G_1 es un p-subgrupo de Sylow de G_0.*

DEMOSTRACIÓN. Si π_L es un primo de L entonces, para todo $\sigma \in G = \mathrm{Gal}(L/K)$, $\sigma\pi_L$ sigue siendo un primo de L y por lo tanto $\sigma\pi_L = u_\sigma \pi_L$ para algún $u_\sigma \in U_L$. Así, $u_\sigma = \sigma\pi_L/\pi_L \in U_L$ y tiene sentido definir

$$\psi_{i,L}(\sigma) := \lambda_i(u_\sigma).$$

Para el caso $i = 0$, si $\sigma, \tau \in G_0$ entonces

$$(\sigma\tau)\pi_L = \tau(u_\sigma \pi_L) = \tau(u_\sigma)\tau(\pi_L) = (\tau u_\sigma)u_\tau \pi_L$$

con $u_\sigma, u_\tau \in U_L$. Notemos ahora que $\tau u_\sigma \equiv u_\sigma \pmod{\mathfrak{p}_L}$ ya que $\tau \in G_0$. Se sigue que

$$(\tau\sigma)\pi_L \equiv u_\sigma \cdot u_\tau \pi_L \pmod{\mathfrak{p}_L}$$

y así

$$\psi_{0,L}(\tau\sigma) = \lambda_{0,L}((\tau\sigma)\pi_L/\pi_L) \equiv u_\sigma u_\tau \pmod{\mathfrak{p}_L} \equiv \psi_{0,L}(\tau)\psi_{0,L}(\sigma) \pmod{\mathfrak{p}_L},$$

i.e., $\psi_{0,L}$ es un homomorfismo.

Nótese ahora que el núcleo de $\psi_{0,L}$ consiste de aquellos $\sigma \in G_0$ tales que $u_\sigma \equiv 1 \pmod{\mathfrak{p}_L}$, i.e., tales que $u_\sigma - 1 \in \mathfrak{p}_L$, i.e., $\sigma\pi_L/\pi_L - 1 \in \mathfrak{p}_L$, i.e., $\sigma\pi_L/\pi_L - 1 = t\pi_L$, y por lo tanto $\sigma\pi_L - \pi_L = t\pi_L^2 \in \mathfrak{p}_L^2$, de donde se sigue que $\sigma \in G_1$.

Para $i \geq 1$, el argumento es similar.

Las partes (1), (2) y (3) son consecuencia directa de lo anterior. □

Corolario 1.78. *Toda extensión finita de Galois de campos locales es soluble, i.e., su grupo de Galois $G = \mathrm{Gal}(L/K)$ es soluble.*

DEMOSTRACIÓN. Como $G/G_0 \simeq \mathrm{Gal}(L/K)$, entonces G/G_0 es cíclico. Además, en la filtración

$$\cdots \subseteq G_i \subseteq \cdots \subseteq G_1 \subseteq G_0 \subseteq G$$

los cocientes G_i/G_{i+1} son abelianos por el corolario anterior. □

Corolario 1.79. *Si L/K es una extensión finita mansa de campos locales, entonces no tiene ramificación superior, i.e., si G_i son los grupos de ramificación de $G = \mathrm{Gal}(L/K)$, entonces $G_i = 0$ para $i \geq 1$.*

DEMOSTRACIÓN. En efecto, si L_0 es la mayor extensión no ramificada de K contenida en L y si $p = \mathrm{car}\,(K)$, entonces

$$e = e(L/K) = e(L/L_0)e(L_0/K) = e(L/L_0) = [L : L_0],$$

la penúltima igualdad porque L_0/K es no ramificada y la última igualdad porque L/L_0 es totalmente ramificada. Se sigue que $e = [L : L_0] = |\mathrm{Gal}(L/L_0)| = |G_0|$. Ahora, como para toda $i \geq 1$ se tiene que $G_i \subseteq G_1$ y G_1 es un p-grupo, entonces los G_i, para $i \geq 1$, también son p-grupos que además están contenidos

en G_0, cuyo orden $|G_0| = e$ no es divisible por p porque L/K es mansa. Se sigue que los $G_i = 0$ para $i \geq 1$. □

Los grupos de ramificación de una extensión finita L/K de campos locales se pueden estudiar mediante la siguiente función, donde usamos que $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ por (1.40) y ponemos $G = \mathrm{Gal}(L/K)$:

$$i_G : G \longrightarrow \mathbb{Z}$$

es la función dada por: $i_G(\sigma) := v_L(\sigma\alpha - \alpha)$ si $\sigma \neq 1$. Observemos que $i_G(\sigma)$ es un entero > 0 si $\sigma \neq 1$; se define $i_G(1) = +\infty$. Los números $i_G(\sigma)$ no dependen de la elección del generador α de $\mathcal{O}_L$ ya que si α' es otro generador, entonces $\alpha' = u\alpha$ con $u \in U_K$ y así

$$\begin{aligned} v_L(\sigma\alpha' - \alpha') \quad & v_L(\sigma(u\alpha) - u\alpha) = v_L(u\sigma\alpha - u\alpha) \\ - \quad & v_L(u(\sigma\alpha - \alpha)) = v_L(u) + v_L(\sigma\alpha - \alpha) \\ - \quad & v_L(\sigma\alpha - \alpha). \end{aligned}$$

Lema 1.80. *Los números $i_G(\sigma)$ satisfacen las propiedades siguientes:*

(1) $i_G(\sigma) \geq s + 1$ *si y sólo si* $\sigma \in G_s$.

(2) $i_G(\tau\sigma\tau^{-1}) = i_G(\sigma)$.

(3) $i_G(\sigma\tau) \geq \min\{i_G(\sigma), i_G(\tau)\}$.

Demostración. (1): Por definición de G_s y de i_G, es claro que

$$G_s = \{\sigma \in G \ : \ i_G(\sigma) \geq s + 1\}.$$

(2): Se sigue de (1) y de que los G_s son subgrupos normales de G.

(3): Se sigue de

$$\begin{aligned} i_G(\sigma\tau) \quad & - \quad v_L(\sigma\tau(x) - x) = v_L(\sigma(\tau x - x) + \sigma x - x) \\ & > \quad \min\{v_L(\sigma(\tau x - x)), v_L(\sigma x - x)\} \\ & - \quad \min\{v_L(\tau x - x), v_L(\sigma x - x)\} \quad \text{ya que } v_L(\sigma(y)) = v_L(y) \\ & - \quad \min\{i_G(\tau), i_G(\sigma)\}. \end{aligned}$$

□

Grupos de ramificación y unidades superiores. Los dos resultados siguientes relacionan los grupos de ramificación con los grupos de unidades superiores:

sea L/K una extensión finita de Galois de campos locales y sea L_0 la mayor extensión no ramificada de K contenida en L. Sea π_L un elemento primo de L y sea $G = \mathrm{Gal}(L/K)$.

Proposición 1.81. *Con la notación anterior, si $i \geq 0$ es un entero, entonces un elemento σ del grupo de inercia G_0 pertenece a G_i si y sólo si*

$$\sigma(\pi_L)/\pi_L \equiv 1 \text{ mód } \mathfrak{p}_L^i,$$

i.e., $\sigma \in G_i$ si y sólo si $\sigma(\pi_L)/\pi_L \in U_L^{(i)}$.

DEMOSTRACIÓN. Como $v_L(\sigma(\pi_L)) = v_L(\pi_L)$, entonces $\sigma(\pi_L)/\pi_L \in U_L$. Ahora, como $G_0 = \mathrm{Gal}(L_0/K)$, reemplazando K por L_0 y G por G_0 nos reducimos al caso de una extensión totalmente ramificada L/K. En este caso, por la proposición (1.40) el elemento π_L es tal que $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Se sigue que

$$\begin{aligned} i_G(\sigma) &- v_L(\sigma(\pi_L) - \pi_L) \\ &- v_L(\pi_L(\sigma(\pi_L)/\pi_L - 1)) \\ &- v_L(\pi_L) + v_L(\sigma(\pi_L)/\pi_L - 1) \\ &- 1 + v_L(\sigma(\pi_L)/\pi_L - 1) \end{aligned}$$

y así

$$\begin{aligned} \sigma \in G_i &\Leftrightarrow i_G(\sigma) \geq i + 1 \\ &\Leftrightarrow 1 + v_L(\sigma(\pi_L)/\pi_L - 1) \geq i + 1 \\ &\Leftrightarrow v_L(\sigma(\pi_L)/\pi_L - 1) \geq i \\ &\Leftrightarrow \sigma(\pi_L)/\pi_L - 1 \equiv 0 \text{ mód } \mathfrak{p}_L^i \\ &\Leftrightarrow \sigma(\pi_L)/\pi_L \equiv 1 \text{ mód } \mathfrak{p}_L^i \\ &\Leftrightarrow \sigma(\pi_L)/\pi_L \in U_L^{(i)} = 1 + \mathfrak{p}_L^i. \end{aligned}$$

□

Recordando ahora que $G_{i+1} \lhd G_i$, la proposición anterior se puede refinar para dar información sobre los cocientes G_i/G_{i+1}:

Proposición 1.82. *Sea L/K una extensión finita de campos locales con grupo de Galois G. Sea π_L un elemento primo de L. Entonces, para cada entero*

$i \geq 0$ la función que asigna a cada $\sigma \in G_i$ el cociente $\sigma(\pi_L)/\pi_L \in U_L^{(i)}$ induce por paso al cociente un monomorfismo

$$\vartheta_i : G_i/G_{i+1} \rightarrowtail U_L^{(i)}/U_L^{(i+1)}$$

que no depende del primo π_L elegido.

DEMOSTRACIÓN. Observemos primero que ϑ_i no depende del primo π_L. En efecto, si π' es otro primo de L, entonces $\pi' = u\pi_L$ con $u \in U_L$ y así

$$\sigma(\pi')/\pi' = \sigma(\pi_L)/\pi_L \cdot \sigma(u)/u,$$

y como $\sigma \in G_i$, entonces $v_L(\sigma(u) - u) \geq i + 1$, i.e., $\sigma(u) \equiv u$ mód $\mathfrak{p}_L^{i+1}$, i.e., $\sigma(u) = u + \varepsilon\pi_L^{i+1}$ por lo que $\sigma(u)/u = 1 + \varepsilon'\pi_L^{i+1} \in U_L^{(i+1)}$ con $\varepsilon' = \varepsilon/u \in \mathcal{O}_L$, i.e., $\sigma(u)/u = 1$ en $U_L^{(i)}/U_L^{(i+1)}$. Se sigue que $\sigma(\pi')/\pi' = \sigma(\pi_L)/\pi_L$ en $U_L^{(i)}/U_L^{(i+1)}$ y por lo tanto ϑ_i no depende de la elección de π.

La función ϑ_i es un homomorfismo ya que si $\sigma, \tau \in G_i$, entonces poniendo $u := \tau(\pi)/\pi \in U_L$ observamos que

$$\sigma(u)/u = \frac{\sigma\tau(\pi)/\sigma(\pi)}{\tau(\pi)/\pi},$$

por lo que

$$\sigma\tau(\pi)/\pi = (\sigma(\pi)/\pi)(\tau(\pi)/\pi)(\sigma(u)/u)$$

y por lo que probamos en el párrafo previo $\sigma(u)/u = 1$ en $U_L^{(i)}/U_L^{(i+1)}$ y así

$$\sigma\tau(\pi)/\pi = (\sigma(\pi)/\pi) \cdot (\tau(\pi)/\pi) \quad \text{en } U_L^{(i)}/U_L^{(i+1)},$$

lo cual muestra que ϑ_i es un homomorfismo.

Finalmente, si $\vartheta_i(\sigma) = \sigma(\pi)/\pi = 1$ en $U_L^{(i)}/U_L^{(i+1)}$, entonces $\sigma(\pi)/\pi \in U_L^{(i+1)}$ y así, por la proposición previa $\sigma \in G_{i+1}$, i.e., $\sigma = 1$ en G_i/G_{i+1}, i.e., ϑ_i es inyectiva. □

1.9 Anexo 1: Extensiones de Galois infinitas

Sea k un campo y sea k^s una cerradura separable de k. Sea $G_k := \mathrm{Gal}(k^s/k)$ el grupo de Galois correspondiente. La extensión k^s/k en general es de grado infinito, pero contiene (y de hecho está generada por) todas las extensiones finitas de Galois de k; probaremos en esta sección que

$$\mathrm{Gal}(k^s/k) = \varprojlim_K \mathrm{Gal}(K/k)$$

(el límite inverso de los grupos de Galois de las subextensiones finitas de Galois K/k). Así, $\mathrm{Gal}(k^s/k)$ es el límite inverso de grupos finitos, i.e., es un *grupo profinito* y viene equipado con una topología natural, la *topología de Krull*, donde la identidad $1 \in \mathrm{Gal}(k^s/k)$ tiene una base de vecindades consistente de subgrupos normales, a saber, los subgrupos

$$G_K := \mathrm{Gal}(k^s/K) \subseteq \mathrm{Gal}(k^s/k)$$

donde las K/k son extensiones finitas de Galois contenidas en k^s/k. Es decir, para cada $\sigma \in G_k$ las clases laterales σG_K forman una base de vecindades de σ, donde K/k recorre el conjunto de todas las subextensiones finitas de Galois de k^s/k. Con esta topología, la operación de grupo de $G_k = \mathrm{Gal}(k^s/k)$

$$G_k \times G_k \longrightarrow G_k, \qquad (\sigma, \tau) \mapsto \sigma\tau$$

es continua ya que la imagen inversa de un básico abierto $\sigma\tau G_K$ de $\sigma\tau$ contiene a la vecindad abierta $\sigma G_K \times \tau G_K$ de (σ, τ). Similarmente, la operación

$$G_k \longrightarrow G_k, \qquad \sigma \mapsto \sigma^{-1}$$

es continua, de tal forma que $G_k = \mathrm{Gal}(k^s/k)$ es un grupo topológico y de hecho:

Teorema 1.83 (Krull). *Si Ω/k es una extensión de Galois (finita o infinita), entonces el grupo de Galois $G = \mathrm{Gal}(\Omega/k)$ es Hausdorff y compacto con respecto a la topología de Krull.*

DEMOSTRACIÓN. (1): Sean $\sigma \neq \tau$ en G. Entonces existe una subextensión finita de Galois K/k de Ω/k tal que $\sigma|_K \neq \tau|_K$, es decir, $\sigma\mathrm{Gal}(\Omega/K) \neq \tau\mathrm{Gal}(\Omega/K)$, y por lo tanto $\sigma\mathrm{Gal}(\Omega/K) \cap \tau\mathrm{Gal}(\Omega/K) = \emptyset$ (ya que las clases laterales son disjuntas), i.e., G es Hausdorff.
(2): Para mostrar que G es compacto, consideremos el homomorfismo

$$h : G \longrightarrow \prod_K \mathrm{Gal}(K/k)$$

dado por: $\sigma \mapsto \prod_K \sigma|_K$, donde K/k recorre todas las subextensiones finitas de Galois de $\mathrm{Gal}(\Omega/k)$. Los grupos finitos $\mathrm{Gal}(K/k)$ se consideran discretos (y por lo tanto, compactos), de tal forma que su producto es compacto por el teorema de Tychonoff.

El homomorfismo h es inyectivo ya que $\sigma|_K = 1$ para toda K implica claramente que $\sigma = 1$.

Los conjuntos

$$U = \prod_{K \neq K_0} \mathrm{Gal}(K/k) \times \{\overline{\sigma}\},$$

donde K_0/k es cualquier *subextensión finita* de Galois de Ω/k y $\overline{\sigma} \in \mathrm{Gal}(K_0/k)$, forman una sub-base de vecindades abiertas del producto $\prod_K \mathrm{Gal}(K/k)$.

Ahora, como $\mathrm{Gal}(K_0/k)$ es un cociente de $G = \mathrm{Gal}(\Omega/k)$, si $\sigma \in G$ es un levantamiento de $\overline{\sigma}$, entonces $h^{-1}(U) = \sigma\mathrm{Gal}(\Omega/K_0)$, lo cual muestra que h es un homomorfismo continuo.

Más aún, como $h(\sigma\mathrm{Gal}(\Omega/K_0)) = h(G) \cap U$, entonces h es una aplicación abierta.

Mostraremos que $h(G)$ es cerrado: en efecto, para cada par $L' \supseteq L$ de subextensiones finitas de Galois de Ω/k consideremos el conjunto

$$M_{L'/L} = \left\{ \prod_K \sigma_K \in \prod_K \mathrm{Gal}(K/k) \ : \ \sigma_{L'}|_L = \sigma_L \right\}.$$

Es claro entonces que

$$h(G) = \bigcap_{L' \supseteq L} M_{L'/L}.$$

Mostraremos que cada $M_{L'/L}$ es cerrado: si $\mathrm{Gal}(L/k) = \{\sigma_1, \ldots, \sigma_n\}$ y $S_i \subseteq \mathrm{Gal}(L'/k)$ es el conjunto de extensiones de σ_i a L', entonces

$$M_{L'/L} = \bigcup_{i=1}^{n} \left(\prod_{K \neq L', L} \mathrm{Gal}(K/k) \times S_i \times \{\sigma_i\} \right),$$

lo cual muestra que $M_{L'/L}$ es cerrado; se sigue que $h(G)$ es cerrado y así h es un homeomorfismo de G en un subconjunto cerrado $h(G)$ del producto $\prod_K \mathrm{Gal}(K/k)$ y por lo tanto es compacto. □

Así, dado un campo k, al considerar el grupo de Galois $G_k = \mathrm{Gal}(k^s/k)$ ya estamos considerando todos los grupos de Galois finitos $\mathrm{Gal}(K/k)$, y entonces k^s/k es el objeto más importante en teoría de Galois. Sin embargo, se tiene el problema de que el teorema principal de la teoría de Galois, la correspondencia entre las subextensiones de k^s/k y los subgrupos de $\mathrm{Gal}(k^s/k)$ ya no es válida en su forma usual (véase el ejemplo 24 al final de esta sección) y debe reformularse tomando en cuenta la topología natural (de Krull) de G_k. Luego de esta

consideración, el teorema principal de la teoría de Galois se puede formular ahora como sigue:

Teorema 1.84. *Sea Ω/k una extensión de Galois (finita o infinita) con grupo de Galois $G = \mathrm{Gal}(\Omega/k)$. Entonces:*

(1) *La función*

$$K \longmapsto \mathrm{Gal}(\Omega/K)$$

establece una biyección entre el conjunto de todas las subextensiones K/k de Ω/k y el conjunto de todos los subgrupos cerrados de $G = \mathrm{Gal}(\Omega/k)$. La inversa de esta función es la aplicación

$$H \longmapsto \Omega^H,$$

donde $H \subseteq G = \mathrm{Gal}(\Omega/k)$ es un subgrupo cerrado y $\Omega^H \subseteq \Omega$ es el campo fijo de H.

(2) *Los subgrupos abiertos de $G = \mathrm{Gal}(\Omega/k)$ corresponden a subextensiones finitas de Ω/k.*

DEMOSTRACIÓN. (i): Notemos primero que un subgrupo abierto H de $G = \mathrm{Gal}(\Omega/k)$ también es cerrado ya que es el complemento de la unión de sus clases laterales (que son abiertas) distintas de H en $\mathrm{Gal}(\Omega/k)$.
(ii): Ahora, si K/k es cualquier subextensión de Ω/k y si $\{K_i/k\}$ es la familia de todas las subextensiones finitas de K/k, entonces $K = \bigcup_i K_i$ y por lo tanto

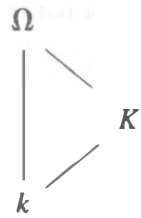
$$\mathrm{Gal}(\Omega/K) = \bigcap_i \mathrm{Gal}(\Omega/K_i),$$

donde las K_i/k recorren las subextensiones finitas de K/k. Ahora, cada K_i está contenido en alguna extensión finita de Galois L_i de k (por ejemplo, en su cerradura normal) y así

$$\mathrm{Gal}(\Omega/K_i) \supseteq \mathrm{Gal}(\Omega/L_i),$$

y por lo tanto cada $\sigma \in \mathrm{Gal}(\Omega/K_i)$ tiene la vecindad abierta $\sigma\mathrm{Gal}(\Omega/L_i) \subseteq \mathrm{Gal}(\Omega/K_i)$ y consecuentemente $\mathrm{Gal}(\Omega/K_i)$ es abierto en G. Por (i) se sigue entonces que $\mathrm{Gal}(\Omega/K_i)$ también es cerrado y así $\mathrm{Gal}(\Omega/K) = \bigcap_i \mathrm{Gal}(\Omega/K_i)$ es cerrado y por lo tanto la función del teorema tiene imagen donde debe.

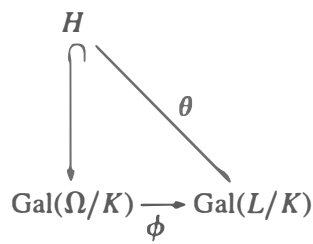
(iii): La función $K \mapsto \mathrm{Gal}(\Omega/K)$ es inyectiva ya que si K es cualquier campo intermedio:



entonces Ω/K también es Galois, y por lo tanto $K = \Omega^{\mathrm{Gal}(\Omega/K)}$. Así, si $\mathrm{Gal}(\Omega/K) = \mathrm{Gal}(\Omega/K')$ entonces

$$K = \Omega^{\mathrm{Gal}(\Omega/K)} = \Omega^{\mathrm{Gal}(\Omega/K')} = K'.$$

(iv): Para la suprayectividad tenemos que probar que si H es un subgrupo cerrado de $\mathrm{Gal}(\Omega/k)$ entonces $H = \mathrm{Gal}(\Omega/K)$, donde $K = \Omega^H$ es el campo fijo de H. Claramente $H \subseteq \mathrm{Gal}(\Omega/K) = \mathrm{Gal}(\Omega/\Omega^H)$. Recíprocamente, sea $\sigma \in \mathrm{Gal}(\Omega/K)$. Si L/K es una subextensión finita de Galois de Ω/K, entonces $\sigma\mathrm{Gal}(\Omega/L)$ es una vecindad abierta básica de σ en $\mathrm{Gal}(\Omega/K)$. Consideremos ahora el diagrama siguiente:



donde observamos que $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\Omega/K)/\mathrm{Gal}(\Omega/L)$ y ϕ es el epimorfismo canónico. Afirmamos que la composición θ es un epimorfismo. En efecto, si $\theta(H) = H \subseteq \mathrm{Gal}(L/K)$, como este último grupo es finito, por teoría de Galois de extensiones finitas existe un campo intermedio $K \subseteq L^{\overline{H}} \subseteq L$ tal que $\mathrm{Gal}(L/L^H) = H$ y se tiene que

$$K \subseteq L^{\overline{H}} = L^H \subseteq \Omega^H = K,$$

por lo que $K = L^{\overline{H}}$ y así $H = \mathrm{Gal}(L/K)$.

Se sigue que, para $\sigma \in \mathrm{Gal}(\Omega/K)$, su imagen $\overline{\sigma} \in \mathrm{Gal}(L/K) - H$ proviene, bajo θ, de un $\tau \in H$, i.e., existe $\tau \in H$ tal que $\tau|_L = \sigma|_L$ y por lo tanto $\tau \in H \cap \sigma\mathrm{Gal}(\Omega/L)$, i.e., $H \cap \sigma\mathrm{Gal}(\Omega/L) \neq \emptyset$ y consecuentemente

σ pertenece a la cerradura de H, i.e., $\sigma \in H$ ya que H es cerrado por hipótesis; se sigue que $H = \mathrm{Gal}(\Omega/K)$, lo cual prueba la suprayectividad requerida, y esto finaliza la demostración de la parte (1).

Para la parte (2), si H es un subgrupo abierto de $\mathrm{Gal}(\Omega/k)$, entonces por la observación al principio de la demostración, H también es cerrado y así es de la forma $H = \mathrm{Gal}(\Omega/K)$. Ahora, $\mathrm{Gal}(\Omega/k)$ es la unión disjunta de las clases laterales abiertas de H y como $\mathrm{Gal}(\Omega/k)$ es compacto, entonces un número finito de estas clases laterales debe cubrir a $\mathrm{Gal}(\Omega/k)$, y como las clases laterales siempre son ajenas entre sí, entonces el número de clases laterales de H en $\mathrm{Gal}(\Omega/k)$ es finito, i.e., $H = \mathrm{Gal}(\Omega/K) \subseteq \mathrm{Gal}(\Omega/k)$ es de índice finito y esto implica que K/k es de grado finito. □

1.9.1 Grupos profinitos

En la sección anterior vimos que el grupo topológico $G = \mathrm{Gal}(\Omega/k)$ tiene la propiedad de que su identidad $1 \in G$ tiene una base de vecindades consistente de subgrupos normales $N \subseteq G$. Esto nos lleva a la definición siguiente:

Definición 1.85. Un *grupo profinito* es un grupo topológico G que es Hausdorff, compacto y tiene una base de vecindades abiertas de la identidad $1 \in G$ consistente de subgrupos normales.

Observaciones: (1). La última condición es equivalente a la condición de que G es totalmente disconexo, i.e., todo elemento de G es su propia componente conexa.

(2). Necesitaremos usar más adelante los hechos siguientes acerca de grupos topológicos en general: sean G un grupo topológico y H la intersección de todas las vecindades del elemento neutro 1 de G. Entonces:

(i) H es un subgrupo de G.

(ii) H es la cerradura $\{1\}$ de $\{1\}$.

(iii) G/H es Hausdorff.

(iv) G es Hausdorff si y sólo si $H = 1$.

La parte (i) se sigue de la continuidad de las operaciones de grupo. Para (ii) se tiene que: $a \in H \Leftrightarrow a \in U$, para todas las vecindades U del $1 \in G$, y esto último sucede si y sólo si $a \in \{1\}$. Notamos ahora que (ii) implica que

las clases laterales de H son cerradas y por lo tanto los puntos son cerrados en G/H, por lo que G/H es Hausdorff. La parte (iv) se sigue de (iii) y (ii).

Ejemplo 20. Además de los grupos de Galois $G = \mathrm{Gal}(\Omega/k)$ anteriores, obviamente los grupos finitos G con la topología discreta, son grupos profinitos. Veremos a continuación que los grupos profinitos generales no están muy lejos de los grupos finitos; de hecho un grupo profinito es el límite inverso (proyectivo) de grupos finitos:

Teorema 1.86. (1) *Si G es un grupo profinito y N recorre la familia de subgrupos normales abiertos de G, entonces*

$$G \simeq \varprojlim_{N} G/N,$$

(isomorfismo y homeomorfismo).

(2) *Recíprocamente, si $\{G_i, f_{ij}\}$ es un sistema inverso de grupos finitos, con la topología discreta, entonces*

$$G = \varprojlim G_i$$

es un grupo profinito.

DEMOSTRACIÓN. Observemos primero que si $H \lhd G$ es un subgrupo abierto normal, como G es compacto N sólo puede tener un número finito de clases laterales en G ya que estas clases laterales forman una cubierta abierta disjunta de G. Así, el cociente G/N es un grupo finito y por lo tanto el límite en (1) es de grupos finitos.

Para demostrar (1), sea G un grupo profinito y sea $\mathcal{N} := \{N_i : i \in I\}$ la familia de abiertos normales de G. Así, cada $G_i := G/N_i$ es un grupo finito. Ordenemos la familia $\mathcal{N}$ (más bien, al conjunto de índices I) mediante: $i \leq j$ si $N_i \supseteq N_j$, de tal forma que $(I, \leq)$ es un *conjunto dirigido* y además tenemos las proyecciones canónicas

$$f_{ij} : G_j = G/N_j \longrightarrow G/N_i = G_i$$

siempre que $i \leq j$. Se tiene entonces un *sistema inverso* $\{G_i, f_{ij}\}$ de grupos finitos y mostraremos que el morfismo natural

$$f : G \longrightarrow \varprojlim_{i \in I} G_i$$

dado por: $\sigma \mapsto \prod_{i\in I} \sigma_i$, donde $\sigma_i := \sigma \mod (N_i)$, es un isomorfismo y un homeomorfismo.

Para comenzar, f es inyectiva ya que su núcleo es la intersección $\bigcap_{i\in I} N_i$, la cual es $\{1\}$ porque G es Hausdorff.

Mostraremos ahora que f es continuo: los conjuntos

$$U_S := \prod_{i\notin S} G_i \times \prod_{i\in S} \{1_{G_i}\}$$

forman una sub-base de vecindades abiertas del 1 en $\prod_{i\in I} G_i$, donde S recorre la familia de subconjuntos finitos de I. Se tiene entonces que

$$f^{-1}(U_S \cap \varprojlim_{i\in I} G_i) = \bigcap_{i\in S} N_i,$$

y por lo tanto f es continua.

Observemos ahora que como G es compacto, la imagen de f es cerrada en $\varprojlim G_i$. Y por otro lado, esta imagen es densa ya que si

$$\overline{\sigma} = \prod_{i\in I} \sigma_i \in \varprojlim G_i$$

y $\overline{\sigma}(U_S \cap \varprojlim G_i)$ es una vecindad abierta básica de $\overline{\sigma}$, entonces podemos elegir un $\sigma \in G$ tal que, bajo el morfismo $G \to G/N_k$ (donde $N_k = \bigcap_{i\in S} N_i$), va a dar a σ_k, de tal forma que $\sigma \mod (N_i) = \sigma_i$ para toda $i \in S$, i.e., $f(\sigma) \in \overline{\sigma}(U_S \cap \varprojlim_i G_i)$. Se sigue que $f(G)$ es denso en $\varprojlim G_i$, y por lo tanto $f(G) = \varprojlim_i G_i$, i.e., f es suprayectiva.

Ahora, como G es compacto, f manda cerrados en cerrados y por lo tanto f es una función abierta. Se sigue que

$$f : G \longrightarrow \varprojlim_{i\in I} G_i$$

es un isomorfismo y un homeomorfismo.

Para (2), sea $\{G_i, f_{ij}\}$ un sistema inverso de grupos finitos. Considerando a los grupos G_i como espacios topológicos discretos y por lo tanto compactos,

se sigue que el grupo $G := \varprojlim_{i \in I} G_i$ es un subgrupo cerrado del grupo topológico $\prod_{i \in I} G_i$, el cual es Hausdorff y compacto y por lo tanto G también es Hausdorff y compacto. Más aún, si

$$U_S = \prod_{i \notin S} G_i \times \prod_{i \in S} H_i,$$

donde S es un subconjunto finito de I y $H_i \lhd G$ es un subgrupo normal, entonces los subgrupos normales

$$U_S \cap G$$

forman una base de vecindades abiertas del $1 \in G$, i.e., G es un grupo profinito. □

Corolario 1.87. *Sea G un grupo profinito. Si H es un subgrupo cerrado de G, entonces*

$$H \simeq \varprojlim_{i} H/H \cap N_i,$$

donde los N_i recorren la familia de subgrupos normales abiertos de G.

DEMOSTRACIÓN. Si U_i es un subgrupo abierto normal de H, entonces $U_i = V_i \cap H$ para alguna vecindad abierta V_i del 1 en G. Ahora, como G es compacto totalmente disconexo, entonces V_i contiene un subgrupo abierto normal N_i, y por lo tanto $N_i \cap H \subseteq U_i$. Hemos mostrado así que la familia $\{N_i \cap H\}$ es *cofinal* en la familia de todos los subgrupos abiertos normales U_i de H. Se sigue que

$$\varprojlim H/H \cap N_i \simeq \varprojlim H/U_i \simeq H.$$

El último isomorfismo es el del teorema anterior. □

Corolario 1.88. *Sea G un grupo profinito. Si H es un subgrupo cerrado de G, entonces*

$$G/H \simeq \varprojlim_{i} G/N_i H,$$

donde N_i recorren la familia de subgrupos normales abiertos de G.

DEMOSTRACIÓN. Mostraremos primero que G/H es *profinito*. Claramente G/H es compacto. Resta mostrar que es totalmente disconexo. Para esto, sea $x \in G - H$ arbitrario. Entonces, para cada $h \in H$ existe una vecindad abierta y compacta $V_h \subseteq H$ que no contiene a x ya que G es totalmente disconexo. Se

sigue entonces que $H \subseteq \bigcup_{h \in H} V_h$ y como H es compacto (porque es cerrado en el compacto G), entonces $H \subseteq V_{h_1} \cup \cdots \cup V_{h_n} =: V$ (una subcubierta finita). Así, V es abierta y compacta y contiene a H pero no a x. Se sigue que G/H es totalmente disconexo.

Habiendo ya mostrado que G/H es profinito, como los subgrupos normales de G/H son de la forma $N_i H/H$ donde los N_i son subgrupos normales de G, entonces, por el teorema anterior aplicado a G/H, tenemos que

$$G/H \simeq \varprojlim_i (G/H)/(N_i H/H) \simeq \varprojlim_i G/N_i H.$$

□

Ejemplos de grupos profinitos

Ejemplo 21. El grupo de Galois $\mathrm{Gal}(\Omega/k)$ de una extensión de Galois Ω/k es un grupo topológico Hausdorff y compacto, por el teorema de Krull, en el cual los subgrupos de la forma $\mathrm{Gal}(\Omega/K)$ (que son normales), para K/k una extensión de Galois finita, forman una base de vecindades abiertas del $1 \in \mathrm{Gal}(\Omega/k)$, i.e., $\mathrm{Gal}(\Omega/k)$ es un grupo profinito y de hecho como

$$\mathrm{Gal}(\Omega/k)/\mathrm{Gal}(\Omega/K) \simeq \mathrm{Gal}(K/k),$$

entonces, por el teorema anterior

$$\mathrm{Gal}(\Omega/k) = \varprojlim_K \mathrm{Gal}(K/k).$$

Ejemplo 22. Si $p \in \mathbb{Z}$ es un primo, entonces los grupos $\mathbb{Z}/p^n\mathbb{Z}$, para $n \in \mathbb{N}$, junto con los morfismos naturales $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ para $n \geq m$, forman un sistema inverso:

$$\cdots \to \mathbb{Z}/p^{m+1}\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^{m-1}\mathbb{Z} \to \cdots \to \mathbb{Z}/p\mathbb{Z}$$

cuyo límite inverso es, por el ejemplo 17 después de (1.59),

$$\mathbb{Z}_p := \varprojlim_m \mathbb{Z}/p^m\mathbb{Z},$$

el cual es un grupo profinito, que de hecho es un anillo: *el anillo de enteros p-ádicos.*

Ejemplo 23. Los grupos (de hecho, anillos) $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, junto con las proyecciones canónicas $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ siempre que $m|n$ (i.e., ordenamos $\mathbb{N}$ mediante la división), forman un sistema inverso cuyo límite

$$\widehat{\mathbb{Z}} := \varprojlim_{m} \mathbb{Z}/m\mathbb{Z}$$

es un grupo profinito, que de hecho es un anillo: *el anillo de Prüfer*, y es la *completación* de $\mathbb{Z}$. Nótese que se tienen isomorfismos

$$\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}.$$

También, si cada natural n se descompone como producto de primos $n = \prod_p p^{n_p}$, entonces, por el teorema chino del residuo, se tiene una descomposición

$$\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p.$$

Ejemplo 24. Si $\mathbb{F}_q$ es un campo finito y $\mathbb{F}_q^{al}$ es una cerradura algebraica de $\mathbb{F}_q$, entonces

$$\mathrm{Gal}(\mathbb{F}_q^{al}/\mathbb{F}_q) \simeq \varprojlim_{n} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$$

donde $n \in \mathbb{N}$. Ahora, sabemos que cada $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ es cíclico de orden n (generado por el automorfismo de Frobenius correspondiente) y así $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$. Se sigue que

$$\mathrm{Gal}(\mathbb{F}_q^{al}/\mathbb{F}_q) \simeq \varprojlim_{n} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim_{n} \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}.$$

Obsérvese ahora que si Fr es el Frobenius de $\mathbb{F}_q^{al}$ y

$$\Phi = \langle \mathrm{Fr} \rangle = \{\mathrm{Fr}^n \ : \ n \in \mathbb{Z}\}$$

es el subgrupo cíclico de $\mathrm{Gal}(\mathbb{F}_q^{al}/\mathbb{F}_q)$ generado por el Frobenius, entonces

$$(\mathbb{F}_q^{al})^{\Phi} = \mathbb{F}_q = (\mathbb{F}_q^{al})^{\mathrm{Gal}(\mathbb{F}_q^{al}/\mathbb{F}_q)},$$

i.e., Φ y $\mathrm{Gal}(\mathbb{F}_q^{al}/\mathbb{F}_q)$ tienen el mismo campo fijo; sin embargo, observamos que mandando al $\mathrm{Fr} \in \Phi$ al $1 \in \mathbb{Z}$ se tiene un isomorfismo $\Phi \simeq \mathbb{Z}$ y así $\Phi \subsetneq \mathrm{Gal}(\mathbb{F}_q^{al}/\mathbb{F}_q)$ ya que $\mathbb{Z} \subsetneq \widehat{\mathbb{Z}}$. El problema es que Φ no es un subgrupo cerrado de $\mathrm{Gal}(\mathbb{F}_q^{al}/\mathbb{F}_q)$. Por esto tiene que corregirse la formulación del teorema principal para extensiones de Galois infinitas.

1.10 Anexo 2: Traza, norma y discriminante

En este anexo recolectamos algunos resultados sobre la norma, traza y discriminante de una extensión de campos que usamos en el texto, tanto en este capítulo como en los restantes. Si K/k es una extensión finita de campos y $n = [K : k]$, dado un elemento $\alpha \in K$ sea $L_\alpha : K \to K$ la función dada por multiplicación por el elemento α, i.e., si $a \in K$ se define $L_\alpha(a) := \alpha \cdot a$. Es fácil ver que L_α es una aplicación k-lineal. Ahora, si $\mathcal{B}$ es una base de K sobre k y si $\mathcal{B}'$ es otra base, sean $[L_\alpha]_\mathcal{B}$ y $[L_\alpha]_{\mathcal{B}'}$ las matrices asociadas a L_α en las bases $\mathcal{B}, \mathcal{B}'$ respectivamente. Si A es la matriz de cambio de base, se tiene que $[L_\alpha]_\mathcal{B} = A^{-1}[L_\alpha]_{\mathcal{B}'}A$. Se sigue que $\det[L_\alpha]_\mathcal{B} = \det[L_\alpha]_{\mathcal{B}'}$ y que $\mathrm{Tr}[L_\alpha]_\mathcal{B} = \mathrm{Tr}[L_\alpha]_{\mathcal{B}'}$, de tal forma que se puede definir $\det(L_\alpha)$ y $\mathrm{Tr}(L_\alpha)$ usando cualquier base de K/k.

Definición 1.89. Si K/k es una extensión finita de campos, dado cualquier elemento $\alpha \in K$, se definen su *norma* $N_{K/k}(\alpha)$ y su *traza* $\mathrm{Tr}_{K/k}(\alpha)$ mediante

$$N_{K/k}(\alpha) := \det(L_\alpha) \qquad \text{y} \qquad \mathrm{Tr}_{K/k}(\alpha) := \mathrm{Tr}(L_\alpha).$$

El lema siguiente resume algunas propiedades elementales de la norma y traza que se siguen directamente de las propiedades del determinante y traza de una matriz:

Lema 1.90. *Sea K/k una extensión finita de campos de grado $n = [K : k]$.*

(1) *Si $\alpha \in K$, entonces $\mathrm{Tr}_{K/k}(\alpha) \in k$ y la función $\mathrm{Tr}_{K/k} : K \to k$ es un morfismo aditivo; más aún, es k-lineal.*

(2) *Si $\alpha \in k$, entonces $\mathrm{Tr}_{K/k}(\alpha) = n\alpha$.*

(3) *Si $\alpha \in K^*$, entonces $N_{K/k}(\alpha) \in k^*$ y la función $N_{K/k} : K^* \to k^*$ es un morfismo multiplicativo.*

(4) *Si $\alpha \in k$, entonces $N_{K/k}(\alpha) = \alpha^n$.*

(5) *Si $\chi(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ es el polinomio característico de L_α, entonces la traza y la norma de α están dadas por*

$$N_{K/k}(\alpha) = (-1)^n b_0 \qquad \text{y} \qquad \mathrm{Tr}_{K/k}(\alpha) = -b_{n-1}.$$

□

El resultado siguiente muestra que si conocemos el polinomio mínimo de un elemento $\alpha \in K$, entonces es fácil calcular la norma y traza de ese elemento.

Proposición 1.91. *Sea K/k una extensión finita de campos de grado $n = [K : k]$. Si $\alpha \in K$ y $p(x) = \mathrm{Irr}(\alpha, k) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ es el polinomio mínimo de α sobre k, entonces*

$$N_{K/k}(\alpha) = (-1)^n a_0^{n/m} \qquad \text{y} \qquad \mathrm{Tr}_{K/k}(\alpha) = -\frac{n}{m}a_{m-1}.$$

DEMOSTRACIÓN. Sea $\varphi : K \to \mathrm{End}_k(K) = \mathrm{Hom}_k(K, K)$ la aplicación $\varphi(\alpha) := L_\alpha$. Es fácil ver que $L_{\alpha+\beta} = L_\alpha + L_\beta$ y que $L_{\alpha\beta} = L_\alpha \circ L_\beta$, de tal forma que φ es un morfismo de anillos. Más aún, si $a \in k$ y $\alpha \in K$, entonces $L_{a\alpha} = aL_\alpha$, de tal forma que φ es k-lineal. Nótese que como el anillo K es un campo, entonces φ es inyectiva ya que no es el morfismo cero. La inyectividad de φ implica que el polinomio mínimo de α y el polinomio mínimo de L_α son iguales.

Ahora, si $\chi(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ es el polinomio característico de L_α, entonces, por el teorema de Hamilton-Cayley, el polinomio mínimo divide al polinomio característico y ambos tienen los mismos factores irreducibles. Así, como $p(x) = \mathrm{Irr}(\alpha, k)$ es irreducible, comparando grados se sigue que

$$\chi(x) = p(x)^{n/m},$$

donde notamos que $m|n$ ya que $m = [k(\alpha) : k]$ y $k(\alpha)$ es un campo intermedio de la extensión K/k (que tiene grado $n = [K : k]$).

Finalmente, por el lema anterior, $N_{K/k}(\alpha) = (-1)^n b_0$ y $\mathrm{Tr}_{K/k}(\alpha) = -b_{n-1}$, y como $\chi(x) = p(x)^{n/m}$, entonces $b_0 = a_0^{n/m}$ y $b_{n-1} = (n/m)a_{m-1}$, de donde se sigue el resultado deseado. □

Corolario 1.92. *Si K/k es una extensión finita y $\alpha, \beta \in K$ tienen el mismo polinomio mínimo, entonces tienen la misma norma y la misma traza.*

□

En ocasiones es fácil obtener el polinomio mínimo de un elemento α y así es fácil calcular su traza y su norma por el resultado anterior. Sin embargo, en otras ocasiones es difícil hallar el polinomio mínimo de un elemento y por lo tanto se necesitan otros métodos para calcular su norma y traza. A continuación veremos que para extensiones de Galois se tiene una descripción de la traza y norma en términos del grupo de Galois correspondiente y como consecuencia obtendremos también una propiedad de transitividad para la norma y la traza. Antes necesitaremos el lema siguiente:

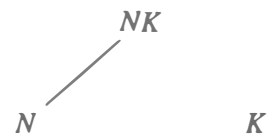
Lema 1.93. *Sea K/k una extensión finita totalmente inseparable.*

(1) *Si $a \in K$, entonces $a^{[K:k]} \in k$.*

(2) *Más generalmente, si N/k es cualquier otra extensión finita de Galois y si $a \in NK$, entonces $a^{[K:k]} \in N$.*

DEMOSTRACIÓN. (1): Sea $n = [K : k]$. Si $a \in K$ y si $\operatorname{car}(k) = p$, como a es totalmente inseparable, entonces el polinomio mínimo de a tiene una sola raíz, i.e., es de la forma $\operatorname{Irr}(a, k) = x^{p^m} - b = (x - a)^{p^m}$, donde $p^m = \operatorname{gr}(\operatorname{Irr}(a, k)) = [k(a) : k]$ y por lo tanto $a^{[k(a):k]} = b \in k$. Así, como $[k(a) : k]$ divide a $[K : k] = n$, entonces $a^n \in k$.

(2): Como N/k es Galois, entonces $N \cap K$ es una extensión separable de k y como K/k es totalmente inseparable, entonces $N \cap K = k$. Por el teorema de las irracionalidades naturales, Artin [2], se sigue que $[NK \,.\, K] = [N : k]$. Por lo tanto, en el diagrama



se tiene que $[NK : N] = [K : k]$.

Finalmente, la extensión NK/N es totalmente inseparable y así, por la parte (1), se debe tener que $a^{[K:k]} = a^{[NK:N]} \in N$ para todo $a \in NK$. □

El resultado principal es:

Teorema 1.94. *Sea K/k una extensión finita de grado n y denotemos su grado de inseparabilidad mediante $[K : k]_i$. Sean $\sigma_1, \ldots, \sigma_r$ los r distintos k-monomorfismos de K en una cerradura algebraica k^{al} de k. Si $a \in K$, entonces:*

$$(1)\ N_{K/k}(a) = \left(\prod_j \sigma_j(a) \right)^{[K:k]_i}$$

$$(2)\ \operatorname{Tr}_{K/k}(a) = [K : k]_i \cdot \sum_j \sigma_j(a).$$

DEMOSTRACIÓN. Recordemos que si S es la cerradura separable de k en K, entonces $r = [S : k]$ y $[K : k]_i = [K : S]$ de tal forma que $r[K : k]_i = [K : k] = n$. Sean $\sigma_1, \ldots, \sigma_r$ los r distintos k-monomorfismos de K en una cerradura algebraica k^{al} de k; para $a \in K$ consideremos el polinomio siguiente (con coeficientes en k^{al}):

$$g(x) := \left(\prod_{j=1}^{r} (x - \sigma_j(a)) \right)^{[K:k]_i}$$

Obsérvese que el grado de $g(x)$ es $r[K : k]_i = [K : k] = n$. Probaremos ahora que:

(i) $g(x) \in k[x]$,
y
(ii) $g(x)$ tiene las mismas raíces que $p(x) = \mathrm{Irr}(a, k)$.

Suponiendo que esto ya ha sido probado, se sigue que $p(x) | g(x)$ y como todas las raíces de $g(x)$ son raíces de $p(x)$, entonces el único factor irreducible de $g(x)$ es $p(x)$ y por lo tanto $g(x) = p(x)^{n/m}$, donde $m = \mathrm{gr}(p(x))$. En la demostración de (1.91) se mostró que $p(x)^{n/m}$ es el polinomio característico $\chi(x)$ del morfismo L_a y consecuentemente $g(x) = \chi(x)$. Por lo tanto, si $g(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$, por (1.91) se tiene que

$$N_{K/k}(a) = (-1)^n c_0 \qquad \text{y} \qquad \mathrm{Tr}_{K/k}(a) = -c_{n-1}.$$

Finalmente, por la definición $(*)$ de $g(x)$ se tiene que

$$c_0 = \left(\prod_{j=1}^{r} (-\sigma_j(a)) \right)^{[K:k]_i} = (-1)^{r[K:k]_i} \left(\prod_{j=1}^{r} \sigma_j(a) \right)^{[K:k]_i}$$

$$c_{n-1} = -[K : k]_i \cdot \sum_{j=1}^{r} \sigma_j(a)$$

lo cual nos da las fórmulas deseadas para la norma (ya que $(-1)^{r[K:k]_i} = (-1)^n$) y para la traza. Resta entonces probar las afirmaciones (i) y (ii).

Comenzamos con (ii): nótese primero que cada raíz $\sigma_j(a)$ de $g(x)$ es una raíz de $p(x)$, ya que cada σ_j es un k-monomorfismo y como $a = \mathrm{id}(a) = \sigma_0(a)$ es raíz de $p(x) = \mathrm{Irr}(a, k)$, entonces también $\sigma_j(a)$ es raíz de $p(x)$ ya que σ_j fija a k. Por otra parte, si $b \in k^{al}$ es una raíz de $p(x)$, entonces, por la unicidad de los campos de descomposición, existe un $\tau : k^{al} \to k^{al}$ tal que $\tau(a) = b$, y

como $\tau|_k$ es uno de los σ_j, digamos $\tau|_k = \sigma_i$, entonces $b = \tau(a) = \sigma_i(a)$, i.e., $b = \sigma_i(a)$ es raíz de $g(x)$. Esto prueba (ii).

Para probar (i), sea N la cerradura normal de S/k. Entonces N/k es Galois y por lo tanto separable. También KN/K es Galois y, por el teorema de las irracionalidades naturales, Artin [2], $[KN : K]$ divide a $[N : S]$. Se sigue que $[KN : N]$ divide a $[K : S] = [K : k]_i$ ya que

$$[KN : N][N : S] = [KN : S] = [KN : K][K : S].$$

Ahora, la extensión KN/N es totalmente inseparable ya que K/S lo es. Por el lema (1.93) previo, para $c \in KN$ se tiene que $c^{[K:k]_i} \in N$.

Por otra parte, como KN es la composición de una extensión de Galois de S y una extensión totalmente inseparable (y por lo tanto normal) de S, entonces KN/S es normal y consecuentemente se tiene que $\sigma_j(K) \subseteq KN$ para toda j, y por lo tanto, ya que $a \in K$, entonces $\sigma_j(a) \in KN$ y como por el lema previo $(KN)^{[K:k]_i} \subseteq N$, se sigue que $\sigma_j(a)^{[K:k]_i} \in N$, i.e., los coeficientes de $g(x)$ están en N. Notemos ahora que si τ es cualquier elemento de $\mathrm{Gal}(k^{al}/k)$, entonces

$$\{(\tau\sigma_1)|_K, \ldots, (\tau\sigma_r)|_K\} = \{\sigma_1, \ldots, \sigma_r\},$$

de tal forma que $\tau(g) = g$ y por lo tanto los coeficientes de $g(x)$ están en el campo fijo de $\mathrm{Gal}(k^{al}/k)$. Observamos ahora que este campo fijo es la cerradura totalmente inseparable de k en k^{al}, ya que k^{al}/k es normal. Se sigue que los coeficientes de g son inseparables sobre k. Por otra parte, como los coeficientes de $g(x)$ están en N y N/k es separable, entonces estos coeficientes de g son separables sobre k y por lo tanto son separables e inseparables sobre k y así deben estar en k, i.e., $g(x) \in k[x]$ como se quería. □

Obsérvese ahora que si K/k es Galois de grado n, entonces, con la notación anterior $r = n$ y $[K : k]_i = 1$ (ya que K/k es separable). El corolario siguiente es entonces inmediato:

Corolario 1.95. *Si K/k es una extensión finita de Galois y $G = \mathrm{Gal}(K/k)$, entonces para todo $a \in K$ se tiene que:*

(1) $N_{K/k}(a) = \prod_{\sigma \in G} \sigma(a).$

(2) $\mathrm{Tr}_{K/k}(a) = \sum_{\sigma \in G} \sigma(a).$ □

Ejemplo 25. Sea k un campo de característica $\neq 2$ y sea $K = k(\sqrt{d})$ para algún $d \in k - k^2$. Entonces $\mathrm{Gal}(K/k) = \{id, \sigma\}$, donde σ es la *conjugación* $\sigma(\sqrt{d}) = -\sqrt{d}$. Entonces

$$N_{K/k}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

y

$$\mathrm{Tr}_{K/k}(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a.$$

Ejemplo 26. Sea k un campo que contiene una raíz primitiva n-ésima de la unidad ω y sea K/k la extensión de grado n dada por $K = k(\sqrt[n]{a})$ con $a \in k - k^n$. Entonces, existe un automorfismo σ de K tal que $\sigma(\sqrt[n]{a}) = \omega\sqrt[n]{a}$ y por lo tanto el orden de σ es n, de tal forma que $\mathrm{Gal}(K/k) = \{\sigma, \sigma^2, \ldots, \sigma^n = id\}$ es cíclico generado por σ. Se tiene entonces que

$$\begin{aligned} N_{K/k}(\sqrt[n]{a}) \qquad & \sigma^0(\sqrt[n]{a})\sigma^1(\sqrt[n]{a}) \cdots \sigma^{n-1}(\sqrt[n]{a}) \\ & \sqrt[n]{a}\,\omega\sqrt[n]{a} \cdots \omega^{n-1}\sqrt[n]{a} \\ & \omega^{n(n-1)/2}(\sqrt[n]{a})^n \\ & \omega^{n(n-1)/2} a. \end{aligned}$$

Obsérvese ahora que si n es impar, entonces $n(n-1)/2$ es múltiplo de n y por lo tanto $\omega^{n(n-1)/2} = 1$. Por otra parte, si n es par entonces $n(n-1)/2$ no es múltiplo de n y así $\omega^{n(n-1)/2} \neq 1$; sin embargo, $\left(\omega^{n(n-1)/2}\right)^2 = 1$ y por lo tanto $\omega^{n(n-1)/2} = -1$. Se sigue que

$$\omega^{n(n-1)/2} = \left\{ \begin{array}{ll} 1 & \text{si } n \text{ es impar} \\ -1 & \text{si } n \text{ es par} \end{array} \right\} = (-1)^{n+1}$$

y así $N_{K/k}(\sqrt[n]{a}) = (-1)^{n+1} a$.

Para la traza observamos que ω es raíz del polinomio

$$\frac{x^n - 1}{x - 1} = 1 + x + \cdots + x^{n-1}$$

y por lo tanto

$$\mathrm{Tr}_{K/k}(\sqrt[n]{a}) = \sqrt[n]{a} + \omega\sqrt[n]{a} + \cdots + \omega^{n-1}\sqrt[n]{a} = (1 + \omega + \cdots + \omega^{n-1})\sqrt[n]{a} = 0.$$

Nótese que este cálculo de la norma y traza de $\sqrt[n]{a}$ se pudo haber hecho observando que el polinomio mínimo de $\sqrt[n]{a}$ es $x^n - a$.

En los ejemplos anteriores calculamos la norma y traza de un elemento primitivo de la extensión K/k, i.e., de un elemento $a \in K$ tal que $K = k(a)$. Si uno quisiera calcular la norma y traza de un elemento $b \in K$ que no genera a K sobre k, nuestros cálculos se podrían complicar; sin embargo, el resultado siguiente nos dice que esto se puede facilitar usando la transitividad de la norma y traza para torres de campos:

Teorema 1.96. *Si $K \supseteq M \supseteq k$ es una torre de extensiones finitas, entonces:*

(1) $N_{K/k} = N_{M/k} \circ N_{K/M}$.

(2) $\mathrm{Tr}_{K/k} = \mathrm{Tr}_{M/k} \circ \mathrm{Tr}_{K/M}$.

DEMOSTRACIÓN. Sea k^{al} una cerradura algebraica de k y sean $\sigma_1, \ldots, \sigma_r$ los r distintos k-monomorfismos de M en k^{al} y sean $\tau_1, \ldots, \tau_s$ los s distintos M-monomorfismos de K en k^{al}. Por la unicidad de los campos de descomposición, podemos extender cada σ_i y cada τ_j a automorfismos $\tilde{\sigma}_i, \tilde{\tau}_j : k^{al} \to k^{al}$. Cada $\tilde{\sigma}_i\tau_j$ es un k-monomorfismo de K en k^{al}; de hecho, cualquier k-monomorfismo ρ de K en k^{al} es de esta forma ya que $\rho|_M : M \to k^{al}$ tiene que ser uno de los σ_i, y por lo tanto la función $\tilde{\sigma}_i^{-1}\rho$ es un k-monomorfismo de K en k^{al} que fija a M y así debe ser de uno de los τ_j, i.e., $\tilde{\sigma}_i^{-1}\rho = \tau_j$ de tal forma que $\rho = \tilde{\sigma}_i\tau_j$ para algún j.

Ahora, si $a \in K$ entonces, por el teorema previo,

$$N_{K/k}(a) = \left(\prod_{i,j} \tilde{\sigma}_i\tau_j(a)\right)^{[K:k]_i} \qquad \text{y} \qquad N_{K/M}(a) = \left(\prod_j \tau_j(a)\right)^{[K:M]_i}$$

de donde se sigue que

$$\begin{aligned} N_{M/k}(N_{K/M}(a)) &= \left(\prod_i \sigma_i \left(\prod_j \tau_j(a)\right)^{[K:M]_i}\right)^{[M:k]_i} \\ &\quad \left(\prod_{i,j} \tilde{\sigma}_i\tau_j(a)\right)^{[K:M]_i[M:k]_i} \\ &\quad \left(\prod \rho(a)\right)^{[K:k]_i} \\ &= N_{K/k}(a). \end{aligned}$$

Un cálculo similar prueba la fórmula para la traza. □

Como una consecuencia de este teorema, se tiene que la existencia de un elemento con traza no cero es un criterio para separabilidad:

Corolario 1.97. *Una extensión finita K/k es separable si y sólo si el morfismo $\mathrm{Tr}_{K/k} : K \to k$ no es el morfismo cero. Más aún, en este caso la traza $\mathrm{Tr}_{K/k}$ es suprayectiva.*

DEMOSTRACIÓN. Si K/k es separable, sea N la cerradura normal de K/k. Por el teorema anterior sabemos que $\mathrm{Tr}_{N/k} \neq 0$ implica que $\mathrm{Tr}_{K/k} \neq 0$, de tal forma que basta probar que $\mathrm{Tr}_{N/k} \neq 0$. Para esto, pongamos $\mathrm{Gal}(N/k) = \{\sigma_1, \ldots, \sigma_n\}$. Entonces, por el corolario (1.95) para $a \in N$ se tiene que

$$\mathrm{Tr}_{N/k}(a) = \sum_j \sigma_j(a),$$

pero como los σ_i son independientes por el teorema de Dedekind, entonces existe un $a \in N$ tal que $\sum_j \sigma_j(a) \neq 0$, i.e., tal que $\mathrm{Tr}_{N/k}(a) \neq 0$.

Recíprocamente, supongamos $\mathrm{Tr}_{K/k} \neq 0$. Si K/k no fuera separable, para comenzar se tendría entonces que car $(k) = p > 0$. Sea S la cerradura separable de k en K. Entonces $S \neq K$ y K/S es una extensión totalmente inseparable, de tal forma que $[K : S] = p^t$ para algún $t \geq 1$.

Ahora, si $a \in K$, por el teorema anterior $\mathrm{Tr}_{K/k}(a) = \mathrm{Tr}_{S/k}\left(\mathrm{Tr}_{K/S}(a)\right)$. Por otra parte, si $\sigma_1, \ldots, \sigma_r$ son los r distintos S-monomorfismos de K en k^{al} entonces, por (1.94),

$$\mathrm{Tr}_{K/S}(a) = [K : S]_i \left(\sum_{j=1}^{r} \sigma_j(a) \right)$$

donde $[K : S]_i = [K : S] = p^t$ con $t \geq 1$ (ya que K/S es totalmente inseparable). Pero como car $(k) = p$ y $[K : S]_i = p^t$, entonces $(*)$ implica que $\mathrm{Tr}_{K/S}(a) = 0$ y por lo tanto

$$\mathrm{Tr}_{K/k}(a) = \mathrm{Tr}_{S/k}\left(\mathrm{Tr}_{K/S}(a)\right) = 0$$

para todo $a \in K$, i.e., $\mathrm{Tr}_{K/k}(a) = 0$ para cualquier $a \in K$, en contradicción con la hipótesis de que $\mathrm{Tr}_{K/k} \neq 0$.

Finalmente, si $\alpha \in K$ es tal que $\mathrm{Tr}_{K/k}(\alpha) = \beta \neq 0$, $\beta \in k$, entonces dado cualquier $\gamma \in k$, como $\beta \neq 0$, podemos escribir $\gamma = \delta\beta$ con $\delta \in k$. Poniendo

$\alpha' := \alpha\delta \in K$ se tiene que

$$\mathrm{Tr}_{K/k}(\alpha') = \mathrm{Tr}_{K/k}(\delta\beta) = \delta \mathrm{Tr}_{K/k}(\alpha) = \delta\beta = \gamma,$$

i.e., $\mathrm{Tr}_{K/k}$ es suprayectiva. □

Observación. En el caso particular cuando se tiene una extensión finita de campos finitos $\mathbb{F}_{q^n}/\mathbb{F}_q$, como estas extensiones son separables, se sigue que la traza $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ es *suprayectiva*. En este caso, también la norma es suprayectiva:

Proposición 1.98. *Si $\overline{L}/K$ es una extensión finita de campos finitos, entonces la norma $N_{\overline{L}/\overline{K}} : \overline{L} \to K$ es suprayectiva.*

Demostración. Si $|K| = q = p^r$ y $n = [\overline{L} : K]$, entonces $|\overline{L}| = q^n$. Como el grupo de Galois $\mathrm{Gal}(L/K)$ es cíclico generado por el automorfismo de Frobenius $\sigma : \alpha \mapsto \alpha^q$, entonces la norma $N = N_{\overline{L}/\overline{K}}$ está dada, para $\alpha \in \overline{L}^*$, por

$$\begin{aligned} N(\alpha) &\prod_{i=0}^{n-1} \sigma^i(\alpha) = \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha) = \alpha\alpha^q\alpha^{q^2}\cdots\alpha^{q^{n-1}} \\ &= \alpha^{1+q+q^2+\cdots+q^{n-1}} \end{aligned}$$

y su núcleo consiste en aquellos $\alpha \in \overline{L}^*$ tales que

$$\alpha^{1+q+q^2+\cdots+q^{n-1}} = \alpha^{(q^n-1)/(q-1)} = 1,$$

y así el núcleo está dado por raíces $(q^n-1)/(q-1)$-ésimas de la unidad y por lo tanto su orden es $\leq (q^n-1)/(q-1)$; se sigue que el orden de su imagen es

$$|\mathrm{Im}\,(N)| = \frac{|\overline{L}^*|}{|\mathrm{Ker}\,(N)|} \geq \frac{|\overline{L}^*|}{(q^n-1)/(q-1)} = \frac{(q^n-1)}{(q^n-1)/(q-1)} = q-1$$

y como K^* tiene orden $(q-1)$ e $\mathrm{Im}\,(N) \subseteq K^*$, entonces $\mathrm{Im}\,(N) = K^*$. □

El discriminante de una extensión. Para finalizar, recordamos el concepto de *discriminante* de una *extensión finita separable* L/K de grado $n = [L : K]$: si $\alpha_1, \ldots, \alpha_n$ es una base de L/K, el *discriminante de esta base* es

$$D(\alpha_1, \ldots, \alpha_n) := \det\left[\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right]_{n\times n} \in K,$$

donde $\mathrm{Tr}_{L/K} : L \to K$ es la *traza* de la extensión.

Recordamos que si L/K es separable de grado n y si N/K es normal tal que $L \subseteq N$ y $\sigma_1, \ldots, \sigma_n : L \rightarrowtail N$ son las n K-inmersiones de L en N, entonces la traza de L/K está dada por

$$\mathrm{Tr}_{L/K}(a) = \sum_{i=1} \sigma_i(a),$$

y $\mathrm{Tr}_{L/K} : L \to K$ es un morfismo aditivo. Se sigue que si $\alpha_1, \ldots, \alpha_n$ es una base de L/K, entonces

$$D(\alpha_1, \ldots, \alpha_n) = [\det(\sigma_i(\alpha_j)]^2$$

ya que si $M := (\sigma_i(\alpha_j))_{n\times n}$ y $A := M^t M = (t_{ij})_{n\times n}$, donde M^t es la matriz transpuesta, como

$$\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = t_{ij},$$

entonces

$$\begin{aligned} D(\alpha_1, \ldots, \alpha_n) &.- \det\left[\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right] = \det(t_{ij}) \\ &- \det(M^t M) = \det(M)^2 = \det[\sigma_i(\alpha_j)]^2. \end{aligned}$$

Proposición 1.99. *Sea L/K una extensión finita separable de grado n y sea $\alpha_1, \ldots, \alpha_n$ una base de L/K.*

(1) *Si $\beta_1, \ldots, \beta_n$ es otra base de L/K, entonces*

$$D(\beta_1, \ldots, \beta_n) = \det(A)^2 D(\alpha_1, \ldots, \alpha_n)$$

donde A es la matriz de cambio de base.

(2) $D(\alpha_1, \ldots, \alpha_n) \neq 0$.

DEMOSTRACIÓN. La matriz $A = (a_{ij})$ está dada escribiendo una base en términos de la otra: $\beta_j = \sum a_{kj}\alpha_k$ y así

$$
\begin{aligned}
D(\beta_1, \ldots, \beta_n) \quad & [\det(\sigma_i(\beta_j))]^2 \\
& [\det(\sum_{k=1}^{n} a_{kj}\sigma_i(\alpha_k))]^2 \\
& \left(\det[\sigma_i(\alpha_k)][a_{jk}]^t\right)^2 \quad \text{por definición de producto} \\
& (\det[\sigma_i(\alpha_k)])^2(\det[a_{jk}])^2 \\
& D(\alpha_1, \ldots, \alpha_n)\det(A)^2.
\end{aligned}
$$

Para (2), recordemos que si N/K es una extensión normal finita que contiene a L, las n K-inmersiones $\sigma_i : L \rightarrowtail N$ están dadas como sigue: como L/K es separable entonces, por el teorema del elemento primitivo, existe un elemento $\gamma \in L$ tal que $L = K(\gamma)$ y si $m(x) = \text{Irr}(\gamma, K)$ es el mónico irreducible de γ, entonces $\text{gr}(m(x)) = n = [L : K]$ y $m(x)$ es separable por lo que tiene exactamente n raíces distintas: $\gamma = \gamma_1, \ldots, \gamma_n$ en N. Se define entonces $\sigma_i : L \rightarrowtail N$ mediante $\sigma_i(\gamma) := \gamma_i$.

Ahora, para la base $1, \gamma, \ldots, \gamma^{n-1}$ de L/K se tiene, usando el determinante de Vandermonde

$$D(1, \gamma, \ldots, \gamma^{n-1}) = [\det(\sigma_i(\gamma^j))]^2 = \prod_{i>j}(\sigma_i(\gamma) - \sigma_j(\gamma)) \neq 0$$

(es distinto de cero porque $\sigma_i(\gamma) = \gamma_i \neq \gamma_j = \sigma_j(\gamma)$ cuando $i \neq j$).

Finalmente, el resultado se sigue de la parte (1). □

La parte (1) de la proposición anterior nos dice que para cualesquiera dos bases de L/K sus discriminantes son iguales módulo cuadrados, i.e., son iguales en el grupo cociente $K^*/(K^*)^2$:

Definición 1.100. Si L/K es una extensión finita separable, el *discriminante de la extensión* es la clase lateral

$$\Delta_{L/K} := D(\alpha_1, \ldots, \alpha_n) \in K^*/(K^*)^2,$$

para cualquier base $\alpha_1, \ldots, \alpha_n$ de L/K.

1.11 Ejercicios

1. Demuestre que si K es un campo de car $(K) = p > 0$, entonces cualquier valor absoluto de K es ultramétrico.
2. Demuestre que, en la métrica inducida por un valor absoluto ultramétrico, todo "triángulo" es isósceles y todo punto interior de una bola abierta es un centro de la bola.
3. Sea $\phi : \mathbb{Q}_p \to \mathbb{Q}_q$ un isomorfismo y un homeomorfismo. Demuestre que $p = q$.
4. Sea K, v un campo valuado discreto y $\mathfrak{p}_K$ su ideal máximo. Defina la topología $\mathfrak{p}_K$-ádica en K tomando los conjuntos $\alpha + \mathfrak{p}_K^n$ $(n \geq 0)$ como vecindades abiertas de $\alpha \in K$. Demuestre que la completación de K con respecto a la topología $\mathfrak{p}_K$-ádica coincide con la completación $\widehat{K}$ de K con respecto a la valuación v.
5. Demuestre que un campo valuado discreto completo no es numerable.
6. Sea $\alpha \in \mathbb{Q}_p$ una raíz del polinomio $f(x) = x^p - x - 1 \in \mathbb{Q}_p[x]$. Demuestre que $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ es una extensión normal y no ramificada de grado p.
7. Si $u \in U_{\mathbb{Q}_p}$ es una unidad y β es una raíz del polinomio $g(x) = x^p - x - u \in \mathbb{Q}_p[x]$, demuestre que $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha)$ con α como en el ejercicio anterior.
8. Demuestre que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. En particular, demuestre que dados $\alpha \in \mathbb{Z}_p$ y $n \geq 1$, existe un $a \in \mathbb{Z}$ con $0 \leq a \leq p^n - 1$ tal que $|\alpha - a|_p \leq p^{-n}$. Más aún, este a es único con las propiedades anteriores.
9. Demuestre que para todo $\alpha \in \mathbb{Z}_p$ existe una sucesión $\{a_n\}$ en $\mathbb{Z}$ (con la valuación p-ádica) tal que $\lim_{n\to\infty} \{a_n\} = \alpha$ y tal que:
   - $0 \leq a_n \leq p^n - 1$.
   - $a_n \equiv a_{n-1}$ (mód p^{n-1}), para todo n.
   - La sucesión $\{a_n\}$ anterior es única con las propiedades anteriores.
10. Demuestre que $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, es decir, demuestre que para todo $\alpha \in \mathbb{Q}_p$ existe un entero $n \geq 0$ tal que $p^n \alpha \in \mathbb{Z}_p$.
11. Si $\alpha, \beta \in \mathbb{Q}_p$, demuestre que $|\alpha - \beta|_p \leq p^{-n}$ si y sólo si $\alpha - \beta \in p^n \mathbb{Z}_p$.
12. Considere el primo $p = 7$ y considere las congruencias

$$x^2 \equiv 2 \text{ mód } 7^n.$$

    - Para $n = 1$ observe que la congruencia $x^2 \equiv 2$ mód 7 tiene las soluciones $x \equiv 3$ mód 7 y $x \equiv -3$ mód 7.
    - Para $n = 2$ observe que cualquier solución de la congruencia $x^2 \equiv 2$ mód 7^2 al reducirla módulo 7 debe dar una solución de

la congruencia $x^2 \equiv 2 \mod 7$. Encuentre las soluciones de la congruencia $x^2 \equiv 2 \mod 7^2$.

- Demuestre que para cada $n \geq 1$ la congruencia $x^2 \equiv 2 \mod p^n$ tiene a lo más dos soluciones.
- Demuestre que dada una solución a_n de la congruencia $x^2 \equiv 2 \mod 7^n$, existe una única solución a_{n+1} de la congruencia $x^2 \equiv 2 \mod 7^{n+1}$ tal que $a_{n+1} \equiv a_n \mod 7^n$.
- Calcule algunos términos de la sucesión $\{a_n\}$ de soluciones de la congruencia $x^2 \equiv 2 \mod 7^n$; digamos muestre que

$$\{a_n\} = (3, 10, 108, 2166, \dots).$$

- Demuestre que la sucesión $\{a_n\}$ anterior es de Cauchy en la valuación 7-ádica.
- Sea $\alpha := \lim_{n\to\infty} \{a_n\} \in \mathbb{Q}_7$. Demuestre que $\alpha \in \mathbb{Q}_7$ es una raíz de la ecuación $x^2 = 2$, i.e. $\alpha = \sqrt{2} \in \mathbb{Q}_7$. Se sigue que el campo $\mathbb{Q}_7$ contiene propiamente a $\mathbb{Q}$.

13. En forma análoga, demuestre que la ecuación $x^2 + 1 = 0$ tiene una solución en $\mathbb{Q}_5$, i.e, que $i = \sqrt{-1} \in \mathbb{Q}_5$. Sin embargo, muestre que $x^2 + 1 = 0$ no tiene una solución en $\mathbb{Q}_7$.
14. Demuestre que para cada primo p, la inclusión $\mathbb{Q} \subseteq \mathbb{Q}_p$ es propia.
15. Sea $p^n : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ el morfismo de grupos abelianos dado por $\alpha \mapsto p^n\alpha$. Demuestre que para todo $n \geq 1$ se puede definir un homomorfismo $\varphi : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ tal que la sucesión de grupos abelianos siguiente es exacta:

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varphi} \mathbb{Z}/p^n\mathbb{Z} \to 0.$$

Se sigue que $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

16. Sea p un primo racional y $|\ |_p$ el valor absoluto p-ádico.
    - Sea m un número natural. Demuestre que $|m!|_p = p^{-M}$, donde $M = [m/p] + [m/p^2] + [m/p^3] + \cdots$, $[\ ]$ la función *mayor entero*.
    - Concluya de lo anterior que si $|\ |$ es el valor absoluto usual, entonces $|m!| > p^{-m/(p-1)}$.
    - Poniendo $m = a_0 + a_1 p + \cdots + a_T p^T$ con $0 \leq a_i < p$, suponga que $m! = p^M \cdot N$, donde $p \nmid N$. Demuestre que

$$(p-1)M = m - \sum_{i=0}^{T} a_i$$

y que

$$N \equiv (-1)^M \prod_i (a_i!) \text{ (mód } p).$$

17. Sea $K, |\ |_v$ un campo valuado no arquimediano y sean A el anillo de sucesiones de Cauchy en K y M el ideal (máximo) de A de sucesiones que convergen a 0 (véase la demostración del teorema (1.11)). Si $(a_n) \in A - M$ demuestre que la sucesión de números reales $|a_n|_v$ se estaciona, i.e., existe un $N \in \mathbb{N}$ tal que $|a_n|_v = |a_m|_v$ para todo $m, n \geq N$.
18. **(Lema de Krasner).** Si $K, |\ |_v$ es un campo no arquimediano completo, L/K es finita de Galois y $\alpha, \alpha' \in L$ son conjugados sobre K, demuestre que para todo $a \in K$ se tiene que

$$|a - \alpha|_L \geq |\alpha - \alpha'|_L.$$

19. Sea $K, |\ |_v$ un campo no arquimediano completo. Si $f(x) \in \mathcal{O}_K[x]$ es un polinomio con discriminante d y si $\alpha \in \mathcal{O}_K$ satisface que $|f(\alpha)|_v < |d|^2$, use el lema de Hensel para mostrar que $f(x)$ tiene una raíz en $\mathcal{O}_K$. *Sugerencia*: Use el hecho de que el discriminante d de un polinomio $f(x)$ se puede escribir como $d = u(x)f(x) + v(x)f'(x)$ con $u(x), v(x) \in \mathcal{O}_K[x]$.
20. Demuestre que la conjetura de Fermat es falsa localmente, es decir, si $p \geq 3$ es cualquier primo impar, demuestre que para todo campo q-ádico $\mathbb{Q}_q$ existen enteros $\alpha, \beta, \gamma \in \mathbb{Z}_q \setminus \{0\}$ tales que

$$\alpha^p + \beta^p = \gamma^p.$$

Sugerencias: Como p es impar, cambiando γ por $-\gamma$ basta probar que la ecuación $\alpha^p + \beta^p + \gamma^p = 0$ tiene soluciones no triviales en $\mathbb{Z}_q$. Se tienen entonces dos casos: si $q \neq p$, considere el polinomio $f(x)$ $x^p + q^p + (-1)^p$, su reducción $\overline{f}(x)$ en $\mathbb{F}_q[x]$ y observe que

$$f(x) = x^p - \overline{1} = (x - \overline{1})(x^{p-1} + x^{p-2} + \cdots + x + \overline{1}),$$

donde $\overline{1}$ no es raíz del segundo factor ya que $p \neq q = \text{car}\,(\mathbb{F}_q)$; por lo tanto, existe $\overline{\alpha} \in \mathbb{F}_q \setminus \{\overline{1}\}$ tal que $\overline{f}(\overline{\alpha}) = 0$. Use entonces el lema de Hensel. En el segundo caso, $q = p$, de nuevo considere el polinomio $f(x) = x^p + p^p + (-1)^p$ y su derivada $f'(x) = px^{p-1}$. Muestre que $|f(1)|_p = |p^p|_p = p^{-p}$ y $|f'(1)|_p = |p|_p = p^{-1}$, por lo que $|f(1)|_p = p^{-p} < p^{-2} = |f'(1)|_p^2$ ya que $p \geq 3$. Aplique entonces el lema de Hensel (1.21).

21. Sea k un campo perfecto de característica $p > 0$. Muestre que toda extensión finita totalmente inseparable del campo $k((T))$ es isomorfa a una extensión de la forma $k((T^{q^{-1}}))$, donde q es una potencia de p.
22. Sea $K, |\ |_v$ un campo local con valor absoluto normalizado (i.e., $|a|_v = q^{-v(a)}$, donde q es el orden del campo residual K) y sea μ una medida de Haar en el grupo aditivo de K (que es localmente compacto por (1.60)). Demuestre que para todo subconjunto medible $E \subseteq K$ y para todo $\alpha \in K$ se tiene que

$$\mu(\alpha E) = |\alpha|_v \cdot \mu(E).$$

Sugerencias: Suponga primero que $\alpha \neq 0$ y muestre que la homotecia $L_\alpha : \beta \mapsto \alpha\beta$ es un automorfismo del grupo aditivo de K y concluya entonces que L_α transforma la medida de Haar μ en uno de sus múltiplos $m(\alpha)\mu$. Después muestre que el factor $m(\alpha)$ es precisamente $|\alpha|_v$. Para esto último, como $m(\alpha)$ y $|\alpha|_v$ son multiplicativos, observe que se puede asumir que $\alpha \in \mathcal{O}_K$. Entonces, tomando $E = \mathcal{O}_K$ verifique que $E = \mathcal{O}_K$ es la unión de $|\mathcal{O}_K/\alpha\mathcal{O}_K|$ clases laterales módulo αE y por lo tanto $\mu(E) = |\mathcal{O}_K/\alpha\mathcal{O}_K|\mu(\alpha E)$, y así $m(\alpha) = |\mathcal{O}_K/\alpha\mathcal{O}_K|^{-1}$. Finalmente, como $|\mathcal{O}_K/\alpha\mathcal{O}_K| = q^{v(\alpha)}$ se sigue que

$$m(\alpha) = q^{-v(\alpha)} = |\alpha|_v.$$

23. Usando el ejercicio anterior y la demostración del corolario (1.69), demuestre que si K es un campo local de característica $p \geq 0$ y $m \geq 1$ es un entero coprimo con p (arbitrario si $p = 0$) entonces

$$[K^* : K^{*m}] = m[U_K : U_K^m] = mq_K^{v_K(m)}|\mu_m(K)|,$$

donde q_K es el orden del campo residual de K, $\mu_m(K)$ es el grupo de raíces m-ésimas de la unidad en K y v_K es la valuación de K. *Sugerencia*: Muestre que $[U_K^{(i)} : U_K^{(i+v_K(m))}] = q_K^{v_K(m)}$.
24. Si $p \neq 2$ es un primo impar y $b \in (\mathbb{Z}_p)^*$ es una unidad tal que existe un entero $\alpha \in \mathbb{Z}_p$ que satisface $\alpha^2 \equiv b$ mód $p\mathbb{Z}_p$, demuestre que b es el cuadrado de un elemento de $(\mathbb{Z}_p)^*$. *Sugerencia*: aplique el lema de Hensel a $x^2 - b$. Usando lo anterior, demuestre que $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 4$. Calcule el índice de $(\mathbb{Q}_2^*)^2$ en $\mathbb{Q}_2^*$.
25. Sea L/K una extensión finita de campos valuados discretos completos tal que la extensión de campos residuales L/K es separable.

(i) Demuestre que existe un campo intermedio L_1 de L/K tal que L_1/K es mansa y para todo campo intermedio M de L/K se tiene que M/K es mansa si y sólo si $M \subseteq L_1$.

(ii) Si car $(K) = p > 0$, demuestre que $[L : L_1]$ es una potencia de p.

(iii) Si L/K es normal y $G = \mathrm{Gal}(L/K)$, demuestre que L_1/K es normal y L_1 es el campo fijo del grupo de ramificación G_1 de G.

(iv) Observe que, por la parte (3) del corolario (1.58), la composición de todas las subextensiones finitas mansas de K contenidas en una cerradura algebraica fija K^{al} de K es también es mansa. Esta composición se denota K_{mr} y se llama la *máxima extensión mansa* de K. Su maximalidad implica que K_{mr}/K es Galois. Demuestre que si car $(K) = p > 0$, entonces

$$\mathrm{Gal}(K_{mr}/K) \simeq \prod_{q \neq p} \mathbb{Z}_q.$$

26. Demuestre que, en general, la composición de dos extensiones totalmente ramificadas L_1/K y L_2/K no es totalmente ramificada.

27. Sea L/K una extensión totalmente ramificada de campos valuados discretos completos y sea π_L un primo de L. Demuestre que

$$f(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (x - \sigma\pi_L)$$

es el polinomio de Eisenstein de π_L sobre K.

28. Muchas cuestiones de análisis en campos no arquimedianos completos $K, |\ |_v$ (de característica 0) son más sencillas que sus contrapartes en $\mathbb{R}$ ó $\mathbb{C}$. Los resultados siguientes son en ese sentido:

(i) El rearreglo de series y la suma de series dobles es fácil: si $a_{ij} \in K$, $i, j = 0, 1, 2, \ldots$, supongamos que para todo real $\varepsilon > 0$ existe un real $N(\varepsilon)$ tal que $|a_{ij}|_v < \varepsilon$ siempre que máx$(i, j) \geq N(\varepsilon)$. Demuestre que las dos series siguientes convergen y sus sumas son iguales:

$$\sum_i \left(\sum_j a_{ij} \right) \quad \text{y} \quad \sum_j \left(\sum_i a_{ij} \right).$$

(ii) Dada una serie de potencias con coeficientes $a_i \in K$:

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

se puede definir su *radio de convergencia* R como

$$R := \frac{1}{\limsup_{n\to\infty} |a_n|_v^{1/n}}$$

de tal forma que $0 \leq R \leq \infty$, todo esto en analogía con los casos usuales de $\mathbb{R}$ ó $\mathbb{C}$. Sea $D_f \subseteq K$ el conjunto de los elementos $a \in K$ tal que la serie $f(x)$ converge. Demuestre que:

- Si $R = 0$, entonces $D_f = \{0\}$.
- Si $R = \infty$, entonces $D_f = K$.
- Si $0 < R < \infty$ y si $|a_n|_v R^n \to 0$, entonces

$$D_f = \{a \in K \ : \ |a|_v \leq R\}.$$

- Si $0 < R < \infty$ y si $|a_n|_v R^n \not\to 0$, entonces

$$D_f = \{a \in K \ : \ |a|_v < R\}.$$

Observe que si R no está en la imagen de $|\ |_v : K \to \mathbb{R} \cup \{\infty\}$, entonces los dos conjuntos D_f anteriones son iguales.

(iii) El resultado siguiente muestra que la técnica de continuación analítica en términos de series de potencias que se usa en la teoría de funciones de variable compleja no se transfiere en forma directa al análisis no arquimediano, de tal forma que tuvieron que elaborarse otras técnicas de continuación analítica, debidas a Krasner (*quesos suizos*) y Tate (*espacios rígidos*). El resultado a que nos referimos es el siguiente: Sea $f(x) = \sum_{j=0}^{\infty} a_j x^j$ una serie de potencias con los $a_j \in K$ y sea D_f su dominio de convergencia. Si $\alpha \in D_f$, para cada $0 \leq m < \infty$ pongamos

$$b_m := \sum_{j \geq m} \binom{j}{m} a_j \alpha^{j-m}.$$

Entonces, la serie

$$g(x) := \sum_{m=0}^{\infty} b_m x^m$$

tiene dominio de convergencia D_f y además

$$f(a + \alpha) = g(a)$$

para todo $a \in D_f$. *Sugerencia*: Primero note que $g(x)$ claramente converge y luego, dado $a \in D_f$, evalúe $f(a + \alpha)$ observando que queda una suma doble y entonces use el inciso (i) anterior. Esto muestra que $D_g \supseteq D_f$. Luego invierta los papeles de f y g.

(iv) Usando el inciso anterior, muestre que una función $f(x)$ definida por una serie de potencias con coeficientes en K es continua en su dominio de convergencia.

(v) El teorema siguiente muestra el marcado contraste con la situación usual de $\mathbf{R}$ ó $\mathbb{C}$:

Teorema (Strassmann). *Sea $K, |\ |_v$ un campo no arquimediano completo y sea*

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

una serie de potencias con los $a_i \in K$. Supongamos que $\{a_i\} \to 0$ de tal forma que $f(x)$ converge en $\mathcal{O}_K$, pero que no todos los a_i son 0. Entonces, existe a lo más un número finito de elementos $\alpha \in \mathcal{O}_K$ tales que $f(\alpha) = 0$. Más precisamente, existen a lo más N tales α, donde N es el entero definido por

$$(*) \qquad |a_N|_v = \max |a_i|_v \qquad \text{y} \qquad |a_i|_v < |a_N|_v \quad \text{para } i > N.$$

DEMOSTRACIÓN. Por inducción sobre N. Si $N = 0$ y $f(\alpha) = 0$ para algún $\alpha \in \mathcal{O}_K$, entonces

$$a_0 = -\sum_{n \geq 1} a_n \alpha^n,$$

lo cual es una contradicción ya que la desigualdad de $(*)$ y $N = 0$ implican que

$$\left| \sum_{n \geq 1} a_n \alpha^n \right|_v \leq \max_{n \geq 1} |a_n \alpha^n|_v \leq \max_{n \geq 1} |\alpha^n|_v < |a_0|_v.$$

Supongamos ahora que $N > 0$ y que $f(\alpha) = 0$ con $\alpha \in \mathcal{O}_K$. Sea $b \in \mathcal{O}_K$. Entonces

$$f(b) = f(b) - f(\alpha) = \sum a_n (b^n - \alpha^n) = (b - \alpha) \sum_{n \geq 1} \sum_{j < n} a_n b^j \alpha^{n-1-j}.$$

Por (i) podemos rearreglar esta suma en potencias de b de tal forma que

$$f(b) = (b - \alpha)g(b),$$

donde $g(x) = \sum b_j x^j$ con los $b_j = \sum_{r \geq 0} a_{j+1+r}\alpha^r$. De $(*)$ se sigue que

$$\begin{aligned} |b_j|_v &< |a_N|_v \qquad \text{para todo } j \\ |b_{N-1}|_v &= |a_N|_v \\ |b_j|_v &< |a_N|_v \qquad \text{para } j > N-1. \end{aligned}$$

Por lo tanto, la serie $g(x)$ satisface las hipótesis del teorema pero con $N-1$ en lugar de N. Por hipótesis de inducción, $g(x)$ tiene a lo más $N-1$ ceros $b \in \mathcal{O}_K$ y como $f(c) = 0$ implica que $c = \alpha$ ó $g(c) = 0$, entonces $f(x)$ tiene a lo más N ceros, como se deseaba. □

(vi) Sean $f(x), g(x)$ dos series de potencias con coeficientes en K tales que convergen en $\mathcal{O}_K$ y además $f(\alpha) = g(\alpha)$ para un número infinito de $\alpha \in \mathcal{O}_K$. Use el teorema de Strassmann para mostrar que $f(x) = g(x)$, i.e., ambas series tienen los mismos coeficientes.

(vii) Supongamos ahora que car $(K) = 0$ y sea $f(x)$ una serie de potencias con coeficientes en K que converge en $\mathcal{O}_K$. Use el teorema de Strassmann para mostrar que si $f(x)$ es periódica, entonces es constante.

(viii) Determine el dominio de convergencia D_E y D_L en $\mathbb{Q}_p$ de las series siguientes:

$$\exp_p(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots$$

$$\log_p(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots + (-1)^{n+1}\frac{x^n}{n} + \cdots$$

- Muestre que si $a, b \in D_E$, entonces $\exp_p(a+b) = \exp_p(a)\exp_p(b)$.
- Muestre que si $a, b \in 1 + p\mathbb{Z}_p$, entonces $\log_p(ab) = \log_p(a) + \log_p(b)$.

Sugerencia: La convergencia de $\log_p$ es fácil. Para $\exp_p$ use el primer inciso del ejercicio 16.

29. Sea $K/\mathbb{Q}_p$ una extensión finita y sean $\mathcal{O}_K$ su anillo de enteros y $\mathfrak{p}_K$ su ideal máximo. Extienda la definición de las series $\exp_p$ y $\log_p$ del inciso anterior

a K. Sea $e = e(K/\mathbb{Q}_p)$. Demuestre que, para $n > \dfrac{e}{p-1}$, las series $\exp_p$ y $\log_p$ anteriores inducen isomorfismos continuos, inversos uno del otro:

$$\mathfrak{p}_K^n \xrightarrow{\exp_p} U_K^{(n)} \qquad \text{y} \qquad \mathfrak{p}_K^n \xleftarrow{\log_p} U_K^{(n)}.$$

Capítulo 2

El morfismo de reciprocidad para campos locales

En este capítulo estudiaremos los grupos de Galois de las extensiones (de Galois) de un campo local K, en particular de la extensión K_s/K dada por una cerradura separable de K que, como sabemos, contiene a todas las extensiones finitas de Galois de K. En este sentido, el objetivo es tratar de determinar la estructura del grupo de Galois $G_K := \mathrm{Gal}(K_s/K)$. La teoría que desarrollaremos determinará el grupo G_K módulo su grupo conmutador, i.e., la abelianización G_K^{ab} del grupo G_K, de tal forma que sólo obtendremos información sobre las extensiones abelianas de K. Esto se hará estableciendo una correspondencia entre las extensiones abelianas L de K y ciertos subgrupos del grupo multiplicativo K^*, dados por el morfismo de norma $N_{L/K}$. Esta correspondencia está dada por el *morfismo de reciprocidad de Artin*:

$$(\ ,L/K) : K^* \longrightarrow \mathrm{Gal}(L/K)^{ab}$$

que construiremos usando el método de Neukirch [30]. Comenzamos estudiando la norma $N_{L/K}$ en extensiones cíclicas de grado primo.

2.1 La norma en campos locales

En esta sección, siguiendo a Hasse [15], estudiamos el morfismo de norma $N_{L/K} : L \to K$ para extensiones de campos locales, en especial su acción en los grupos de unidades superiores respectivos, enfocándonos al caso de *extensiones cíclicas L/K de grado primo*, donde después de un análisis detallado de la acción de la norma en los grupos de unidades superiores, se obtendrá como una consecuencia importante que, cuando L/K es cíclica de grado primo ℓ, entonces el grupo cociente $K^*/N_{L/K}L^*$ es cíclico de grado $\ell = [L : K]$; éste es un resultado importante que incluye las llamadas dos desigualdades

fundamentales, que después se generalizará en (2.30) al caso cuando L/K es abeliana, para probar que $[K^* : N_{L/K}L^*] = [L : K]$, por una reducción al caso cíclico anterior.

Los lemas siguientes nos serán de utilidad para estudiar el morfismo de norma y para comparar filtraciones:

Lema 2.1. *Sean A y B grupos abelianos filtrados por subgrupos A_n y B_n respectivamente, $n \geq 0$:*

$$A = A_0 \supseteq A_1 \supseteq \cdots \qquad B = B_0 \supseteq B_1 \supseteq \cdots .$$

Supongamos además que A y B son completos y Hausdorff en las topologías definidas por estas filtraciones (i.e., los morfismos canónicos $A \to \varprojlim A/A_n$ y $B \to \varprojlim B/B_n$ son isomorfismos, en particular $\bigcap_{n\geq 0} A_n = 0$ y $\bigcap_{n\geq 0} B_n = 0$).

Sea $u : A \to B$ un morfismo de grupos filtrados, i.e., un homomorfismo de grupos tal que $u(A_n) \subseteq B_n$ para toda $n \geq 0$. Sean

$$\tilde{u}_n : A_n/A_{n+1} \longrightarrow B_n/B_{n+1}$$

los morfismos inducidos por paso al cociente. Entonces:

(1) *Si los $\tilde{u}_n$ son suprayectivos para toda $n \geq 0$, entonces u también lo es.*

(2) *Si los $\tilde{u}_n$ son inyectivos para toda $n \geq 0$, entonces u también es inyectivo.*

DEMOSTRACIÓN. (1): Sea $b \in B$ arbitrario. Como $\tilde{u}_0 : A_0/A_1 \twoheadrightarrow B_0/B_1$ es suprayectivo, entonces existe un $a_0 \in A_0$ tal que $u(a_0) - b = b_1 \in B_1$. Ahora, para este $b_1 \in B_1$ como $\tilde{u}_1 : A_1/A_2 \twoheadrightarrow B_1/B_2$ es suprayectivo, entonces existe un $a_1 \in A_1$ tal que $u(a_1) + b_1 = b_2 \in B_2$ y por lo tanto

$$u(a_0 + a_1) - b = u(a_0) - b + u(a_1) = b_1 + u(a_1) = b_2 \in B_2.$$

Continuando de esta forma construimos dos sucesiones: $\{a_n\}$ en A y $\{b_n\}$ en B, tales que la serie $a_0 + a_1 + \cdots$ converge a un elemento $a \in A$ porque A es completo y Hausdorff. Más aún, como $u(a) - b \in B_n$ para todo $n \geq 0$ y como $\bigcap_{n\geq 0} B_n = 0$, entonces $u(a) = b$.

(2): Mostraremos por inducción que $\mathrm{Ker}\,(u) \subseteq A_n$ para toda $n \geq 0$. En efecto, como $\tilde{u}_n : A_n/A_{n+1} \rightarrowtail B_n/B_{n+1}$ es inyectivo, entonces

$$\mathrm{Ker}\,(u) \cap A_n = \mathrm{Ker}\,(u) \cap A_{n+1},$$

y por lo tanto $\mathrm{Ker}\,(u) \subseteq A_n$ implica que $\mathrm{Ker}\,(u) \subseteq A_{n+1}$. Se sigue que $\mathrm{Ker}\,(u) \subseteq \bigcap_{n\geq 0} A_n = 0$. □

Lema 2.2. *Sea L/K una extensión finita de campos locales, separable y de grado primo ℓ. Si $\gamma \in \mathfrak{p}_L$, entonces*

$$N_{L/K}(1+\gamma) = 1 + N_{L/K}(\gamma) + \mathrm{Tr}_{L/K}(\gamma) + \mathrm{Tr}_{L/K}(\delta)$$

para algún $\delta \in \mathcal{O}_L$ tal que $v_L(\delta) \geq 2v_L(\gamma)$.

DEMOSTRACIÓN. Sea $G = \mathrm{Gal}(L/K)$ y supongamos que $\gamma \in \mathfrak{p}_L^n$. Si $A \subseteq G$ es un subconjunto (finito) pongamos

$$\gamma^A := \prod_{\sigma \in A} \sigma(\gamma);$$

entonces:

$$(*) \qquad N_{L/K}(1+\gamma) = \prod_{\sigma \in G} \sigma(1+\gamma) = \prod_{\sigma \in G} (1+\sigma(\gamma)) = \sum_{A \subseteq G} \gamma^A$$

Si definimos $n(A) := |A|$ (el cardinal del conjunto A), observemos que:

Si $n(A) = 0$, entonces $A = \emptyset$ y el sumando correspondiente en $(*)$ es 1.

Si $n(A) = 1$, entonces $A = \{\sigma\}$ y hay $\ell = |G|$ de estos conjuntos con un solo elemento y los sumandos correspondientes en $(*)$ son: $\sum_{\sigma \in G} \gamma^\sigma = \mathrm{Tr}_{L/K}(\gamma)$.

Si $n(A) = \ell = |G|$, entonces $A = G$ y el sumando correspondiente en $(*)$ es $\gamma^G = \prod_{\sigma \in G} \sigma(\gamma) = N_{L/K}(\gamma)$.

Si $n(A) \neq 0, 1, \ell$, entonces como G es cíclico de orden primo ℓ, se tiene que $\sigma A \neq A$ para todo $\sigma \neq 1$ de G. Sean $A_1, A_2, \ldots, A_r$ los subconjuntos de G con $n(A_i) \geq 2$. Se tiene entonces que

$$N_{L/K}(1+\gamma) = 1 + \mathrm{Tr}_{L/K}(\gamma) + N_{L/K}(\gamma) + \sum_{i=1}^{r} \sum_{\sigma} \gamma^{\sigma A_i},$$

donde

$$\sum_{\sigma \in G} \gamma^{\sigma A} = \mathrm{Tr}_{L/K}(\gamma^A) \in \mathrm{Tr}_{L/K}\left(\mathfrak{p}_L^{2n}\right),$$

ya que $n(A) \geq 2$ y $\gamma \in \mathfrak{p}_L^n$. □

2.1.1 La norma en extensiones cíclicas de grado primo

Si L/K es una extensión de campos locales, cíclica de grado primo ℓ, entonces poniendo $e = e(L/K)$ y $f = f(L/K)$, como $ef = \ell$, entonces $e = 1$ y $f = \ell$ ó $e = \ell$ y $f = 1$. En el primer caso se tiene que L/K es no ramificada y en el segundo caso L/K es totalmente ramificada. Este último caso lo separaremos en dos subcasos: si $p = \text{car}\,(K)$, entonces $p \neq \ell$ ó $p = \ell$; en el primer subcaso L/K es mansa totalmente ramificada, y en el segundo subcaso L/K es totalmente ramificada de grado $\ell = p$. A continuación describimos la acción de la norma $N_{L/K}$ sobre los grupos de unidades superiores $U^{(i)}$ correspondientes en cada uno de los tres casos anteriores.

Extensiones no ramificadas de campos locales. Si L/K es una extensión finita no ramificada de campos locales, como $\text{Gal}(L/K) \simeq \text{Gal}(L/K)$ y este último grupo es cíclico, generado por el Frobenius, entonces L/K es cíclica.

Proposición 2.3. *Si L/K es una extensión finita no ramificada de campos locales, entonces la norma $N_{L/K}$ manda $U_L^{(i)}$ en $U_K^{(i)}$ para toda $i \geq 0$.*

DEMOSTRACIÓN. Si $\alpha = 1 + \gamma \in 1 + \mathfrak{p}_L^i = U_L^{(i)}$, entonces por el lema (2.2):

$$N_{L/K}(\alpha) = 1 + N_{L/K}(\gamma) + \text{Tr}_{L/K}(\gamma) + \text{Tr}_{L/K}(\delta)$$

con $\delta \in \mathcal{O}_L$ tal que $v_L(\delta) \geq 2v_L(\gamma)$. Se sigue que

$$(*) \qquad N_{L/K}(\alpha) \equiv 1 + \text{Tr}_{L/K}(\gamma) \text{ mód } \mathfrak{p}_L^i$$

ya que $v_L(\gamma) \geq i$ porque $\gamma \in \mathfrak{p}_L^i$. Ahora, como L/K es no ramificada, entonces un primo π_K de K permanece primo en L y así $\mathfrak{p}_L^i \cap K = \mathfrak{p}_K^i$, y por lo tanto $(*)$ implica que $N_{L/K}(\alpha) \equiv 1$ mód $\mathfrak{p}_K^i$ ya que $\gamma \in \mathfrak{p}_L^i$ implica que $\sigma(\gamma) \in \mathfrak{p}_L^i$ para toda $\sigma \in \text{Gal}(L/K)$ y por lo tanto $\text{Tr}_{L/K}(\gamma) \in \mathfrak{p}_L^i$; y como $\text{Tr}_{L/K}(\gamma) \in K$, entonces $\text{Tr}_{L/K}(\gamma) \in \mathfrak{p}_L^i \cap K = \mathfrak{p}_K^i$. Pero $N_{L/K}(\alpha) \equiv 1$ mód $\mathfrak{p}_K^i$ quiere decir que $N_{L/K}(\alpha) = 1 + \theta$ con $\theta \in \mathfrak{p}_K^i$, y por lo tanto $N_{L/K}(\alpha) \in U_K^{(i)}$. □

El resultado siguiente describe la acción de la norma $N_{L/K}$ con respecto a las filtraciones $U^{(i)}$ respectivas en el caso cuando L/K es no ramificada:

Proposición 2.4. *Sea L/K una extensión finita no ramificada de campos locales de grado n. Entonces:*

(1) *Un elemento primo π_K de K también es primo de L.*

(2) *Si* $\lambda_{i,F}$ *son los epimorfismos de* (1.65) *para el campo* F, *entonces los diagramas siguientes conmutan:*

$$\begin{array}{ccc} L^* & \xrightarrow{v_L} & \mathbb{Z} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \times n} \\ K & \xrightarrow[v_K]{} & \mathbb{Z} \end{array} \qquad \begin{array}{ccc} U_L & \xrightarrow{\lambda_{0,L}} & \overline{L}^* \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{\overline{L}/\overline{K}}} \\ U_K & \xrightarrow[\lambda_{0,K}]{} & \overline{K}^* \end{array} \qquad \begin{array}{ccc} U_L^{(i)} & \xrightarrow{\lambda_{i,L}} & \overline{L} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{\overline{L}/\overline{K}}} \\ U_K^{(i)} & \xrightarrow[\lambda_{i,K}]{} & K \end{array}$$

DEMOSTRACIÓN. (1) es precisamente (1.36)(3). Denotemos a este elemento primo común por π.

Para (2), como $f(L/K) = n = [L : K]$, entonces por definición de v_L se tiene que para todo $\alpha \in L^*$:

$$v_L(\alpha) = \frac{1}{n} v_K(N_{L/K}(\alpha)),$$

i.e., $v_K(N_{L/K}(\alpha)) = n \cdot v_L(\alpha)$ y por lo tanto el primer diagrama conmuta.

Para el segundo diagrama, como L/K es no ramificada se tiene un isomorfismo $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L/K)$, $\sigma \mapsto \overline{\sigma}$ y por lo tanto $\overline{N_{L/K}(\alpha)} = N_{\overline{L}/\overline{K}}(\overline{\alpha})$, y así el segundo diagrama conmuta. Para el tercer diagrama, el lema (2.2) nos dice que

$$\begin{aligned} N_{L/K}(1 + \varepsilon\pi^i) &= 1 + N_{L/K}(\varepsilon\pi^i) + \mathrm{Tr}_{L/K}(\varepsilon\pi^i) + \mathrm{Tr}_{L/K}(\delta) \\ &= 1 + (N_{L/K}\varepsilon)\pi^{ni} + (\mathrm{Tr}_{L/K}\varepsilon)\pi^i + \mathrm{Tr}_{L/K}(\delta) \end{aligned}$$

(la segunda igualdad es porque $\pi \in K$ y por lo tanto queda fijo bajo la acción de $\mathrm{Gal}(L/K)$); aquí δ es tal que $v_L(\delta) \geq 2v_L(\varepsilon\pi^i) = 2i$ y consecuentemente $v_L(\mathrm{Tr}_{L/K}(\delta) \geq 2i$. Se sigue que

$$N_{L/K}(1 + \varepsilon\pi^i) \equiv 1 + (\mathrm{Tr}_{L/K}\varepsilon)\pi^i \ (\mathrm{mód}\ \pi^{i+1})$$

ya que $ni, 2i \geq i + 1$. Usando esta congruencia, como $\lambda_{i,L}(1 + \varepsilon\pi^i) = \overline{\varepsilon} \in L$, se tiene que

$$\begin{aligned} \lambda_{i,K}(N_{L/K}(1 + \varepsilon\pi^i)) &- \lambda_{i,K}(1 + (\mathrm{Tr}_{L/K}\varepsilon)\pi^i) \ (\mathrm{mód}\ \pi^{i+1}) \\ &- \mathrm{Tr}_{L/K}\varepsilon \ (\mathrm{mód}\ \pi^{i+1}) \\ &\quad \mathrm{Tr}_{\overline{L}/\overline{K}}(\overline{\varepsilon}) \\ &\quad \mathrm{Tr}_{\overline{L}/\overline{K}}(\lambda_{i,L}(1 + \varepsilon\pi^i)), \end{aligned}$$

i.e., el último diagrama conmuta. □

Corolario 2.5. *Si L/K es una extensión finita no ramificada de campos locales, entonces:*

(1) $N_{L/K}(U_L^{(i)}) = U_K^{(i)}$ *para toda* $i \geq 1$.

(2) $N_{L/K}(U_L) = U_K$.

(3) $K^*/N_{L/K}L^* \simeq \mathbb{Z}/n\mathbb{Z}$, *donde* $n = [L : K]$.

(4) $N_{L/K}L^* \simeq (\pi^n) \times U_K$, *donde* $n = [L : K]$ *y* $\pi \in K$ *es un primo.*

DEMOSTRACIÓN. (1): Por (2.3) $N_{L/K}$ induce por paso al cociente morfismos

$$N_{L/K} : U_L^{(i)}/U_L^{(i+1)} \longrightarrow U_K^{(i)}/U_K^{(i+1)}$$

y por la conmutatividad del tercer diagrama en la proposición anterior, para $i \geq 1$, se tienen entonces diagramas conmutativos:

$$\begin{array}{ccc} U_L^{(i)}/U_L^{(i+1)} & \xrightarrow{\lambda_{i,L}} & L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{\overline{L}/\overline{K}}} \\ U_K^{(i)}/U_K^{(i+1)} & \xrightarrow[\lambda_{i,K}]{} & K \end{array}$$

donde los morfismos horizontales son isomorfismos y la traza es suprayectiva en campos finitos. Se sigue que la norma es suprayectiva en los cocientes $U^{(i)}/U^{(i+1}$ y así, por el lema (2.1), la norma $N_{L/K} : U_L^{(i)} \twoheadrightarrow U_K^{(i)}$ es suprayectiva, lo cual prueba (1).

Para (2), consideremos ahora el siguiente diagrama conmutativo con renglones exactos (por (1.65)):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^{(1)} & \longrightarrow & U_L & \xrightarrow{\lambda_{0,L}} & L^* & \longrightarrow & 0 \\ & & {\scriptstyle N_{L/K}}\downarrow & & {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{\overline{L}/\overline{K}}} & & \\ 0 & \longrightarrow & U_K^{(1)} & \longrightarrow & U_K & \xrightarrow[\lambda_{0,K}]{} & \overline{K}^* & \longrightarrow & 0 \end{array}$$

donde el cuadrado de la derecha es el segundo diagrama de la proposición previa y el cuadrado de la izquierda conmuta porque $N_{L/K}$ manda $U_L^{(1)}$ en $U_K^{(1)}$ por (2.3) y es la restricción de la norma $N_{L/K} : U_L \to U_K$. Si ahora denotamos con N', N, N'' a las tres normas que aparecen en este diagrama, la sucesión

núcleo-conúcleo del lema de la serpiente (véase Rotman [34]) asociada a este diagrama es

$$0 \to \operatorname{Ker} N' \to \operatorname{Ker} N \to \operatorname{Ker} N'' \xrightarrow{\partial} \operatorname{Coker} N' \to \operatorname{Coker} N \to \operatorname{Coker} N'' \to 0$$

donde por la parte (1) de este corolario $\operatorname{Coker}(N') = U_K^{(1)}/N_{L/K}(U_L^{(1)}) = 0$, el segundo conúcleo es $U_K/N_{L/K}(U_L)$ y el tercer conúcleo es $\overline{K}^*/N_{\overline{L}/\overline{K}}(\overline{L}^*)$, y por lo tanto se tiene la sucesión exacta:

$$0 \to U_K/N_{L/K}(U_L) \xrightarrow{\lambda_{0,L}} \overline{K}^*/N_{\overline{L}/\overline{K}}(\overline{L}^*) \to 0,$$

i.e., $\lambda_{0,L}$ es un isomorfismo. El resultado se sigue del hecho que $N_{L/K} : L \to K$ es suprayectiva en campos finitos (1.98).

Para (3), consideremos el diagrama conmutativo con renglones exactos:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \times n} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow[v_K]{} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

donde la sucesión núcleo-conúcleo asociada satisface que

$$\operatorname{Coker}(N_{L/K} : U_L \to U_K) = U_K/N_{L/K}U_L = 0$$

por la parte (2). Se tiene entonces que

$$\operatorname{Coker}(N_{L/K} : L^* \to K^*) \simeq \operatorname{Coker}(n : \mathbb{Z} \to \mathbb{Z}),$$

i.e., $K^*/N_{L/K}L^* \simeq \mathbb{Z}/n\mathbb{Z}$.

Para (4), la elección de un elemento primo π de K (y de L, por la proposición anterior) escinde las sucesiones exactas del diagrama anterior, donde se ha identificado a $\mathbb{Z}$ con el grupo (π) generado por π. Se tiene entonces que $L^* \simeq (\pi) \times U_L$ y $K^* \simeq (\pi) \times U_K$, y estos isomorfismos son compatibles con la acción de $\operatorname{Gal}(L/K)$. Se sigue que

$$N_{L/K}(L^*) \simeq N_{L/K}((\pi) \times U_L) \simeq (\pi^n) \times N_{L/K}(U_L) \simeq (\pi^n) \times U_K$$

ya que $\pi \in K$ implica que $N_{L/K}(\pi) = \pi^n$. □

Extensiones mansas totalmente ramificadas cíclicas de grado primo. A continuación consideraremos el caso de una extensión L/K cíclica mansa de

grado $\ell \neq p = \text{car}(K)$. El resultado siguiente describe la acción de la norma $N_{L/K}$ con respecto a las filtraciones $U^{(i)}$ respectivas en este caso:

Teorema 2.6. *Sea L/K una extensión de campos locales, cíclica de grado primo ℓ, mansa totalmente ramificada. Entonces:*

(1) *Para un elemento primo π_L de L, el elemento $\pi_K = \pi_L^{\ell}$ es un primo de K.*

(2) *Los diagramas siguientes conmutan (donde $\overline{L} = K$):*

$$\begin{array}{ccc} L^* & \xrightarrow{v_L} & \mathbb{Z} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle id} \\ K^* & \xrightarrow{v_K} & \mathbb{Z} \end{array} \qquad \begin{array}{ccc} U_L & \xrightarrow{\lambda_{0,L}} & \overline{L}^* \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \phi_\ell} \\ U_K & \xrightarrow[\lambda_{0,K}]{} & \overline{K}^* \end{array} \qquad \begin{array}{ccc} U_L^{(\ell i)} & \xrightarrow{\lambda_{\ell i,L}} & \overline{L} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \times\bar{\ell}} \\ U_K^{(i)} & \xrightarrow[\lambda_{i,K}]{} & K \end{array}$$

donde $\lambda_{i,F}$ son los epimorfismos de (1.65), *id es el morfismo identidad, ϕ_ℓ es el morfismo $\alpha \mapsto \alpha^\ell$ y $\times\bar{\ell}$ es multiplicación por $\bar{\ell} \in K$, si $i \geq 1$.*

(3) *Si $\ell \nmid i$, entonces $N_{L/K}U_L^{(i)} = N_{L/K}U_L^{(i+1)}$*

DEMOSTRACIÓN. Como L/K es totalmente ramificada, $e = [L : K] = \ell$ y así (1) es precisamente (1.34).

Para (2), como $f = f(L/K) = 1$, entonces por (1.41), para todo $\alpha \in L^*$ se tiene que

$$v_L(\alpha) = \frac{1}{f} v_K(N_{L/K}(\alpha)) = v_K N_{L/K}(\alpha)$$

y así el primer diagrama conmuta.

Para el segundo diagrama, como L/K es Galois, entonces para todo $\sigma \in \text{Gal}(L/K)$ y todo $\alpha \in \mathcal{O}_L$, usando el epimorfismo $\text{Gal}(L/K) \twoheadrightarrow \text{Gal}(L/K) = \{id\}$ se tiene que $\sigma(\alpha) = \overline{\alpha}$. Se sigue que para $\alpha \in U_L$:

$$\begin{aligned} \lambda_{0,K} N_{L/K}(\alpha) &= \lambda_{0,K}\left(\prod_{i=1}^{\ell} \sigma^i(\alpha)\right) \quad (\sigma \text{ un generador de } \text{Gal}(L/K)) \\ &= \prod_{i=1}^{\ell} \sigma^i(\alpha) = \prod_{i=1}^{\ell} \overline{\alpha} \\ &\overline{\alpha}^{\ell} = \phi_\ell(\overline{\alpha}) = \phi_\ell \lambda_{0,L}(\alpha), \end{aligned}$$

y por lo tanto el segundo diagrama conmuta.

Para el tercer diagrama, como $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, si

$$1 + \varepsilon\pi_L^{\ell i} \in U_L^{\ell i} = 1 + \pi_L^{\ell i}\mathcal{O}_L = 1 + \pi_L^{\ell i}\mathcal{O}_K[\pi_L],$$

podemos pensar que $\varepsilon \in \mathcal{O}_K$ y observamos que $\pi_L^{\ell i} = (\pi_L^{\ell})^i = \pi_K^i$ de tal forma que $1 + \varepsilon\pi_L^{\ell i} = 1 + \varepsilon\pi_K^i \in U_K^{(i)} \subseteq K$. Se tiene entonces que

$$\begin{aligned} N_{L/K}(1 + \varepsilon\pi_L^{\ell i}) &= \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(1 + \varepsilon\pi_L^{\ell i}) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(1 + \varepsilon\pi_K^i) \\ & (1 + \varepsilon\pi_K^i)^{\ell} \qquad \text{ya que } \varepsilon \in K \\ & 1 + \ell\varepsilon\pi_K^i \text{ mód } \pi_K^{i+1}. \end{aligned}$$

Se sigue que

$$\begin{aligned} \lambda_{i,K} N_{L/K}(1 + \varepsilon\pi_L^{\ell i}) &- \lambda_{i,K}(1 + \ell\varepsilon\pi_K^i) \\ & \overline{\ell} \cdot \overline{\varepsilon} \\ &= \overline{\ell} \cdot \lambda_{\ell i, L}(1 + \varepsilon\pi_L^{\ell i}), \end{aligned}$$

y por lo tanto el tercer diagrama conmuta.

Para (3), si $\ell \nmid i$, para $1 + \varepsilon\pi_L^i \in U_L^{(i)}$ con $\varepsilon \in \mathcal{O}_L$, como $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ podemos pensar que $\varepsilon \in \mathcal{O}_K$, y así se tiene que

$$\begin{aligned} N_{L/K}(1 + \varepsilon\pi_L^i) &= \prod_{j=0}^{\ell-1}(1 + \sigma^j(\varepsilon\pi_L^i)) = \prod_{j=0}^{\ell-1}(1 + \varepsilon\sigma^j(\pi_L^i)) \\ & \text{ya que } \varepsilon \in \mathcal{O}_K \subseteq K \\ &- \prod_{j=0}^{\ell-1}(1 + \varepsilon\zeta^j\pi_L^i) \\ & \text{ya que por (1.56)(1) } \sigma(\pi_L) = \zeta\pi_L, \text{ donde } \zeta \in K \\ & \text{es una raíz primitiva } \ell\text{-ésima de la unidad.} \\ & 1 - (-\varepsilon\pi_L^i)^{\ell} \\ &- 1 - (-\varepsilon)^{\ell}\pi_K^i \qquad \text{ya que } \pi_L^{\ell} = \pi_K \end{aligned}$$

y, similarmente,

$$\begin{aligned} N_{L/K}(1+\varepsilon\pi_L^{i+1}) &= \prod_{j=0}^{\ell-1}(1+\sigma^j(\varepsilon\pi_L^{i+1})) = \prod_{j=0}^{\ell-1}(1+\varepsilon\sigma^j(\pi_L^{i+1})) \\ &= \prod_{j=0}^{\ell-1}(1+\varepsilon\zeta^j\pi_L^{i+1}) = \prod_{j=0}^{\ell-1}(1+(\varepsilon\pi_L)\zeta^j\pi_L^i) \\ &= 1-(-\varepsilon\pi_L\pi_L^i)^\ell = 1-(-\varepsilon\pi_L)^\ell\pi_K^i \end{aligned}$$

y como los lados derechos de las dos igualdades anteriores son de la misma forma en $U_K^{(i)}$, se sigue que los lados izquierdos están incluidos uno en la imagen del otro, i.e., $N_{L/K}U_L^{(i)} = N_{L/K}U_L^{(i+1)}$. □

Corolario 2.7. *Sea L/K una extensión de campos locales, cíclica de grado primo ℓ, mansa totalmente ramificada. Entonces:*

(1) $N_{L/K}U_L^{(\ell i)} = U_K^{(i)}$ *para* $i \geq 1$.

(2) $N_{L/K}U_L^{(1)} = U_K^{(1)}$.

(3) $K^*/N_{L/K}L^*$ *es cíclico de orden* ℓ.

DEMOSTRACIÓN. (1) se sigue como en la demostración de (2.5)(1), usando la conmutatividad del tercer diagrama en el teorema anterior, el hecho de que multiplicación por $\bar{\ell}$ es un isomorfismo y el lema (2.1).

Para (2), por la parte (3) del teorema anterior se tienen las igualdades siguientes donde la última igualdad es por la parte (1) de este corolario:

$$N_{L/K}U_L^{(1)} = N_{L/K}U_L^{(1+1)} = \cdots = N_{L/K}U_L^{(\ell-1)} = N_{L/K}U_L^{(\ell)} = U_K^{(1)}.$$

Para (3), usando los cuadrados conmutativos del teorema anterior, considere el diagrama conmutativo con renglones exactos siguiente:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^{(1)} & \longrightarrow & U_L & \xrightarrow{\lambda_{0,L}} & \overline{L}^* & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \phi_\ell} & & \\ 0 & \longrightarrow & U_K^{(1)} & \longrightarrow & U_K & \xrightarrow[\lambda_{0,K}]{} & K^* & \longrightarrow & 0 \end{array}$$

donde denotamos sus morfismos verticales por g', g, ϕ_ℓ de tal forma que como por la parte (2) de este corolario $\operatorname{Coker}(g') = U_K^{(1)}/N_{L/K}U_L^{(1)} = 0$, entonces la

sucesión núcleo-conúcleo asociada es

$$0 \to \text{Coker}\,(g) \to \text{Coker}\,(\phi_\ell) \to 0,$$

i.e.,

$$(a) \qquad U_K/N_{L/K}U_L \simeq \overline{K}^*/(\overline{L}^*)^\ell.$$

Finalmente consideremos el diagrama siguiente, donde $f = f(L/K) = 1$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle 1} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow[v_K]{} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

y denotando sus morfismos verticales por g', g, 1, notando que Ker (1) = 0 y Coker (1) = 0, la sucesión núcleo-conúcleo se vuelve

$$0 \to \text{Coker}\,(g') \to \text{Coker}\,(g) \to 0,$$

i.e.,

$$(b) \qquad U_K/N_{L/K}U_L \simeq K^*/N_{L/K}L^*.$$

Entonces, de (a) y (b) se sigue que $K^*/N_{L/K}L^* \simeq U_K/N_{L/K}U_L \simeq K^*/(\overline{L}^*)^\ell$, y este último grupo es cíclico de orden ℓ ya que $\ell \neq \text{car}\,(K)$. □

El caso que nos falta, cuando $\ell = [L : K] = \text{car}\,(K) = p$, es un poco más complicado y para estudiarlo necesitaremos calcular la traza de algunos ideales, donde usaremos los resultados siguientes sobre el *diferente* de una extensión L/K. Recordemos los hechos pertinentes:

2.1.2 El diferente de una extensión

En esta sección consideramos un invariante de una extensión de campos locales L/K relacionado con el discriminante $\Delta_{L/K}$, pero más sutil. La construcción la daremos en una situación un poco más general: si L/K es una extensión finita separable de campos valuados discretos completos, entonces la traza $\text{Tr}_{L/K} : L \twoheadrightarrow K$ es suprayectiva (1.97) y la forma bilineal $\text{Tr}_{L/K}(xy)$ es no degenerada en L. El conjunto

$$\mathcal{D}_{L/K}^{-1} := \{y \in L \ : \ \text{Tr}_{L/K}(xy) \in \mathcal{O}_K \quad \text{para todo } x \in \mathcal{O}_L\}$$

satisface las propiedades siguientes:

(1) $\mathcal{D}_{L/K}^{-1}$ *es un* $\mathcal{O}_L$*-submódulo de* L.

En efecto, claramente es cerrado bajo sumas ya que la traza es aditiva. Ahora, si $z \in \mathcal{D}_{L/K}^{-1}$ y $\lambda \in \mathcal{O}_L$, entonces para todo $x \in \mathcal{O}_L$ se tiene que $\mathrm{Tr}_{L/K}(x\lambda z) = \mathrm{Tr}_{L/K}((x\lambda)z) \in \mathcal{O}_K$, ya que $x\lambda \in \mathcal{O}_L$ y $z \in \mathcal{D}_{L/K}^{-1}$.

(2) $\mathrm{Tr}_{L/K}(\mathcal{D}_{L/K}^{-1}) \subseteq \mathcal{O}_K$.

Esto es obvio tomando $x = 1 \in \mathcal{O}_L$.

(3) *Más aún, si* E *es cualquier* $\mathcal{O}_L$*-submódulo de* L *tal que* $\mathrm{Tr}_{L/K}(E) \subseteq \mathcal{O}_K$, *entonces* $E \subseteq \mathcal{D}_{L/K}^{-1}$.

En efecto, si $z \in E \subseteq L$, entonces para toda $x \in \mathcal{O}_L$ se tiene que $xz \in E$, ya que E es $\mathcal{O}_L$-submódulo. Se sigue que $\mathrm{Tr}_{L/K}(xz) \in \mathcal{O}_K$ por hipótesis, y por lo tanto $z \in \mathcal{D}_{L/K}^{-1}$, i.e., $E \subseteq \mathcal{D}_{L/K}^{-1}$.

De (2) y (3) se sigue que:

(4) $\mathcal{D}_{L/K}^{-1}$ *es el mayor* $\mathcal{O}_L$*-submódulo de* L *tal que su traza está contenida en* $\mathcal{O}_K$. *En particular, como* $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}_K$, *entonces* $\mathcal{O}_L \subseteq \mathcal{D}_{L/K}^{-1}$ *y* $\mathcal{D}_{L/K}^{-1}$ *es un ideal fraccionario de* L, *al que se llama el* codiferente de L/K, *y su inverso* $\mathcal{D}_{L/K}$ *es un ideal (entero) de* $\mathcal{O}_L$, *al que se llama el* diferente de L/K.

A continuación demostramos varios resultados sobre el codiferente y el diferente de una extensión que usaremos para calcularlo en el caso cuando L/K es una extensión totalmente ramificada de campos locales.

Sean L/K una extensión de campos valuados discretos completos, separable y finita de grado n y $\alpha_1, \ldots, \alpha_n$ una base de L/K; dado un $z \in L$, escribámoslo como $z = x_1\alpha_1 + \cdots + x_n\alpha_n$ con los $x_i \in K$. Para cada α_i consideremos las trazas

$$\mathrm{Tr}_{L/K}(\alpha_i z) = x_1 \mathrm{Tr}_{L/K}(\alpha_i\alpha_1) + \cdots + x_n \mathrm{Tr}_{L/K}(\alpha_i\alpha_n)$$

(donde las x_i salen de las trazas porque están en K); observemos entonces que el sistema de ecuaciones lineales homogéneas

$$\mathrm{Tr}_{L/K}(\alpha_i z) = 0, \qquad 1 \leq i \leq n$$

sólo tiene la solución trivial ya que si no fuera así, i.e., si existiera una solución $z \neq 0$ de $(*)$, entonces multiplicando las ecuaciones $(*)$ por elementos

arbitrarios $a_i \in K$ y sumando obtenemos

$$\sum_{i=1}^{n} \mathrm{Tr}_{L/K}(a_i \alpha_i z) = 0,$$

y como la traza es aditiva, se sigue que

$$\mathrm{Tr}_{L/K}((a_1\alpha_1 + \cdots + a_n\alpha_n)z) = 0,$$

donde $(a_1\alpha_1 + \cdots + a_n\alpha_n)z$ es un elemento arbitrario de L. Se tiene entonces que la traza es cero en L, lo cual no es posible ya que L/K es separable (1.97). Así $(*)$ sólo tiene la solución trivial $z = 0$. Se sigue que las ecuaciones no homogéneas

$$(**) \qquad \mathrm{Tr}_{L/K}(\alpha_i z) = b_i \qquad \text{con } b_i \in K,\ 1 \leq i \leq n$$

tienen solución única. En particular, para cada $j = 1, \ldots, n$ existe una única solución α'_j de las ecuaciones $\mathrm{Tr}_{L/K}(\alpha_i z) = \delta_{ij}$ (la delta de Kronecker).

Lema 2.8. *Si L/K es una extensión de campos valuados discretos completos, separable y finita de grado n y $\alpha_1, \ldots, \alpha_n$ es una base de L/K, sean α'_j las soluciones únicas de $\mathrm{Tr}_{L/K}(\alpha_i z) = \delta_{ij}$; entonces los elementos $\alpha'_1, \ldots, \alpha'_n$ forman una base de L/K (llamada la* base complementaria *de $\alpha_1, \ldots, \alpha_n$). Más aún, si $\theta = y_1\alpha'_1 + \cdots + y_n\alpha'_n \in L$, con los $y_i \in K$, entonces*

$$y_i = \mathrm{Tr}_{L/K}(\theta\alpha_i)$$

y si $\xi = x_1\alpha_1 + \cdots + x_n\alpha_n \in L$, con los $x_i \in K$, entonces

$$x_i = \mathrm{Tr}_{L/K}(\xi\alpha'_i).$$

DEMOSTRACIÓN. Para la primera afirmación basta probar que los α'_i son linealmente independientes. Para esto, si $0 = y_1\alpha'_1 + \cdots + y_n\alpha'_n$, con los $y_j \in K$, multiplicando por los α_i y tomando la traza obtenemos

$$0 = \mathrm{Tr}_{L/K}(y_1\alpha'_1\alpha_i + \cdots + y_n\alpha'_n\alpha_i) = y_1\mathrm{Tr}_{L/K}(\alpha'_1\alpha_i) + \cdots + y_n\mathrm{Tr}_{L/K}(\alpha'_n\alpha_i) = y_i$$

la última igualdad porque $\mathrm{Tr}_{L/K}(\alpha'_j\alpha_i) = \delta_{ij}$.

Para la segunda afirmación, multiplicando θ por α_i obtenemos

$$\theta\alpha_i = y_1\alpha'_1\alpha_i + \cdots + y_n\alpha'_n\alpha_i,$$

de tal forma que

$$\mathrm{Tr}_{L/K}(\theta\alpha_i) = y_1\mathrm{Tr}_{L/K}(\alpha_1\alpha_i) + \cdots + y_n\mathrm{Tr}_{L/K}(\alpha_n\alpha_i) = y_i,$$

la última igualdad porque $\mathrm{Tr}_{L/K}(\alpha'_j\alpha_i) = \delta_{ij}$. □

Corolario 2.9. *Si L/K es una extensión de campos valuados discretos completos, separable y finita de grado n y $\alpha_1, \ldots, \alpha_n$ es una $\mathcal{O}_K$-base de $\mathcal{O}_L$, entonces la base complementaria α_j' es una $\mathcal{O}_K$-base de $\mathcal{D}_{L/K}^{-1}$.*

DEMOSTRACIÓN. Dado $\gamma \in L$ escribámoslo como $\gamma = y_1\alpha_1' + \cdots + y_n\alpha_n'$ con $y_i \in K$. Entonces

$$\begin{aligned}
\gamma \in \mathcal{D}_{L/K}^{-1} &\Leftrightarrow \operatorname{Tr}_{L/K}(\gamma\mathcal{O}_L) \subseteq \mathcal{O}_K \qquad \text{por definición de } \mathcal{D}_{L/K}^{-1} \\
&\Leftrightarrow \operatorname{Tr}_{L/K}(\gamma\alpha_i) \in \mathcal{O}_K,\ \ 1 \le i \le n, \qquad \text{porque } \{\alpha_i\} \text{ es base de } \mathcal{O}_L \\
&\Leftrightarrow y_i \in \mathcal{O}_K,\ \ 1 \le i \le n, \qquad \text{por la segunda parte del lema.}
\end{aligned}$$

Esto implica que todo $\gamma \in \mathcal{D}_{L/K}^{-1}$ es combinación lineal de los α_i' con coeficientes en $\mathcal{O}_K$. □

Para el caso de extensiones de campos locales totalmente ramificadas L/K de grado n, se sabe que $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ con π_L un primo de L de tal forma que $1, \pi_L, \ldots, \pi_L^{n-1}$ es una $\mathcal{O}_K$-base de $\mathcal{O}_L$, y en este caso se puede ser más explícito con la base complementaria de las π_L^i anteriores. Para esto necesitaremos el siguiente resultado de Euler, válido en la situación general que estamos considerando:

Lema 2.10 (Euler). *Si K es un campo valuado discreto completo, $L = K(\alpha)$ y $f(x) = \operatorname{Irr}(\alpha, K)$, entonces*

$$\operatorname{Tr}_{L/K}\left(\frac{f(x)}{x-\alpha}\frac{\alpha^i}{f'(\alpha)}\right) = x^i$$

para $0 \le i \le n-1$ y donde $f'(x)$ es la derivada de $f(x)$.

DEMOSTRACIÓN. Como L/K es separable las raíces de $f(x)$ son distintas, digamos $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$, y el grupo de Galois $G = \operatorname{Gal}(L/K)$ permuta estas raíces. Entonces

$$(\dagger)\quad \operatorname{Tr}_{L/K}\begin{pmatrix} f(x) & \alpha^i \\ x-\alpha & f'(\alpha)\end{pmatrix} = \sum_{\sigma\in G}\begin{matrix}\sigma(f(x)) & \sigma(\alpha^i) \\ \sigma(x-\alpha) & \sigma(f'(\alpha))\end{matrix} = \sum_{j=0}^{n-1}\begin{matrix} f(x) & \alpha_j^i \\ x-\alpha_j & f'(\alpha_j)\end{matrix}$$

y éste es un polinomio $g(x)$ de grado $\le n-1$.

Por otra parte, como $f(x) = (x - \alpha)(x - \alpha_1)\cdots(x - \alpha_{n-1})$, entonces $f'(x) = \sum_{j=0}^{n-1} \frac{f(x)}{x - \alpha_j}$ y los sumandos $\frac{f(x)}{x - \alpha_j}$ evaluados en α_k son

$$\left.\frac{f(x)}{x - \alpha_j}\right|_{x=\alpha_k} = \begin{cases} f'(\alpha_j) & \text{si } k = j \\ 0 & \text{si } k \neq j. \end{cases}$$

Se sigue que la traza (†) evaluada en α_k es

$$g(x)|_{x=\alpha_k} = \mathrm{Tr}_{L/K}\left(\frac{f(x)}{x - \alpha}\frac{\alpha^i}{f'(\alpha)}\right)\Bigg|_{x=\alpha_k} = \sum_{j=0}^{n-1} \frac{f(x)}{x - \alpha_j}\frac{\alpha_j^i}{f'(\alpha_j)}\Bigg|_{x=\alpha_k} = \alpha_j^i$$

para $0 \leq j \leq n - 1$, y así $(g(x) - x^i)|_{x=\alpha_k} = 0$ para $0 \leq j \leq n - 1$, i.e., $g(x)$ (un polinomio de grado $\leq n - 1$) tiene n ceros comunes con x^i; se sigue que $g(x) = x^i$, como se quería. □

Usando este lema podemos calcular explícitamente una $\mathcal{O}_K$-base del codiferente de una extensión totalmente ramificada L/K, y de hecho lo haremos en la situación más general siguiente: L/K es una extensión finita de campos valuados discretos completos tal que la extensión de campos residuales L/K es separable; entonces, por (1.40) $\mathcal{O}_L$ tiene una $\mathcal{O}_K$-base consistente de potencias de un sólo elemento $\alpha \in \mathcal{O}_L$, i.e., $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Ahora, si $f(x)$ es el polinomio característico de α, entonces los coeficientes de $f(x)$ están en $\mathcal{O}_L$ y en K; se sigue que los coeficientes de $f(x)$ están en $\mathcal{O}_L \cap K = \mathcal{O}_K$. Nótese que todo esto es cierto en el caso cuando L/K es totalmente ramificada.

Teorema 2.11. *Si L/K es una extensión finita de grado n de campos valuados discretos completos tal que la extensión L/K de campos residuales es separable, usando* (1.40) *escribamos $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ con $\alpha \in \mathcal{O}_L$ y sea $f(x)$ el polinomio característico de α. Entonces los elementos $\alpha^i/f'(\alpha)$, para $0 \leq i \leq n - 1$, son una base del $\mathcal{O}_K$-módulo $\mathcal{D}_{L/K}^{-1}$.*

Demostración. Como $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una $\mathcal{O}_K$-base de $\mathcal{O}_L$, escribiendo $f(x) = (x - \alpha)(b_0 + b_1 x + \cdots + b_{n-1}x^{n-1})$ con los $b_i \in L$, mostraremos primero que los elementos

$$\frac{b_i}{f'(\alpha)}, \qquad 0 \leq i \leq n - 1$$

son una base complementaria del codiferente $\mathcal{D}_{L/K}^{-1}$. En efecto, por el lema de Euler,

$$\begin{aligned} x^i &= \mathrm{Tr}_{L/K}\left(\frac{f(x)}{(x-\alpha)}\frac{\alpha^i}{f'(\alpha)}\right) \\ &= \mathrm{Tr}_{L/K}\left((b_0+b_1x+\cdots+b_{n-1}x^{n-1})\frac{\alpha^i}{f'(\alpha)}\right) \\ &= \mathrm{Tr}_{L/K}\left(\frac{b_0\alpha^i}{f'(\alpha)}\right)+\cdots+\mathrm{Tr}_{L/K}\left(\frac{b_{n-1}\alpha^i}{f'(\alpha)}\right)x^{n-1} \end{aligned}$$

y comparando coeficientes se sigue que

$$\mathrm{Tr}_{L/K}\left(\frac{b_j\alpha^i}{f'(\alpha)}\right)=\delta_{ij}$$

y ésta es precisamente la condición (**) para que $b_j/f'(\alpha)$ sea una base complementaria de L/K, y por el corolario (2.9) ésta es una $\mathcal{O}_K$-base de $\mathcal{D}_{L/K}^{-1}$.

Para calcular los coeficientes b_j escribamos $f(x)=\sum_{i=0}^{n}a_ix^i$ con $a_n=1$. Como $f(\alpha)=0$, entonces

$$\begin{array}{cc} f(x) & \dfrac{f(x)-f(\alpha)}{x-\alpha} \quad \dfrac{\sum_{i>0}a_ix^i-\sum_{i>0}a_i\alpha^i}{x-\alpha} \\ x-\alpha & \end{array}$$

$$\sum_{i=1}^{n}a_i\left(\frac{x^i-\alpha^i}{x-\alpha}\right)=\sum_{i=1}^{n}a_i(x^{i-1}+\alpha x^{i-2}+\cdots+\alpha^{i-1})$$

y así, igualando coeficientes con $\dfrac{f(x)}{x-\alpha}=b_0+b_1x+\cdots+b_{n-1}x^{n-1}$, obtenemos

$$\begin{aligned} b_0 &\quad a_1+a_2\alpha+\cdots+a_n\alpha^{n-1} \\ b_1 &\quad a_2+a_3\alpha+\cdots+a_n\alpha^{n-2} \\ b_2 &\quad a_3+a_4\alpha+\cdots+a_n\alpha^{n-3} \end{aligned}$$

$$\begin{aligned} b_{n-2} &- a_{n-1}+a_n\alpha=a_{n-1}+\alpha \\ b_{n-1} &- a_n=1 \end{aligned}$$

y como el polinomio característico $f(x)$ tiene coeficientes $a_j \in \mathcal{O}_K$, entonces los elementos de la base $b_i/f'(\alpha)$ los podemos reemplazar por

$$\begin{aligned}
&\frac{b_{n-1}}{f'(\alpha)} \qquad \frac{1}{f'(\alpha)} \\
&\frac{b_{n-2}}{f'(\alpha)} \qquad \frac{a_{n-1}}{f'(\alpha)} + \frac{a_n\alpha}{f'(\alpha)} = a_{n-1}\frac{1}{f'(\alpha)} + \frac{\alpha}{f'(\alpha)} \\
&\frac{b_{n-3}}{f'(\alpha)} \quad - \quad a_{n-2}\frac{1}{f'(\alpha)} + a_{n-1}\frac{\alpha}{f'(\alpha)} + \frac{\alpha^2}{f'(\alpha)}
\end{aligned}$$

$$\frac{b_0}{f'(\alpha)} \qquad a_1\frac{1}{f'(\alpha)} + a_2\frac{\alpha}{f'(\alpha)} + \cdots + a_{n-1}\frac{\alpha^{n-2}}{f'(\alpha)} + \frac{\alpha^{n-1}}{f'(\alpha)}$$

de tal forma que se obtiene la base equivalente

$$0 \le i \le n-1$$

de $\mathcal{D}_{L/K}^{-1}$. □

El corolario siguiente nos dice quién es exactamente el diferente de una extensión como las consideradas:

Corolario 2.12. *Si L/K es una extensión finita de grado n de campos valuados discretos completos tal que la extensión L/K de campos residuales es separable, usando* (1.40) *escribamos $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ con $\alpha \in \mathcal{O}_L$ y sea $f(x)$ el polinomio característico de α. Entonces, $\mathcal{D}_{L/K} = (f'(\alpha))$.*

DEMOSTRACIÓN. Por la proposición anterior $\alpha^i/f'(\alpha)$, $0 \le i \le n-1$, con $n = [L : K]$, es una $\mathcal{O}_K$-base de $\mathcal{D}_{L/K}^{-1}$. Entonces, si $\gamma \in L$, como $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ se tiene que

$$\begin{aligned}
\gamma \in \mathcal{O}_L \quad &\Leftrightarrow \quad \gamma \text{ es una combinación lineal de los } \alpha^i \text{ con coeficientes en } \mathcal{O}_K \\
&\Leftrightarrow \quad \gamma/f'(\alpha) \text{ es una combinación lineal de los } \alpha^i/f'(\alpha) \\
&\qquad\qquad \text{con coeficientes en } \mathcal{O}_K \\
&\Leftrightarrow \quad \gamma/f'(\alpha) \in \mathcal{D}_{L/K}^{-1} \text{ porque } \{\alpha^i/f'(\alpha)\} \text{ es una } \mathcal{O}_K\text{-base de } \mathcal{D}_{L/K}^{-1} \\
&\Leftrightarrow \quad \gamma \in f'(\alpha)\mathcal{D}_{L/K}^{-1},
\end{aligned}$$

de donde se sigue que $\mathcal{O}_L = f'(\alpha)\mathcal{D}_{L/K}^{-1}$, i.e., $\mathcal{D}_{L/K} = (f'(\alpha))$. □

El cálculo anterior se puede refinar para el caso de L/K normal, de grado n, introduciendo los grupos de ramificación de $G = \mathrm{Gal}(L/K)$. Sabemos por (1.74) que los grupos de ramificación G_i de G son triviales para i suficientemente grande y están determinados por la función i_G definida por $i_G(\tau) = v_L(\tau(\alpha) - \alpha)$, donde $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ (véase (1.75)(2)). Entonces, si $f(x) \in \mathcal{O}_K[x]$ es el polinomio mínimo de α (que es igual al polinomio característico en este caso, véase §1.10), entonces $\sigma_i(\alpha)$ para $0 \leq i \leq n-1$ son todas las raíces de $f(x)$ (tomando $\sigma_0 = id$) y así $f(x) = \prod_{i=0}^{n-1}(x - \sigma_i(\alpha))$, por lo que $f'(x) = \prod_{i=1}^{n-1}(\alpha - \sigma_i(\alpha))$ y así, para la valuación v_L se tiene que

$$v_L(f'(\alpha)) = \sum_{i=1}^{n-1} v_L(\alpha - \sigma_i(\alpha)) = \sum_{i=1}^{n-1} i_G(\sigma_i).$$

Observemos ahora que la función i_G es constante, de valor i, en los conjuntos $G_{i-1} - G_i$ ya que $\tau \in G_{i-1} - G_i$ si y sólo si $i_G(\tau) > i$ e $i_G(\tau) \not\geq i+1$, i.e., si y sólo si $i_G(\tau) = i$. También, como $G_{i-1} \supsetneq G_i$, entonces $|G_{i-1} - G_i| = |G_{i-1}| - |G_i|$. Se sigue que

$$\begin{aligned}\sum i_G(\tau) &= \sum_{i\geq 0} i(|G_{i-1}| - |G_i|) = \sum_{i\geq 0} i((|G_{i-1}| - 1) - (|G_i| - 1)) \\ &- ((|G_0| - 1) - (|G_1| - 1)) + 2((|G_1| - 1) - (|G_2| - 1)) \\ &\quad +3((|G_2| - 1) - (|G_3| - 1)) + \cdots \\ &= (|G_0| - 1) + (|G_1| - 1) + (|G_2| - 1) + \cdots,\end{aligned}$$

de tal forma que juntando esta igualdad con (∗), hemos probado:

Proposición 2.13. *Sea L/K una extensión finita normal de grado n de campos valuados discretos completos tal que la extensión L/K de campos residuales es separable; usando* (1.40) *escribamos $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ con $\alpha \in \mathcal{O}_L$ y sea $f(x)$ el polinomio mínimo de α. Sea $G = \mathrm{Gal}(L/K)$; entonces*

$$v_L(f'(\alpha)) = \sum_{\tau \neq id} i_G(\tau) = \sum_{i\geq 0}(|G_i| - 1),$$

donde los G_i son los grupos de ramificación de L/K.

□

La proposición siguiente también nos servirá para el cálculo de la traza que necesitamos:

Proposición 2.14. *Sea L/K una extensión finita separable de campos valuados discretos completos. Sean I un ideal fraccionario de K y J un ideal fraccionario de L. Entonces*

$$\mathrm{Tr}_{L/K}(J) \subseteq I \quad \Leftrightarrow \quad J \subseteq I\mathcal{D}_{L/K}^{-1}.$$

DEMOSTRACIÓN. Si $I = 0$, el resultado es trivial. Supongamos entonces que $I \neq 0$. Entonces

$$\begin{aligned}
\mathrm{Tr}_{L/K}(J) \subseteq I \quad &\Leftrightarrow \quad I^{-1}\mathrm{Tr}_{L/K}(J) \subseteq \mathcal{O}_K \\
&\Leftrightarrow \quad \mathrm{Tr}_{L/K}(I^{-1}J) \subseteq \mathcal{O}_K \\
&\qquad \text{ya que } I \subseteq K \text{ y la traza es } K\text{-lineal.} \\
&\Leftrightarrow \quad I^{-1}J \subseteq \mathcal{D}_{L/K}^{-1} \quad \text{por (3) de la definición de } \mathcal{D}_{L/K}^{-1} \\
&\Leftrightarrow \quad J \subseteq I\mathcal{D}_{L/K}^{-1}.
\end{aligned}$$

□

Extensiones totalmente ramificadas de grado $p = \mathrm{car}\,(K)$. Consideraremos ahora el caso que nos falta de una extensión de Galois L/K totalmente ramificada de grado $\ell = \mathrm{car}\,(K) = p$. Para comenzar, por (1.54), $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, $L = K(\pi_L)$ para π_L un elemento primo de L y $\overline{L} = K$. Como L/K es cíclica de grado p, sea σ un generador de $G = \mathrm{Gal}(L/K)$. Recordemos que la función i_G definida en (1.80) es: $i_G(\tau) = v_L(\tau(\pi_L) - \pi_L)$ si $\tau \neq 1$ y pongamos

$$t := i_G(\sigma) - 1.$$

Como $i_G(\sigma) > 0$ por (1.80), entonces $t \geq 0$.

Ahora, si $t = 0$ entonces $i_G(\sigma) = 1$ y así $G = G_0$. Nótese que entonces $G_1 = 1$ ya que G_1 es un p-subgrupo de Sylow de G (que es de orden p), y por lo tanto $G_1 = 1$ ó $G_1 = G$, pero $\sigma \notin G_1$ ya que de lo contrario se tendría que $i_G(\sigma) = 1 + 1$ y consecuentemente $t = i_G(\sigma) - 1 \geq 1$, lo que contradice la hipótesis de que $t = 0$. Se sigue que $G_1 = 1$ y por lo tanto $G_j = 1$ para toda $j \geq 1$ cuando $t = 0$.

Ahora, si $t > 0$, como $i_G(\sigma) = t + 1$, entonces, por (1.80), $\sigma \in G_t$ y por lo tanto $G_t = G$; se sigue que

$$G = G_0 = G_1 = \cdots = G_t.$$

Mostraremos ahora que $G_{t+1} = 1$ y consecuentemente se tendrá que

$$1 = G_{t+1} = G_{t+2} = \cdots .$$

En efecto, como G_{t+1} es un subgrupo de G que tiene orden p, entonces G_{t+1} es trivial o es igual a G. Si sucediera que $G_{t+1} = G$, entonces $\sigma \in G_{t+1}$ y por lo tanto $i_G(\sigma) \geq (t+1)+1 > t+1 = i_G(\sigma)$, lo cual es una contradicción. Se sigue que $G_{t+1} = 1$.

Podemos entonces pensar al entero t como el mayor entero tal que $\sigma \in G_t$, o usando (1.81), como el mayor entero tal que $\sigma(\pi_L)/\pi_L \in U_L^{(t)}$. Escribamos entonces

$$(\dagger) \qquad \sigma(\pi_L)/\pi_L = 1 + \gamma\pi_L^t$$

con $\gamma \in U_L \subseteq U_K \cdot U_L^{(1)}$. Nótese que el entero t no depende del elemento primo π_L de L ni del generador σ de $G = \mathrm{Gal}(L/K)$, lo primero por las observaciones antes de (1.80) y lo segundo porque

$$(*) \qquad \sigma^i(\pi_L)/\pi_L^i \equiv 1 + i\gamma\pi_L^t \text{ mód } \pi_L^{t+1},$$

donde esto último sucede ya que por (†) $\sigma(\pi_L)/\pi_L = 1 + \gamma\pi_L^t$ con $\gamma \in U_L \subseteq U_K \cdot U_L^{(1)}$. Se sigue que

$$\left(\frac{\sigma\pi_L}{\pi_L}\right)^i = (1+\gamma\pi_L^t)^i \equiv 1 + i\gamma\pi_L^t \text{ mód } \pi_L^{t+1}.$$

Ahora, para el caso que nos interesa, podemos calcular explícitamente su diferente: si L/K es una extensión cíclica totalmente ramificada de grado ℓ, como antes sea $t = i_G(\sigma) - 1$ para σ un generador de $G = \mathrm{Gal}(L/K)$. Sean π_L un primo de L y $f(x)$ el polinomio de Eisenstein correspondiente. Entonces, $\sigma^i(\pi_L)$ para $0 \leq i \leq \ell - 1$ son todas las raíces de $f(x)$ y así, por (2.13) se tiene que

$$v_L(f'(\pi_L)) = \sum_{i=1}^{\ell-1} i_G(\sigma^i) = \sum_{i \geq 0}(|G_i| - 1)$$

donde G_i son los grupos de ramificación de L/K. Ahora, como vimos antes de la subsección sobre el diferente, los grupos de ramificación de L/K son $G_i = G$ para $0 \leq i \leq t$ y $G_i = 1$ para $i \geq t+1$; y como $|G| = \ell$, entonces

$$v_L(f'(\pi_L)) = \sum_{i=0}^{t}(|G_i| - 1) = \sum_{i=0}^{t}(\ell - 1) = (t+1)(\ell - 1).$$

Hemos así probado:

Corolario 2.15. *Sea L/K una extensión cíclica totalmente ramificada de grado ℓ y sea t definido como antes. Si $m = (t+1)(\ell-1)$, entonces $v_L(f'(\pi_L)) = m$ y por lo tanto $f'(\pi_L) = u\pi_L^m$ con $u \in U_L$, es decir, el diferente de L/K es*

$$\mathcal{D}_{L/K} = \mathfrak{p}_L^m.$$

DEMOSTRACIÓN. La afirmación es consecuencia de los cálculos previos y de (2.12) y (2.13). □

Usando el corolario anterior y los resultados previos sobre el diferente de una extensión, podemos calcular la traza siguiente:

Lema 2.16. *Sea L/K una extensión cíclica totalmente ramificada de grado ℓ y sea t definido como antes. Para $i \geq 0$ pongamos*

$$r(i) := t + 1 + [(i-1-t)/\ell] = \left[\frac{(t+1)(\ell-1)+i}{\ell}\right],$$

donde $[m]$ es el mayor entero $\leq m$. Entonces

$$\mathrm{Tr}_{L/K}(\pi_L^i \mathcal{O}_L) = \pi_K^{r(i)}\mathcal{O}_K.$$

DEMOSTRACIÓN. Si $r \geq 0$ es cualquier entero, por (2.14) y (2.15) se tiene que

$$\begin{aligned}
\mathrm{Tr}_{L/K}(\mathfrak{p}_L^i) \subseteq \mathfrak{p}_K^r \quad &\Leftrightarrow \quad \mathfrak{p}_L^i \subseteq \mathfrak{p}_K^r \mathcal{D}_{L/K}^{-1} = \mathfrak{p}_K^r \mathfrak{p}_L^{-m} \\
&\quad \text{ya que } \mathcal{D}_{L/K} = (f'(\pi_L)) = \mathfrak{p}_L^m \text{ con } m = (t+1)(\ell-1) \\
&\Leftrightarrow \quad \mathfrak{p}_L^i \subseteq \mathfrak{p}_L^{r\ell}\mathfrak{p}_L^{-m} \\
&\quad \text{ya que } \mathfrak{p}_L^\ell = \mathfrak{p}_K \text{ porque } \pi_L^\ell = \pi_K \\
&\Leftrightarrow \quad \mathfrak{p}_L^i \subseteq \mathfrak{p}_L^{r\ell-m}
\end{aligned}$$

y esto último sucede si y sólo si $r\ell - m \leq i$, i.e., si y sólo si $r \leq (m+i)/\ell$.

Ahora, como $\mathrm{Tr}_{L/K}$ es $\mathcal{O}_K$-lineal, entonces $\mathrm{Tr}_{L/K}(\mathfrak{p}_L^i)$ es un ideal de $\mathcal{O}_K$ y por lo tanto es de la forma $\mathfrak{p}_K^{r(i)}$ con $r(i)$ el mayor entero posible, que en vista de la desigualdad anterior es el mayor entero $\leq (m+i)/\ell$, i.e., $r(i) = [(m+i)/\ell]$ como se quería. □

El resultado principal describe la acción de la norma $N_{L/K}$ con respecto a las filtraciones $U^{(i)}$ respectivas en este caso:

Teorema 2.17. *Sea L/K una extensión de campos locales, cíclica totalmente ramificada de grado $p = \mathrm{car}(\overline{K})$. Sea π_L un primo de L (de tal forma que $\pi_K = N_{L/K}\pi_L$ es primo de K) y sea t como antes. Para un entero $i > 1$ definamos la función $\psi(i) = \psi_{L/K}(i)$ mediante*

$$\psi(i) := \begin{cases} i & \text{si} \quad i \leq t \\ t + p(i-t) & \text{si} \quad i \geq t. \end{cases}$$

Entonces:

(1) *La norma $N_{L/K}$ manda U_L en U_K y para $i \geq 1$ manda $U_L^{(\psi(i))}$ en $U_K^{(i)}$ y $U_L^{(\psi(i)+1)}$ en $U_K^{(i+1)}$.*

(2) *Los diagramas siguientes conmutan (donde, como L/K es totalmente ramificada, $\overline{L} = \overline{K}$) y $\phi_p : \overline{\theta} \mapsto \overline{\theta}^p$:*

$$\begin{array}{ccc} L^* & \xrightarrow{v_L} & \mathbb{Z} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle id} \\ K^* & \xrightarrow[v_K]{} & \mathbb{Z} \end{array} \qquad \begin{array}{ccc} U_L & \xrightarrow{\lambda_{0,L}} & \overline{L}^* \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \phi_p} \\ U_K & \xrightarrow[\lambda_{0,K}]{} & K^* \end{array}$$

si $1 \leq i < t$:

$$\begin{array}{ccc} U_L^{(i)} & \xrightarrow{\lambda_{i,L}} & \overline{L} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \phi_p} \\ U_K^{(i)} & \xrightarrow[\lambda_{i,K}]{} & K \end{array}$$

si $i = t$:

$$\begin{array}{ccc} U_L^{(t)} & \xrightarrow{\lambda_{t,L}} & \overline{L} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \overline{\theta} \mapsto \overline{\theta}^p - \overline{\gamma}^{p-1}\overline{\theta}} \\ U_K^{(t)} & \xrightarrow[\lambda_{t,K}]{} & \overline{K} \end{array}$$

si $i > t$, *de tal forma que* $\psi(i) = t + p(i-t)$:

$$\begin{array}{ccc} U_L^{(\psi(i))} & \xrightarrow{\lambda_{\psi(i),L}} & \overline{L} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \bar{\theta}\mapsto(\bar{\theta})(-\bar{\gamma}^{p-1})} \\ U_K^{(i)} & \xrightarrow[\lambda_{i,K}]{} & K. \end{array}$$

(3) *La norma es suprayectiva en el tercero y quinto diagramas.*

DEMOSTRACIÓN. Para comenzar, observemos que como L/K es totalmente ramificada, por (1.54) $L = K(\pi_L)$ con π_L un primo de L y raíz de un polinomio de Eisenstein $f(x)$ con coeficientes en $\mathcal{O}_K$. Entonces, si a_0 es el término independiente de $f(x)$, por (1.90)(5) $N_{L/K}(\pi_L) = \pm a_0$ y como $f(x)$ es de Eisenstein, entonces a_0 es un primo π_K de K. Las afirmaciones (1) y (2) se probarán simultáneamente.

La conmutatividad de los primeros dos diagramas se prueba como en (2.6) y es fácil probar que $N_{L/K}U_L \subseteq U_K$ y $N_{L/K}U_L^{(1)} \subseteq U_K^{(1)}$.

Para el tercer diagrama, observemos primero que como $1 \leq i < t$, entonces $\psi(i) = i$ y $\psi(i) + 1 = i + 1$; ahora pongamos $\varepsilon = 1 + \theta\pi_L^i \in U_L^{(i)}$ con $\theta \in U_L$. Entonces, por el lema (2.2):

$$N_{L/K}(\varepsilon) = 1 + N_{L/K}(\theta)\pi_K^i + \mathrm{Tr}_{L/K}(\theta\pi_L^i) + \mathrm{Tr}_{L/K}(\theta\delta)$$

(ya que $N_{L/K}(\pi_L) = \pi_K$) con $v_L(\delta) \geq 2i$. El lema previo implica que

$$v_K(\mathrm{Tr}_{L/K}(\pi_L^i)) \geq r(i) = t + 1 + \left\lceil i - \frac{1}{p} - t \right\rceil$$

y

$$v_K(\mathrm{Tr}_{L/K}(\delta)) \geq r(2i) = t + 1 + \left\lceil 2i - \frac{1}{p} - t \right\rceil.$$

Ahora, como $t + 1 + \left\lceil i - \frac{1}{p} - t \right\rceil = \left\lceil \frac{(t+1)(p-1)+i}{p} \right\rceil$ y como $1 \leq i < t$ implica que $(i + 1)(p - 1) < (t + 1)(p - 1)$, entonces

$$(i + 1)p - i = (i + 1)(p - 1) + 1 \leq (t + 1)(p - 1)$$

y por lo tanto $(i + 1)p \leq (t + 1)(p - 1) + i$ y así $\left\lceil \frac{(t+1)(p-1)+i}{p} \right\rceil \geq i + 1$, por lo que

$$v_K(\mathrm{Tr}_{L/K}(\pi_L^i) \geq r(i) := \left\lceil \frac{(t + 1)(p - 1) + i}{p} \right\rceil \geq i + 1.$$

En forma análoga se prueba que $v_K(\mathrm{Tr}_{L/K}(\delta)) \geq i+1$. Se sigue entonces que

$$N_{L/K}(\varepsilon) \qquad 1 + N_{L/K}(\theta)\pi_K^i + \mathrm{Tr}_{L/K}(\theta\pi_L^i) + \mathrm{Tr}_{L/K}(\theta\delta)$$
$$1 + N_{L/K}(\theta)\pi_K^i \text{ mód } \mathfrak{p}_K^{i+1},$$

y como $N_{L/K}(\theta)\pi_K^i \in \mathfrak{p}_K^i$, entonces la congruencia anterior muestra que $N_{L/K}$ manda $U_L^{(i)}$ en $U_K^{(i)}$ y $U_L^{(i+1)}$ en $U_K^{(i+1)}$, lo cual prueba (1) en este caso. Más aún, como $\theta \in U_L \subseteq U_K \cdot U_L^{(1)}$, entonces

$$N_{L/K}(\theta\pi_L^i) = N_{L/K}(\theta)\pi_K^i \equiv \theta^p \pi_K^i \text{ mód } \mathfrak{p}_K^{i+1}$$

(porque $\theta \in \mathcal{O}_K$ y $[L:K] = p$) y así $N_{L/K}(\varepsilon) \equiv 1 + \theta^p\pi_K^i$ mód $\mathfrak{p}_K^{i+1}$, por lo que

$$\lambda_{i,K} \circ N_{L/K}(\varepsilon) \equiv \overline{\theta}^p \text{ mód } \mathfrak{p}_K^{i+1} \;=\; \phi_p \circ \lambda_{i,L}(\varepsilon),$$

i.e., el tercer diagrama conmuta.

Para el cuarto diagrama, $i = t$ y así $\psi(i) = t$, $(i+1)(p-1) = (t+1)(p-1)$, por lo que $(i+1)p - i - 1 = (t+1)(p-1)$, y consecuentemente

$$r(i) = \left[\frac{(t+1)(p-1)+i}{p}\right] = \left[\frac{(i+1)p-1}{p}\right] = \left[(i+1) - \frac{1}{p}\right] = i.$$

Entonces, para $\varepsilon = 1 + \theta\pi_L^t \in U_L^{(t)}$, por (2.2) se tiene que

$$N_{L/K}(\varepsilon) = 1 + N_{L/K}(\theta)\pi_K^t + \mathrm{Tr}_{L/K}(\theta\pi_L^t) + \mathrm{Tr}_{L/K}(\theta\delta)$$

con $v_K(\delta) \geq 2t$, por lo que $\mathrm{Tr}_{L/K}(\theta\delta) \in \mathfrak{p}_K^{2t} \subseteq \mathfrak{p}_K^{t+1}$ y así

$$(*) \qquad N_{L/K}(\varepsilon) \equiv 1 + N_{L/K}(\theta\pi_L^t) + \mathrm{Tr}_{L/K}(\theta\pi_L^t) \text{ mód } \mathfrak{p}_K^{t+1}$$

donde, por el lema anterior, notando que para $i = t$ se tiene que $r(i) = r(t) = t$, se sigue que $\mathrm{Tr}_{L/K}(\theta\pi_L^t) \in \mathfrak{p}_K^t$ y $\mathrm{Tr}_{L/K}(\theta\pi_L^{t+1}) \in \mathfrak{p}_K^{t+1}$, y consecuentemente $(*)$ implica que $N_{L/K}$ manda $U_L^{(t)}$ en $U_K^{(t)}$ y $U_L^{(t+1)}$ en $U_K^{(t+1)}$.

Ahora, para calcular $N_{L/K}(\varepsilon)$, recordando la definición de t escribamos

$$\sigma(\pi_L)/\pi_L = 1 + \gamma\pi_L^t \qquad \text{con } \gamma \in U_L.$$

Entonces, como $N_{L/K}(\sigma(\pi_L)/\pi_L) = 1$, se tiene que

$$1 = N_{L/K}(\sigma(\pi_L)/\pi_L) \qquad N_{L/K}(1 + \gamma\pi_L^t)$$
$$1 + N_{L/K}(\gamma)\pi_K^t + \mathrm{Tr}_{L/K}(\gamma\pi_L^t) \text{ mód } \pi_K^{t+1}$$

y así

$$\mathrm{Tr}_{L/K}(\gamma\pi_L^t) \equiv -N_{L/K}(\gamma)\pi_K^t \equiv -\gamma^p\pi_K^t \text{ mód } \pi_K^{t+1},$$

la última congruencia porque $N_{L/K}(\gamma) \equiv \gamma^p$ mód π_L ya que $U_L \subseteq U_K \cdot U_L^{(1)}$ y $N_{L/K}$ actúa en los elementos de K elevando a la potencia p; se sigue que

$$\begin{aligned} N_{L/K}(1+\theta\gamma\pi_L^t) &\equiv 1 + N_{L/K}(\gamma)N_{L/K}(\theta)\pi_K^t + \mathrm{Tr}_{L/K}(\gamma\theta\pi_L^t) \text{ mód } \pi_K^{t+1} \\ &\equiv 1 + \gamma^p\theta^p\pi_K^t + \theta\,\mathrm{Tr}_{L/K}(\gamma\pi_L^t) \text{ mód } \pi_K^{t+1} \text{ ya que } \theta \in \mathcal{O}_K \\ &\equiv 1 + \gamma^p\theta^p\pi_K^t - \theta\gamma^p\pi_K^t \text{ mód } \pi_K^{t+1} \\ &\equiv 1 + \gamma^p\pi_K^t(\theta^p - \theta) \text{ mód } \pi_K^{t+1}. \end{aligned}$$

Se sigue que

$$\lambda_{t,K} \circ N_{L/K}(1+\theta\gamma\pi_L^t) \equiv \lambda_{t,K}(1+\gamma^p(\theta^p-\theta)\pi_K^t) \equiv \overline{\gamma}^p(\overline{\theta}^p - \overline{\theta}) \text{ mód } \pi_K^{t+1}$$

y denotando con μ al morfismo $\overline{\theta} \mapsto \overline{\theta}^p - \overline{\gamma}^{p-1}\overline{\theta}$, entonces

$$\mu \circ \lambda_{t,L}(1+\theta\gamma\pi_L^t) = \mu(\theta\gamma) = \theta\gamma^p - \overline{\gamma}^{p-1}\theta\gamma = \overline{\gamma}^p(\overline{\theta}^p - \overline{\theta})$$

por lo que el cuarto diagrama conmuta.

Para el quinto diagrama, $i > t$ y así $(i+1)p - (i+1) = (i+1)(p-1) > (t+1)(p-1)$, por lo que

$$(i+1)p - (t+1)(p-1) - 1 \geq i+1.$$

Y como $i > t$, entonces $\psi(i) := t + p(i-t) = (i+1)p - (t+1)(p-1) - 1$, por lo que la desigualdad anterior dice que $\psi(i) \geq i+1$ y se tiene que

$$r(\psi(i)) = \left[\frac{(t+1)(p-1) + \psi(i)}{p}\right] = \left[\frac{(i+1)p - 1}{p}\right] = \left[i + 1 - \frac{1}{p}\right] = i$$

y

$$r(\psi(i)+1) = \left[\frac{(t+1)(p-1) + \psi(i) + 1}{p}\right] = \left[\frac{(i+1)p - 1 + 1}{p}\right] = i+1.$$

Entonces, si $\varepsilon = 1 + \theta\pi_L^{\psi(i)} \in U_L^{(\psi(i))}$, como $r(\psi(i)) = i$, por el lema anterior se tiene que $\mathrm{Tr}_{L/K}(\theta\pi_L^{\psi(i)}) \in \mathfrak{p}_K^i$. También, como $N_{L/K}(\theta\pi_L^{\psi(i)}) = N_{L/K}(\theta)\pi_K^{\psi(i)} \in \mathfrak{p}_K^{\psi(i)}$ y como $\mathfrak{p}_K^{\psi(i)} \subseteq \mathfrak{p}_K^{i+1}$ ya que $\psi(i) \geq i+1$, entonces por el

lema (2.2) aplicado a $\varepsilon = 1 + \theta\pi_L^{\psi(i)}$ se tiene que

$$\begin{aligned} N_{L/K}(\varepsilon) \qquad & 1 + N_{L/K}(\theta\pi_L^{\psi(i)}) + \mathrm{Tr}_{L/K}(\theta\pi_L^{\psi(i)}) + \mathrm{Tr}_{L/K}(\theta\delta) \\ & 1 + \mathrm{Tr}_{L/K}(\theta\pi_L^{\psi(i)}) \text{ mód } \mathfrak{p}_K^{i+1} \end{aligned}$$

con $v_K(\delta) \geq 2\psi(i)$ y la congruencia es porque $\psi(i), 2\psi(i) \geq i+1$ y con $\mathrm{Tr}_{L/K}(\theta\pi_L^{\psi(i)}) \in \mathfrak{p}_K^i$. Se sigue que $N_{L/K}$ manda $U_L^{(\psi(i))}$ en $U_K^{(i)}$, y similarmente la norma manda $U_L^{(\psi(i)+1)}$ en $U_K^{(i+1)}$.

Usando ahora que $N_{L/K}(\pi_L) = \pi_K$, como $[L : K] = p$, por definición de la valuación en L se tiene que $\pi_L^p = \pi_K$ salvo una unidad de K; entonces los elementos de $U_L^{(\psi(i))} = U_L^{(t+p(i-t))}$ los podemos escribir de la forma

$$\varepsilon = 1 + \theta\pi_L^{t+p(i-t)} = 1 + \theta\pi_L^{p(i-t)}\pi_L^t = 1 + \theta\pi_K^{i-t}\pi_L^t$$

con $\theta \in \mathcal{O}_K$. Entonces la congruencia de arriba queda

$$\begin{aligned} N_{L/K}(1 + \theta\gamma\pi_L^{t+p(i-t)}) \qquad & 1 + \mathrm{Tr}_{L/K}(\gamma\theta\pi_L^{t+p(i-t)}) \text{ mód } \pi_K^{i+1} \\ - \quad & 1 + \mathrm{Tr}_{L/K}((\theta\pi_K^{i-t})\gamma\pi_L^t) \text{ mód } \pi_K^{i+1} \\ - \quad & 1 + \theta\pi_K^{i-t}\mathrm{Tr}_{L/K}(\gamma\pi_L^t) \text{ mód } \pi_K^{i+1} \\ & 1 - \theta\pi_K^{i-t}\gamma^p\pi_K^t \text{ mód } \pi_K^{i+1} \\ & 1 - \theta\pi_K^i\gamma^p \text{ mód } \pi_K^{i+1}, \end{aligned}$$

la penúltima congruencia por el cálculo $\mathrm{Tr}_{L/K}(\gamma\pi_L^t) \equiv -\gamma^p\pi_K^t$ mód π_K^{i+1} que hicimos para el cuarto diagrama. Se sigue que

$$\lambda_{i,K} \circ N_{L/K}(1 + \theta\gamma\pi_L^{t+p(i-t)}) \equiv \lambda_{i,K}(1 - \theta\gamma^p\pi_K^i) \equiv -\overline{\theta}\overline{\gamma}^p \text{ mód } \pi_K^{i+1},$$

y denotando con μ al morfismo vertical derecho del quinto diagrama, se tiene que

$$\mu \circ \lambda_{t+p(i-t),L}(1 + \theta\gamma\pi_L^{t+p(i-t)}) \equiv \mu(\overline{\theta}\overline{\gamma}) \equiv -\overline{\theta}\overline{\gamma}\overline{\gamma}^{p-1} \equiv -\overline{\theta}\overline{\gamma}^p \text{ mód } \pi_K^{i+1},$$

i.e., el quinto diagrama conmuta.

Para la parte (3) del teorema, en el tercer diagrama ϕ_p es un isomorfismo y así la suprayectividad de la norma en el tercer diagrama se sigue como en (2.5)(1) usando la conmutatividad del tercer diagrama en el teorema anterior y el lema (2.1). Similarmente para la norma en el quinto diagrama, usando el hecho de que multiplicación por $-\overline{\gamma}^{p-1}$ es un isomorfismo. □

Corolario 2.18. *Sea L/K una extensión de campos locales cíclica totalmente ramificada de grado $p = \text{car}\,(K)$ y sea t como antes. Entonces:*

(1) $N_{L/K}U_L^{(\psi(i)+1)} = U_K^{(i+1)}$ *para todo* $i \geq t$.

(2) $N_{L/K}U_L^{(t+1)} = U_K^{(t+1)}$.

(3) $K^*/N_{L/K}L^*$ *es cíclico de orden* p.

DEMOSTRACIÓN. (1): Como $i + 1 > t$, entonces

$$\psi(i+1) = t + p(i+1-t) = t + p(i-t) + p > t + p(i-t) + 1 = \psi(i) + 1$$

por lo que

$$U_L^{(\psi(i+1))} \subseteq U_L^{(\psi(i)+1)}$$

y la parte (1) del teorema anterior nos dice que

$$(**) \qquad N_{L/K}U_L^{(\psi(i)+1)} \subseteq U_K^{(i+1)}.$$

Ahora, como $i + 1 > t$, se sigue que

$$\begin{aligned} U_K^{(i+1)} \quad & N_{L/K}U_L^{(\psi(i+1))} \quad \text{por la parte (3) del teorema previo} \\ \subseteq \quad & N_{L/K}U_L^{(\psi(i)+1)} \quad \text{por } (*) \\ \subset \quad & U_K^{(i+1)} \quad \text{por } (**) \end{aligned}$$

y así las inclusiones anteriores son igualdades, en particular $U_K^{(i+1)} = N_{L/K}U_L^{(\psi(i)+1)}$ como se quería. La parte (2) es un caso particular de (1) notando que $\psi(t) = t$.

Para (3), considere primero el diagrama conmutativo (por el diagrama (4) del teorema)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^{(t+1)} & \longrightarrow & U_L^{(t)} & \xrightarrow{\lambda_{t,L}} & \overline{L} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \mu} & & \\ 0 & \longrightarrow & U_K^{(t+1)} & \longrightarrow & U_K^{(t)} & \xrightarrow[\lambda_{t,K}]{} & K & \longrightarrow & 0 \end{array}$$

donde μ es el morfismo del diagrama (4) del teorema anterior, i.e., $\mu(\overline{\theta}) = \overline{\theta}^p - \overline{\gamma}^{p-1}\overline{\theta}$. Denotemos los tres morfismos verticales por N', N, μ y notemos

que Coker $(N') = 0$ por la parte (2) de este corolario, de tal forma que la sucesión núcleo-conúcleo implica que

$$\text{Coker}\,(N) = U_K^{(t)}/N_{L/K}U_L^{(t)} \simeq .\text{Coker}\,(\mu).$$

Calculemos ahora el conúcleo de μ: es claro que $\overline{\gamma} \neq 0$ está en el núcleo de μ. Entonces

$$\mu(\overline{\theta}) = \overline{\theta}^p - \overline{\gamma}^{p-1}\overline{\theta} = \overline{\gamma}^p((\overline{\theta}/\overline{\gamma})^p - \overline{\theta}/\overline{\gamma}) = \overline{\gamma}^p(\wp(\overline{\theta}/\overline{\gamma}))$$

con $\overline{\gamma}^p \neq 0$ y donde $\wp : K \to K$ es el morfismo de Artin-Schreier $\wp(\alpha) = \alpha^p - \alpha$, (véase el Anexo 2). Se sigue que $\text{Im}\,(\mu) = \overline{\gamma}^p \text{Im}\,(\wp) \simeq \text{Im}\,(\wp) = \wp(K)$ y por lo tanto

$$(a) \qquad U_K^{(t)}/N_{L/K}U_L^{(t)} \simeq \overline{K}/\wp(\overline{K}).$$

Mostraremos ahora que

$$(b) \qquad N_{L/K} : U_L/U_L^{(i)} \longrightarrow U_K/U_K^{(i)}$$

es un isomorfismo para toda $1 \leq i \leq t$ por inducción sobre $i \geq 1$.

En efecto, consideremos el diagrama conmutativo siguiente:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^{(t-1)}/U_L^{(t)} & \longrightarrow & U_L/U_L^{(t-1)} & \longrightarrow & U_L/U_L^{(t)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N'} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N''} & & \\ 0 & \longrightarrow & U_K^{(t-1)}/U_K^{(t)} & \longrightarrow & U_K/U_K^{(t-1)} & \longrightarrow & U_K/U_K^{(t)} & \longrightarrow & 0 \end{array}$$

donde los morfismos verticales son inducidos por la norma $N_{L/K}$. Observamos ahora que N' es un isomorfismo por la conmutatividad del tercer diagrama en el teorema previo y N es un isomorfismo por hipótesis de inducción. Se sigue que N'' también es un isomorfismo.

Consideremos ahora el diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^{(t)} & \longrightarrow & U_L & \longrightarrow & U_L/U_L^{(t)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \\ 0 & \longrightarrow & U_K^{(t)} & \longrightarrow & U_K & \longrightarrow & U_K/U_K^{(t)} & \longrightarrow & 0 \end{array}$$

donde, denotando los morfismos verticales por N', N, N'' y usando el hecho de que el núcleo y el conúcleo de N'' son 0 por el paso (b) anterior, de la sucesión núcleo-conúcleo se sigue que

$$(c) \qquad U_L/N_{L/K}U_K \simeq U_K^{(t)}/N_{L/K}U_L^{(t)}.$$

Finalmente, consideremos el diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle f=1} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow[v_K]{} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

donde $f = f(L/K) = 1$ y la sucesión núcleo-conúcleo implican que

$$(d) \qquad U_K/N_{L/K}U_L \simeq K^*/N_{L/K}L^*.$$

Los isomorfismos (a), (c) y (d) implican que

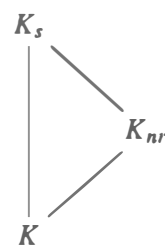
$$K^*/N_{L/K}L^* \simeq K/\wp(K),$$

y este último grupo cociente es cíclico de orden p. □

2.2 Levantamientos de Frobenius

El automorfismo de Frobenius es uno de los principales personajes de la teoría que desarrollaremos, y en esta sección comenzamos mostrando que si L/K es una extensión finita de Galois de campos locales, todo $\sigma \in \mathrm{Gal}(L/K)$ se vuelve el Frobenius de una extensión asociada a L/K (2.20).

Sea K un campo local y sea $K_s = K_{sep}$ una cerradura separable de K. En el diagrama de extensiones siguiente:



se tiene el epimorfismo canónico

$$\rho_K : \mathrm{Gal}(K_s/K) \twoheadrightarrow \mathrm{Gal}(K_{nr}/K) \simeq \widehat{\mathbb{Z}}$$

dado como sigue: ya que $\mathrm{Gal}(K_{nr}/K) \simeq \widehat{\mathbb{Z}}$ está generado topológicamente por el Frobenius Fr_K y el isomorfismo $\mathrm{Gal}(K_{nr}/K) \simeq \widehat{\mathbb{Z}}$ está dado por $\mathrm{Fr}_K^{\alpha} \mapsto \alpha \in \widehat{\mathbb{Z}}$, entonces ρ_K está definido mediante restricción: $\sigma \mapsto \sigma|_{K_{nr}} = \mathrm{Fr}_K^{\alpha} \mapsto \alpha$.

Ahora, si L/K es una extensión finita de campos locales, sabemos por (1.51) que $L_{nr} = LK_{nr}$ y si $L_0 = L \cap K_{nr}$, entonces L/L_0 es totalmente ramificada y L_0/K es no ramificada; y por lo tanto,

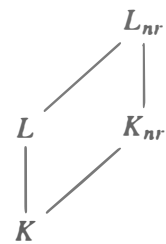
$$f(L/K) = f(L/L_0)f(L_0/K) = f(L_0/K) = [L_0 : K].$$

Ahora, si L/K es una extensión finita separable de campos locales (donde asumimos que $L_s = K_s$) y si $\iota : \mathrm{Gal}(L_s/L) \hookrightarrow \mathrm{Gal}(K_s/K)$ es la inclusión natural, $L_0 := L \cap K_{nr}$ y $f(L/K) = [L_0 : K]$, entonces el diagrama siguiente conmuta:

$$\begin{array}{ccc} \mathrm{Gal}(L_s/L) & \xrightarrow{\rho_L} & \mathrm{Gal}(L_{nr}/L) \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle f(L/K)} \\ \mathrm{Gal}(K_s/K) & \xrightarrow{\rho_K} & \mathrm{Gal}(K_{nr}/K) \end{array}$$

i.e., $\rho_K = f(L/K)\rho_L$, en particular, $\mathrm{Fr}_L|_{K_{nr}} = \mathrm{Fr}_K^{f(L/K)}$.

Para comenzar, pasemos de la extensión L/K a la extensión L_{nr}/K en el diagrama siguiente:



y consideremos el epimorfismo canónico $\rho_{L/K} : \mathrm{Gal}(L_{nr}/K) \twoheadrightarrow \mathrm{Gal}(K_{nr}/K) \simeq \widehat{\mathbb{Z}}$ dado por $\sigma \mapsto \sigma|_{K_{nr}} = \mathrm{Fr}_K^{\alpha} \mapsto \alpha$ y pongamos

$$\mathrm{Frob}(L/K) := \{\tilde{\sigma} \in \mathrm{Gal}(L_{nr}/K) \ : \ \rho_{L/K}(\tilde{\sigma}) \in \mathbb{N} \subseteq \widehat{\mathbb{Z}}\},$$

donde enfatizamos que $0 \notin \mathbb{N}$.

Lema 2.19. *Sea L/K una extensión finita de Galois de campos locales. Entonces:*

(1) *La aplicación natural* $\rho : \mathrm{Frob}(L/K) \longrightarrow \mathrm{Gal}(L/K)$ *dada por restricción:* $\widetilde{\sigma} \mapsto \widetilde{\sigma}|_L$, *es suprayectiva.*

(2) *El conjunto* $\mathrm{Frob}(L/K)$ *es cerrado bajo productos pero no es cerrado bajo inversos y* $1 \notin \mathrm{Frob}(L/K)$.

DEMOSTRACIÓN. (1): Dado un $\sigma \in \mathrm{Gal}(L/K)$, su restricción $\sigma|_{L_0}$ es tal que $\sigma|_{L_0} = (\mathrm{Fr}_K|_{L_0})^n$ para algún entero $n \geq 1$. Sea $\widetilde{\mathrm{Fr}} \in \mathrm{Gal}(L_{nr}/K)$ cualquier extensión de $\mathrm{Fr}_K \in \mathrm{Gal}(K_{nr}/K)$ a L_{nr}. Entonces, como $\sigma\widetilde{\mathrm{Fr}}^{-n}|_{L_0} = id_{L_0}$ (por la elección de n) se sigue que $\sigma\widetilde{\mathrm{Fr}}^{-n}|_L \in \mathrm{Gal}(L/L_0) \simeq \mathrm{Gal}(L_{nr}/K_{nr})$ y por lo tanto $\sigma\widetilde{\mathrm{Fr}}^{-n}|_L = \tau|_L$ para algún $\tau \in \mathrm{Gal}(L_{nr}/K_{nr})$.

Ahora, poniendo $\widetilde{\sigma} := \tau\widetilde{\mathrm{Fr}}^n$ observamos que $\widetilde{\sigma} \in \mathrm{Frob}(L/K)$ ya que

$$\widetilde{\sigma}|_{K_{nr}} = \tau\widetilde{\mathrm{Fr}}^n|_{K_{nr}} = \widetilde{\mathrm{Fr}}^n|_{K_{nr}} = \mathrm{Fr}_K^n$$

(la segunda igualdad porque $\tau|_{K_{nr}} = id$ y la última igualdad por definición de $\widetilde{\mathrm{Fr}}$). Se sigue que

$$\rho_K(\widetilde{\sigma}) = \widetilde{\sigma}|_{K_{nr}} = \mathrm{Fr}_K^n$$

y como bajo el isomorfismo $\mathrm{Gal}(K_{nr}/K) \simeq \widehat{\mathbb{Z}}$ se tiene que $\mathrm{Fr}_K^n \mapsto n \in \widehat{\mathbb{Z}}$, hemos así probado que $\rho_K(\widetilde{\sigma}) = n \in \mathbb{N} \subseteq \widehat{\mathbb{Z}}$, i.e., $\widetilde{\sigma} \in \mathrm{Frob}(L/K)$.

Finalmente se tiene que

$$\widetilde{\sigma}|_L = \tau\widetilde{\mathrm{Fr}}^n|_L = \sigma$$

por definición de $\widetilde{\sigma}$ y así ρ es suprayectiva.

Para (2), es claro que $1 \notin \mathrm{Frob}(L/K)$ porque $\rho_K(id_{L_{nr}}) = id_{K_{nr}} = \mathrm{Fr}_K^0$ y $0 \notin \mathbb{N}$. Que $\mathrm{Frob}(L/K)$ es cerrado bajo productos es porque si $\widetilde{\sigma}_1, \widetilde{\sigma}_2 \in \mathrm{Frob}(L/K)$, entonces

$$\rho_K(\widetilde{\sigma}_1\widetilde{\sigma}_2) = \rho_K(\widetilde{\sigma}_1)\rho_K(\widetilde{\sigma}_2) = \mathrm{Fr}_K^{\alpha_1}\mathrm{Fr}_K^{\alpha_2} = \mathrm{Fr}_K^{\alpha_1+\alpha_2} = \alpha_1 + \alpha_2 = \rho_K(\widetilde{\sigma}_1) + \rho_K(\widetilde{\sigma}_2),$$

y así $\rho_K(\widetilde{\sigma}_1\widetilde{\sigma}_2) = \rho_K(\widetilde{\sigma}_1) + \rho_K(\widetilde{\sigma}_2) \in \mathbb{N}$. □

Sea $\sigma \in \mathrm{Gal}(L/K)$; si $\widetilde{\sigma} \in \mathrm{Frob}(L/K) \subseteq \mathrm{Gal}(L_{nr}/K)$ es tal que $\rho(\widetilde{\sigma}) = \sigma$, diremos que $\widetilde{\sigma}$ es un *levantamiento* de σ. La propiedad que nos interesa de este levantamiento es que para cada elemento σ de $\mathrm{Gal}(L/K)$, su levantamiento $\widetilde{\sigma}$ es el Frobenius Fr_Σ de la subextensión Σ/K de L_{nr}/K dada por el campo fijo Σ de $\widetilde{\sigma}$:

Proposición 2.20. *Sea* $\widetilde{\sigma} \in \mathrm{Gal}(L_{nr}/K)$ *un levantamiento de* $\sigma \in \mathrm{Gal}(L/K)$ *y sea* $\Sigma = L_{nr}^{\langle\widetilde{\sigma}\rangle}$ *el campo fijo de* $\widetilde{\sigma}$. *Entonces:*

(1) $[\Sigma : K] < \infty$.

(2) *Si* $\Sigma_0 = \Sigma \cap K_{nr}$, *entonces* Σ_0 *es el campo fijo de* $\widetilde{\sigma}|_{K_{nr}} \in \mathrm{Gal}(K_{nr}/K)$ *y* $\widetilde{\sigma}|_{K_{nr}} = \mathrm{Fr}_K^{[\Sigma_0:K]}$, *i.e.,* $\rho_{\Sigma/K}(\widetilde{\sigma}) = f(\Sigma/K) = [\Sigma_0 : K]$.

(3) $\Sigma_{nr} = L_{nr}$.

(4) $\widetilde{\sigma} = \mathrm{Fr}_\Sigma \in \mathrm{Gal}(\Sigma_{nr}/\Sigma)$.

Demostración. (2): Es claro que Σ_0 es el campo fijo de $\widetilde{\sigma}|_{K_{nr}} = \rho_{\Sigma/K}(\widetilde{\sigma}) \in \mathrm{Gal}(K_{nr}/K)$ y así

$$\mathrm{Gal}(K_{nr}/\Sigma_0) \simeq \langle \widetilde{\sigma}|_{K_{nr}} \rangle \subseteq \mathrm{Gal}(K_{nr}/K)$$

por lo que $\widetilde{\sigma}|_{K_{nr}} = \mathrm{Fr}_K^{[\Sigma_0:K]}$, i.e., $\rho_{\Sigma/K}(\widetilde{\sigma}|_{K_{nr}}) = [\Sigma_0 : K] = f(\Sigma/K)$.

(1): Por (1.52) con $L = \Sigma$ se tiene que

$$[\Sigma : \Sigma_0] = [\Sigma_{nr} : K_{nr}] = [\Sigma K_{nr} : K_{nr}] \leq [L_{nr} : K_{nr}] = [L : K] < \infty$$

y como Σ_0/K es no ramificada por (1.52), entonces

$$[\Sigma_0 : K] = f(\Sigma/K) < \infty$$

y por lo tanto $[\Sigma : K] = [\Sigma : \Sigma_0][\Sigma_0 : K] < \infty$.

(3): Como $\Sigma \subseteq L_{nr}$, entonces $\Sigma_{nr} \subseteq L_{nr}$ y así se tiene el epimorfismo canónico

$$\rho_{L/\Sigma} : \mathrm{Gal}(L_{nr}/\Sigma) \twoheadrightarrow \mathrm{Gal}(\Sigma_{nr}/\Sigma).$$

Ahora, como $\mathrm{Gal}(L_{nr}/\Sigma) = \langle\widetilde{\sigma}\rangle$ es un grupo (profinito, véase §1.9) cíclico generado por $\widetilde{\sigma}$ por definición de $\Sigma = L_{nr}^{\langle\widetilde{\sigma}\rangle}$, entonces para cada $n \geq 1$ se tienen epimorfismos

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(L_{nr}/\Sigma)/\mathrm{Gal}(L_{nr}/\Sigma)^n$$

dados por: $1 \ (\mathrm{mód}\ n) \mapsto \widetilde{\sigma}$ mód $\mathrm{Gal}(L_{nr}/\Sigma)^n$. Se sigue que la composición

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(L_{nr}/\Sigma)/\mathrm{Gal}(L_{nr}/\Sigma)^n \to \mathrm{Gal}(\Sigma_{nr}/\Sigma)/\mathrm{Gal}(\Sigma_{nr}/\Sigma)^n \to \mathbb{Z}/n\mathbb{Z}$$

es un isomorfismo y por lo tanto

$$\mathrm{Gal}(L_{nr}/\Sigma)/\mathrm{Gal}(L_{nr}/\Sigma)^n \simeq \mathrm{Gal}(\Sigma_{nr}/\Sigma)/\mathrm{Gal}(\Sigma_{nr}/\Sigma)^n$$

i.e., el epimorfismo canónico

$$\rho_{L/\Sigma} : \mathrm{Gal}(L_{nr}/\Sigma) \twoheadrightarrow \mathrm{Gal}(\Sigma_{nr}/\Sigma)$$

es un isomorfismo y consecuentemente en la torre de extensiones $\Sigma \subseteq \Sigma_{nr} \subseteq L_{nr}$ se debe tener que $\mathrm{Gal}(L_{nr}/K_{nr}) = \{1\}$, i.e., $[L_{nr} : \Sigma_{nr}] = 1$, i.e., $L_{nr} = \Sigma_{nr}$.

Finalmente, como

$$\rho_{\Sigma}(\widetilde{\sigma}) = \frac{1}{f(\Sigma/K)}\rho_K(\widetilde{\sigma}) = \frac{1}{f(\Sigma/K)}[\Sigma_0 : K] = 1$$

la última igualdad por (1), entonces $\widetilde{\sigma}$ va a dar al generador Fr_{Σ} de $\mathrm{Gal}(\Sigma_{nr}/\Sigma)$, lo cual prueba (4). □

2.3 El morfismo de Neukirch

Si L/K es una extensión finita de Galois de campos locales, en esta sección, siguiendo a Neukirch [30], construimos un isomorfismo de grupos

$$\Psi_{L/K} : K^*/N_{L/K}L^* \longrightarrow \mathrm{Gal}^{ab}(L/K)$$

donde $\mathrm{Gal}^{ab}(L/K)$ es la abelianización del grupo de Galois $\mathrm{Gal}(L/K)$. Este isomorfismo se llama *el isomorfismo de reciprocidad local* o *isomorfismo de Artin local*. La construcción que daremos, debida a J. Neukirch [30], es elemental y procede construyendo primero un homomorfismo (llamado el *morfismo de Neukirch*):

$$\Upsilon_{L/K} : \mathrm{Gal}^{ab}(L/K) \longrightarrow K^*/N_{L/K}L^*,$$

probando después que $\Upsilon_{L/K}$ es un isomorfismo, para definir el morfismo de reciprocidad $\Psi_{L/K}$ como el inverso de $\Upsilon_{L/K}$. Comenzamos con la construcción del morfismo de Neukirch.

Definición 2.21. Sea L/K una extensión finita de Galois de campos locales y sea $\mathrm{Frob}(L/K)$ el conjunto de levantamientos de Frobenius de L/K (véase (2.19)). Se define

$$\widetilde{\Upsilon}_{L/K} : \mathrm{Frob}(L/K) \longrightarrow K^*/N_{L/K}L^*$$

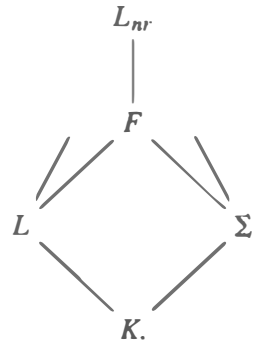
mediante

$$\Upsilon_{L/K}(\widetilde{\sigma}) := N_{\Sigma/K}(\pi_{\Sigma}) \text{ mód } N_{L/K}L^*,$$

donde $\Sigma = L_{nr}^{\langle\widetilde{\sigma}\rangle}$ es el campo fijo de $\widetilde{\sigma}$ y π_{Σ} es un elemento primo de Σ.

Lema 2.22. $\Upsilon_{L/K} : \mathrm{Frob}(L/K) \longrightarrow K^*/N_{L/K}L^*$ *es una función bien definida, i.e., no depende de la elección del primo* π_{Σ} *en el campo fijo* Σ *de* $\widetilde{\sigma}$.

DEMOSTRACIÓN. Sean π_1, π_2 elementos primos de Σ. Entonces, $\pi_1 = u\pi_2$ para alguna unidad $u \in U_\Sigma$. Sea $F = \Sigma L$ el campo compuesto correspondiente:



Como Σ/K y L/K son de grado finito, entonces F/K también es de grado finito. Más aún, F/Σ es no ramificada ya que $L_{nr} = \Sigma_{nr}$ y F/Σ está contenida en Σ_{nr}/Σ, y así $N_{F/\Sigma}(U_F) = U_\Sigma$ por (2.5); en particular, $u \in U_\Sigma$ lo podemos escribir como $u = N_{F/\Sigma}(\varepsilon)$ para algún $\varepsilon \in U_F$. Se sigue que

$$\begin{aligned} N_{\Sigma/K}(\pi_1) &= N_{\Sigma/K}(\pi_2 u) = N_{\Sigma/K}(\pi_2)N_{\Sigma/K}(u) \\ &= N_{\Sigma/K}(\pi_2)N_{\Sigma/K}(N_{F/\Sigma}(\varepsilon)) \\ &= N_{\Sigma/K}(\pi_2)N_{L/K}(N_{F/L}(\varepsilon)), \end{aligned}$$

la última igualdad por la conmutatividad del diagrama anterior.

Por lo tanto, $N_{\Sigma/K}(\pi_1)$ es igual a $N_{\Sigma/K}(\pi_2)$ módulo un factor en $N_{L/K}L^*$, i.e., $N_{\Sigma/K}(\pi_1) \equiv N_{\Sigma/K}(\pi_2)$ mód $N_{L/K}L^*$. □

Para mostrar que la función $\Upsilon_{L/K}$ induce un homomorfismo de grupos

$$\Upsilon_{L/K} : \mathrm{Gal}(L/K) \longrightarrow K^*/N_{L/K}L^*$$

necesitaremos el resultado siguiente:

Teorema 2.23. *Sean $\widetilde{\sigma}_1, \widetilde{\sigma}_2, \widetilde{\sigma}_3 \in \mathrm{Frob}(L/K)$ tales que $\widetilde{\sigma}_3 = \widetilde{\sigma}_2\widetilde{\sigma}_1$ y sean Σ_1, Σ_2, Σ_3 los campos fijos correspondientes. Si π_1, π_2, π_3 son primos en $\Sigma_1, \Sigma_2, \Sigma_3$, entonces*

$$N_{\Sigma_3/K}(\pi_3) \equiv N_{\Sigma_1/K}(\pi_1)N_{\Sigma_2/K}(\pi_2) \text{ mód } N_{L/K}L^*.$$

DEMOSTRACIÓN. (Neukirch). Sea $\widetilde{\mathrm{Fr}}_K \in \mathrm{Frob}(L/K) \subseteq \mathrm{Gal}(L_{nr}/K)$ un levantamiento del Frobenius $\mathrm{Fr}_K \in \mathrm{Gal}(K_{nr}/K)$ y sea Σ el campo fijo de

$\widetilde{\mathrm{Fr}}_K$. Entonces $\Sigma_0 := \Sigma \cap K_{nr} = K$ ya que por (2.20) Σ_0 es el campo fijo de $\widetilde{\mathrm{Fr}}_K|_{K_{nr}} = \mathrm{Fr}_K$.

Sea L'/K la menor extensión de Galois contenida en L_{nr}/K tal que $L, \Sigma, \Sigma_i \subseteq L'$, donde Σ_i son los campos del enunciado del lema. Entonces $L'_{nr} = L_{nr}$ y los automorfismos $\widetilde{\sigma}_i$ del enunciado se pueden considerar elementos de $\mathrm{Frob}(L'/K)$. Si probamos que

$$N_{\Sigma_3/K}\pi_3 \equiv N_{\Sigma_1/K}\pi_1 N_{\Sigma_2/K}\pi_2 \text{ mód } N_{L'/K}L'^*,$$

como $N_{L'/K}L'^* \subseteq N_{L/K}L^*$ ya que $L \subseteq L'$, entonces la congruencia del teorema ya estaría probada. Podemos suponer entonces, sin perder generalidad, que L contiene a los campos Σ, Σ_i.

Pongamos $n_i = \rho_K(\widetilde{\sigma}_i) = [\Sigma_0^i : K]$ por (2.20)(2). Como $\widetilde{\sigma}_3 = \widetilde{\sigma}_2\widetilde{\sigma}_1$, entonces $n_3 = n_1 + n_2$. Consideremos ahora el automorfismo $\widetilde{\sigma}_4 := \widetilde{\mathrm{Fr}}_K^{-n_2}\widetilde{\sigma}_1\widetilde{\mathrm{Fr}}_K^{n_2}$; entonces $n_4 := \rho_K(\widetilde{\sigma}_4) = n_1$. Más aún, el campo fijo de $\widetilde{\sigma}_4$ es $\Sigma_4 := \mathrm{Fr}_K^{n_2}(\Sigma_1)$ y está contenido en L. Además $\pi_4 := \mathrm{Fr}_K^{n_2}(\pi_1)$ es un primo de Σ_4. Como $N_{\Sigma_4/K}\pi_4 = N_{\Sigma_1/K}\pi_1$ y como los π_i son primos de L porque L/Σ_i es no ramificada ya que $\Sigma_i^{nr} = L_{nr}$. Entonces la congruencia que debemos probar es

$$N_{\Sigma_3/K}\pi_3 \equiv N_{\Sigma_4/K}\pi_4 N_{\Sigma_2/K}\pi_2 \text{ mód } N_{L/K}L^*.$$

Pongamos $\tau_i := \widetilde{\mathrm{Fr}}_K^{n_i}\widetilde{\sigma}_i^{-1} \in \mathrm{Gal}(L_{nr}/K_{nr})$. Entonces

$$\begin{aligned}
\tau_3 &= \widetilde{\mathrm{Fr}}_K^{n_3}\widetilde{\sigma}_3^{-1} = \widetilde{\mathrm{Fr}}_K^{n_1+n_2}(\widetilde{\sigma}_2\widetilde{\sigma}_1)^{-1} \\
&\quad \widetilde{\mathrm{Fr}}_K^{n_1}\widetilde{\mathrm{Fr}}_K^{n_2}\widetilde{\sigma}_1^{-1}\widetilde{\sigma}_2^{-1} = \widetilde{\mathrm{Fr}}_K^{n_1}(\widetilde{\mathrm{Fr}}_K^{n_2}\widetilde{\sigma}_1^{-1}\widetilde{\mathrm{Fr}}_K^{-n_2})\widetilde{\mathrm{Fr}}_K^{n_2}\widetilde{\sigma}_2^{-1} \\
&- \quad \widetilde{\mathrm{Fr}}_K^{n_1}\widetilde{\sigma}_4^{-1}\tau_2 \\
&\quad \widetilde{\mathrm{Fr}}_K^{n_4}\widetilde{\sigma}_4^{-1}\tau_2 \quad \text{ya que } n_1 = n_4 \\
&\quad \tau_4\tau_2
\end{aligned}$$

y además $\tau_i(\pi_i) = \widetilde{\mathrm{Fr}}_K^{n_i}\widetilde{\sigma}_i^{-1}(\pi_i) = \widetilde{\mathrm{Fr}}_K^{n_i}(\pi_i)$ ya que $\pi_i \in \Sigma_i$ y Σ_i es el campo fijo de $\widetilde{\sigma}_i$. Pongamos

$$\widehat{\pi}_i := \prod_{j=0}^{n_i-1} \widetilde{\mathrm{Fr}}_K^j(\pi_i).$$

Entonces por (1.27)(2) $v_L(\widehat{\pi}_i) = \sum_{j=0}^{n_i-1} v_L(\pi_i) = n_i$ ya que $v_L(\pi_i) = 1$ porque los π_i son primos de L. Se sigue que $v_L(\widehat{\pi}_3\widehat{\pi}_2^{-1}\widehat{\pi}_4^{-1}) = n_3 - n_2 - n_4 =$

$n_3 - n_2 - n_1 = n_3 - n_3 = 0$ y así $\widehat{\pi}_3\widehat{\pi}_2^{-1}\widehat{\pi}_4^{-1} =: \varepsilon \in U_L$. Por otra parte,

$$\frac{\widetilde{\mathrm{Fr}}_K(\widehat{\pi}_i)}{\widehat{\pi}_i} = \frac{\prod_{j=0}^{n_i-1}\widetilde{\mathrm{Fr}}_K^{j+1}(\pi_i)}{\prod_{j=0}^{n_i-1}\widetilde{\mathrm{Fr}}_K^{j}(\pi_i)} = \frac{\widetilde{\mathrm{Fr}}_K^{n_i}(\pi_i)}{\pi_i} = \frac{\tau_i(\pi_i)}{\pi_i}$$

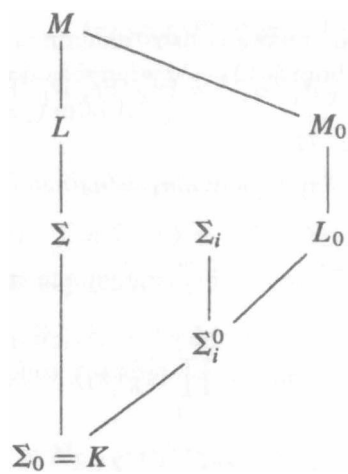
por lo que

$$\begin{aligned}\frac{\widetilde{\mathrm{Fr}}_K(\varepsilon)}{\varepsilon} &= \widetilde{\mathrm{Fr}}_K^{n_3}(\pi_3)\pi_3^{-1}\widetilde{\mathrm{Fr}}_K^{n_2}(\pi_2^{-1})\pi_2\widetilde{\mathrm{Fr}}_K^{n_4}(\pi_4^{-1})\pi_4\\ &= \tau_3(\pi_3)\pi_3^{-1}\tau_2(\pi_2^{-1})\pi_2\tau_4(\pi_4^{-1})\pi_4\end{aligned}$$

y como π_i son primos de L, entonces difieren por unidades, digamos $\pi_3\pi_2^{-1} = \varepsilon_2 \in U_L$, $\pi_4^{-1}\tau_2(\pi_3) = \varepsilon_4 \in U_L$ (ya que $\tau_2\pi_3$ también es primo de L); por lo tanto, podemos escribir

$$\begin{aligned}\widetilde{\mathrm{Fr}}_K(\varepsilon)\varepsilon^{-1} &= \tau_3(\pi_3)\pi_3^{-1}\tau_2(\pi_2^{-1})\pi_2\tau_4(\pi_4^{-1})\pi_4\\ &= (\tau_4\tau_2)(\pi_3)\varepsilon_2^{-1}\pi_2^{-1}\tau_2(\pi_2^{-1})\pi_2\tau_4\tau_2(\pi_3)^{-1}\tau_4(\varepsilon_4)\varepsilon_4^{-1}\tau_2(\pi_3)\\ &= \tau_2(\varepsilon_2)\varepsilon_2^{-1}\tau_4(\varepsilon_4)\varepsilon_4^{-1}.\end{aligned}$$

Pongamos $L_0 = L \cap K_{nr}$ y sea M_0/L_0 la subextensión no ramificada de L_{nr}/L_0 de grado $n = [L : K]$. Consideremos el campo compuesto $M := M_0L$:



Entonces, $M \cap K_{nr} = M_0$ y M/L es no ramificada de grado n, M/M_0 es Galois y $\mathrm{Gal}(M/M_0) \simeq \mathrm{Gal}(L/L_0)$.

Como M/L es no ramificada, $N_{M/L} : U_M \to U_L$ es un isomorfismo por (2.5) y así para $\varepsilon, \varepsilon_2, \varepsilon_4 \in U_L$ existen unidades $u, u_2, u_4 \in U_M$ tales que $N_{M/L}(u) = \varepsilon$, $N_{M/L}(u_2) = \varepsilon_2$ y $N_{M/L}(u_4) = \varepsilon_4$. Usando la igualdad para $\widetilde{\mathrm{Fr}}_K(\varepsilon)\varepsilon^{-1}$ anterior, esto significa que

$$\widetilde{\mathrm{Fr}}_K(N_{M/L}u)N_{M/L}u^{-1} = \tau_2(N_{M/L}u_2)N_{M/L}u_2^{-1}\tau_4(N_{M/L}u_4)N_{M/L}u_4^{-1},$$

i.e.,

$$N_{M/L}(\widetilde{\mathrm{Fr}}_K(u)(u^{-1})) \quad - \quad N_{M/L}(\tau_2(u_2)u_2^{-1})N_{M/L}(\tau_4(u_4)u_4^{-1})$$
$$N_{M/L}(\tau_2(u_2)u_2^{-1}\tau_4(u_4)u_4^{-1}),$$

i.e.,

$$N_{M/L}\left(\frac{\widetilde{\mathrm{Fr}}_K(u)(u^{-1})}{\tau_2(u_2)u_2^{-1}\tau_4(u_4)u_4^{-1}}\right) = 1$$

y así, por el Teorema 90 de Hilbert (Anexo 1, (2.72)), existe un $\beta \in M$ tal que

$$(*) \qquad \frac{\widetilde{\mathrm{Fr}}_K(u)(u^{-1})}{\tau_2(u_2)u_2^{-1}\tau_4(u_4)u_4^{-1}} = \beta^{-1}\mathrm{Fr}_L(\beta)$$

ya que Fr_L es el generador de $\mathrm{Gal}(M/L)$. Ahora, como M/L es no ramificada, entonces un primo π_L de L también es primo de M y así, para $\beta \in M$ escribiéndolo como $\beta = \pi_L^i\theta$ con $\theta \in U_M$, se tiene que

$$\alpha := \beta^{-1}\mathrm{Fr}_L(\beta) = \pi_L^{-i}\theta^{-1}\mathrm{Fr}_L(\pi_L^i\theta) = \pi_L^{-i}\theta^{-1}\pi_L^i\mathrm{Fr}_L(\theta) = \theta^{-1}\mathrm{Fr}_L(\theta),$$

i.e., podemos pensar que $\beta \in U_M$. Se tiene entonces que

$$N_{M/M_0}\widetilde{\mathrm{Fr}}_K(u)(u^{-1}) = N_{M/M_0}\widetilde{\mathrm{Fr}}_K(\beta)(\beta^{-1})$$

ya que $N_{M/M_0}(\tau_i(u_i)u_i^{-1}) = 1$ porque $u_i \in M$ y $\tau_i \in \mathrm{Gal}(M/M_0)$. Y como N_{M/M_0} conmuta con $\widetilde{\mathrm{Fr}}_K$ y Fr_L, entonces

$$(\dagger) \qquad \widetilde{\mathrm{Fr}}_K(N_{M/M_0}u)N_{M/M_0}u^{-1} = \mathrm{Fr}_L(N_{M/M_0}\beta)N_{M/M_0}\beta^{-1}.$$

Ahora, como L/L_0 y Σ/Σ_0 son totalmente ramificadas y $\Sigma_0 = K$, entonces L/Σ es no ramificada de grado $f = [L_0 : K]$. Se sigue que $\widetilde{\mathrm{Fr}}_K^f = \mathrm{Fr}_L$ y poniendo

$$\lambda := \prod_{j=0}^{f-1} \widetilde{\mathrm{Fr}}_K^j(\beta) \in M^*,$$

donde observamos que como $\beta \in U_M$ entonces $\widetilde{\mathrm{Fr}}_K^j(\beta) \in U_M$ y así $\lambda \in U_M$. Además,

$$\frac{\widetilde{\mathrm{Fr}}_K(\lambda)}{\lambda} = \frac{\widetilde{\mathrm{Fr}}_K(\beta)\widetilde{\mathrm{Fr}}_K^2(\beta)\cdots\widetilde{\mathrm{Fr}}_K^f(\beta)}{\beta\widetilde{\mathrm{Fr}}_K(\beta)\cdots\widetilde{\mathrm{Fr}}_K^{f-1}(\beta)} = \frac{\widetilde{\mathrm{Fr}}_K^f(\beta)}{\beta} = \frac{\mathrm{Fr}_L(\beta)}{\beta}$$

por lo que, substituyendo en (†) y usando el hecho de que la norma conmuta con el Frobenius, obtenemos

$$\begin{aligned}
\widetilde{\mathrm{Fr}}_K(N_{M/M_0}u)(N_{M/M_0}u^{-1}) &= \mathrm{Fr}_L(N_{M/M_0}\beta)N_{M/M_0}\beta^{-1} \\
&= N_{M/M_0}(\mathrm{Fr}_L(\beta)\beta^{-1}) \\
&= N_{M/M_0}(\widetilde{\mathrm{Fr}}_K(\lambda)\lambda^{-1}) \\
&= \widetilde{\mathrm{Fr}}_K(N_{M/M_0}\lambda)N_{M/M_0}\lambda^{-1} \\
&\text{ya que } \tau_i \in \mathrm{Gal}(M/M_0) \\
&= \widetilde{\mathrm{Fr}}_K(\gamma)\gamma^{-1}
\end{aligned}$$

donde $\gamma := N_{M/M_0}(\lambda) \in U_{M_0}$. Se sigue que

$$\widetilde{\mathrm{Fr}}_K(\gamma)^{-1}\widetilde{\mathrm{Fr}}_K(N_{M/M_0}u) = \gamma^{-1}N_{M/M_0}u,$$

i.e., $\widetilde{\mathrm{Fr}}_K(\gamma^{-1}N_{M/M_0}u) = \gamma^{-1}N_{M/M_0}u$, i.e., $\gamma^{-1}N_{M/M_0}u$ queda fijo bajo $\widetilde{\mathrm{Fr}}_K$ y por lo tanto está en K^*. Pongamos $\alpha := \gamma^{-1}N_{M/M_0}u \in K^*$. Entonces

$$\begin{aligned}
N_{L/L_0}\varepsilon &= N_{L/L_0}(N_{M/L}u) \quad \text{por definición de } \varepsilon = N_{M/L}u \\
&= N_{M_0/L_0}(N_{M/M_0}u) \quad \text{por la conmutatividad del diagrama anterior} \\
&= N_{M_0/L_0}(\alpha\gamma) \quad \text{por definición de } \alpha \\
&= N_{M_0/L_0}(\gamma)\alpha^n \quad \text{ya que } \alpha \in K \subseteq L_0 \text{ y } n = [M_0 : L_0]
\end{aligned}$$

y

$$\begin{aligned}
N_{M_0/L_0}(\gamma) &= N_{M_0/L_0}N_{M/M_0}\left(\prod_{j=0}^{f-1}\widetilde{\mathrm{Fr}}_K^j\beta\right) = N_{M/L_0}\left(\prod_{j=0}^{f-1}\widetilde{\mathrm{Fr}}_K^j\beta\right) \\
&= \prod_{j=0}^{f-1}\widetilde{\mathrm{Fr}}_K^j(N_{M/L_0}\beta) = N_{L_0/K}(N_{M/L_0}\beta) \\
&\quad \text{ya que } \widetilde{\mathrm{Fr}}_K|_{L_0} \text{ es un generador de } \mathrm{Gal}(L_0/K) \\
&= N_{M/K}(\beta).
\end{aligned}$$

Así,

$$\begin{aligned} N_{L/L_0}\varepsilon &= N_{M_0/L_0}(\gamma)\alpha^n = N_{M/K}(\beta)\alpha^n \\ &= N_{L/K}(N_{M/L}\beta)\alpha^n \\ &= N_{L/K}(\alpha N_{M/L}\beta) \quad \text{ya que } \alpha \in K \text{ y } n = [L:K]. \end{aligned}$$

Se sigue que

$$N_{L/L_0}(\widehat{\pi}_i) \;-\; N_{L/L_0}\left(\prod_{j=0}^{n_i-1} \widetilde{\mathrm{Fr}}_K^{\,j}(\pi_i)\right) \quad \text{por definición de } \widehat{\pi}_i$$

$$\prod_{j=0}^{n_i-1} \widetilde{\mathrm{Fr}}_K^{\,j}(N_{L/L_0}\pi_i) = \prod_{j=0}^{n_i-1} \widetilde{\mathrm{Fr}}_K^{\,j}(N_{\Sigma_i/\Sigma_i^0}\pi_i)$$

porque $N_{L/L_0} = N_{\Sigma_i/\Sigma_i^0}$

$$-\; N_{\Sigma_i^0/K}(N_{\Sigma_i/\Sigma_i^0}\pi_i) \quad \text{ya que } \widetilde{\mathrm{Fr}}_K|_{\Sigma_i^0} \text{ es generador del grupo } \mathrm{Gal}(\Sigma_i^0/K) \text{ de orden } n_i$$

$$N_{\Sigma_i/K}\pi_i.$$

Por lo que

$$\begin{aligned} N_{\Sigma_3/K}\pi_3 N_{\Sigma_2/K}\pi_2^{-1} N_{\Sigma_4/K}\pi_4^{-1} \qquad & N_{L/L_0}(\widehat{\pi}_3) N_{L/L_0}(\widehat{\pi}_2)^{-1} N_{L/L_0}(\widehat{\pi}_4)^{-1} \\ - \;& N_{L/L_0}(\widehat{\pi}_3\widehat{\pi}_2^{-1}\widehat{\pi}_4^{-1}) \\ - \;& N_{L/L_0}(\varepsilon) \\ - \;& N_{L/K}(\alpha N_{M/L}\beta) \in N_{L/K}L^*. \end{aligned}$$

□

Proposición 2.24. *Sea L/K una extensión finita de Galois de campos locales. Entonces, la función $\widetilde{\Upsilon}_{L/K} : \mathrm{Frob}(L/K) \to K^*/N_{L/K}L^*$ induce el homomorfismo (llamado el* morfismo de Neukirch*)*

$$\Upsilon_{L/K} : \mathrm{Gal}(L/K) \longrightarrow K^*/N_{L/K}L^*$$

como sigue: si $\sigma \in \mathrm{Gal}(L/K)$, sea $\widetilde{\sigma} \in \mathrm{Frob}(L/K)$ un levantamiento de σ; entonces $\Upsilon_{L/K}(\sigma) := \widetilde{\Upsilon}_{L/K}(\widetilde{\sigma})$.

DEMOSTRACIÓN. Mostraremos primero que $\Upsilon_{L/K}$ está bien definido, i.e., que no depende de la elección de los levantamientos $\widetilde{\sigma}$ de σ. En efecto, por (2.19) se tiene un epimorfismo $\mathrm{Frob}(L/K) \twoheadrightarrow \mathrm{Gal}(L/K)$ dado por $\widetilde{\sigma} \mapsto \widetilde{\sigma}|_L$ y así

todo $\sigma \in \mathrm{Gal}(L/K)$ tiene un levantamiento de Frobenius $\tilde{\sigma} \in \mathrm{Frob}(L/K)$. Ahora, si $\tilde{\sigma}_1$ y $\tilde{\sigma}_2$ son dos levantamientos de Frobenius de σ, sean Σ_1 y Σ_2 los campos fijos correspondientes y sean π_1, π_2 elementos primos en Σ_1, Σ_2 respectivamente. Para el epimorfismo

$$\rho_{L/K} : \mathrm{Gal}(L_{nr}/K) \twoheadrightarrow \mathrm{Gal}(K_{nr}/K) \simeq \hat{\mathbb{Z}}$$

dado por $\sigma \mapsto \sigma_{K_{nr}} = \mathrm{Fr}_K^a \mapsto a$; recordemos que si $\tilde{\sigma} \in \mathrm{Frob}(L/K)$, entonces $\rho_K(\tilde{\sigma}) \in \mathbb{N}$; supongamos que $n := \rho_K(\tilde{\sigma}_2) - \rho_K(\tilde{\sigma}_1) \geq 0$.

Si $n = 0$, entonces $\tilde{\sigma}_1|_{K_{nr}} = \tilde{\sigma}_2|_{K_{nr}}$ porque $n = 0$ y como ambos son levantamientos del mismo $\sigma \in \mathrm{Gal}(L/K)$, entonces $\tilde{\sigma}_1|_L = \sigma = \tilde{\sigma}_2|_L$. Se sigue que $\tilde{\sigma}_1 = \tilde{\sigma}_2$.

Si $n > 0$, entonces poniendo $\tilde{\tau} = \tilde{\sigma}_1^{-1}\tilde{\sigma}_2$, el automorfismo $\tilde{\tau}$ es un levantamiento de la identidad $1 \in \mathrm{Gal}(L/K)$. Se sigue que el campo fijo F de $\tilde{\tau}$, en K_{nr}, contiene a L. Ahora, si π_F es un primo de F, entonces por el lema previo

$$\begin{aligned} N_{\Sigma_2/K}(\pi_2) &= N_{\Sigma_1/K}(\pi_1)N_{F/K}(\pi_F) \\ &= N_{\Sigma_1/K}(\pi_1)N_{L/K}(N_{F/L}(\pi_F)) \text{ mód } N_{L/K}L^*, \end{aligned}$$

i.e., $N_{\Sigma_2/K}(\pi_2) \equiv N_{\Sigma_1/K}(\pi_1)$ mód $N_{L/K}L^*$, i.e., $\Upsilon_{L/K}$ está bien definida.

Más aún, $\Upsilon_{L/K}$ es un homomorfismo ya que si $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$, sean $\tilde{\sigma}_1, \tilde{\sigma}_2 \in \mathrm{Frob}(L/K)$ sus levantamientos de Frobenius. Entonces, por (2.19) $\tilde{\sigma}_1\tilde{\sigma}_2 \in \mathrm{Frob}(L/K)$ es un levantamiento de Frobenius de $\sigma_1\sigma_2$ y se tiene que

$$\begin{aligned} \Upsilon_{L/K}(\sigma_1\sigma_2) &- \Upsilon_{L/K}(\tilde{\sigma}_1\tilde{\sigma}_2) = N_{\Sigma/K}(\tilde{\sigma}_1\tilde{\sigma}_2) \\ &- N_{\Sigma_1/K}(\pi_1)N_{\Sigma_2/K}(\pi_2) \text{ mód } N_{L/K}L^* \quad \text{por el lema anterior} \\ &- \tilde{\Upsilon}_{L/K}(\tilde{\sigma}_1)\tilde{\Upsilon}_{L/K}(\tilde{\sigma}_2) \\ &- \Upsilon_{L/K}(\sigma_1)\Upsilon_{L/K}(\sigma_2). \end{aligned}$$

□

Uno de los resultados más importantes de la teoría de campos de clases local es que el morfismo de reciprocidad asocia elementos primos a Frobenius de extensiones no ramificadas. Esto es precisamente el contenido de la proposición siguiente:

Proposición 2.25. *Si L/K es una extensión finita no ramificada de campos locales, entonces $\Upsilon_{L/K} : \mathrm{Gal}(L/K) \to K^*/N_{L/K}L^*$ está dada por*

$$\Upsilon_{L/K}(\mathrm{Fr}_{L/K}) \equiv \pi_K \bmod N_{L/K}L^*$$

para π_K un primo de K y, de hecho, $\Upsilon_{L/K}$ es un isomorfismo.

DEMOSTRACIÓN. Como L/K es no ramificada, entonces L/K es cíclica generada por el Frobenius $\mathrm{Fr}_{L/K}$. Ahora, como $L \subseteq L_{nr}$, el Frobenius $\mathrm{Fr}_{L/K} \in \mathrm{Gal}(L/K)$ se levanta al Frobenius $\mathrm{Fr}_{L_{nr}/K} \in \mathrm{Gal}(L_{nr}/K)$, i.e., $\widetilde{\mathrm{Fr}}_{L/K} = \mathrm{Fr}_{L_{nr}/K}$ y notamos que el campo fijo Σ de $\widetilde{\mathrm{Fr}}_{L/K}$ en L_{nr} es K y por lo tanto

$$\begin{aligned}\Upsilon_{L/K}(\mathrm{Fr}_{L/K}) &= \Upsilon_{L/K}(\mathrm{Fr}_{L_{nr}/K}) \\ &\equiv N_{K/K}(\pi_K) \bmod N_{L/K}L^* \equiv \pi_K \bmod N_{L/K}L^*.\end{aligned}$$

Esto prueba la primera afirmación.

Ahora, como L/K es no ramificada, digamos de grado n, entonces por (2.5)(3) $K^*/N_{L/K}L^* \simeq \mathbb{Z}/n\mathbb{Z}$ es un grupo cíclico de orden n, donde el generador $1 \in \mathbb{Z}/n\mathbb{Z}$ corresponde al primo $\pi_K \pmod{N_{L/K}L^*}$. Como $\mathrm{Gal}(L/K)$ también es cíclico de orden n generado por $\mathrm{Fr}_{L/K}$ y $\Upsilon_{L/K}(\mathrm{Fr}_{L/K}) = \pi_K \bmod N_{L/K}L^*$, entonces $\Upsilon_{L/K}$ es un isomorfismo. □

2.3.1 Propiedades del morfismo de Neukirch

Las proposiciones siguientes expresan la conducta funtorial del morfismo de Neukirch con respecto a extensiones de L y K, su relación con la conjugación y su relación con el morfismo de transferencia.

Proposición 2.26. *Supongamos que L/K y L'/K' son extensiones finitas de Galois de campos locales y supongamos además que $K' \supseteq K$ y $L' \supseteq L$ son finitas. Entonces, el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} \mathrm{Gal}(L'/K') & \xrightarrow{\Upsilon_{L'/K'}} & K'^*/N_{L'/K'}L'^* \\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle N_{K'/K}} \\ \mathrm{Gal}(L/K) & \xrightarrow[\Upsilon_{L/K}]{} & K^*/N_{L/K}L^*. \end{array}$$

donde el morfismo vertical izquierdo es la restricción $\mathrm{res}(\sigma) = \sigma|_L$ y el morfismo vertical derecho es el inducido por la norma $N_{K'/K} : K'^* \to K^*$.

DEMOSTRACIÓN. Sean $\sigma' \in \mathrm{Gal}(L'/K')$ y sea $\sigma := \mathrm{res}(\sigma') = \sigma'|_L \in \mathrm{Gal}(L/K)$. Si $\tilde{\sigma}' \in \mathrm{Frob}(L'/K')$ un levantamiento de σ', entonces $\tilde{\sigma} := \tilde{\sigma}'|_{L_{nr}} \in \mathrm{Gal}(L_{nr}/K)$ es un levantamiento de $\sigma := \sigma'|_L$ ya que

$$\rho_K(\tilde{\sigma}) = \rho_K(\tilde{\sigma}'|_{L_{nr}}) = f(K'/K)\rho_{K'}(\tilde{\sigma}') \in \mathbb{N},$$

donde la última igualdad es por la conmutatividad del segundo diagrama en §2.2, y es un entero positivo porque $\tilde{\sigma}' \in \mathrm{Frob}(L'/K')$. Se sigue que $\tilde{\sigma} \in \mathrm{Frob}(L/K)$.

Ahora, si Σ' es el campo fijo de $\tilde{\sigma}'$, entonces $\Sigma := \Sigma' \cap L_{nr} = \Sigma' \cap \Sigma_{nr}$ es el campo fijo de $\tilde{\sigma}$ y además Σ'/Σ es totalmente ramificada, i.e., $f(\Sigma'/\Sigma) = 1$ por §2.2 ya que $\Sigma = \Sigma' \cap \Sigma_{nr}$.

Para un primo $\pi_{\Sigma'}$ de Σ', el elemento $\pi_\Sigma := N_{\Sigma'/\Sigma}(\pi_{\Sigma'})$ es primo de Σ por (1.54)(2) y (1.87), y se tiene entonces que

$$(*) \quad N_{\Sigma/K}(\pi_\Sigma) = N_{\Sigma/K}(N_{\Sigma'/\Sigma}(\pi_{\Sigma'})) = N_{\Sigma'/K}(\pi_{\Sigma'}) = N_{K'/K}N_{\Sigma'/K'}(\pi_{\Sigma'}).$$

Se sigue que, para $\sigma' \in \mathrm{Gal}(L'/K')$,

$$\begin{aligned} N_{K'/K} \circ \Upsilon_{L'/K'}(\sigma') &= N_{K'/K}\tilde{\Upsilon}_{L'/K'}(\tilde{\sigma}') \\ &- N_{K'/K}(N_{\Sigma'/K'}(\pi_{\Sigma'})) \\ &= N_{\Sigma/K}(\pi_\Sigma) \qquad \text{por } (*) \\ &= \Upsilon_{L/K}(\tilde{\sigma}) = \Upsilon_{L/K}(\sigma) \\ &- \Upsilon_{L/K}(\sigma'|_L) = \Upsilon_{L/K}(\mathrm{res}(\sigma')). \end{aligned}$$

□

Corolario 2.27. *Sean L/K una extensión finita de Galois de campos locales y M/K una subextensión de Galois. Entonces los diagramas siguienes conmutan:*

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/M) & & \mathrm{Gal}(L/K) & & \mathrm{Gal}(M/K) \longrightarrow 1 \\ & & \Upsilon_{L/M}\downarrow & & \Upsilon_{L/K}\downarrow & & \Upsilon_{M/K}\downarrow \\ & & M^*/N_{L/M}L^* & \xrightarrow[N_{M/K}]{} & K^*/N_{L/K}L^* & \xrightarrow[i]{} & K^*/N_{M/K}M^* \longrightarrow 1 \end{array}$$

donde el primer renglón es exacto, con los morfismos naturales y el segundo renglón es exacto con el morfismo i inducido por la identidad $id : K^* \to K^*$.

DEMOSTRACIÓN. Los morfismos del primer renglón están inducidos por inclusiones y la exactitud es por teoría de Galois. Entonces el cuadrado

izquierdo conmuta por la proposición anterior y el cuadrado derecho conmuta también por la misma proposición, ya que el morfismo $i = id = N_{K/K}$. □

Proposición 2.28. *Sea $L \supseteq M \supseteq K$ una torre de campos locales con M/K finita separable y L/M finita de Galois. Si $\sigma \in \mathrm{Gal}(K^{sep}/K)$ y $c_\sigma : \mathrm{Gal}(L/M) \longrightarrow \mathrm{Gal}(\sigma L/\sigma M)$ es el morfismo de conjugación dado por $c_\sigma(\tau) := \sigma\tau\sigma^{-1}|_{\sigma L}$ para $\tau \in \mathrm{Gal}(L/M)$, entonces el diagrama siguiente conmuta:*

$$\begin{array}{ccc} \mathrm{Gal}(L/M) & \xrightarrow{\Upsilon_{L/M}} & M^*/N_{L/M}L^* \\ \Big\downarrow{\scriptstyle c_\sigma} & & \Big\downarrow{\scriptstyle \sigma} \\ \mathrm{Gal}(\sigma L/\sigma M) & \xrightarrow[\Upsilon_{\sigma L/\sigma M}]{} & (\sigma M)^*/N_{\sigma L/\sigma M}(\sigma L)^*. \end{array}$$

DEMOSTRACIÓN. Sea $\tau \in \mathrm{Gal}(L/M)$ y sea $\widetilde{\tau} \in \mathrm{Frob}(L/M) \subseteq \mathrm{Gal}(L_{nr}/M)$ un levantamiento de Frobenius de τ. Sea $\widehat{\tau} \in \mathrm{Gal}(M^{sep}/M)$ una extensión de $\widetilde{\tau}$ a M^{sep}. Entonces $\sigma\widehat{\tau}\sigma^{-1}|_{(\sigma L)_{nr}} \in \mathrm{Frob}(\sigma L/\sigma M)$ es un levantamiento de Frobenius de $c_\sigma(\tau) = \sigma\tau\sigma^{-1} \in \mathrm{Gal}(\sigma L/\sigma M)$ ya que

$$\rho_{\sigma M}(\sigma\widehat{\tau}\sigma^{-1}) = \rho_M(\widehat{\tau}) = \rho_M(\widetilde{\tau}) \in \mathbb{N}.$$

Ahora, si Σ es el campo fijo de $\widetilde{\tau}$, entonces $\sigma\Sigma$ es el campo fijo de $\sigma\widehat{\tau}\sigma^{-1}|_{(\sigma L)_{nr}}$ y si π_Σ es un primo de Σ, entonces $\sigma\pi_\Sigma$ es un primo de $\sigma\Sigma$ por (1.27). Ahora, como

$$N_{\sigma\Sigma/\sigma M}(\sigma\pi_\Sigma) = \sigma N_{\Sigma/M}(\pi_\Sigma),$$

entonces

$$\begin{aligned} \Upsilon_{\sigma L/\sigma M} \circ c_\sigma(\tau) &= \Upsilon_{\sigma L/\sigma M}(\sigma\tau\sigma^{-1}|_{\sigma L}) \\ &\quad \widetilde{\Upsilon}_{\sigma L/\sigma M}(\sigma\widehat{\tau}\sigma^{-1}|_{\sigma L}) = N_{\sigma\Sigma/\sigma M}(\sigma\pi_\Sigma) \\ &- \sigma N_{\Sigma/M}(\pi_\Sigma) = \sigma\Upsilon_{L/M}(\widetilde{\tau}) \\ &\quad \sigma\Upsilon_{L/M}(\tau). \end{aligned}$$

□

El morfismo de transferencia. Sean G un grupo y $H \subseteq G$ un subgrupo de índice finito. Si $G' = [G : G]$ es el subgrupo conmutador de G, entonces el cociente G/G' es abeliano y lo denotamos por G^{ab}. Similarmente,

$H^{ab} = H/H'$. Ahora, como H tiene índice finito n en G, el conjunto de clases laterales derechas de H en G tiene un conjunto completo de representantes R de cardinalidad n, digamos $R = \{\rho_i \ : \ 1 \leq i \leq n\}$, de tal forma que G es la unión disjunta

$$G = \bigcup H\rho_i \qquad \text{con } \rho_i \in R,\ 1 \leq i \leq n.$$

Entonces, dado $\sigma \in G$, para cada $i = 1, \ldots, n$, se tiene que $\sigma\rho_i \in H\rho_{\sigma(i)}$ para un único $\sigma(i)$ entre 1 y n, i.e., $\sigma(i)$ es una permutación del conjunto $1, \ldots, n$. El *morfismo de transferencia de G a H*:

$$V : G^{ab} \longrightarrow H^{ab}$$

se define mediante la fórmula

$$V(\sigma \text{ mód } G') := \prod_i \rho_i \sigma \rho_{\sigma(i)}^{-1} \text{ mód } H'.$$

Por supuesto que tenemos que verificar que V está bien definido, i.e., que no depende de la elección del conjunto de representantes R, que es un homomorfismo y que se anula en G'.

(1) *V es independiente de la elección del conjunto de representantes R.*

En efecto, si $\rho_i' = h_i\rho_i \in H\rho_i$, con $h_i \in H$, $1 \leq i \leq n$ son otros representantes de las clases laterales derechas de H en G, entonces

$$\prod \rho'_i \sigma \rho'^{-1}_{\sigma(i)} \qquad \prod h_i\rho_i\sigma(h_{\sigma(i)}\rho_{\sigma(i)})^{-1} = \prod h_i(\rho_i\sigma\rho_{\sigma(i)}^{-1})h_{\sigma(i)}^{-1}$$

$$\prod h_i \prod \rho_i\sigma\rho_{\sigma(i)}^{-1} \prod h_{\sigma(i)}^{-1} \text{ mód } H'$$

(las clases laterales conmutan porque H/H' es abeliano)

$$= \prod \rho_i\sigma\rho_{\sigma(i)}^{-1} \prod h_i h_{\sigma(i)}^{-1} \text{ mód } H',$$

y como

$$\prod h_i h_{\sigma(i)}^{-1} \text{ mód } H' \equiv \prod (h_i \text{ mód } H') \prod (h_{\sigma(i)}^{-1}) \text{ mód } H' \equiv 1 \text{ mód } H',$$

ya que las clases laterales conmutan y así cada h_i se aparea con algún $h_{\sigma(i)}^{-1}$, se sigue que

$$\prod_i \rho_i' \sigma \rho_{\sigma(i)}'^{-1} \equiv \prod_i \rho_i \sigma \rho_{\sigma(i)}^{-1} \text{ mód } H'$$

(2) *V es un homomorfismo.*

En efecto, si $\sigma, \tau \in G$, entonces

$$\rho_i(\sigma\tau)\rho_{\sigma\tau(i)}^{-1} = \rho_i \sigma \rho_{\sigma(i)}^{-1} \rho_{\sigma(i)} \tau \rho_{\sigma\tau(i)}^{-1}$$

y como $\rho_i \sigma \rho_{\sigma(i)}^{-1} \in H$ y $\rho_i(\sigma\tau)\rho_{\sigma\tau(i)}^{-1} \in H$, entonces la igualdad de arriba implica que $\rho_{\sigma(i)} \tau \rho_{\sigma\tau(i)}^{-1} \in H$; ahora, como $\rho_{\sigma(i)} \tau \rho_{\tau(\sigma(i))}^{-1} \in H$, por la unicidad de los representantes en R se debe tener que $\sigma\tau(i) = \tau(\sigma(i))$. Se sigue que

$$\begin{aligned} V(\sigma\tau) &- \prod \rho_i(\sigma\tau)\rho_{\sigma\tau(i)}^{-1} \equiv \prod \rho_i \sigma \rho_{\sigma(i)}^{-1} \rho_{\sigma(i)} \tau \rho_{\tau(\sigma(i))}^{-1} \text{ mód } H' \\ & \prod \rho_i \sigma \rho_{\sigma(i)}^{-1} \prod \rho_{\sigma(i)} \tau \rho_{\tau(\sigma(i)}^{-1} \text{ mód } H' \\ &= V(\sigma)V(\tau). \end{aligned}$$

(3) *V es trivial en G'.*

En efecto,

$$\begin{aligned} V(\sigma\tau\sigma^{-1}\tau^{-1}) &- V(\sigma)V(\tau)V(\sigma^{-1})V(\tau^{-1}) \text{ mód } H' \\ & V(\sigma)V(\sigma^{-1})V(\tau)V(\tau^{-1}) \text{ mód } H' \\ & \text{(ya que } H/H' \text{ es abeliano)} \\ & 1. \end{aligned}$$

(4) *Otra definición del morfismo de transferencia.*

Sea $\sigma \in G$ y sea $S = \langle \sigma \rangle$ el subgrupo generado por σ. El grupo S actúa por la derecha sobre el conjunto del clases laterales derechas de H en G: si $H\tau$ es una clase lateral derecha y $\sigma^t \in S$, entonces $H\tau\sigma^t$ es otra clase lateral derecha. Las órbitas de esta acción son las clases laterales dobles $H\tau S$, de tal forma que si τ recorre un conjunto completo de representantes de estas clases laterales dobles, entonces G es la unión disjunta

$$G = \bigcup_\tau H\tau S.$$

Sea $f(\tau)$ el orden de la órbita $H\tau S$, i.e., el mayor entero tal que las clases $H\tau\sigma$, $H\tau\sigma^2, \ldots H\tau\sigma^{f(\tau)-1}$ son distintas. Equivalentemente, $f(\tau)$ es el menor entero tal que $\tau\sigma^{f(\tau)} \equiv \tau$ mód H, i.e., tal que $\tau\sigma^{f(\tau)}\tau^{-1} \in H$. Nótese entonces que si τ recorre el conjunto completo de representantes de las clases laterales dobles, entonces los elementos $\tau, \tau\sigma, \ldots, \tau\sigma^{f(\tau)-1}$ forman un conjunto completo de representantes de las clases laterales derechas Hg. Para calcular el morfismo de transferencia en términos de este sistema de representantes, debemos escribir cada producto $\tau\sigma^e \cdot \sigma$ de la forma θt con $\theta \in H$ y t uno de los representantes de las clases laterales dobles. Ahora, $\tau\sigma^e\sigma = \tau\sigma^{e+1}$ es uno de esos representantes, excepto cuando $e = f(\tau) - 1$ y en este caso

$$\tau\sigma^{f(\tau)-1}\sigma = \tau\sigma^{f(\tau)} \equiv \tau \text{ mód } H$$

por definición de $f(\tau)$. Así, en el cálculo del morfismo $V(\sigma)$ los únicos factores que quizá no sean 1 son aquellos que corresponden a los productos $\tau\sigma^{f(\tau)-1}\sigma$, que de hecho son iguales a $\tau\sigma^{f(\tau)}\tau^{-1} \in H$. Hemos así probado que si $\{\tau_i\}$ es un conjunto completo de representantes de las clases laterales dobles $H\sigma S$ y si $f(\tau_i)$ se definen como antes, entonces

$$V(\sigma) = \prod_i \tau_i\sigma^{f(\tau_i)}\tau_i^{-1} \text{ mód } H'.$$

Usaremos la notación $\sigma[\tau_i] := \tau_i\sigma^{f(\tau_i)}\tau_i^{-1} \in H$.

Observación. Como la imagen de $\Upsilon_{L/K} : \mathrm{Gal}(L/K) \to K^*/N_{L/K}L^*$ es abeliana, entonces $\Upsilon_{L/K}$ induce por paso al cociente un homomorfismo

$$\Upsilon_{L/K} : \mathrm{Gal}^{ab}(L/K) \to K^*/N_{L/K}L^*.$$

Proposición 2.29. *Si L/K una extensión finita de Galois de campos locales y M/K es una subextensión, entonces el diagrama siguiente conmuta:*

$$\begin{array}{ccc} \mathrm{Gal}^{ab}(L/K) & \xrightarrow{\Upsilon_{L/K}} & K^*/N_{L/K}L^* \\ {\scriptstyle V}\downarrow & & \downarrow \\ \mathrm{Gal}^{ab}(L/M) & \xrightarrow[\Upsilon_{L/M}]{} & M^*/N_{L/M}L^* \end{array}$$

donde V es el morfismo de transferencia y el morfismo vertical derecho es inducido por la inclusión $K \hookrightarrow M$.

DEMOSTRACIÓN. Sean $G := \mathrm{Gal}(L_{nr}/K)$ y $\widetilde{H} := \mathrm{Gal}(L_{nr}/M)$. Sean $\sigma \in \mathrm{Gal}(L/K)$ y $\widetilde{\sigma} \in \mathrm{Frob}(L/K)$ su levantamiento de Frobenius. Sea Σ el campo fijo de $\widetilde{\sigma}$ y pongamos $\widetilde{S} := \mathrm{Gal}(L_{nr}/\Sigma)$ notando por (2.20) que $\widetilde{\sigma} = \mathrm{Fr}_\Sigma$ es el generador de $\widetilde{S} = \mathrm{Gal}(L_{nr}/\Sigma) = \mathrm{Gal}(\Sigma_{nr}/\Sigma) \subseteq \widetilde{G}$, ya que $\Sigma_{nr} = L_{nr}$ por (2.20). Entonces, la descomposición de $\widetilde{G}$ en clases laterales dobles del párrafo anterior es precisamente

$$\widetilde{G} = \bigcup_{\widetilde{\tau}} \widetilde{H}\widetilde{\tau}\widetilde{S},$$

donde $\widetilde{\tau}$ recorre un conjunto completo de representantes de las clases laterales dobles $\widetilde{H}\widetilde{\tau}\widetilde{S}$.

Poniendo $G = \mathrm{Gal}(L/K)$ y $H = \mathrm{Gal}(L/M)$, entonces G es la unión disjunta de las clases $H\tau_i S$, donde $\tau_i = \widetilde{\tau}_i|_L \in G$ y $S = \langle\sigma\rangle$. Por definición del morfismo de transferencia, para $\sigma \in G$:

$$V(\sigma \bmod G') \equiv \prod \sigma[\tau_i] \bmod H', \tag{1}$$

donde $\sigma[\tau_i] = \tau_i \sigma^{f(\tau_i)} \tau_i^{-1} \in H$.

Pongamos ahora $\widetilde{H}_i := \widetilde{H} \cap \widetilde{\tau}_i \widetilde{S} \widetilde{\tau}_i^{-1}$. Entonces $\widetilde{H}_i$ es un subgrupo de $\widetilde{H}$ que coincide con el subgrupo de $\widetilde{H}$ generado topológicamente por $\widetilde{\sigma}[\widetilde{\tau}_i]$. Notemos ahora que $\widetilde{\tau}_i \widetilde{S}$ es la unión disjunta de las clases $\widetilde{H}_i \widetilde{\tau}_i \widetilde{\sigma}^{f_i}$ para $1 \leq f_i \leq f(\tau_i)$. Poniendo a $\widetilde{H}$ como la unión disjunta de las clases $\widetilde{\vartheta}_{i,k}\widetilde{H}_i$ para $\widetilde{\vartheta}_{i,k} \in \widetilde{H}$, $1 \leq k \leq [\widetilde{H} : \widetilde{H}_i]$, entonces

$$\widetilde{G} = \bigcup_i \widetilde{H}\widetilde{\tau}_i\widetilde{\sigma}^{f_i} = \bigcup_i \left(\bigcup_k \widetilde{\vartheta}_{k,i}\widetilde{H}_i \right) \widetilde{\tau}_i\widetilde{\sigma}^{f_i} = \bigcup_{i,k} \widetilde{\vartheta}_{k,i}\widetilde{\tau}_i\widetilde{S}$$

ya que $\widetilde{\tau}_i\widetilde{S} = \bigcup_i = \widetilde{H}_i\widetilde{\tau}_i\widetilde{\sigma}^{f_i}$.

Entonces, para el campo fijo Σ de $\widetilde{\sigma}$, de hecho Σ es el campo fijo de $\widetilde{S}$ y así, para cualquier $\alpha \in \Sigma$ se tiene que

$$N_{\Sigma/K}(\alpha) = \prod_{i,k} \widetilde{\vartheta}_{i,k}\widetilde{\tau}_i(\alpha). \tag{2}$$

Ahora, si Σ_i es el campo fijo de $\widetilde{\sigma}[\widetilde{\tau}_i]$, entonces

$$(\widetilde{\tau}_i\Sigma)_{nr} = \widetilde{\tau}_i\Sigma_{nr} = \widetilde{\tau}_i L_{nr} = L_{nr},$$

además $\widetilde{\tau}_i\Sigma \subseteq \Sigma_i$ y $\Sigma_i/\widetilde{\tau}_i\Sigma$ es la extensión no ramificada de grado $f(\tau_i)$. Se sigue que para un primo π_Σ de Σ el elemento $\widetilde{\tau}_i(\pi_\Sigma)$ es primo de $\widetilde{\tau}_i\Sigma$ y por lo

tanto de Σ_i. También, como en (2) se tiene que, para $\alpha \in \Sigma_i$,

$$N_{\Sigma_i/M}(\alpha) = \prod_k \widetilde{\vartheta}_{i,k}(\alpha).$$

Se sigue que

$$N_{\Sigma/K}(\pi_\Sigma) = \prod_{i,k} \widetilde{\vartheta}_{i,k}\widetilde{\tau}_i(\pi_\Sigma) = \prod N_{\Sigma_i/M}(\widetilde{\tau}_i(\pi_\Sigma)). \tag{3}$$

Finalmente, como $\widetilde{\sigma}[\widetilde{\tau}_i] \in \mathrm{Frob}(L/M)$ es un levantamiento de Frobenius de $\sigma[\tau_i] \in \mathrm{Gal}(L/M)$, usando (1) y (3) se sigue que

$$\begin{aligned} \Upsilon_{L/K}(\sigma) &= N_{\Sigma/K}(\pi_\Sigma) = \prod_i N_{\Sigma_i/M}(\widetilde{\tau}_i(\pi_\Sigma)) \\ &= \prod_i \Upsilon_{L/M}(\sigma[\tau_i]) = \Upsilon_{L/M}\left(\prod_i \sigma[\tau_i]\right) \\ &= \Upsilon_{L/M}(V(\sigma)). \end{aligned}$$

□

El resultado principal nos dice que el morfismo de Neukirch es un isomorfismo:

Teorema 2.30. *Sea L/K una extensión finita de Galois de campos locales. Entonces, el morfismo de Neukirch $\Upsilon_{L/K} : \mathrm{Gal}^{ab}(L/K) \to K^*/N_{L/K}L^*$ es un isomorfismo.*

DEMOSTRACIÓN. La idea de la demostración es la siguiente: primero consideramos el caso cuando L/K es cíclica de grado primo ℓ. Después, por inducción sobre n, consideramos el caso cuando L/K es cíclica de grado ℓ^n. A continuación consideramos el caso cuando L/K es abeliana finita y hacemos inducción sobre el grado $[L : K]$. Finalmente consideramos el caso general usando que $\mathrm{Gal}(L/K)$ es soluble (1.78).

CASO 1. Supongamos que L/K es cíclica de grado primo ℓ. Entonces, L/K es no ramificada o es totalmente ramificada.

(i) Si L/K es no ramificada, entonces $\Upsilon_{L/K}$ es un isomorfismo por (2.25).

(ii) Si L/K es totalmente ramificada de grado primo ℓ, sea $\widetilde{\sigma}$ un generador del grupo $\mathrm{Gal}(L_{nr}/K_{nr})$. Entonces, por (1.53)(3) $\mathrm{Gal}(L_{nr}/K_{nr}) \simeq \mathrm{Gal}(L/K)$ ya que $L_0 = K$, de tal forma que $\sigma := \widetilde{\sigma}|_L$ es un generador de $\mathrm{Gal}(L/K)$.

Poniendo $\widetilde{\sigma}_1 := \widetilde{\sigma} \cdot \mathrm{Fr}_L \in \mathrm{Gal}(L_{nr}/K)$, como $L_{nr} = L \cap K_{nr}$, se tiene que $\widetilde{\sigma}_1|_L = \widetilde{\sigma}|_L = \sigma$ y $\widetilde{\sigma}_1|_{K_{nr}} = \mathrm{Fr}_L$ y así $\rho_K(\widetilde{\sigma}_1) = 1$, de tal forma que $\widetilde{\sigma}_1 \in \mathrm{Frob}(L/K)$ es un levantamiento de σ. Sea Σ el campo fijo de $\widetilde{\sigma}_1$. Por (2.20) $f_{\Sigma/K} = \rho_K(\widetilde{\sigma}_1) = 1$ de tal forma que Σ/K es totalmente ramificada y además $\mathrm{Gal}(\Sigma/K) \simeq \mathrm{Gal}(\Sigma_{nr}/K_{nr}) \simeq \mathrm{Gal}(L_{nr}/K_{nr})$ ya que $\Sigma_{nr} = L_{nr}$.

Sea M/K una subextensión finita de L_{nr}/K tal que M contiene a L y a Σ. Denotemos por π_Σ y π_L elementos primos de Σ y L respectivamente. Como $\Sigma, L \subseteq M \subseteq L_{nr} = \Sigma_{nr}$ implica que M/Σ y M/L son no ramificados, entonces π_Σ y π_L siguen siendo primos en M y por lo tanto existe una unidad $u \in U_M$ tal que $\pi_\Sigma = \pi_L u$.

Mostraremos ahora que $\Upsilon_{L/K}$ es *inyectiva*. En efecto, supongamos que para el generador σ de $\mathrm{Gal}(L/K)$ se tiene que $\Upsilon_{L/K}(\sigma) = 0$.

Como $f(\Sigma/K) = 1$, entonces $N_{M/M_0}|_\Sigma = \dfrac{1}{f(\Sigma/K)} N_{\Sigma/K} = N_{\Sigma/K}$ y similarmente, como $f(L/K) = 1$, entonces $N_{M/M_0}|_L = N_{L/K}$ Se sigue que

$$\begin{aligned} N_{\Sigma/K}\pi_\Sigma &= N_{M/M_0}\pi_\Sigma = N_{M/M_0}(\pi_L u) = N_{M/M_0}(\pi_L)N_{M/M_0}(u) \\ &= N_{L/K}(\pi_L)N_{M/M_0}(u) \equiv N_{M/M_0}(u) \text{ mód } N_{L/K}L^* \end{aligned}$$

y como $0 = \Upsilon_{L/K}(\sigma) \equiv N_{\Sigma/K}(\pi_\Sigma)$ mód $N_{L/K}L^*$, entonces $N_{\Sigma/K}\pi_\Sigma \in N_{L/K}L^*$, por lo que de la congruencia anterior se sigue que $N_{M/M_0}(u) \in N_{L/K}L^*$ también, i.e., $N_{M/M_0}(u) = N_{L/K}(\varepsilon)$ para algún $\varepsilon \in L^*$ (de hecho, $\varepsilon \in U_L$ ya que $v_L(\varepsilon) = v_K(N_{L/K}(\varepsilon)) = 0$). Así, como $N_{L/K} = N_{M/M_0}|_L$ se tiene que $N_{M/M_0}(u) = N_{M/M_0}(\varepsilon)$ y por lo tanto $N_{M/M_0}(u\varepsilon^{-1}) = 1$; entonces, por el Teorema 90 de Hilbert (Anexo 1, (2.72)) existe un $\beta \in M$ tal que $u\varepsilon^{-1} = \widetilde{\sigma}(\beta)/\beta$. Se sigue que para el elemento $\pi := \pi_L \varepsilon \widetilde{\sigma}_1(\beta)/\beta \in M$ se tiene que

$$\begin{aligned} \frac{\widetilde{\sigma}(\pi)}{\pi} &= \frac{\widetilde{\sigma}(\pi_L\varepsilon)}{\pi_L\varepsilon}\frac{\widetilde{\sigma}(\widetilde{\sigma}_1(\beta)\beta^{-1})}{\widetilde{\sigma}_1(\beta)\beta^{-1}} = \frac{\widetilde{\sigma}_1(\pi_L\varepsilon)}{\pi_L\varepsilon}\frac{\widetilde{\sigma}\widetilde{\sigma}_1(\beta)}{\widetilde{\sigma}_1(\beta)}\frac{\widetilde{\sigma}(\beta^{-1})}{\beta^{-1}} \\ &= \frac{\widetilde{\sigma}_1(\pi_\Sigma u^{-1}\varepsilon)}{\pi_\Sigma u^{-1}\varepsilon}\frac{\widetilde{\sigma}_1\widetilde{\sigma}(\beta)}{\widetilde{\sigma}_1(\beta)}\frac{\widetilde{\sigma}(\beta^{-1})}{\beta^{-1}} \quad \text{ya que } \widetilde{\sigma}\widetilde{\sigma}_1 = \widetilde{\sigma}_1\widetilde{\sigma} \\ &= \frac{\widetilde{\sigma}_1(\pi_\Sigma)}{\pi_\Sigma}\frac{\widetilde{\sigma}_1(u^{-1}\varepsilon)}{u^{-1}\varepsilon}\widetilde{\sigma}_1\left(\frac{\widetilde{\sigma}(\beta)}{\beta}\right)\widetilde{\sigma}(\beta)^{-1}\beta = \frac{\widetilde{\sigma}_1(\pi_\Sigma)}{\pi_\Sigma} = 1, \end{aligned}$$

ya que Σ es el campo fijo de $\widetilde{\sigma}_1$ y $\pi_\Sigma \in \Sigma$. Se sigue que $\widetilde{\sigma}(\pi) = \pi$ para el generador $\widetilde{\sigma}$ y por lo tanto $\pi \in M_0$. Observamos ahora que como π es un primo

de M (ya que es igual a π_L por una unidad), lo anterior es una contradicción con el hecho de que $v_M(\pi) = [M : M_0]v_{M_0}(\pi) \neq 1$ ya que $M \neq M_0$ por ser totalmente ramificada. Se sigue que $\Upsilon_{L/K}(\sigma) = 0$ no es posible y por lo tanto $\Upsilon_{L/K}$ es inyectiva.

Ahora, como L/K es totalmente ramificada, por (2.7) y (2.18) el grupo $K^*/N_{L/K}L^*$ es cíclico de orden $\ell = [L : K]$ con $\Upsilon_{L/K} : \mathrm{Gal}(L/K) \rightarrowtail K^*/N_{L/K}L^*$ inyectivo; se sigue que $\Upsilon_{L/K}$ debe ser un isomorfismo.

Caso 2. L/K es cíclica de grado ℓ^n, ℓ primo y $n \geq 1$. Usaremos inducción sobre n para mostrar que $\Upsilon_{L/K}$ es un isomorfismo: sea M un campo intermedio de L/K tal que $[L : M] = \ell$. Entonces, consideremos el diagrama del corolario (2.27). Mostraremos que en este diagrama $N_{M/K}$ es inyectiva. En efecto, supongamos que no lo es, i.e., que para todo $\beta \notin N_{L/M}L^*$ existe un $\alpha \in L^*$ tal que $N_{L/K}\alpha = N_{M/K}\beta$. Entonces, $N_{M/K}N_{L/M}(\alpha) = N_{M/K}\beta$, i.e., $N_{M/K}((N_{L/M}\alpha)\beta^{-1}) = 1$ y así, por el Teorema 90 de Hilbert (Anexo 1, (2.72)) existe un $\beta_1 \in M^*$ tal que para el generador σ de $\mathrm{Gal}(L/K)$ se tiene que $(N_{L/M}\alpha)\beta^{-1} = \beta_1/\sigma(\beta_1)$, i.e., $\beta = N_{L/M}\alpha\sigma(\beta_1)/\beta_1$. Observemos que como $\beta \notin N_{L/M}L^*$, entonces $\beta_1 \notin N_{L/M}L^*$.

Repitiendo esta construcción ahora para β_1 y por recurrencia $(n-1)$ veces, se obtiene que

$$\beta = N_{L/M}(\alpha')\tau(\beta')$$

para algún $\alpha' \in L^*$ y $\beta' \in M^*$, donde $\tau \in \mathbb{Z}[\mathrm{Gal}(L/K)]$ está dado por

$$\tau = (\sigma - 1)^{\ell^{n-1}} = \sigma^{\ell^{n-1}} - 1 + \ell f(\sigma)$$

para algún polinomio $f(x) \in \mathbb{Z}[x]$. Se sigue que $\tau(\beta') = \sigma^{\ell^{n-1}}(\beta')/\beta' \cdot \gamma^{\ell}$ para un $\gamma \in M^*$; por lo tanto $\beta = N_{L/M}(\alpha'\gamma)\sigma^{\ell^{n-1}}(\beta')/\beta'$ ya que $\gamma \in M^*$ implica que $N_{L/M}(\alpha'\gamma) = N_{L/M}(\alpha')\gamma^{\ell}$.

Notando ahora que $\sigma^{\ell^{n-1}}$ es un generador de $\mathrm{Gal}(L/M)$ ya que tiene grado $\ell = [L : M]$, y que $\beta' \in M$ implica que $\sigma^{\ell^{n-1}}(\beta') = \beta'$, entonces $\beta = N_{L/M}(\alpha'\gamma)$, lo cual contradice la hipótesis de que $\beta \notin N_{L/M}L^*$. Se sigue que $N_{M/K}$ es inyectiva.

Usando esto probaremos que $\Upsilon_{L/K}$ es inyectiva. En efecto, si $\Upsilon_{L/K}(\sigma) = 0$ para $\sigma \in \mathrm{Gal}(L/K)$, de nuevo considerando el diagrama de (2.27) observamos que L/M es cíclica de grado ℓ y M/K es cíclica de grado $< \ell^n$ y así, por hipótesis de inducción se tiene que $\Upsilon_{L/M}$ y $\Upsilon_{M/K}$ son isomorfismos; usando el cuadrado derecho $\Upsilon_{L/K}(\sigma) = 0$ implica que σ está en el núcleo del morfismo

horizontal superior derecho y así proviene de un $\sigma \in \mathrm{Gal}(L/M)$ y para este σ la conmutatividad del cuadrado izquierdo implica que $\Upsilon_{L/M}(\sigma) = 0$ y como $\Upsilon_{L/M}$ es un isomorfismo esto implica que $\sigma = id$ y así el σ de $\mathrm{Gal}(L/K)$ también es la identidad, i.e., $\Upsilon_{L/K}$ es inyectivo.

Para probar que $\Upsilon_{L/K}$ es suprayectivo, sea $\alpha \in K^*$; entonces considerando su clase mód $N_{L/K}L^*$, si mandamos esta clase a α mód $N_{M/K}M^*$ en el grupo derecho de la sucesión inferior de (2.27), como $\Upsilon_{M/K}$ es un isomorfismo entonces existe un único $\sigma \in \mathrm{Gal}(M/K)$ tal que $\Upsilon_{M/K}(\sigma) = \alpha$ mód $N_{M/K}M^*$. Levantando este σ a un $\tau \in \mathrm{Gal}(L/K)$, i.e., tal que $\tau|_M = \sigma$, se sigue que $\Upsilon_{L/K}(\tau) = \Upsilon_{M/K}(\sigma) = \alpha$ mód $N_{M/K}M^*$ por la conmutatividad del cuadrado derecho en (2.27).

Entonces, α mód $N_{L/K}L^*$ y $\Upsilon_{L/K}(\tau)$ van a dar al mismo α mód $N_{M/K}M^*$ y consecuentemente, por la exactitud de la sucesión inferior de (2.27), su cociente proviene de un γ mód $N_{L/M}L^*$ con $\gamma \in M^*$. Pero como $\Upsilon_{L/M}$ es un isomorfismo, entonces existe un único $\tau_1 \in \mathrm{Gal}(L/M)$ tal que $\Upsilon_{L/M}(\tau_1) = \gamma$ mód $N_{L/M}L^* \mapsto \alpha$ mód $N_{L/K}L^*/\Upsilon_{L/K}(\tau)$, y así, mandando τ_1 a $\widehat{\tau}_1 \in \mathrm{Gal}(L/K)$ se tiene que

$$\Upsilon_{L/K}(\tau\widehat{\tau}_1) = \alpha \text{ mód } N_{L/K}L^*,$$

i.e., $\Upsilon_{L/K}$ es suprayectivo.

Caso 3. Supongamos ahora que L/K es abeliana finita. La suprayectividad de $\Upsilon_{L/K}$ se prueba como en el caso anterior por inducción sobre $[L : K]$, eligiendo una subextensión cíclica M/K de L/K.

Para la inyectividad de $\Upsilon_{L/K}$, supongamos que M/K es una subextensión cíclica de grado ℓ^n de L/K. Si $\Upsilon_{L/K}(\sigma) = 0$ para $\sigma \in \mathrm{Gal}(L/K)$, entonces el cuadrado izquierdo del diagrama del corolario (2.27) implica que $0 = \Upsilon_{L/K}(\sigma) = \Upsilon_{M/K}(\sigma|_M)$, donde por hipótesis de inducción $\Upsilon_{M/K}$ es inyectivo; se sigue que $\sigma|_M = id$ y por lo tanto $\mathrm{Ker}\,\Upsilon_{L/K}$ está contenido en el núcleo del morfismo natural

$$\mathrm{Gal}(L/K) \longrightarrow \prod_M \mathrm{Gal}(M/K),$$

donde M/K recorre todas las subextensiones cíclicas de L/K. Pero este núcleo es trivial ya que $\mathrm{Gal}(L/K)$ es abeliano y por lo tanto se descompone como el producto de grupos cíclicos. Se sigue que $\sigma = id$ y por lo tanto $\Upsilon_{L/K}$ es inyectivo.

CASO 4. Si L/K es una extensión finita de Galois arbitraria. Por (1.78), $\mathrm{Gal}(L/K)$ es un grupo soluble. Si no es abeliano, su grupo conmutador $\mathrm{Gal}(L/K)'$ no es trivial. Sea M su campo fijo, i.e., $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)'$. En el diagrama conmutativo del corolario (2.27), como $\mathrm{Gal}(M/K) = \mathrm{Gal}^{ab}(L/K)$ se tiene que $\Upsilon_{M/K}$ es un isomorfismo por el caso (3). Entonces, si $\Upsilon_{L/K}(\sigma) = 0$, la conmutatividad del cuadrado derecho implica que $\Upsilon_{M/K}(\sigma|_M) = 0$ y por lo tanto $\sigma|_M = id$ y así, por la exactitud de la sucesión superior en el diagrama de (2.27), se tiene que $\sigma \in \mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)'$, i.e., $\Upsilon_{L/K}$ es inyectiva. La suprayectividad se sigue como en (3) ó (2). □

2.4 El morfismo de reciprocidad local

Definición 2.31. El inverso del isomorfismo de Neukirch

$$\Upsilon_{L/K} : \mathrm{Gal}^{ab}(L/K) \to K^*/N_{L/K}L^*$$

del último teorema de la sección anterior, se denota por

$$\Psi_{L/K} : K^*/N_{L/K}L^* \longrightarrow \mathrm{Gal}^{ab}(L/K)$$

y se llama el *morfismo de reciprocidad local.* También se suele usar el nombre de *símbolo de norma residual* para el isomorfismo $\Psi_{L/K}$ y la notación siguiente: si $\alpha \in K^*$ es un representante de la clase $\overline{\alpha} \in K^*/N_{L/K}L^*$, se usa la notación

$$\Psi_{L/K}(\overline{\alpha}) = (\alpha, L/K) \in \mathrm{Gal}^{ab}(L/K).$$

Nótese que el morfismo de reciprocidad $(\ \ , L/K) \quad K^*/N_{L/K}L^* \longrightarrow \mathrm{Gal}^{ab}(L/K)$ induce un epimorfismo:

$$(\ \ , L/K) : K^* \twoheadrightarrow \mathrm{Gal}^{ab}(L/K)$$

al que también se le llama *morfismo de reciprocidad* o *símbolo de norma residual.*

El nombre de *símbolo de norma residual* proviene del hecho de que $(\alpha, L/K)$ determina cuándo $\alpha \in K^*$ es una norma de L^*:

$(\alpha, L/K) = 1 = id \in \mathrm{Gal}^{ab}(L/K)$ si y sólo si α es una norma de L^*.

Observación. Si L/K es una *extensión abeliana*, entonces $G^{ab} = G$ y así el teorema anterior (i.e., la ley de reciprocidad local) nos da una descripción de su grupo de Galois:

$$\Psi_{L/K} : K^*/N_{L/K}L^* \simeq \mathrm{Gal}(L/K).$$

El problema de calcular explícitamente el símbolo de norma residual $(\alpha, L/K)$ para una extensión L/K y un elemento $\alpha \in K^*$ dados, es en general difícil. Sin embargo, en el caso cuando L/K es finita no ramificada, la proposición (2.25) leída en términos del morfismo de reciprocidad nos da una fórmula que involucra al elemento de Frobenius correspondiente, expresando en forma natural que la ley de reciprocidad asocia elementos primos al automorfismo de Frobenius correspondiente:

Proposición 2.32. *Sean L/K una extensión finita no ramificada de grado n de campos locales y $\alpha \in K^*$. Sean $\mathrm{Fr}_{L/K} \in \mathrm{Gal}(L/K)$ el automorfismo de Frobenius y $v_K : K^* \to \mathbb{Z}$ la valuación normalizada de K. Entonces,*

$$(\alpha, L/K) = \mathrm{Fr}_{L/K}^{v_K(\alpha)}.$$

DEMOSTRACIÓN. Por (2.25) $(\pi_K, L/K) = \mathrm{Fr}_{L/K}$ y $(\ \ , L/K) : K^*/N_{L/K} \to \mathrm{Gal}(L/K)$ es un isomorfismo. Ahora, si $u \in U_K$, como por (2.5) $N_{L/K} : U_L \simeq U_K$, entonces existe una unidad $\varepsilon \in U_L$ tal que $u = N_{L/K}(\varepsilon) \in N_{L/K}(L^*)$ y así $(u, L/K) = 1$. Entonces, para todo $\alpha \in L^*$, escribiéndolo como $\alpha = \pi_K^{v_K(\alpha)}u$ con $u \in U_K$, se tiene que

$$(\alpha, L/K) = (\pi_K^{v_K(\alpha)}u, L/K) = (\pi_K, L/K)^{v_K(\alpha)}(u, L/K) = \mathrm{Fr}_{L/K}^{v_K(\alpha)}.$$

□

Corolario 2.33. *Sea L/K una extensión abeliana finita. Entonces, el morfismo de reciprocidad*

$$(\ \ , L/K) : K^* \to \mathrm{Gal}(L/K)$$

lleva al grupo de unidades U_K en el subgrupo de inercia de $\mathrm{Gal}(L/K)$.

DEMOSTRACIÓN. Sea G_0 el subgrupo de inercia de $G = \mathrm{Gal}(L/K)$ y sea $L_0 = L^{G_0}$ el campo fijo correspondiente. La extensión L_0/K es no ramificada por (1.50). Por la proposición anterior la imagen de U_K en $\mathrm{Gal}(L_0/K) = G/G_0$ es trivial; por lo tanto, la imagen de U_K en $G = \mathrm{Gal}(L/K)$ está contenida en G_0.

Recíprocamente, sea $t \in G_0$; entonces existe $a \in K^*$ tal que $t = (a, L/K)$. Pongamos $f = [L_0 : K]$. Como $(a, L/K) = t \in G_0$ es trivial en L_0 y como el orden del grupo $\mathrm{Gal}(L_0/K)$ es f, la proposición anterior muestra que f divide a $v_K(a)$ y por lo tanto existe $b \in L^*$ tal que $v_K(a) = v_K(N(b))$. Si ponemos $u = a \cdot N(b)^{-1}$, entonces $u \in U_K$ y

$$(u, L/K) = (a \cdot N(b)^{-1}, L/K) = (a, L/K)(N(b)^{-1}, L/K) = (a, L/K) = t$$

ya que $N(b)^{-1}$ es una norma y por lo tanto $(N(b)^{-1}, L/K) = 1$; se sigue que la imagen de U_K es precisamente G_0. □

Propiedades funtoriales del morfismo de reciprocidad. Las proposiciones (2.26), (2.29) y (2.28) interpretadas en términos del morfismo $\Psi_{L/K}$ inverso del morfismo de Neukirch $\Upsilon_{L/K}$ expresan la conducta funtorial del morfismo de reciprocidad con respecto a extensiones de L y de K:

Proposición 2.34. (1) *Sea L/K una extensión finita de Galois. Entonces:*

(1) *Si L'/K' es una extensión finita de Galois de campos locales tales que $K' \supseteq K$ y $L' \supseteq L$ son finitas, entonces el diagrama siguiente conmuta:*

$$\begin{array}{ccc} K'^* & \xrightarrow{(\ ,L'/K')} & \mathrm{Gal}^{ab}(L'/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ K^* & \xrightarrow[(\ ,L/K)]{} & \mathrm{Gal}^{ab}(L/K) \end{array}$$

en particular:

(i) *Si $L = L'$, i.e., si $L \supseteq K' \supseteq K$, entonces el diagrama siguiente conmuta:*

$$\begin{array}{ccc} K'^* & \xrightarrow{(\ ,L/K')} & \mathrm{Gal}^{ab}(L/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow \\ K^* & \xrightarrow[(\ ,L/K)]{} & \mathrm{Gal}^{ab}(L/K) \end{array}$$

(ii) *Si $K = K'$, i.e., si $L' \supseteq L \supseteq K$, entonces el diagrama siguiente conmuta:*

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,L'/K)} & \mathrm{Gal}^{ab}(L'/K) \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ K^* & \xrightarrow[(\ ,L/K)]{} & \mathrm{Gal}^{ab}(L/K). \end{array}$$

(2) *Si M es un campo intermedio de L/K y V es el morfismo de transferencia, el diagrama siguiente conmuta:*

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,L/K)} & \mathrm{Gal}^{ab}(L/K) \\ \downarrow & & \downarrow{\scriptstyle V} \\ M^* & \xrightarrow[(\ ,L/M)]{} & \mathrm{Gal}^{ab}(L/M) \end{array}$$

(3) *Sea $L \supseteq M \supseteq K$ una torre de extensiones finitas de campos locales con M/K separable y L/M Galois. Si $\sigma \in \mathrm{Gal}(K^{sep}/K)$, entonces el diagrama siguiente conmuta:*

$$\begin{array}{ccc} M^* & \xrightarrow{(\ ,L/M)} & \mathrm{Gal}^{ab}(L/M) \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle c_\sigma} \\ (\sigma M)^* & \xrightarrow[(\ ,\sigma L/\sigma M)]{} & \mathrm{Gal}^{ab}(\sigma L/\sigma M) \end{array}$$

donde $\sigma : M^* \to \sigma M^*$ está dada por $\sigma : a \mapsto \sigma a$, y c_σ es el morfismo inducido por la aplicación $\sigma : M^* \to \sigma M^*$ anterior y la conjugación: $\tau \mapsto \sigma\tau\sigma^{-1}$ de $\mathrm{Gal}(\sigma L/\sigma M) \xrightarrow{\simeq} \mathrm{Gal}(L/M)$.

La conmutatividad de este diagrama se puede reescribir en la forma:

$$\sigma(\alpha, L/M)\sigma^{-1} = (\sigma\alpha, \sigma L/\sigma M).$$

DEMOSTRACIÓN. El primer diagrama de (1) es (2.26) y los otros dos diagramas son inmediatos de (1). El diagrama de (2) es (2.29) y el diagrama de (3) es (2.28). □

Observación. La compatibilidad anterior nos permite pasar al límite inverso sobre todas las extensiones normales de K y así podemos definir el símbolo $(\alpha, L/K)$ para todas las extensiones abelianas L de K; en particular, para la

máxima extensión abeliana $L = K^{ab}$ del campo local K obtenemos el morfismo de reciprocidad:

$$\Psi_K := \Psi_{K^{ab}/K} = (\ ,K^{ab}/K) : K^* \longrightarrow \mathrm{Gal}(K^{ab}/K),$$

y pasando al límite sobre los diagramas de (1)(i), (2) y (3) en la proposición anterior obtenemos:

Corolario 2.35. *Sea* L/K *una extensión separable y sean* L^{ab} *y* K^{ab} *las máximas extensiones abelianas correspondientes. Entonces:*

(1) *Los diagramas siguientes conmutan:*

$$\begin{array}{ccc} L^* & \xrightarrow{(\ ,L^{ab}/L)} & \mathrm{Gal}(L^{ab}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ K^* & \xrightarrow[(\ ,K^{ab}/K)]{} & \mathrm{Gal}(K^{ab}/K) \end{array} \qquad \begin{array}{ccc} K^* & \xrightarrow{(\ ,K^{ab}/K)} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow & & \downarrow{\scriptstyle v} \\ L^* & \xrightarrow[(\ ,L^{ab}/L)]{} & \mathrm{Gal}(L^{ab}/L). \end{array}$$

(2) *El diagrama* (3) *de* (2.34) *se vuelve la fórmula*

$$\sigma(\alpha, K^{ab}/M)\sigma^{-1} = (\sigma\alpha, K^{ab}/\sigma M).$$

□

2.5 Grupos de normas y campos de clases locales

El problema principal de la teoría de campos es clasificar todas las extensiones de Galois L/K de un campo dado K mediante *objetos aritméticos* de K, es decir, dar una ley mediante la cual todas estas extensiones L puedan ser construidas a partir de K usando solamente la estructura interna del campo K; es decir, se busca una ley que clasifique las extensiones L/K mediante objetos directamente asociados al campo K. Veremos a continuación que la ley de reciprocidad local resuelve el problema anterior para *extensiones abelianas* L de K en el sentido de que nos da una biyección entre estas extensiones abelianas y los subgrupos cerrados de índice finito (en la topología natural de K^*) del grupo K^*; al final mostramos que estos subgrupos cerrados de índice finito son los subgrupos de norma:

Definición 2.36. Un subgrupo $M \subseteq K^*$ se llama un *subgrupo de normas* si existe una extensión finita L/K tal que $M = N_{L/K}L^*$.

Ejemplo. Sea $m \geq 1$ un entero y sea M_m el conjunto de elementos $a \in K^*$ tales que $v_K(a) \equiv 0 \pmod{m}$; se sigue de la proposición (2.32) y de la definición de símbolo de norma residual (2.31) que M_m es el grupo de normas de la extensión K_m de K no ramificada de grado m.

Lema 2.37. *Los grupos de normas de un campo local K tienen índice finito en K^*. Más aún, si $H = N_{L/K}L^* \subseteq K^*$, con L/K una extensión finita de campos locales, entonces el índice del grupo de normas $N_{L/K}L^*$ en K^* divide al grado $[L : K]$ y es igual a este grado si y sólo si L/K es abeliana.*

DEMOSTRACIÓN. En efecto, si $H = N_{L/K}L^*$, con L/K finita, por la ley de reciprocidad $K^*/N_{L/K}L^* \simeq \mathrm{Gal}^{ab}(L/K)$ y este último grupo es un cociente del grupo finito $\mathrm{Gal}(L/K)$. Se sigue que

$$|K^*/N_{L/K}L^*| = |\mathrm{Gal}^{ab}(L/K)| \leq |\mathrm{Gal}(L/K)| = [L : K]$$

y la igualdad se da si y sólo si L/K es abeliana. □

Observamos ahora que la restricción a extensiones abelianas de nuestros métodos se debe a que extensiones no abelianas dan los mismos subgrupos de normas que las abelianas:

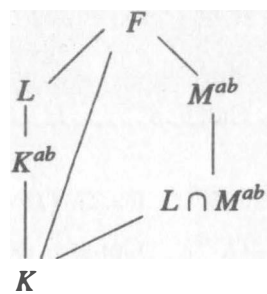
Proposición 2.38. *Sea L/K una extensión finita de campos locales y sea K^{ab} la máxima extensión abeliana de K contenida en L. Entonces,*

$$N_{L/K}L^* = N_{K^{ab}/K}(K^{ab})^*.$$

DEMOSTRACIÓN. Como $L \supseteq K^{ab} \supseteq K$, se tiene una inclusión

$$N_{L/K}L^* \subseteq N_{K^{ab}/K}(K^{ab})^*.$$

Para la otra inclusión, sea F/K una extensión normal que contiene a L y consideremos el diagrama de campos siguiente:



y sean $G = \mathrm{Gal}(F/K)$, $H = \mathrm{Gal}(F/L)$ y $G' = [G : G]$ el subgrupo conmutador de G. Sea M^{ab} la máxima extensión abeliana de K contenida en F, de tal forma que $\mathrm{Gal}(F/M^{ab}) = G'$ y $\mathrm{Gal}(M^{ab}/K) = G/G'$.

Observemos que para la intersección $L \cap M^{ab}$ se tiene que

$$(*) \qquad L \cap M^{ab} = F^{H \cdot G'}$$

ya que como $L = F^H$ y $M^{ab} = F^{G'}$, entonces

$$(1) \qquad L \cap M^{ab} = F^H \cap F^{G'} \subseteq F^{H \cdot G'},$$

y recíprocamente, como $H \subseteq H \cdot G'$ entonces $F^H \supseteq F^{H \cdot G'}$ y de modo similar $G' \subseteq H \cdot G'$ implica que $F^{G'} \supseteq F^{H \cdot G'}$, y así

$$(2) \qquad L \cap M^{ab} = F^H \cap F^{G'} \supseteq F^{H \cdot G'},$$

(1) y (2) prueban (*).

Ahora, como $\mathrm{Gal}(F/L \cap M^{ab}) = \mathrm{Gal}(F/F^{H \cdot G'}) = HG'$, entonces

$$\mathrm{Gal}(L \cap M^{ab}/K) = G/HG'$$

y este grupo es abeliano ya que contiene al subgrupo conmutador G' de G. Así, como $L \cap M^{ab} \subseteq L$, entonces se debe tener que

$$(3) \qquad L \cap M^{ab} \subseteq K^{ab}$$

por definición de K^{ab}.

Finalmente, como $K^{ab} \subseteq F$ y la extensión K^{ab}/K es abeliana, entonces $K^{ab} \subseteq M^{ab}$ por definición de M^{ab}. Se sigue que

$$(4) \qquad K^{ab} \subseteq L \cap M^{ab},$$

y de (3), (4) y (*) se tiene que

$$K^{ab} = L \cap M^{ab} = F^{H \cdot G'}.$$

Se sigue que

$$\mathrm{Gal}(F/K^{ab}) = H \cdot G'$$

y

$$\mathrm{Gal}(K^{ab}/K) = G/(H \cdot G').$$

Ahora, sea $\xi \in N_{K^{ab}/K}(K^{ab})^*$. Como ξ es una norma de K^{ab}, la ley de reciprocidad nos dice que $(\xi, K^{ab}/K) = 1$ en $\mathrm{Gal}(K^{ab}/K) = G/(H \cdot G')$.

Considerando entonces a $(\xi, F/K) \in G^{ab} = G/G'$, su proyección sobre G/HG' corresponde a formar $(\xi, K^{ab}/K) = 1$ por el diagrama de (2.35)(2). Se sigue que $(\xi, F/K)$ está en el núcleo de $G/G' \to G/HG'$, i.e.,

$$(\xi, F/K) \in H/H' = \mathrm{Gal}^{ab}(F/L).$$

Ahora, por (2.35)(1) el diagrama siguiente conmuta

$$\begin{array}{lll} L^* & \xrightarrow{(\ ,F/L)} & \mathrm{Gal}^{ab}(F/L) \quad = H/H' \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ K^* & \xrightarrow[(\ ,F/K)]{} & \mathrm{Gal}^{ab}(F/K) \quad = G/G' \end{array}$$

y como la ley de reciprocidad $(\ , F/L)$ es suprayectiva, existe $\lambda \in L^*$ tal que

$$(\xi, F/K) = (N_{L/K}(\lambda), F/K).$$

Pero el núcleo del morfismo de norma residual es el grupo de normas $N_{L/K}(F^*)$, y como $\xi \cdot N_{L/K}(\lambda)^{-1}$ está en este núcleo por la igualdad anterior, entonces existe un $\zeta \in F^*$ tal que $N_{F/K}(\zeta) = \xi \cdot N_{L/K}(\lambda)^{-1}$, i.e.,

$$\xi = N_{L/K}(\lambda) N_{F/K}(\zeta);$$

y consecuentemente $\xi = N_{L/K}(\lambda \cdot N_{F/K}(\zeta)) \in N_{L/K}L^*$. □

Así, usando la ley de reciprocidad sólo se pueden clasificar extensiones abelianas.

El resultado siguiente establece la correspondencia entre las extensiones abelianas (finitas) de un campo local K y los subgrupos de normas del grupo multiplicativo K^* de K. Antes, recordemos que una función continua $f : X \to Y$ entre espacios topológicos se llama *propia* si la imagen inversa de cualquier compacto de Y es compacto en X.

Teorema 2.39. *Sea K un campo local. Entonces:*

(1) *La función*

$$L \mapsto N_{L/K}L^*$$

es una biyección entre el conjunto de extensiones abelianas finitas de K y el conjunto de subgrupos de normas de K^*.

(2) *Esta biyección invierte inclusiones.*

(3) $N(LL') = NL \cap NL'$.

(4) $N(L \cap L') = N(L) \cdot N(L')$.

(5) *Cualquier subgrupo de K^* que contenga un subgrupo de normas es un subgrupo de normas.*

(6) *Si L/K es una extensión finita de grado n, entonces $N_{L/K} : L^* \to K^*$ es continua y propia. Se sigue que el grupo $N_{L/K}L^*$ es cerrado de índice finito en K^*, i.e., es abierto.*

DEMOSTRACIÓN. (3): Si L, L' son extensiones abelianas finitas, entonces la transitividad de la norma nos da

$$N(LL') \subseteq NL \cap NL',$$

(obsérvese que la composición LL'/K es abeliana ya que L/K y L'/K lo son).

Recíprocamente, si $a \in NL \cap NL'$, entonces el elemento

$$(a, LL'/K) \in \mathrm{Gal}(LL'/K)$$

tiene proyecciones triviales (porque es norma para cada uno de los factores) $(a, L/K) = 1$ y $(a, L'/K) = 1$ en los correspondientes $\mathrm{Gal}(L/K)$ y $\mathrm{Gal}(L'/K)$, de tal forma que $(a, LL'/K) = 1$ y por lo tanto $a \in N(LL')$.

(2): Usando (3) observemos que

$$NL \supseteq NL' \Leftrightarrow N(LL') = NL \cap NL' = NL' \Leftrightarrow [LL' : K] = [L' : K] \Leftrightarrow L \subseteq L'.$$

(1): Notemos que (2) implica que la función $L \mapsto NL$ es *inyectiva* y por lo tanto establece la biyección deseada.

(5): Si $N' \subseteq K^*$ es un subgrupo que contiene a un subgrupo de normas NL, entonces

$$(N', L/K) = \mathrm{Gal}(L/L')$$

para un campo intermedio L' de L/K. Observamos entonces que como $N' \supseteq NL$, entonces N' es la preimagen de $\mathrm{Gal}(L/L')$ bajo el morfismo

$$(\ , L/K) : K^* \longrightarrow \mathrm{Gal}(L/K),$$

i.e., es el núcleo de

$$(\ , L'/K) : K^* \longrightarrow \mathrm{Gal}(L'/K),$$

de tal forma que $N' = NL'$ como se requería.

(4): Como $L \cap L' \subseteq L$ y $L \cap L' \subseteq L'$, entonces por (2):

$$N(L \cap L') \supseteq NL \qquad \text{y} \qquad N(L \cap L') \supseteq NL',$$

y por lo tanto

$$N(L \cap L') \supseteq NL \cdot NL'.$$

Recíprocamente, como $L, L' \subseteq LL'$ entonces $N(LL') \subseteq NL$ y $N(LL') \subseteq NL'$ por (2), y así

$$N(LL') \subseteq NL \cdot NL',$$

es decir, $NL \cdot NL'$ contiene a un subgrupo de normas, de tal forma que por (5) debe ser de la forma

$$NL \cdot NL' = NL''$$

para L''/K finita abeliana. Finalmente, como $NL \subseteq NL''$ y $NL' \subseteq NL''$, se sigue de (2) que $L'' \subseteq L \cap L'$ y por lo tanto

$$NL \cdot NL' = NL'' \supseteq N(L \cap L').$$

(6): Si $a \in L^*$, entonces $N_{L/K}(a)$ es por definición el producto de los conjugados de a (sobre K) y como el grupo de Galois $G_K := \mathrm{Gal}(K_s/K)$ actúa continuamente sobre L^*, entonces $N_{L/K}$ es continua.

Para mostrar que $N_{L/K}$ es propia, observemos que para cada subconjunto compacto V de K^* su imagen bajo la valuación $v_K : K^* \twoheadrightarrow \mathbb{Z}$ es compacta y por lo tanto finita. Más aún, si U_K es el grupo de unidades de K, entonces U_K es compacto ya que K es un campo local, y así $V' := V \cap U_K$ es también un subconjunto compacto de U_K. Ahora, como U_L es compacto, en el diagrama conmutativo siguiente

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle n} & & \\
0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow[v_K]{} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

la imagen inversa $N_{L/K}^{-1}(V')$ es un subconjunto compacto de U_L y por lo tanto es un subconjunto compacto de L^*. Pero V es una unión finita de trasladados de V' ya que $v_K(V)$ es finito; se sigue que $N_{L/K}^{-1}(V)$ es una unión finita de trasladados del conjunto compacto $N_{L/K}^{-1}(V')$, y por lo tanto $N_{L/K}^{-1}(V)$ es compacto.

Para la segunda afirmación, como $N_{L/K}$ es una función propia entre espacios Hausdorff localmente compactos, entonces es *cerrada* y por lo tanto $N_{L/K}L^*$ es cerrado en K^*. Finalmente, de la ley de reciprocidad se sigue que $N_{L/K}L^*$ tiene índice finito en K^*. □

Observación. Las partes (3) y (4) del teorema anterior implican que si tomamos como una base de abiertos del $1 \in K^*$ a los subgrupos de normas $N_{L/K}L^*$ de K^*, donde L/K recorre las extensiones finitas de Galois de K, se tiene una topología en K^* a la que se llama la *topología de norma.* Observamos también que por la parte (6) del teorema anterior, si L/K es finita el grupo $N_{L/K}L^*$ es cerrado de índice finito (i.e., es abierto) en K^*, en la topología de K^* inducida por la valuación; se sigue que *la topología natural de K^* es más fina que la topología de norma.*

Si K es un campo local, el *grupo de normas universales* de K, denotado $\mathcal{N}_K$, es la intersección de todos los subgrupos de normas de K^*.

Teorema 2.40. *Sea K un campo local. Entonces:*

(1) *Si L/K es una extensión finita, entonces*

$$N_{L/K}\mathcal{N}_L = \mathcal{N}_K.$$

(2) *En la topología de norma, los subgrupos abiertos de K^* son los subgrupos cerrados de índice finito.*

(3) *Si K_s es una cerradura separable de K, entonces el grupo de normas universales $\mathcal{N}_K$ es el núcleo del morfismo de reciprocidad*

$$(\ ,K_s/K) : K^* \longrightarrow \mathrm{Gal}^{ab}(K_s/K).$$

(4) *K^* es Hausdorff en la topología de norma si y sólo si el grupo de normas universales*

$$\mathcal{N}_K := \bigcap_L N_{L/K}L^*$$

es trivial.

DEMOSTRACIÓN. (1): Si $a \in N_{L/K}\mathcal{N}_L$, queremos mostrar que $a \in N_{F/K}F^*$ para todas las extensiones F/K. Observemos primero que para la composición LF se tiene que $N_{LF/L}(LF)^* \supseteq \mathcal{D}_L$, y por la transitividad de la norma se tiene que

$$a \in N_{L/K}(N_{LF/L}(LF)^*) \subseteq N_{LF/K}(LF)^* = N_{F/K}(N_{LF/F}(LF)^*) \subseteq N_{F/K}F^*,$$

y por lo tanto $a \in N_{F/K}F^*$ como se quería.

Recíprocamente, si $a \in \mathcal{N}_K$, sea F/L una extensión finita; consideremos el conjunto $\Omega_a(F)$ de todos aquellos elementos $b \in L^*$ cuya norma es igual a a y que son normas de elementos de F, i.e.,

$$\Omega_a(F) = N_{F/L}F^* \cap N_{L/K}^{-1}(a).$$

Observamos que como $N_{L/K}$ es una aplicación propia, entonces los conjuntos $\Omega_a(F)$ son compactos para todas las extensiones F de L. Ahora, como $a \in \mathcal{N}_K$ entonces $a \in N_{F/K}F^*$ para cada extensión F de L; así, si $a = N_{F/K}(b_F)$ para algún $b_F \in F^*$, entonces $N_{F/L}(b_F) \in \Omega_a(F)$ y por lo tanto los conjuntos $\Omega_a(F)$ son no vacíos. Variando los campos F los conjuntos $\Omega_a(F)$ forman una familia decreciente, por (2.39)(3), de subconjuntos compactos no vacíos de $\Omega_a(L)$; así, por compacidad su intersección es no vacía, i.e., existe $b \in \bigcap_F \Omega_a(F)$, y es claro que $b \in \mathcal{N}_L$ (por definición de $\mathcal{N}_L$) y $N_{L/K}(b) = a$, i.e., $a \in N_{L/K}\mathcal{N}_L$.

(2): Si N es un subgrupo de K^*, entonces K^* es la unión de todas las clases laterales de N y por lo tanto

$$(\dagger) \qquad N = K^* - \bigcup_{aN \neq N} aN.$$

Así, si N es abierto, entonces las clases laterales aN también son abiertas y por lo tanto N es cerrado. Y como N es abierto en la topología de norma, entonces debe contener alguna vecindad abierta $N_{L/K}L^*$ del 1, i.e., $N \supseteq N_{L/K}L^*$ y como $N_{L/K}L^*$ es de índice finito en K^* por el lema (2.37), entonces N es de índice finito también.

Recíprocamente, si N es cerrado de índice finito, entonces la unión en (†) es de un número finito de clases laterales $aN \neq N$, cada una de las cuales es cerrada y por lo tanto la unión también es cerrada y consecuentemente N es abierto.

(3): Si $a \in K^*$, entonces $a \in \mathcal{N}_K$ si y sólo si $a \in \bigcap_L N_{L/K}L^*$ para toda extensión abeliana L/K por (2.38), y por la ley de reciprocidad esto sucede si

y sólo si $(a, L/K) = 1$ para toda extensión abeliana L/K, i.e., si y sólo si a está en el núcleo del morfismo de reciprocidad $(\ , K_s/K) : K^* \longrightarrow \mathrm{Gal}^{ab}(K_s/K)$.

(4): Trivial. □

Definición 2.41. Si K es un campo y L/K es una extensión abeliana finita asociada a un subgrupo de normas $N \subseteq K^*$ bajo la correspondencia del teorema (2.39), se dice que L *es el campo de clases de* N. Nótese entonces que por la *ley de reciprocidad* (2.31) se tiene que

$$\mathrm{Gal}(L/K) \simeq K^*/N.$$

De la discusión anterior y de la ley de reciprocidad se sigue que si ya conociéramos el grupo de normas $N_{L/K}L^*$ de una extensión abeliana L/K, entonces ya conoceríamos el grupo de Galois de L/K. Así, la clasificación de las extensiones abelianas se seguirá de la clasificación de subgrupos de K^* que son subgrupos de norma. Éste es el objetivo fundamental de la siguiente sección.

2.6 El teorema de existencia

El teorema de existencia que probaremos en esta sección nos dice que el conjunto de subgrupos de índice finito de K^* coincide con el conjunto de subgrupos de norma de K^*. Ya sabemos por (2.37) que todo subgrupo de normas $N_{L/K}(L^*) \subseteq K^*$ es de índice finito, así que sólo falta probar que dado un subgrupo de índice finito $H \subseteq K^*$ *existe* una extensión finita abeliana L/K tal que $H = N_{L/K}(L^*)$. Ésta es la *existencia* de donde toma su nombre el teorema. Para probar este teorema probaremos primero que la topología de norma es Hausdorff o, equivalentemente, por (2.40)(4), probaremos que el grupo de normas universales $\mathcal{N}_K$ es trivial y para esto debemos apelar a la estructura aritmética de K de tal forma que ésta es la parte del argumento que es más sutil.

Antes de probar lo anterior mostramos un caso especial del teorema de existencia:

Lema 2.42 (Teorema de ramificación). *Sea K un campo local. Todo subgrupo de índice finito de K^* que contiene al grupo de unidades U_K de K, es un grupo de normas de alguna extensión no ramificada de K. Una condición necesaria y suficiente para que L/K sea no ramificada es que $N_{L/K}L^* \supseteq U_K$.*

DEMOSTRACIÓN. Por (2.5), toda unidad de K es una norma de toda extensión no ramificada de K. Ahora sea N un subgrupo de índice finito de K^* que contiene a U_K; digamos $n = [K^* : N]$. Observemos que de la sucesión exacta

$$0 \quad U_K \longrightarrow K^* \xrightarrow{v_K} \mathbb{Z} \longrightarrow$$

se tiene que $\mathbb{Z} \simeq K^*/U_K$ y así, si $N \subseteq K^*$ es un subgrupo de índice finito n que contiene a U_K, entonces N/U_K es un subgrupo de K^*/N de índice n y por lo tanto corresponde, bajo el isomorfismo anterior, al subgrupo $n\mathbb{Z} \subseteq \mathbb{Z}$, i.e., $N = v_K^{-1}(n\mathbb{Z})$, por lo que N está determinado por su índice n.

Consideremos ahora una extensión no ramificada K_n/K de grado n; entonces $[K^* : N_{K_n/K}K_n^*] = [K_n : K] = n$, y por (2.5) se tiene que $U_K = N_{K_n/K}K_n^*$. Se sigue que $N = N_{K_n/K}K_n^*$. La segunda afirmación es ahora trivial. □

Teorema 2.43 (Teorema de existencia). *Sea K un campo local. Un subgrupo de índice finito $N \subseteq K^*$ es un subgrupo de normas si y sólo si N es cerrado de índice finito (i.e., N es abierto en la topología natural de K^*).*

DEMOSTRACIÓN. Si N es un subgrupo de normas de índice finito, entonces $N = N_{L/K}L^*$ para L/K una extensión finita abeliana. Por el teorema (2.39)(6) anterior la función

$$N_{L/K} : L^* \to K^*$$

es continua y propia, y por lo tanto la imagen $N = N_{L/K}L^*$ es cerrada en K^*.

La implicación que falta es la importante y es donde toma su nombre el teorema: debemos probar que si $N \subseteq K^*$ es un subgrupo cerrado (en la topología natural de K^*) y de índice finito, entonces *existe* una extensión abeliana finita L/K tal que $N_{L/K}L^* = N$.

Para probar esto necesitaremos los resultados siguientes, de los cuales se derivará formalmente el teorema de existencia:

Afirmación. *Para cada número primo p, existe un campo K_p con la propiedad de que si el campo L contiene a K_p, entonces la aplicación $x \mapsto x^p$ de L^* en sí mismo tiene núcleo compacto y su imagen contiene al grupo de normas universales $\mathcal{N}_L$.*

Esta afirmación es la que resulta difícil de probar, y pospondremos su demostración hasta el final de esta sección. Como consecuencia de esta afirmación, se tiene:

Proposición 2.44. *Si K es un campo local, el grupo de normas universales $\mathcal{N}_K$ es divisible y de hecho igual a $\bigcap_n (K^*)^n$.*

DEMOSTRACIÓN. Mostraremos que para cada primo p se tiene que $\mathcal{N}_K^p = \mathcal{N}_K$. Para esto, si $a \in \mathcal{N}_K$ consideremos el conjunto de todos los campos L tales que L/K es finita y además $L \supseteq K_p$, donde K_p es el campo cuya existencia garantiza la afirmación anterior. Denotemos por

$$\Omega_\alpha(L) := \{\beta \in K^* \ : \ \beta^p = \alpha \ \text{ y } \ \beta \in N_{L/K} L^*\}.$$

Los conjuntos $\Omega_\alpha(L)$ son finitos y por lo tanto compactos. Observemos ahora que como $\alpha \in \mathcal{N}_K$, por la proposición (2.40)(1) se sigue que $\alpha \in N_{L/K}\mathcal{N}_L$; de la afirmación anterior se sigue que $\alpha \in N_{L/K}(L^{*p})$. Por lo tanto, existe un $\beta \in N_{L/K}L^*$ tal que $\alpha = \beta^p$; se sigue que $\Omega_\alpha(L)$ es no vacío, para cada tal campo L. Como en la demostración de (2.40)(1), la intersección de los conjuntos $\Omega_\alpha(L)$ es no vacía por la compacidad, y así existe un elemento $\beta \in \bigcap_L \Omega_\alpha(L)$, de tal forma que para este elemento se tiene que $\beta \in \mathcal{N}_K$ (por definición de los $\Omega_\alpha(L)$) y además $\beta^p = \alpha$; se sigue que $\mathcal{N}_K$ es divisible.

Más aún, como $K^* \supseteq \mathcal{N}_K$ se sigue que $K^{*n} \supseteq \mathcal{D}_K$ para cada natural n y por lo tanto $\mathcal{N}_K \subseteq \bigcap_n K^{*n}$. Recíprocamente, si $\alpha \in \bigcap_n K^{*n}$ y si la extensión L/K es de grado n, entonces $\alpha = \beta^n$ (ya que $\alpha \in K^{*n}$) y por lo tanto $\alpha = N_{L/K}\beta$; se sigue que $\beta \in \mathcal{N}_K$.

Finalmente observamos que un elemento de $\bigcap_n K^{*n}$ debe ser una unidad. En (2.45)(2) mostraremos que esta intersección es de hecho igual a $\{1\}$. □

Usando la proposición anterior, probaremos el teorema de existencia: sea $N \subseteq K^*$ un subgrupo cerrado de índice finito n. Entonces, $(K^*)^n \subseteq N$ y por lo tanto $\mathcal{N}_K \subseteq N$ por la proposición anterior. Se sigue que

$$\bigcap_L (N_{L/K}L^* \cap U_K) = \mathcal{N}_K \cap U_K \subseteq \mathcal{N}_K \subseteq N.$$

Ahora, como $N_{L/K}L^* \cap U_K$ es compacta para cada L, y como N es abierto, entonces existe un campo L tal que $N_{L/K}L^* \cap U_K \subseteq N$. Obtenemos entonces una inclusión:

$$(\dagger) \qquad N_{L/K}L^* \cap U_K(N_{L/K}L^* \cap N) \subseteq N$$

ya que si el elemento a pertenece al lado izquierdo, entonces $a \in N_{L/K}L^*$ y podemos escribirlo como $a = a'a''$ con $a' \in U_K$ y $a'' \in N_{L/K}L^* \cap N$; se sigue

que $a' = a(a'')^{-1} \in N_{L/K}L^*$ y por lo tanto $a' \in U_K \cap N_{L/K}L^*$ y $a' \in N$; se sigue que $a \in N$ como se quería.

Observamos ahora que el grupo $N_{L/K}L^* \cap N$ es cerrado de índice finito (ya que es la intersección de dos tales grupos); por lo tanto, el producto $U_K(N_{L/K}L^* \cap N)$ también es cerrado de índice finito. Como este grupo contiene a U_K, entonces es un grupo de normas por el lema (2.42). Por el teorema (2.39)(3) el grupo $N_{L/K}L^* \cap (U_K(N_{L/K}L^* \cap N))$ también es un grupo de normas; y por (†) N contiene a este grupo de normas y así, por (2.39)(5), N es un grupo de normas también. □

Corolario 2.45. *Sea K un campo local. Entonces*

(1) *Un subgrupo de índice finito de K^* es un grupo de normas si y sólo si contiene a un grupo $U_K^{(n)}$ para n suficientemente grande.*

(2) *El grupo $\mathcal{N}_K = \{1\}$ y por lo tanto la topología de norma es Hausdorff.*

DEMOSTRACIÓN. (1): Por (2.5)(1) los grupos $U_K^{(n)}$ son grupos de normas (de alguna extensión no ramificada de K) y así, si N contiene a uno de estos $U_K^{(n)}$, entonces N es grupo de normas también.

Recíprocamente, si $N \subseteq K^*$ es un subgrupo de normas de índice $n = [K^* N]$, entonces $U_K \subseteq N$ y como $U_K = U_K^{(0)}$, entonces para m suficientemente grande (en particular, coprimo con car (K)) se tiene que $\left(U_K^{(0)}\right)^m \subseteq N$, donde, por la proposición (1.67),

$$\left(U_K^{(0)}\right)^m = U_K^{(v_K(m))};$$

y así $U_K^{(v_K(m))} \subseteq N$, como se quería.

(2): Por (2.5)(1) los grupos $U_K^{(n)}$ son grupos de norma y por lo tanto son cerrados; claramente, su intersección es $\{1\}$ ya que U_K es Hausdorff compacto por (1.60). □

La parte (1) del corolario siguiente mejora al corolario (2.33):

Corolario 2.46. *Sea K un campo local. Entonces:*

(1) *Si $G_0 \subseteq \mathrm{Gal}(K^{ab}/K)$ es el grupo de inercia (1.50)(4) de la máxima extensión abeliana K^{ab} de K, entonces el morfismo de reciprocidad restringido a U_K es un isomorfismo $\Psi_K|_{U_K} : U_K \to G_0$ de grupos topológicos.*

(2) *El grupo de Galois $\mathrm{Gal}(K^{ab}/K)$ es una extensión de $\widehat{\mathbb{Z}}$ por U_K.*

DEMOSTRACIÓN. Pongamos $G_K := \mathrm{Gal}(K^{ab}/K)$. Se tiene entonces un diagrama conmutativo con renglones exactos:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \Psi_K} & & \downarrow{\scriptstyle \Psi_K} & & \downarrow{\scriptstyle i} & & \\ 0 & \longrightarrow & G_0 & \longrightarrow & G_K & \longrightarrow & \widehat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

donde el renglón de abajo es exacto ya que se tiene un isomorfismo $G_K/G_0 \simeq \widehat{\mathbb{Z}}$, i es la inyección canónica, Ψ_K es el morfismo de reciprocidad y su restricción a U_K.

Observamos ahora que la topología de U_K está definida por sus subgrupos cerrados de índice finito y U_K es compacto en esta topología y el núcleo del morfismo de reciprocidad $\Psi_K|_{U_K}$ es la inter ección de estos grupos, el cual es $\{1\}$ por el corolario anterior. Esto prueba (1), y (2) se sigue de (1) y de la exactitud de la sucesión exacta inferior del diagrama de arriba. □

Resta probar la **afirmación** que usamos en la demostración del teorema de existencia. Esto lo haremos en la subsección siguiente.

2.6.1 Símbolos locales

Para comenzar, observemos que la **afirmación** para campos locales usada en la sección anterior es consecuencia del teorema siguiente:

Teorema 2.47. *Sea K un campo local y sea L una extensión finita de K que contiene al grupo de raíces p-ésimas de la unidad, para p un primo dado. Si $\xi \in L^*$ y si ξ es una norma de toda extensión cíclica de L de grado p, entonces $\xi \in L^{*p}$.*

Corolario 2.48 (Afirmación). *Sean K un campo local, p un entero primo y $K_p := K(\mu_p)$ el campo obtenido adjuntando el grupo de raíces p-ésimas de la unidad a K. Si $L \supseteq K(\mu_p)$ es cualquier extensión, entonces la aplicación $x \mapsto x^p$ de L^* en sí mismo tiene núcleo compacto y su imagen contiene al grupo de normas universales $\mathcal{N}_L$.*

DEMOSTRACIÓN. (Del corolario). Claramente, el núcleo de $x \mapsto x^p$ es finito y por lo tanto compacto. Para la imagen L^{*p} de la aplicación, observemos que si $\xi \in \mathcal{N}_L$ entonces, en particular, es una norma de toda extensión cíclica de L de grado p y así, por el teorema anterior, $\xi \in L^{*p}$; es decir, $\mathcal{N}_L \subseteq L^{*p}$. □

Resta entonces probar el teorema anterior. Esto lo haremos considerando separadamente los casos de cuando $p \neq \text{car}(K)$ y cuando $p = \text{car}(K)$. En el primer caso usamos teoría de Kummer y en el segundo caso teoría de Artin-Schreier.

Teoría de Kummer. Trasladando los resultados de teoría de Kummer del Anexo 1 al contexto cuando *K es un campo local*, recordemos primero, de (1.72), que: *si K es un campo local, entonces:*

(1) *Si $n \geq 1$ es coprimo con* car (K) *(arbitrario si* car $(K) = 0$*), entonces $(K^*)^n$ es un subgrupo de índice finito en K^*.*

(2) *Si* car $(K) = p > 0$, *entonces $(K^*)^n$ es un subgrupo abierto de índice finito en K^* si y sólo si $p \nmid n$.*

Observemos ahora que si K es un campo local, $n \geq 1$ es un entero coprimo con car (K) y $L = K(\sqrt[n]{K^*})$ es la máxima extensión de Kummer de exponente n del campo K, entonces por *teoría de Kummer* (Anexo 1, (2.76)) y por la observación anterior de que $K^*/(K^*)^n$ es finito, se tiene un isomorfismo

$$\text{Hom}(\text{Gal}(L/K), \mu_n) \simeq K^*/(K^*)^n. \tag{1}$$

Más aún, como L/K es abeliana, entonces por la *ley de reciprocidad*

$$\text{Gal}(L/K) \simeq K^*/N_{L/K}L^*, \tag{2}$$

y como L/K es de exponente n, entonces n anula a los elementos de este grupo y por lo tanto

$$(K^*)^n \subseteq N_{L/K}L^*.$$

De los isomorfismos (1) y (2) se sigue que

$$|K^*/(K^*)^n| = |\text{Gal}(L/K)| = |K^*/N_{L/K}L^*|$$

y consecuentemente $(K^*)^n$ y $N_{L/K}L^*$ tienen el mismo índice (finito) en K^* y además, $(K^*)^n \subseteq N_{L/K}L^*$. Se sigue que

$$(K^*)^n = N_{L/K}L^*, \tag{3}$$

y por lo tanto $(K^*)^n$ es un grupo de normas y el isomorfismo (2), dado por *teoría de campos de clases local*, es

$$\text{Gal}(L/K) \simeq K^*/(K^*)^n. \tag{4}$$

Hemos así probado que:

Proposición 2.49. *Si K es un campo local, $n \geq 1$ es un entero coprimo con* car (K) *y $L = K(\sqrt[n]{K^*})$ es la máxima extensión de Kummer de exponente n del campo K, entonces*

$$\mathrm{Gal}(L/K) \simeq K^*/(K^*)^n.$$

□

Antes de proseguir notemos que ya hemos probado el teorema (2.43) en el caso cuando $p \neq$ car (K):

Corolario 2.50. *Sean K un campo local y p un primo distinto de* car (K). *Sea L una extensión finita de K que contiene al grupo de raíces p-ésimas de la unidad. Si $\xi \in L^*$ y si ξ es una norma de toda extensión cíclica de L de grado p, entonces $\xi \in L^{*p}$.*

DEMOSTRACIÓN. Por (2.73) en el Anexo 1, toda extensión cíclica de L de grado p es de la forma $L' = L(\sqrt[p]{b})$ para algún $b \in L$ y por (3) se tiene entonces que $(L^*)^p \simeq N_{L'/L}(L')^*$, y así, si $\xi \in L^*$ es una norma de toda extensión cíclica de L, entonces $\xi \in (L^*)^p$. □

El símbolo de Hilbert. Continuando con las observaciones anteriores notamos que de (1), (2) y (4) se sigue que el *apareamiento bilineal*

$$\mathrm{Gal}(L/K) \times \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \longrightarrow \mu_n$$

dado por $(\sigma, \chi) \mapsto \chi(\sigma)$, en vista de los isomorfismos (1) y (4) dados por teoría de Kummer y teoría de campos de clases, respectivamente, se vuelve el apareamiento bilineal

$$K^*/(K^*)^n \times K^*/(K^*)^n \longrightarrow \mu_n,$$

al cual se le denota $\left(\frac{a,b}{\mathfrak{p}_K}\right)_n$ y se le llama el *símbolo de Hilbert*. (Enfatizamos el carácter local del símbolo de Hilbert usando en su notación al ideal de valuación $\mathfrak{p}_K$). Explícitamente, el símbolo de Hilbert se calcula como sigue: dados $a, b \in K^*$, denotemos la imagen de $a \in K^*$ bajo el isomorfismo de reciprocidad

$$(\ , K(\sqrt[n]{b})/K) : K^*/(K^*)^n \simeq \mathrm{Gal}(K(\sqrt[n]{b})/K)$$

como $\sigma_a := (a, K(\sqrt[n]{b})/K)$.

Ahora, la imagen de $b \in K^*$ bajo el isomorfismo de teoría de Kummer (2.76) en el Anexo 1:

$$K^*/(K^*)^n \simeq \mathrm{Hom}(\mathrm{Gal}(K(\sqrt[n]{b})/K), \mu_n)$$

es el carácter $\chi_b : \mathrm{Gal}(K(\sqrt[n]{b})/K) \to \mu_n$ dado por $\chi_b(\tau) := \tau(\sqrt[n]{b})/\sqrt[n]{b}$.

Entonces, la definición del símbolo de Hilbert es

$$\left(\frac{a, b}{\mathfrak{p}_K}\right)_n = \chi_b(\sigma_a) = \frac{\sigma_a(\sqrt[n]{b})}{\sqrt[n]{b}} = \frac{(a, K(\sqrt[n]{b})/K)(\sqrt[n]{b})}{\sqrt[n]{b}}$$

Hemos así probado el teorema siguiente, que relaciona al símbolo de Hilbert con el símbolo de norma residual:

Teorema 2.51. *Sean K un campo local, $n \geq 1$ un entero coprimo con* car (K) *y $a, b \in K^*$. Entonces, el símbolo de Hilbert está dado explícitamente por la fórmula*

$$\left(\frac{a, b}{\mathfrak{p}_K}\right)_n = \frac{(a, K(\sqrt[n]{b})/K)(\sqrt[n]{b})}{\sqrt[n]{b}}$$

donde $(a, K(\sqrt[n]{b})/K) \in \mathrm{Gal}(K(\sqrt[n]{b})/K)$ es el símbolo de norma residual.

□

El teorema siguiente lista algunas propiedades básicas del símbolo de Hilbert:

Teorema 2.52. *Sean K un campo local y $n \geq 1$ un entero coprimo con* car (K). *Supongamos que $\mu_n \subseteq K$. El símbolo de Hilbert satisface:*

(1) *Es lineal en ambas variables:*

(i) $\left(\frac{a,bb'}{\mathfrak{p}_K}\right) = \left(\frac{a,b}{\mathfrak{p}_K}\right) \cdot \left(\frac{a,b'}{\mathfrak{p}_K}\right)$.

(ii) $\left(\frac{aa',b}{\mathfrak{p}_K}\right) = \left(\frac{a,b}{\mathfrak{p}_K}\right) \cdot \left(\frac{a',b}{\mathfrak{p}_K}\right)$.

(2) $\left(\frac{a,b}{\mathfrak{p}_K}\right) = 1$ *si y sólo si a es una norma de la extensión $K(\sqrt[n]{b})/K$.*

(3) $\left(\frac{a,-a}{\mathfrak{p}_K}\right) = 1 = \left(\frac{a,1-a}{\mathfrak{p}_K}\right)$.

(4) $\left(\frac{a,b}{\mathfrak{p}_K}\right) = \left(\frac{b,a}{\mathfrak{p}_K}\right)^{-1}$.

(5) *Si* $\left(\frac{a,b}{\mathfrak{p}_K}\right) = 1$ *para todo $b \in K^*$, entonces $a \in (K^*)^n$.*

DEMOSTRACIÓN. (1) es consecuencia de la bilinealidad del apareamiento que define al símbolo de Hilbert.

(2): Si a es una norma de $K(\sqrt[n]{b})/K$, entonces $(a, K(\sqrt[n]{b})/K) = 1$ y por (2.51)

$$\left(\frac{a, b}{\mathfrak{p}_K}\right) = \frac{(a, K(\sqrt[n]{b})/K)(\sqrt[n]{b})}{\sqrt[n]{b}} = \frac{1(\sqrt[n]{b})}{\sqrt[n]{b}} = 1.$$

Recíprocamente, si $\left(\frac{a,b}{\mathfrak{p}_K}\right) = 1$, entonces por (2.51) $(a, K(\sqrt[n]{b})/K)(\sqrt[n]{b}) = \sqrt[n]{b}$, i.e., $\sigma = (a, K(\sqrt[n]{b})/K)$ fija a $\sqrt[n]{b}$, y como $K(\sqrt[n]{b})$ está generado por K y $\sqrt[n]{b}$, entonces σ fija a todo $K(\sqrt[n]{b})$, i.e., $\sigma = id$, i.e., $(a, K(\sqrt[n]{b})/K) = 1$ y así, por la ley de reciprocidad, a es una norma de $K(\sqrt[n]{b})$.

(3): Si $L = K(\sqrt[n]{b})$, pongamos $b = \beta^n \in K$ y factorizando el polinomio $x^n - b$ en $L[x]$ se obtiene

$$x^n - b = x^n - \beta^n = \prod_{j=0}^{n-1}(x - \omega^j\beta),$$

donde $\omega \in \mu_n$ es una raíz primitiva de la unidad.

Observemos ahora que si $\beta^m = b \in K$ para algún $m \leq n$, entonces por (2.73) en el Anexo 1, $m|n$. Sea d el mayor divisor de n tal que $\beta^d = b \in K$ y pongamos $n = dt$; entonces $L = K(\beta)$ es cíclica de orden t sobre K y los K-conjugados de $x - \omega^i\beta$ son los elementos $x - \omega^j\beta$ tales que $j \equiv i$ mód (d). Se sigue que

$$x^n - b = \prod_{i=0}^{d-1} N_{K(\beta)/K}(x - \omega^i\beta) = N_{K(\beta)/K}\left(\prod_{i=0}^{d-1}(x - \omega^i\beta)\right)$$

y por lo tanto $x^n - b$ es una norma de $K(\beta)/K$. De (2) se sigue que

$$\left(\frac{x^n - b, b}{\mathfrak{p}_K}\right) = 1.$$

Poniendo $x = 0, b = -a$ y $x = 1, b = 1 - a$ en la igualdad anterior se obtiene (3).

(4): Probaremos que (3) $\Rightarrow$ (4). En efecto,

$$
\begin{aligned}
1 &- \left(\frac{ab, -ab}{\mathfrak{p}_K}\right) && \text{por (3)} \\
&- \left(\frac{a, -ab}{\mathfrak{p}_K}\right)\left(\frac{b, -ab}{\mathfrak{p}_K}\right) && \text{por (1)} \\
&\quad \left(\frac{a, -a}{\mathfrak{p}_K}\right)\left(\frac{a, b}{\mathfrak{p}_K}\right)\left(\frac{b, a}{\mathfrak{p}_K}\right)\left(\frac{b, -b}{\mathfrak{p}_K}\right) && \text{por (1)} \\
&- 1 \cdot \left(\frac{a, b}{\mathfrak{p}_K}\right)\left(\frac{b, a}{\mathfrak{p}_K}\right) \cdot 1 && \text{por (3)} \\
&- \left(\frac{a, b}{\mathfrak{p}_K}\right)\left(\frac{b, a}{\mathfrak{p}_K}\right)
\end{aligned}
$$

y esta última igualdad es (4).

(5): Esta propiedad nos dice que el apareamiento de Hilbert es no degenerado y esto se demuestra observando que si $\left(\frac{a,b}{\mathfrak{p}_K}\right) = 1$ para todo $b \in K^*$ entonces, por (2), $\left(\frac{b,a}{\mathfrak{p}_K}\right) = 1$ para todo $b \in K^*$ y así, por (2.51), $(b, K(\sqrt[n]{a})/K)(\sqrt[n]{a}) = \sqrt[n]{a}$ para todo $b \in K^*$, i.e., $(b, K(\sqrt[n]{a})/K)$ fija a $\sqrt[n]{a}$ para todo $b \in K^*$. Pero como la imagen de K^* es densa en $\mathrm{Gal}^{ab}(K_s/K)$, se sigue que $\mathrm{Gal}^{ab}(K_s/K)$ fija a $\sqrt[n]{a}$ y por lo tanto $\sqrt[n]{a} \in K^*$ y así, $a \in (K^*)^n$. □

Nótese que de las propiedades del símbolo de Hilbert se puede deducir de nuevo el teorema (2.43) para primos $p \neq \mathrm{car}\,(K)$, es decir, tenemos otra demostración del corolario (2.50):

Corolario 2.53. *Sean K un campo local y p un primo distinto de* $\mathrm{car}\,(K)$. *Sea L una extensión finita de K que contiene al grupo de raíces p-ésimas de la unidad. Si $\xi \in L^*$ y si ξ es una norma de toda extensión cíclica de L de grado p, entonces $\xi \in L^{*p}$.*

DEMOSTRACIÓN. Si ξ es una norma, entonces por la propiedad (2) $\left(\frac{a,\xi}{\mathfrak{p}_K}\right) = 1$ para toda a y así, por (4), $\left(\frac{\xi,a}{\mathfrak{p}_K}\right) = 1$ para toda a; de (5) se sigue que $\xi \in (K^*)^n$. □

Para terminar la demostración del teorema (2.43) sólo falta considerar el caso cuando el primo p es igual a la característica del campo K. Los métodos son similares, reemplazando teoría de Kummer con teoría de Artin-Schreier.

Teoría de Artin-Schreier. Trasladando los resultados de teoría de Artin-Schreier del Anexo 2 al contexto cuando K es un campo local de característica $p \neq 0$ y se tiene una extensión cíclica L/K de grado n divisible por p, comenzamos observando que *no* podemos proceder como en el caso de teoría de Kummer (2.50), ya que cuando car $(K) = p \neq 0$, el grupo $(K^*)^p$ *no* tiene índice finito en K^* porque, claramente, $(K^*)^p$ es *cerrado* en K^* pero *no es abierto*:

En efecto, recordemos primero que los campos locales K de característica $p \neq 0$ son de la forma

$$K = \mathbb{F}((t)),$$

i.e., son campos de series formales sobre un campo finito $\mathbb{F}$ de característica p. La identificación anterior se hace al elegir un parámetro uniformizador π de K y mandando este parámetro a t.

Para mostrar que $(K^*)^p$ no es abierto, consideremos la siguiente sucesión de elementos de K^*:

$$u_n := 1 + t^p + t^{p^2} + \cdots + t^{p^n} + t^{p^n+1}.$$

Claramente, $u_n \notin (K^*)^p$; sin embargo su límite

$$u := \lim_{n\to\infty} \{u_n\} = \sum_{j=0}^{\infty} t^{p^j}$$

es una potencia p-ésima, i.e., $u \in (K^*)^p$; por lo tanto el complemento de $(K^*)^p$ no es cerrado y así $(K^*)^p$ no es abierto y consecuentemente no tiene índice finito en K^*.

Ya que no podemos proceder como en (2.50), la idea es proceder como en (2.53), donde usamos las propiedades del símbolo de Hilbert (2.52) definido usando teoría de Kummer, sólo que ahora usaremos la teoría de Artin-Schreier del Anexo 2 para definir los símbolos correspondientes.

El símbolo de Artin-Schreier. Sea K un campo local de característica $p \neq 0$. Sean K_s una cerradura separable de K y $G_K := \mathrm{Gal}(K_s/K)$. El apareamiento

$$\text{(1)} \qquad \mathrm{Hom}(\mathrm{Gal}(K_s/K), \mathbb{Z}/p\mathbb{Z}) \times \mathrm{Gal}(K_s/K) \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

dado por $(\chi, \sigma) \mapsto \chi(\sigma)$, en vista del isomorfismo de la teoría de Artin-Schreier (Anexo 2, (2.82)):

$$\text{(2)} \qquad \mathrm{Hom}(\mathrm{Gal}(K_s/K), \mathbb{Z}/p\mathbb{Z}) \simeq K/\wp(K)$$

y del isomorfismo dado por la ley de reciprocidad

$$\mathrm{Gal}^{ab}(K_s/K) \simeq K^*/N_{L/K}(L^*) \tag{3}$$

se vuelve el apareamiento:

$$K/\wp(K) \times K^*/N_{L/K}(L^*) \longrightarrow \mathbb{Z}/p\mathbb{Z} \tag{4}$$

al cual se denota $[a, b\rangle_{\mathfrak{p}_K}$ y se llama el *símbolo de Artin-Schreier* o *símbolo de Hilbert semiaditivo*. Explícitamente este símbolo está definido como sigue: por teoría de Artin-Schreier (Anexo 2), un elemento $a \in K$ define un carácter

$$\chi_a : G_K \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

mediante $\chi_a(\sigma) := \sigma(\alpha) - \alpha$, donde α es una solución de $x^p - x - a = 0$. Y para un elemento $b \in K^*$, si denotamos su imagen, bajo el morfismo de reciprocidad, como $\sigma_b := (b, K_s/K)$, entonces la definición del símbolo de Artin-Schreier es

$$[a, b\rangle_{\mathfrak{p}_K} := \chi_a(\sigma_b) = \sigma_b(\alpha) - \alpha = (b, K_s/K)(\alpha) - \alpha,$$

para $a \in K$, $b \in K^*$ y α una solución de la ecuación $x^p - x - a = 0$. Hemos así probado el teorema siguiente, que relaciona el símbolo de Artin-Schreier con el símbolo de norma residual:

Teorema 2.54. *Sea K un campo local de característica $p \neq 0$. Sean $a \in K$ y $b \in K^*$. Entonces*

$$[a, b\rangle_{\mathfrak{p}_K} = (b, K_s/K)(\alpha) - \alpha,$$

donde $\alpha \in \wp^{-1}(a)$ es cualquier solución de la ecuación $x^p - x = a$.

□

Las propiedades básicas del símbolo de Artin-Schreier son:

Teorema 2.55. *Sea K un campo local de característica $p \neq 0$. El símbolo de Artin-Schreier satisface las propiedades siguientes:*

(1) *Es lineal en ambas variables:*

(i) $[a, bb'\rangle_{\mathfrak{p}_K} = [a, b\rangle_{\mathfrak{p}_K} + [a, b'\rangle_{\mathfrak{p}_K}$.
(ii) $[a + a', b\rangle_{\mathfrak{p}_K} = [a, b\rangle_{\mathfrak{p}_K} + [a', b\rangle_{\mathfrak{p}_K}$.

(2) $[a, b\rangle_{\mathfrak{p}_K} = 0$ *si y sólo si* b *es una norma de* $K(\alpha)/K$, *donde* $\wp(\alpha) = a$.

(3) $[a, a\rangle_{\mathfrak{p}_K} = 0$ *para todo* $a \in K^*$.

(4) *Si* $[a, b\rangle_{\mathfrak{p}_K} = 0$ *para todo* $b \in K^*$, *entonces* $a \in \wp(K)$.

DEMOSTRACIÓN. (1) es consecuencia de la bilinealidad del apareamiento (Anexo 2, (2.81)) que define al símbolo de Artin-Schreier.

(2): Si b es una norma de $K(\alpha)/K$, entonces el símbolo de norma residual $(a, K(\alpha)/K) = 1$ y por (2.54)

$$[a, b\rangle_{\mathfrak{p}_K} = (b, K(\alpha)/K)(\alpha) - \alpha = 1(\alpha) - \alpha = 0.$$

Recíprocamente, si $[a, b\rangle_{\mathfrak{p}_K} = 0$, entonces por (2.54) el símbolo de norma residual es $(b, K(\alpha)/K)(\alpha) = \alpha$, i.e., $\sigma := (b, K(\alpha)/K)$ fija a α y como $K(\alpha)$ es generado por α y K entonces σ fija a todo $K(\alpha)$, i.e., $\sigma = id$, i.e. $(b, K(\alpha)/K) = 1$ y así, por la ley de reciprocidad, b es una norma de $K(\alpha)$.

(3): Observemos primero que si $a \in \wp(K)$, i.e., si $a = \wp(\alpha)$ con $\alpha \in K$, entonces por (2.54)

$$[a, a\rangle_{\mathfrak{p}_K} = (a, K_s/K)(\alpha) - \alpha = \alpha - \alpha = 0$$

(la penúltima igualdad es porque $\alpha \in K$ y así queda fija bajo $(a, K_s/K) \in \mathrm{Gal}(K_s/K)$).

Supongamos ahora que $a \notin \wp(K)$. Entonces la extensión $K(\alpha)/K$ es cíclica de grado p y como los conjugados de α son los elementos $\alpha + j$ con $j \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, se sigue que

$$N_{K(\alpha)/K}(\alpha) = \prod_{j=0}^{p-1}(\alpha + j) = a,$$

i.e., a es una norma de $K(\alpha)/K$ y por lo tanto $[a, a\rangle_{\mathfrak{p}_K} = 0$ por la parte (2).

(4): Si $[a, b\rangle_{\mathfrak{p}_K} = 0$ para todo $b \in K^*$, entonces, para $\sigma_b := (b, K_s/K)$, por (2.54) se tiene que

$$0 = [a, b\rangle_{\mathfrak{p}_K} = \sigma_b(\alpha) - \alpha,$$

i.e., $\sigma_b(\alpha) = \alpha$ para todo $b \in K^*$ y como los σ_b son densos en G_K, entonces α queda fijo por todo G_K y por lo tanto $\alpha \in K$, y así, $a = \wp(\alpha) \in \wp(K)$. □

Para poder probar el caso restante del teorema (2.43), necesitamos calcular explícitamente el símbolo de Artin-Schreier. Este resultado es la *fórmula de*

Schmid (2.59), y para demostrarla recordamos primero los conceptos involucrados. Comenzamos recordando que los campos locales K de característica $p \neq 0$ son de la forma

$$K = \mathbb{F}((t)),$$

i.e., son campos de series formales sobre un campo finito $\mathbb{F}$ de característica p. El campo $K = \mathbb{F}((t))$ se puede ver como la completación de un campo valuado F, donde F es una extensión de grado de trascendencia 1 de $\mathbb{F}$, o lo que es lo mismo, F es el campo de funciones racionales de una curva algebraica (irreducible, lisa y completa) X definida sobre el campo finito $\mathbb{F}$. Ahora, si $\Omega^1(F)$ es el F-espacio vectorial de 1-formas diferenciales meromorfas de F (ver el Anexo 3), entonces $\Omega^1(F)$ tiene dimensión 1 sobre F y si t es un parámetro uniformizador, la diferencial dt de t es una base de $\Omega^1(F)$. Así, si $\omega \in \Omega^1(F)$ es una forma diferencial meromorfa, podemos escribir $\omega = fdt$ con $f \in F$.

Un invariante local importante de la forma diferencial meromorfa $\omega = fdt$ es su *residuo* que se define como sigue (ver el Anexo 3): usando que $K = \mathbb{F}((t))$, identifiquemos $f \in K$ con su imagen en $\mathbb{F}((t))$; entonces podemos escribir

$$f = \sum_{n \gg -\infty} a_n t^n$$

con $a_n \in \mathbb{F}$ y $n \gg -\infty$ quiere decir que $a_n = 0$ para casi todo $n < 0$. En particular, el coeficiente a_{-1} de t^{-1} en la expansión anterior de f está definido y a este coeficiente se le llama el *residuo* de $\omega = fdt$ y se denota

$$\mathrm{Res}(\omega) := a_{-1}.$$

Se prueba, véase (2.84) en el Anexo 3, que esta definición es independiente de la elección del parámetro local t.

Los dos lemas siguientes serán usados en la demostración de la fórmula de Schmid (2.59) para el símbolo de Artin-Schreier de un campo local de característica p. El primer lema es un caso particular de la fórmula de Schmid cuando la segunda variable es el parámetro local del campo K:

Lema 2.56. *Sea $K = \mathbb{F}_q((t))$ un campo local de característica $p \neq 0$ con parámetro local t y campo residual $\mathbb{F}_q$, $q = p^n$. Si $a \in K$ y t es el parámetro local, entonces*

$$[a, t\rangle_{\mathfrak{p}_K} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \mathrm{Res}_t \left(a \frac{dt}{t} \right),$$

donde $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ es la traza de la extensión $\mathbb{F}_q/\mathbb{F}_p$.

DEMOSTRACIÓN. Probaremos primero que

$$[a, t\rangle_{\mathfrak{p}_K} = [c, t\rangle_{\mathfrak{p}_K}$$

para $c = \mathrm{Res}(a \cdot \frac{dt}{t})$.

Escribamos al elemento a como una serie de potencias en t:

$$(\dagger) \qquad a = \sum_n a_n t^n = \sum_{n<0} a_n t^n + a_0 + \sum_{n>0} a_n t^n.$$

Por la aditividad en a de las funciones $[a, t\rangle_{\mathfrak{p}_K}$ y $[\mathrm{Res}(a\frac{dt}{t}), t\rangle_{\mathfrak{p}_K}$, se sigue que podemos considerar por separado a cada sumando de a en (†).

(i): El sumando de enmedio a_0 (constante) es tal que

$$\mathrm{Res}(a_0 \frac{dt}{t}) = a_0$$

y la fórmula a probar es la tautología $[a_0, t\rangle_{\mathfrak{p}_K} = [a_0, t\rangle_{\mathfrak{p}_K}$.

(ii): Para el sumando $\tilde{a} := \sum_{n>0} a_n t^n$ se tiene que $\mathrm{Res}\left(\tilde{a}\frac{dt}{t}\right) = 0$, y debemos entonces probar que $[\tilde{a}, t\rangle_{\mathfrak{p}_K} = 0$. Para esto observemos que $\tilde{a} \in \wp(K)$, porque si ponemos $\alpha := \sum_{j=0}^{\infty} \tilde{a}^{p^j} \in K$ entonces $\wp(\alpha) = \alpha^p - \alpha = -\tilde{a}$, ya que al considerar α^p se recorren los sumandos de α un lugar y al restar $\alpha^p - \alpha$ sólo sobrevive el sumando $-\tilde{a}$; se sigue que $\tilde{a} \in \wp(K)$ y así, por (2.54),

$$[\tilde{a}, t\rangle_{\mathfrak{p}_K} = (t, K_s/K)(\alpha) - \alpha = \alpha - \alpha = 0,$$

la penúltima igualdad porque $\alpha \in K$ y así queda fija bajo $(t, K_s/K)$, que es lo que queríamos probar.

(iii): Para el sumando $\tilde{a} := \sum_{n<0} a_n t^n$, como $\tilde{a}$ es *meromorfa* en la suma sólo hay un número finito de sumandos y por la aditividad en la variable a podemos suponer, sin perder generalidad, que sólo hay un sumando, i.e., que $\tilde{a} = ut^{-n}$ con $u \in \mathbb{F}$ y $n > 0$. Se sigue que

$$\mathrm{Res}(\tilde{a}\frac{dt}{t}) = \mathrm{Res}(ut^{-n}\frac{dt}{t}) = \mathrm{Res}(ut^{-n-1}dt) = 0$$

ya que $-n - 1 < -1$, y debemos probar entonces que $[\tilde{a}, t\rangle_{\mathfrak{p}_K}$ 0. Argumentamos por inducción sobre n.

Primero observamos que, por la linealidad (2.55) del símbolo de Artin-Schreier en la segunda variable,

$$[ut^{-n}, t^{-n}\rangle_{\mathfrak{p}_K} = -n[ut^{-n}, t\rangle_{\mathfrak{p}_K} = -n[\widetilde{a}, t\rangle_{\mathfrak{p}_K}$$

y por (2.55)(3) se tiene que

$$0 = [ut^{-n}, ut^{-n}\rangle_{\mathfrak{p}_K} = [ut^{-n}, u\rangle_{\mathfrak{p}_K} + [ut^{-n}, t^{-n}\rangle_{\mathfrak{p}_K} = [ut^{-n}, u\rangle_{\mathfrak{p}_K} - n[\widetilde{a}, t\rangle_{\mathfrak{p}_K};$$

se sigue que

$$0 = [ut^{-n}, u\rangle_{\mathfrak{p}_K} - n[\widetilde{a}, t\rangle_{\mathfrak{p}_K}.$$

Y como $\mathbb{F}$ es finito, y por lo tanto perfecto, entonces $u = \theta^p \in \mathbb{F}$ para algún $\theta \in \mathbb{F}$, de tal forma que

$$[ut^{-n}, u\rangle_{\mathfrak{p}_K} = [\widetilde{a}, u\rangle_{\mathfrak{p}_K} = [\widetilde{a}, \theta^p\rangle_{\mathfrak{p}_K} = p[\widetilde{a}, \theta\rangle_{\mathfrak{p}_K} = 0$$

y por lo tanto en (∗) se tiene que

$$-n[\widetilde{a}, t\rangle_{\mathfrak{p}_K} = 0.$$

Se tienen entonces dos casos:

CASO 1: Si n es *coprimo* con p, entonces la igualdad anterior implica que $[\widetilde{a}, t\rangle_{\mathfrak{p}_K} = 0$, que es lo que queríamos probar.

CASO 2: Si $p|n$, digamos $n = pm$, como antes pongamos $u = \theta^p$. Entonces

$$\widetilde{a} = ut^{-n} = \theta^p t^{-pm} = (\theta t^{-m})^p = \wp(\theta t^{-m}) + \theta t^{-m}$$

y así

$$\begin{aligned} [\widetilde{a}, t\rangle_{\mathfrak{p}_K} &- [\wp(\theta t^{-m}) + \theta t^{-m}, t\rangle_{\mathfrak{p}_K} \\ &- [\wp(\theta t^{-m}), t\rangle_{\mathfrak{p}_K} + [\theta t^{-m}, t\rangle_{\mathfrak{p}_K} \\ &- [\theta t^{-m}, t\rangle_{\mathfrak{p}_K}, \end{aligned}$$

ya que por (2.55),

$$[\wp(\theta t^{-m}), t\rangle_{\mathfrak{p}_K} = (t, K_s/K)(\theta t^{-m}) - \theta t^{-m} = \theta t^{-m} - \theta t^{-m} = 0$$

porque $\theta t^{-m} \in K$.

Si $p \nmid m$, ya terminamos por el caso 1. Si $p|m$, repetimos el proceso. El resultado $[\theta t^{-m}, t\rangle_{\mathfrak{p}_K} = 0$ se sigue por inducción ya que $m < n$.

Finalmente, probamos la fórmula del lema: para esto, consideremos la extensión finita $\mathbb{F}' = \mathbb{F}_q(\alpha)$ donde $\wp(\alpha) = c$ y pongamos $K' = \mathbb{F}'((t))$.

Entonces la extensión K'/K es no ramificada y, por el cálculo del símbolo de norma residual para extensiones no ramificadas (2.32), se tiene que

$$(t, K'/K) = \mathrm{Fr}^{v_K(t)} = \mathrm{Fr},$$

donde Fr es el Frobenius de $\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(\mathbb{F}'/\mathbb{F}_q)$ y donde usamos el hecho de que $v_K(t) = 1$ porque es un parámetro local. Por el teorema (2.54) se tiene entonces que

$$\begin{aligned}
[c, t\rangle_{\mathfrak{p}_K} &= (t, K'/K)(\alpha) - \alpha = \mathrm{Fr}(\alpha) - \alpha \\
&\quad \alpha^q - \alpha = \alpha^{p^f} - \alpha, \qquad \text{donde } q = p^f = |\mathbb{F}_q| \\
&- (\alpha^{p^f} - \alpha^{p^{f-1}}) + (\alpha^{p^{f-1}} - \alpha^{p^{f-2}}) + \cdots + (\alpha^p - \alpha) \\
&\quad (\alpha^p - \alpha)^{p^{f-1}} + (\alpha^p - \alpha)^{p^{f-2}} + \cdots + (\alpha^p - \alpha) \\
&= c^{p^{f-1}} + c^{p^{f-2}} + \cdots + c \\
&- \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c).
\end{aligned}$$

□

Para el segundo lema necesitamos antes un resultado que es el análogo multiplicativo de la expansión en serie de un elemento $\alpha \in K$:

Proposición 2.57 (Hensel). *Sean K un campo discreto completo, $\mathcal{O}_K$ su anillo de enteros, $\mathcal{R} \subseteq \mathcal{O}_K$ un conjunto completo de representantes del campo residual K de K tal que $0 \in \mathcal{R}$, y π un parámetro local de K. Entonces, para cada $\alpha \in K^*$ existen $n \in \mathbb{Z}$, $\theta_i \in \mathcal{R}$, $i \geq 0$, unívocamente determinados, tales que α tiene la expansión siguiente, como un producto convergente:*

$$\alpha = \pi^n \theta_0 \prod_{i \geq 1} (1 + \theta_i \pi^i).$$

Demostración. Descompongamos $\alpha \in K^*$ como $\alpha = \pi^n u_0$, con $n = v_K(\alpha)$ y $u_0 \in U_K$. Usando el isomorfismo (1.65)(1) $U_K/U_K^{(1)} \simeq \overline{K}^*$ (dado por $u \mapsto \overline{u}$), podemos escribir $u_0 \in U_K$ como $u_0 = \theta_0 u_1$ con $\theta_0 \in \mathcal{R}$ y $u_1 \in U_K^{(1)}$, y así $\alpha = \pi^n \theta_0 u_1$.

Ahora, usando el isomorfismo (1.65)(2) $U_K^{(1)}/U_K^{(2)} \simeq K$ (dado por $1+\varepsilon\pi \mapsto \overline{\varepsilon}$), si escribimos $u_1 = 1 + \varepsilon\pi \in U_K^{(1)}$, su imagen bajo el isomorfismo anterior es $\overline{\varepsilon}$ y escogiendo un representante $\theta_1 \in \mathcal{R}$ de $\overline{\varepsilon}$, al considerar el elemento $1 + \theta_1\pi \in U_K^{(1)}$ notamos que al reducir este elemento y a $u_1 = 1 + \varepsilon\pi$ estas reducciones son iguales en K, i.e., $\overline{\varepsilon} = \theta_1 \in K$, y por lo tanto

$u_1(1+\theta_1\pi)^{-1} \in U_K^{(2)}$ y así $u_1 = (1+\theta_1\pi)u_2$ con $u_2 \in U_K^{(2)}$. Se sigue que

$$\alpha = \pi^n\theta_0(1+\theta_1\pi)u_2 \qquad \text{con} \quad u_2 \in U_K^{(2)}.$$

Por inducción, supongamos que ya se probó que

$$\alpha = \pi^n\theta_0(1+\theta_1\pi)\cdots(1+\theta_i\pi^i)u_{i+1} \qquad \text{con} \quad u_{i+1} \in U_K^{(i+1)}$$

Entonces, usando el isomorfismo $U_K^{(i+1)}/U_K^{(i+2)} \simeq K$, si escribimos $u_{i+1} = 1 + \varepsilon\pi^{i+1}$ su imagen bajo este isomorfismo es $\overline{\varepsilon}$ y por lo tanto existe un $\theta_{i+1} \in \mathcal{R}$ tal que $\overline{\varepsilon} = \theta_{i+1} \in K$ y así el elemento $1+\theta_{i+1}\pi^{i+1} \in U_K^{(i+1)}$ es tal que $u_{i+1}(1+\theta_{i+1}\pi^{i+1})^{-1} \in U_K^{(i+2)}$, i.e., $u_{i+1} = (1+\theta_{i+1}\pi^{i+1})u_{i+2}$ con $u_{i+2} \in U_K^{(i+2)}$ y por lo tanto

$$\alpha = \pi^n\theta_0(1+\theta_1\pi)\cdots(1+\theta_i\pi^i)(1+\theta_{i+1}\pi^{i+1})u_{i+2}$$

con $u_{i+2} \in U_K^{(i+2)}$.

Para la unicidad de la descomposición, observamos que n y θ_0 están claramente unívocamente determinados y para los otros factores, si sucediera que

$$\prod(1+\theta_i\pi^i) = \prod(1+\theta'_i\pi^i),$$

entonces en K se tendría que $\overline{\theta}_i = \theta'_i$ y por lo tanto $\theta_i = \theta'_i$ en $\mathcal{R}$. □

El segundo lema que necesitaremos para la fórmula de Schmid nos dice que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t$ se comporta como el símbolo de Artin-Schreier para las normas:

Lema 2.58. *Sea $K = \mathbb{F}_q((t))$ un campo local de característica $p > 0$ con parámetro local t y campo residual $\mathbb{F}_q$, $q = p^f$. Si $a \in K$ y $b \in K^*$ es una norma de la extensión cíclica $L := K(u)$, donde u es una solución de la ecuación de Artin-Schreier $u^p - u = a$, entonces,*

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(a\frac{db}{b}\right) = 0,$$

donde $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ es la traza de la extensión $\mathbb{F}_q/\mathbb{F}_p$.

DEMOSTRACIÓN. Como $b = N_{L/K}(z) = \prod_j \sigma_j(z)$, con $z \neq 0$ en L y σ_j en $\mathrm{Gal}(L/K)$, entonces

$$\frac{db}{b} = \frac{d(Nz)}{Nz} = \sum_j \frac{d\sigma_j(z)}{\sigma_j(z)} = \sum_j \sigma_j\left(\frac{dz}{z}\right) = \mathrm{Tr}_{L/K}\left(\frac{dz}{z}\right)$$

y por lo tanto

$$\mathrm{Res}_t\left(a\frac{db}{b}\right) = \mathrm{Res}_t\left(a\cdot \mathrm{Tr}_{L/K}\frac{dz}{z}\right) = \mathrm{Res}_t\mathrm{Tr}_{L/K}\left(a\frac{dz}{z}\right) = \mathrm{Res}_\pi\left(a\frac{dz}{z}\right)$$

donde $\pi \in L$ es el primo de L arriba del primo $t \in K$ y la última igualdad es por (2.85) en el Anexo 3.

Esto reduce lo que queremos probar a

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\left(a\frac{dz}{z}\right) = 0,$$

y si recordamos que $a = u^p - u$, entonces lo que debemos probar es que

$$(*) \qquad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\left(u^p\frac{dz}{z}\right) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\left(u\frac{dz}{z}\right).$$

Para probar esta última igualdad, escribamo u como una serie

$$u = \sum c_j\pi^j$$

y a $z \neq 0$ en forma de producto usando (2.57)

$$z = \pi^m\theta_0\prod_{i\geq 1}(1+\theta_i\pi^i).$$

Como estamos en característica p, se tiene entonces que

$$u^p = \sum c_j^p\pi^{jp}$$

y la derivada logarítmica de z es

$$\frac{dz}{z} = m\frac{d\pi}{\pi} + \sum_i \frac{i\theta_i\pi^{i-1}d\pi}{1+\theta_i\pi^i} = m\frac{d\pi}{\pi} + \sum_i \frac{i\theta_i\pi^i}{1+\theta_i\pi^i}\frac{d\pi}{\pi}.$$

Se sigue que

$$u^p\frac{dz}{z} = \left(\sum_j c_j^p\pi^{jp}\right)\left(m\frac{d\pi}{\pi} + \sum_i \frac{i\theta_i\pi^i}{1+\theta_i\pi^i}\frac{d\pi}{\pi}\right)$$

y

$$u\frac{dz}{z} = \left(\sum_j c_j\pi^j\right)\left(m\frac{d\pi}{\pi} + \sum_i \frac{i\theta_i\pi^i}{1+\theta_i\pi^i}\frac{d\pi}{\pi}\right)$$

de tal forma que para probar $(*)$ debemos probar las dos igualdades siguientes:

$$(1) \qquad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\left(c_j^p \pi^{jp}\frac{d\pi}{\pi}\right) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\left(c_j \pi^j \frac{d\pi}{\pi}\right)$$

y

(2)

$$i \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\begin{pmatrix} c_j^p \pi^{jp} & \theta_i \pi^i & d\pi \\ & 1+\theta_i\pi^i & \pi \end{pmatrix} = i \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\begin{pmatrix} c_j \pi^j & \theta_i \pi^i & d\pi \\ & 1+\theta_i\pi^i & \pi \end{pmatrix}$$

para $i \geq 1$.

Para probar las igualdades (1) y (2) usaremos el hecho siguiente: *si α es un elemento del campo residual $\mathbb{F}$ de L, entonces*

$$(\dagger) \qquad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}(\alpha^p) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}(\alpha),$$

y esto último se prueba como sigue (aquí $f = [\mathbb{F}_q : \mathbb{F}_p]$ y $m = [\mathbb{F} : \mathbb{F}_q]$):

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}(\alpha^p) &= \alpha^p + \alpha^{p^2} + \cdots + (\alpha^p)^{p^{fm-1}} \\ &= \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{fm}} \\ &= \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{fm-1}} + \alpha^{p^{fm}} - \alpha \\ &= \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}(\alpha) + \alpha^{p^{fm}} - \alpha \\ &= \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}(\alpha), \end{aligned}$$

ya que $\alpha^{p^{fm}} = \alpha$.

Ahora, en la fórmula (1) para $j \geq 1$ el residuo es 0 en ambos lados de la igualdad, y así no hay nada que probar. Lo mismo sucede si $j \leq -1$. En el caso $j = 0$ restante, la igualdad (1) se reduce a probar que

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\left(c_0^p \frac{d\pi}{\pi}\right) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_\pi\left(c_0 \frac{d\pi}{\pi}\right)$$

y los residuos en ambos lados de esta última igualdad son c_0^p y c_0 respectivamente, de tal forma que lo que debemos probar es que

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c_0^p) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c_0)$$

lo cual es precisamente lo que probamos en (†).

Finalmente, para la fórmula (2) notemos que esta igualdad es cierta para $i \equiv 0 \pmod{p}$ ya que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ y así ambos lados de (2) son 0.

Supongamos entonces que $\mathrm{mcd}(i, p) = 1$. Observamos que para $i + j \geq 1$ los residuos en ambos lados de (2) son 0; ahora, si $i \nmid j$ entonces $j = ir + s$ y así

$$c_j \pi^j \begin{matrix} \theta_i \pi^i & d\pi \\ 1 + \theta_i \pi^i & \pi \end{matrix} = c_j \pi^{ir} \begin{matrix} \theta_i \pi^i \\ 1 + \theta_i \pi^i \end{matrix} \pi^{s-1} d\pi,$$

y por lo tanto el cálculo de los residuos en (2) se reduce al caso cuando $i + j \leq 0$ e $i | j$. Ahora, escribiendo

$$\frac{\theta_i \pi^i}{1 + \theta_i \pi^i} = \sum_{k=1}^{\infty} \theta_i^k \pi^{ki}$$

y $j = ir$, los residuos en (2) se calculan como sigue:

$$c_j \pi^j \begin{matrix} \theta_i \pi^i & d\pi \\ 1 + \theta_i \pi^i & \pi \end{matrix} = c_j \pi^{ir} \sum_{k=1}^{\infty} \theta_i^k \pi^{ik} \frac{d\pi}{\pi}$$

donde el coeficiente de π^{-1} se obtiene poniendo $ir = -ik$, i.e., $k = -r = -j/i$ y así el residuo del lado derecho de (2) es

$$c_j \theta_i^{-r} = c_j \theta_i^{-j/i};$$

similarmente para el lado izquierdo de (2). Por lo tanto, la igualdad (2) se reduce a

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \left(c_j \theta_i^{-j/i} \right)^p = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \left(c_j \theta_i^{-j/i} \right),$$

la cual es precisamente (†). Esto completa la demostración del segundo lema. □

El resultado principal es:

Teorema 2.59 (H. L. Schmid). *Sea K un campo local de característica $p \neq 0$, i.e., $K = \mathbb{F}_q((t))$ es un campo de series formales sobre un campo finito $\mathbb{F}_q$, con $q = p^n$. Sean $a \in K$ y $b \in K^*$; entonces*

$$[a, b\rangle_{\mathfrak{p}_K} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \left(\mathrm{Res} \left(a \frac{db}{b} \right) \right).$$

DEMOSTRACIÓN. Escribamos $b \in K^*$ de la forma $b = b_0 t^r$ con $b_0 \in U_K$ una unidad de K^* y $r = v_K(b)$; entonces, por la bilinealidad del símbolo de

Artin-Schreier, se tiene que

$$\begin{aligned}
\langle a, b\rangle_{\mathfrak{p}_K} &= \langle a, b_0 t^r\rangle_{\mathfrak{p}_K} = \langle a, b_0\rangle_{\mathfrak{p}_K} + r\langle a, t\rangle_{\mathfrak{p}_K} \\
&\quad 0 + r\langle a, t\rangle_{\mathfrak{p}_K} \text{ ya que } b_0 \in U_K \text{ es una norma y usamos (2.55)(2).} \\
&- r\langle a, t\rangle_{\mathfrak{p}_K} \\
&- r\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(a\frac{dt}{t}\right) \quad \text{por el lema (2.56)} \\
&- \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(ra\frac{dt}{t}\right).
\end{aligned}$$

Ahora, para $b = b_0 t^r$ se tiene que

$$\frac{db}{b} = \frac{db_0}{b_0} + r\frac{dt}{t}$$

y multiplicando por a se tiene que

$$a\frac{db}{b} - a\frac{db_0}{b_0} = ar\frac{dt}{t},$$

y así, substituyendo en la igualdad previa, se tiene que

$$\begin{aligned}
\langle a, b\rangle_{\mathfrak{p}_K} &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(ra\frac{dt}{t}\right) \\
&- \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(a\frac{db}{b}\right) - \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(a\frac{db_0}{b_0}\right) \\
&= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(a\frac{db}{b}\right),
\end{aligned}$$

ya que b_0 es una unidad y por lo tanto una norma de $K(\wp^{-1}(a))$, y así, por el lema (2.58), se tiene que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{Res}_t\left(a\frac{db_0}{b_0}\right) = 0$. □

Podemos ahora probar el caso que faltaba del teorema (2.43):

Corolario 2.60. *Sea $K = \mathbb{F}((t))$ un campo de característica $p \neq 0$. Si $b \in K^*$ es una norma de toda extensión cíclica de K de grado p, entonces $b \in (K^*)^p$.*

DEMOSTRACIÓN. Como las extensiones cíclicas de grado p de K son de la forma $K(\alpha)$, donde $\wp(\alpha) = a \in K$ por (2.79) en el Anexo 2, entonces por (2.55)(2) se tiene que $\langle a, b\rangle_{\mathfrak{p}_K} = 0$ para toda $a \in K$. Ahora, si b no estuviera en $(K^*)^p$ entonces la diferencial db/b *no* se anularía, ya que $db = 0$ si y sólo si el desarrollo en serie de b es de la forma $\sum a_j t^{pm_j}$.

Entonces, para cada $c \in \mathbb{F}$ podríamos encontrar algún elemento $a \in K$ tal que $\mathrm{Res}(a\frac{db}{b}) = c$. Pero por la fórmula de Schmid,

$$\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}(c) = \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}\left(\mathrm{Res}\left(a\frac{db}{b}\right)\right) = [a, b\rangle_{\mathfrak{p}_K} = 0,$$

lo cual contradice el hecho de que la traza

$$\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p} \cdot \mathbb{F} \to \mathbb{F}_p$$

es suprayectiva (1.97). □

La fórmula de Schmid (2.59) es un ejemplo de un cálculo explícito del símbolo de Hilbert de un campo local K. En general se desea tener una fórmula explícita para el símbolo de Hilbert. Éste es un problema todavía abierto en general, y a continuación recordamos una de las situaciones donde se tiene una tal fórmula en un caso relativamente sencillo, relacionado, para extensiones de grado 2, con la ley de reciprocidad cuadrática:

Una fórmula explícita para el símbolo de Hilbert en el caso manso. Sea K un campo local con campo residual K tal que $\mu_n \subseteq K$. El problema de encontrar fórmulas explícitas para el símbolo de Hilbert $(\frac{a,b}{\mathfrak{p}_K})$ en términos de los elementos a, b de K en general es muy difícil, sin embargo existe una fórmula sencilla en el caso cuando $p \nmid n$, donde $p = \mathrm{car}\,(K)$. En este caso recordemos que las extensiones de Kummer $K(a^{1/n})/K$ son *mansamente ramificadas*, i.e., no involucran ramificación superior (véase (1.79) y el ejemplo 16 antes de (1.57)).

Observemos, para comenzar, que si $p = \mathrm{car}\,(K)$ entonces $\mathrm{car}\,(K) = 0$ ó $\mathrm{car}\,(K) = p$, y se tiene el siguiente resultado:

Lema 2.61. *Sea K un campo local con campo residual K de característica p. Sea $n \geq 1$ un entero tal que $p \nmid n$. Entonces, K contiene al grupo de raíces n-ésimas de la unidad μ_n si y sólo si K contiene una copia μ_n de este grupo de raíces n-ésimas de la unidad. De hecho, el morfismo canónico $\lambda : U_K \to K^*$ induce un isomorfismo de $\mu_n \subseteq U_K$ en $\mu_n \subseteq \overline{K}^*$. Nótese entonces que $n|q-1$, donde $q = |K|$ y además se tiene un isomorfismo*

$$K^*/K^{*n} \longrightarrow \mu_n$$

dado por el paso al cociente de $x \mapsto x^{(q-1)/n}$.

DEMOSTRACIÓN. Supongamos que K contiene a μ_n. Entonces, los representantes multiplicativos (1.17) de μ_n forman un subgrupo μ_n de U_K que bajo el morfismo λ es isomorfo a μ_n. Se sigue que K contiene a μ_n.

Recíprocamente, si K contiene a μ_n, los elementos de μ_n son representantes multiplicativos, por (1.16)(2), y su imagen $\mu_n \subseteq K^*$ bajo λ es isomorfa a μ_n, de tal forma que K contiene a μ_n. □

El teorema siguiente calcula explícitamente el símbolo de Hilbert en el caso manso:

Teorema 2.62. *Sean K un campo local, K su campo residual y $p = \text{car}(K)$. Supongamos que $p \nmid n$ y que $\mu_n \subseteq K$. Sean $a, b \in K^*$; entonces*

$$\left(\frac{a, b}{\mathfrak{p}_K}\right) = c(a, b)^{(q-1)/n},$$

donde $q = |K|$ y $c : K^* \times K^* \to \mu_{q-1}$ es el símbolo manso definido por

$$c(a, b) := \text{pr}\left((-1)^{v_K(a)v_K(b)}\frac{b^{v_K(a)}}{a^{v_K(b)}}\right),$$

donde pr $: U_K \to \mu_{q-1}$ *es la proyección sobre el primer factor de la descomposición $U_K \simeq \mu_{q-1} \times U_K^{(1)}$ de* (1.66).

DEMOSTRACIÓN. Para comenzar, obviamente

$$(-1)^{v_K(a)v_K(b)}\left(\frac{b^{v_K(a)}}{a^{v_K(b)}}\right)$$

es una unidad de K y la función $\langle a, b\rangle := c(a, b)^{(q-1)/n}$ es bilineal (en el sentido multiplicativo); y como también el símbolo de Hilbert $\left(\frac{a,b}{\mathfrak{p}_K}\right)$ es bilineal, entonces podemos suponer que a y b son elementos primos, digamos $a = \pi$, $b = -\pi u$, con u una unidad de K.

Ahora, como

$$\langle \pi, -\pi\rangle = 1 = \left(\frac{\pi, -\pi}{\mathfrak{p}_K}\right)$$

entonces

$$\langle \pi, -\pi u\rangle = \langle \pi, -\pi\rangle\langle \pi, u\rangle = \langle \pi, u\rangle$$

y también

$$\left(\frac{\pi, -\pi u}{\mathfrak{p}_K}\right) = \left(\frac{\pi, -\pi}{\mathfrak{p}_K}\right)\left(\frac{\pi, u}{\mathfrak{p}_K}\right) = \left(\frac{\pi, u}{\mathfrak{p}_K}\right),$$

lo cual nos reduce al caso cuando $a = \pi$ y $b = u \in U_K$. Pongamos entonces $z = \sqrt[n]{u}$ y $K' = K(z)$. Entonces, considerando la reducción $\bar{u} \in \bar{K}$, sea $\alpha = \sqrt[n]{\bar{u}}$ y la extensión $\bar{K}' = \bar{K}(\alpha)$ de $\bar{K}$, la cual es cíclica de grado n; ahora, como el polinomio $x^n - \bar{u}$ tiene la raíz simple $x = \alpha$ en $\bar{K}'$, entonces (por el lema de Hensel) el polinomio $x^n - u$ tiene una raíz $x = v$ en K que se proyecta a α.

Sea K'/K la extensión no ramificada correspondiente a $\bar{K}'/\bar{K}$; entonces $K' = K(v) = K(\sqrt[n]{u})$.

Ahora, por (2.32), como K'/K es no ramificada, el símbolo $(\pi, K'/K)$ es el Frobenius Fr_K de K'/K. Se sigue que

$$\left(\frac{\pi, u}{\mathfrak{p}_K}\right) = \frac{(\pi, K'/K)(v)}{v} = \frac{\mathrm{Fr}_K(v)}{v} = \frac{v^q}{v} = v^{q-1};$$

y, por otra parte,

$$\begin{aligned}\langle \pi, u\rangle &= c(\pi, u)^{(q-1)/n} = \mathrm{pr}\left((-1)^{v_K(\pi)v_K(u)}\frac{u^{v_K(\pi)}}{\pi^{v_K(u)}}\right)^{(q-1)/n} \\ &- \mathrm{pr}\left((-1)^0\frac{u^1}{\pi^0}\right)^{(q-1)/n} = \mathrm{pr}(u)^{(q-1)/n}\end{aligned}$$

y por lo tanto

$$\left(\frac{\pi, u}{\mathfrak{p}_K}\right) = v^{q-1} = (u^{1/n})^{q-1} = u^{(q-1)/n} \equiv \mathrm{pr}(u)^{(q-1)/n} = \langle \pi, u\rangle \mod (\mathfrak{p}_K),$$

i.e.,

$$\left(\frac{\pi, u}{\mathfrak{p}_K}\right) \equiv \langle \pi, u\rangle \mod (\mathfrak{p}_K),$$

y ambos son elementos de μ_{q-1} (para $\langle \pi, u\rangle$ por definición y para $\left(\frac{\pi,u}{\mathfrak{p}_K}\right)$ por el hecho de que $\left(\frac{\pi,u}{\mathfrak{p}_K}\right) \in \mu_n \subseteq \mu_{q-1}$), y como μ_{q-1} es isomorfo a $\bar{K}^*$ bajo el morfismo $U_K \to \bar{K}^*$ que manda $u \mapsto \bar{u}$ mód $\mathfrak{p}_K$ (cuyo núcleo es $U_K^{(1)}$), se sigue

que

$$\left(\frac{\pi, u}{\mathfrak{p}_K}\right) = \langle \pi, u \rangle,$$

como se quería. □

Corolario 2.63. *Sean K un campo local, K su campo residual, $p = \operatorname{car}(K)$ y π un uniformizador de K. Supongamos que $p \nmid n$ y $\mu_n \subseteq K$. Si $u \in U_K$, entonces el símbolo*

$$\left(\frac{\pi, u}{\mathfrak{p}_K}\right) = \operatorname{pr}(u)^{(q-1)/n}$$

es independiente de la elección del elemento primo π de K.

□

Tiene sentido entonces poner, para $u \in U_K$,

$$\left(\frac{u}{\mathfrak{p}_K}\right) := \left(\frac{\pi, u}{\mathfrak{p}_K}\right)$$

de tal forma que, por lo probado anteriormente, $\left(\frac{u}{\mathfrak{p}_K}\right)$ es una raíz n-ésima de la unidad determinada por la congruencia

$$\left(\frac{u}{\mathfrak{p}_K}\right) \equiv u^{(q-1)/n} \text{ mód } \mathfrak{p}_K.$$

A $\left(\frac{u}{\mathfrak{p}_K}\right)$ se le llama el *símbolo de Legendre* o *símbolo residual n-ico*. Ambos nombres los justifica la proposición siguiente:

Proposición 2.64. *Con la notación e hipótesis del corolario anterior, si $p \nmid n$ y $u \in U_K$, entonces*

$$\left(\frac{u}{\mathfrak{p}_K}\right) = 1 \quad \Leftrightarrow u \text{ es una } n\text{-potencia mód } \mathfrak{p}_K.$$

DEMOSTRACIÓN. Sea $\zeta \in U_K = \mu_{q-1} \times U_K^{(1)}$ una raíz primitiva $(q-1)$-ésima de la unidad y pongamos $m = (q-1)/n$. Entonces, ζ^n es una raíz primitiva

m-ésima de la unidad y se tiene que

$$\left(\frac{u}{\mathfrak{p}_K}\right) = \mathrm{pr}(u)^m = 1 \quad \Leftrightarrow \quad \mathrm{pr}(u) \in \mu_m$$

$$\Leftrightarrow \quad \mathrm{pr}(u) = (\zeta^n)^i \quad \text{ya que } \zeta^n \text{ es generador de } \mu_m$$

$$\Leftrightarrow \quad u \equiv \mathrm{pr}(u) \equiv (\zeta^i)^n \text{ mód } \mathfrak{p}_K.$$

□

Para extensiones cuadráticas del campo de números p-ádicos $K = \mathbb{Q}_p$, tenemos:

Corolario 2.65. *Sean $n = 2$ y $p > 2$ un primo racional. Si $a, b \in \mathbb{Q}_p^*$, pongamos $a = p^\alpha a'$ y $b = p^\beta b'$ con $a', b' \in U_{\mathbb{Q}_p}$. Entonces,*

$$\left(\frac{a, b}{p}\right) = (-1)^{\frac{p-1}{2}\alpha\beta} \left(\frac{a'}{p}\right)^\beta \left(\frac{b'}{p}\right)^\alpha.$$

DEMOSTRACIÓN. Por la multiplicatividad del símbolo de Hilbert:

$$\begin{aligned}
\left(\frac{a, b}{p}\right) &= \left(\frac{a'p^\alpha, b'p^\beta}{p}\right) \\
&= \left(\frac{a', b'}{p}\right)\left(\frac{a', p^\beta}{p}\right)\left(\frac{p^\alpha, b'}{p}\right)\left(\frac{p^\alpha, p^\beta}{p}\right) \\
&= \left(\frac{a', b'}{p}\right)\left(\frac{a', p}{p}\right)^\beta \left(\frac{p, b'}{p}\right)^\alpha \left(\frac{p, p}{p}\right)^{\alpha\beta} \\
&= \left(\frac{p, a'}{p}\right)^\beta \left(\frac{p, b'}{p}\right)^\alpha (-1)^{\frac{p-1}{2}\alpha\beta}
\end{aligned}$$

ya que $\left(\frac{a', p}{p}\right) = \left(\frac{p, a'}{p}\right)^{-1} = \left(\frac{p, a'}{p}\right)$ (la segunda igualdad porque $\varepsilon = \varepsilon^{-1}$ en μ_2, el rango del símbolo de Hilbert), $\left(\frac{p, p}{p}\right) = (-1)^{(p-1)/2}$ por el teorema previo y $\left(\frac{a', b'}{p}\right) = 1$ por el mismo teorema ya que a', b' son unidades. Se sigue que

$$\left(\frac{a, b}{p}\right) = (-1)^{\frac{p-1}{2}\alpha\beta} \left(\frac{p, a'}{p}\right)^\beta \left(\frac{p, b'}{p}\right)^\alpha = (-1)^{\frac{p-1}{2}\alpha\beta} \left(\frac{a'}{p}\right)^\beta \left(\frac{b'}{p}\right)^\alpha$$

ya que a' y b' son unidades. □

2.7 El teorema de Kronecker-Weber local

Por el teorema de existencia, todo subgrupo abierto de índice finito $N \subseteq K^*$ es un grupo de normas y así, por el corolario (2.45), contiene a un subgrupo de la forma $U_K^{(n)}$. Podemos entonces definir:

Definición 2.66. Si L/K es una extensión finita de Galois de campos locales y f es el menor entero ≥ 0 tal que $U_K^{(f)} \subseteq N_{L/K}L^*$, entonces el ideal de $\mathcal{O}_K$ dado por

$$\mathfrak{f} := \mathfrak{p}_K^f$$

se llama el *conductor* de la extensión L/K

Proposición 2.67. *Una extensión abeliana finita de campos locales L/K es no ramificada si y sólo si su conductor $\mathfrak{f} = 1$.*

DEMOSTRACIÓN. Si L/K es no ramificada entonces $U_K^{(0)} = U_K = N_{L/K}U_L \subseteq N_{L/K}L^*$ por (2.5) y por lo tanto $f = 0$, i.e., $\mathfrak{f} = 1$.

Recíprocamente, si $\mathfrak{f} = 1$ entonces $U_K := U_K^{(0)} \subseteq N_{L/K}L^*$. Por otra parte, el grupo de normas $N_{L/K}L^*$ contiene algún $U_K^{(n)} = 1 + \pi_K^n\mathcal{O}_K$ por (2.45) y esto, combinado con el hecho de que $1 \in U_K \subseteq N_{L/K}L^*$, implica que $\pi_K^n = (1+\pi_K^n)-1 \in N_{L/K}L^*$ para algún n y por lo tanto $(\pi_K^n)\times U_K \subseteq N_{L/K}L^*$. Sea M/K la extensión no ramificada de grado n. Entonces, el primo π_K de K también es primo de M y como $M^* = (\pi_M) \times U_M$, se tiene que

$$N_{M/K}M^* = N_{M/K}((\pi_M) \times U_M) = (\pi_K^n) \times U_K \subseteq N_{L/K}L^*$$

ya que $N_{M/K}U_M = U_K$ porque M/K es no ramificada, y así, por (2.39)(2), $M \supseteq L$ y por lo tanto L/K es no ramificada. □

Observación. En la demostración anterior vimos que si M/K es una extensión no ramificada de grado f, entonces para $M^* = U_M \times (\pi_K)$ (donde recordamos que como M/K es no ramificada entonces π_K es primo de M también) se tiene que

$$N_{M/K}M^* = N_{M/K}(U_M \times (\pi_K)) = N_{M/K}U_M \times N_{M/K}(\pi_K) = U_K \times (\pi_K^f)$$

ya que como M/K es no ramificada, entonces $N_{M/K}U_M = N_{M/K}U_K$ y por definición de norma $N_{M/K}(\pi_K) = \pi_K^f$, con $f = [M : K]$. Se sigue que *todo subgrupo de normas de K^* contiene un grupo de la forma $U_K \times (\pi_K^f)$.*

Entonces, por el teorema de existencia, *todo subgrupo abierto de índice finito* $N \subseteq K^*$ *contiene un grupo de la forma* $(\pi^f) \times U_K^{(n)}$ que también es de índice finito. Se sigue entonces que toda extensión abeliana finita L/K está contenida en el campo de clases de un grupo de normas de la forma $(\pi^n) \times U_K^{(n)}$. Por esta razón los campos de clases de estos grupos son de interés especial. En el caso de $K = \mathbb{Q}_p$, donde $\pi = p$, probaremos a continuación que el campo de clases del grupo $(p) \times U_K^{(n)}$ es precisamente el campo ciclotómico $\mathbb{Q}_p(\mu_{p^n})$ obtenido adjuntando las raíces p^n-ésimas de la unidad a $\mathbb{Q}_p$. Comenzamos con el resultado siguiente:

Lema 2.68. *Sea* ζ *una raíz primitiva* p^n*-ésima de la unidad. Entonces,*

(1) *La extensión* $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ *es totalmente ramificada de grado* $p^{n-1}(p-1)$.

(2) $\lambda := \zeta - 1$ *es un primo de* $\mathbb{Q}_p(\zeta)$ *y su norma es:* $N_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}(-\lambda) = p$.

(3) *El grupo de Galois*

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^n\mathbb{Z})^*$$

(el grupo de unidades del anillo $\mathbb{Z}/p^n\mathbb{Z}$*).*

DEMOSTRACIÓN. Por el criterio de Eisenstein para $\mathbb{Q}_p$, el polinomio ciclotómico

$$\Phi(x) = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = x^{p^{n-1}(p-1)} + \cdots + x^{p^{n-1}} + 1$$

es irreducible sobre $\mathbb{Q}_p$ y por lo tanto es el polinomio mínimo $\mathrm{Irr}(\zeta, \mathbb{Q}_p)$ de ζ sobre $\mathbb{Q}_p$. Se sigue que $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] = \mathrm{gr}(\Phi) = p^{n-1}(p-1)$. Pongamos $G = \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$. Por definición del polinomio mínimo irreducible,

$$\Phi(x) = \prod_{\sigma \in G} (x - \sigma(\zeta)).$$

Poniendo $x = 1$ en esta factorización, se obtiene

$$p = 1 + \cdots + 1 = \Phi(1) = \prod_{\sigma \in G} (1 - \sigma(\zeta)) = \prod_{\sigma \in G} \sigma(1 - \zeta) = N_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}(1 - \zeta)$$

y como

$$v_{\mathbb{Q}_p(\zeta)}(1 - \sigma(\zeta)) = v_{\mathbb{Q}_p(\zeta)}(\sigma(1 - \zeta)) = v_{\mathbb{Q}_p(\zeta)}(1 - \zeta),$$

entonces

$$v_{\mathbb{Q}_p(\zeta)}(p) = v_{\mathbb{Q}_p(\zeta)}\Big(\prod_{\sigma \in G} \sigma(1-\zeta)\Big) = \sum_{\sigma \in G} v_{\mathbb{Q}_p(\zeta)}(1-\zeta) = [\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] v_{\mathbb{Q}_p(\zeta)}(1-\zeta)$$

y por lo tanto

$$v_{\mathbb{Q}_p(\zeta)}(1-\zeta) = \frac{v_{\mathbb{Q}_p(\zeta)}(p)}{[\mathbb{Q}_p(\zeta):\mathbb{Q}_p]} \in \mathbb{Z}.$$

Finalmente, como $v_{\mathbb{Q}_p(\zeta)}(p) = e$ es el índice de ramificación de $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$, se sigue que esta extensión es totalmente ramificada y $\lambda := \zeta - 1$ es un primo de $\mathbb{Q}_p(\zeta)$. Esto termina la demostración de (1) y (2).

(3) Fácil. □

Teorema 2.69. *El grupo de normas de* $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ *es el grupo* $(p) \times U_{\mathbb{Q}_p}^{(n)}$. *Equivalentemente, el campo de clases del grupo* $(p) \times U_{\mathbb{Q}_p}^{(n)}$ *es el campo ciclotómico* $\mathbb{Q}_p(\mu_{p^n})$.

DEMOSTRACIÓN. Por (1.67), para el campo $K = \mathbb{Q}_p$ (de característica 0) se tienen isomorfismos (para $n \geq 1$ si $p \neq 2$ y para $n \geq 2$ si $p = 2$):

$$U_{\mathbb{Q}_p}^{(n)} = \left(U_{\mathbb{Q}_p}^{(1)}\right)^{p^{n-1}(p-1)} \quad \text{si} \quad p \neq 2 \tag{1}$$

(poniendo $m = p^{n-1}(p-1)$ en (1.67) y observando entonces que $v_p(m) = 1-n$, y así $1 \geq (1-n)+1$ porque $n \geq 1$) y

$$U_{\mathbb{Q}_2}^{(n)} = \left(U_{\mathbb{Q}_2}^{(2)}\right)^{2^{n-2}} \quad \text{si} \quad p = 2 \tag{2}$$

(poniendo $m = 2^{n-2}$ en (1.67) de tal forma que $v_2(m) = 2-n$ y así $2 \geq (2-n)+1$ porque $n \geq 1$).

Esto muestra que $U_{\mathbb{Q}_p}^{(n)} \subseteq N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\mu_{p^n})^*$ si $p \neq 2$. Ahora, para $p = 2$ observemos que como $U_{\mathbb{Q}_2}^{(\nu)} = 1 + 2^\nu\mathbb{Z}_2$, entonces

$$U_{\mathbb{Q}_2}^{(2)} = U_{\mathbb{Q}_2}^{(3)} \cup 5U_{\mathbb{Q}_2}^{(3)} = (U_{\mathbb{Q}_2}^{(2)})^2 \cup 5(U_{\mathbb{Q}_2}^{(2)})^2$$

ya que un entero que es congruente con 1 mod $2^2 = 4$ es congruente con 1 ó 5 mod $2^3 = 8$. Se sigue que

$$U_{\mathbb{Q}_2}^{(n)} = (U_{\mathbb{Q}_2}^{(2)})^{2^{n-1}} \cup 5(U_{\mathbb{Q}_2}^{(2)})^{2^{n-1}}$$

y como $5^{2^{n-2}} = N_{\mathbb{Q}_2(\mu_{2^n})/\mathbb{Q}_2}(2+i)$, entonces $U_{\mathbb{Q}_2}^{(n)} \subseteq N_{\mathbb{Q}_2(\mu_{2^n})/\mathbb{Q}_2}\mathbb{Q}_2(\mu_{2^n})^*$ también en el caso $p = 2$.

Ahora, en el lema (2.68)(2) mostramos que $p = N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}(-\lambda)$ y así $p \in N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\mu_{p^n})^*$; esto, junto con $U_{\mathbb{Q}_p}^{(n)} \subseteq N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\mu_{p^n})^*$,

muestra que

$$(p) \times U_{\mathbb{Q}_p}^{(n)} \subseteq N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\mu_{p^n})^*$$

y claramente este subgrupo tiene índice $p^{n-1}(p-1)$, que es igual al índice del subgrupo $N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\mu_{p^n})^* \subseteq \mathbb{Q}_p^*$ por el isomorfismo

$$\mathbb{Q}_p^*/N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\mu_{p^n})^* \simeq \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)$$

y porque $[\mathbb{Q}_p(\mu_{p^n}) : \mathbb{Q}_p] = p^{n-1}(p-1)$ por (2.68)(1). Se sigue que la inclusión $(*)$ debe ser una igualdad:

$$(p) \times U_{\mathbb{Q}_p}^{(n)} = N_{\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\mu_{p^n})^*,$$

como se quería. □

También necesitaremos el siguiente resultado sobre extensiones no ramificadas de $\mathbb{Q}_p$, que esencialmente es (1.64):

Lema 2.70. *La extensión no ramificada de grado f de $\mathbb{Q}_p$ es el campo de descomposición del polinomio $x^{p^f} - x$ sobre $\mathbb{Q}_p$, es decir, es el campo ciclotómico $\mathbb{Q}_p(\mu_{p^f-1})$.*

DEMOSTRACIÓN. El campo residual de $\mathbb{Q}_p$ es $\mathbb{F}_p$ y así existe una única extensión de grado f de $\mathbb{F}_p$, a saber $\mathbb{F}_{p^f}$ que, de hecho, es el campo de descomposición de $x^{p^f} - x$ sobre $\mathbb{F}_p$. Así, la extensión no ramificada K de $\mathbb{Q}_p$ tiene campo residual $\mathbb{F}_{p^f}$.

Ahora, para el polinomio $f(x) = x^{p^f} - x$ sobre $\mathbb{Q}_p$ se tiene que $f'(x) = p^f x^{p^f-1} - 1$ y así, para todo $a \in \mathcal{O}_K$ se tiene que la valuación

$$|f'(a)|_p = |p^f a^{p^f-1} - 1|_p = 1$$

ya que $|p^f a^{p^f-1}|_p \leq 0$. Entonces, por el lema de Hensel, para todo $\alpha \in \mathbb{F}_{p^f} = \mathcal{O}_K/\mathfrak{p}_K$ existe un $\widehat{\alpha} \in \alpha \subseteq \mathcal{O}_K$ tal que $f(\widehat{\alpha}) = 0$. Así, como el polinomio $f(x)$ se descompone en $\mathbb{F}_{p^f}$ entonces $f(x)$ se descompone en K. Además, el campo de descomposición de $f(x)$ sobre $\mathbb{Q}_p$ no puede ser menor que $K = \mathbb{Q}_p(\mu_{p^f-1})$ ya que su campo residual debe contener al menos p^f elementos. Se sigue que el campo de descomposición de $f(x)$ sobre $\mathbb{Q}_p$ es $K = \mathbb{Q}_p(\mu_{p^f-1})$. □

Como consecuencia de los resultados anteriores, obtenemos la versión local del teorema de Kronecker-Weber:

Teorema 2.71 (Kronecker-Weber local). *Toda extensión abeliana finita L de $\mathbb{Q}_p$ está contenida en un campo ciclotómico $\mathbb{Q}_p(\zeta)$, donde ζ es alguna raíz primitiva de la unidad. En otras palabras, la extensión abeliana máxima $\mathbb{Q}_p^{ab}/\mathbb{Q}_p$ se obtiene adjuntando todas las raíces de la unidad.*

DEMOSTRACIÓN. Sabemos, por la observación después de (2.67), que $(p^f) \times U_{\mathbb{Q}_p}^{(n)} \subseteq N_{L/\mathbb{Q}_p} L^*$ para algunos enteros f y n. Por lo tanto, L está contenido en el campo de clases M del grupo $(p^f) \times U_{\mathbb{Q}_p}^{(n)}$. Pero como

$$(p^f) \times U_{\mathbb{Q}_p}^{(n)} = ((p^f) \times U_{\mathbb{Q}_p}) \cap ((p) \times U_{\mathbb{Q}_p}^{(n)})$$

ya que $(p^f) \subseteq (p)$ y $U_K^{(n)} \subseteq U_K$, entonces por el teorema (2.39)(3) el campo de clases M es el *campo compuesto* $M = M_1 \cdot M_2$ del campo de clases M_1 de $(p^f) \times U_{\mathbb{Q}_p}$ y el campo de clases M_2 del grupo $(p) \times U_{\mathbb{Q}_p}^{(n)}$.

Ahora, por el teorema anterior, M_2 es el campo ciclotómico $\mathbb{Q}_p(\mu_{p^n})$ y si consideramos la extensión no ramificada $F/\mathbb{Q}_p$ de grado f, entonces el primo p de $\mathbb{Q}_p$ es el primo de F y por lo tanto $F^* = (p) \times U_F$; así,

$$N_{F/\mathbb{Q}_p}(F^*) = N_{F/\mathbb{Q}_p}(p) \times N_{F/\mathbb{Q}_p}(U_F) = (p^f) \times U_{\mathbb{Q}_p}$$

y por lo tanto $M_1 = F$, i.e., M_1 es la extensión no ramificada $M_1/\mathbb{Q}_p$ de grado f y así, por el lema (2.70), M_1 es el campo ciclotómico $M_1 = \mathbb{Q}_p(\mu_{p^f-1})$.

Se sigue entonces que

$$M = M_1 \cdot M_2 = \mathbb{Q}_p(\mu_{p^f-1}) \cdot \mathbb{Q}_p(\mu_{p^n}) = \mathbb{Q}_p(\mu_{p^n(p^f-1)}).$$

□

2.8 Anexo 1: Teoría de Kummer

Sea K un campo arbitrario, no necesariamente local; sea $n \geq 1$ un entero coprimo con car (K) y supongamos que K contiene al grupo μ_n de raíces n-ésimas de la unidad. El resultado siguiente, conocido como el *Teorema 90 de Hilbert* ya que ocurre como el número 90 de los 169 teoremas del reporte sobre teoría de números de Hilbert (el famoso Zahlbericht de 1893), es importante para el estudio de extensiones cíclicas, como lo muestra el corolario que le sigue. Recordemos que una extensión L/K se llama *cíclica* si es de Galois y su grupo de Galois es cíclico.

Teorema 2.72 (Teorema 90 de Hilbert). *Sean L/K una extensión cíclica finita y σ un generador de* Gal(L/K). *Entonces, un elemento $a \in L^*$ tiene norma $N_{L/K}(a) = 1$ si y sólo si es de la forma $a = b/\sigma(b)$ para algún $b \in L^*$.*

DEMOSTRACIÓN. Si $a = b/\sigma(b)$ con $b \neq 0$ y si $|G| = n$, entonces

$$N_{L/K}(a) = \prod_{k=0}^{n-1} \sigma^k(a) = a\sigma(a)\cdots\sigma^{n-1}(a) = \frac{b}{\sigma(b)} \cdot \frac{\sigma(b)}{\sigma^2(b)} \cdots \frac{\sigma^{n-1}(b)}{\sigma^n(b)} = 1,$$

ya que $\sigma^n = id$.

Supongamos ahora que $N_{L/K}(a) = 1$. Para $c \in L$ definamos

$$\begin{aligned} b_0 &= ac \\ b_1 &= (a\sigma(a))\sigma(c) \end{aligned}$$

$$b_i = (a\sigma(a)\cdots\sigma^i(a))\sigma^i(c)$$

para $0 \leq i \leq n-1$. Entonces,

$$b_{n-1} = (a\sigma(a)\cdots\sigma^{n-1}(a))\sigma^{n-1}(c) = N(a)\sigma^{n-1}(c) = \sigma^{n-1}(c)$$

ya que $N_{L/K}(a) = 1$. Más aún, para $0 \leq i \leq n-2$, es claro que

$$b_{i+1} = a\sigma(b_i).$$

Pongamos ahora

$$b := b_0 + \cdots + b_{n-1} \in L.$$

Mostraremos a continuación que existe $c \in L$ tal que $b \neq 0$. En efecto, si para todo $c \in L$ se tuviera que $b = 0$, entonces

$$\begin{aligned} 0 \quad & b_0 + b_1 + \cdots + b_{n-1} \\ - \quad & ac + (a\sigma(a))\sigma(c) + \cdots + (a\sigma(a)\cdots\sigma^{n-1}(a))\sigma^{n-1}(c) \\ & \alpha_0\sigma^0(c) + \alpha_1\sigma(c) + \cdots + \alpha_{n-1}\sigma^{n-1}(c) \end{aligned}$$

donde $\alpha_j := a\sigma(a)\cdots\sigma^j(a) \in L^*$, y por lo tanto, los n automorfismos σ^j son dependientes sobre L, en contradicción con el teorema de Dedekind sobre la

independencia de automorfismos. Se sigue que existe $c \in L$ tal que $b \neq 0$ y para esta b se tiene que

$$\begin{aligned}
\sigma(b) &= \sigma(b_0) + \cdots + \sigma(b_{n-1}) \\
&= \frac{b_1}{a} + \cdots + \frac{b_{n-1}}{a} + \sigma^n(c) \qquad \text{ya que } b_{i+1} = a\sigma(b_i) \\
&= \frac{1}{a}(b_1 + \cdots + b_{n-1} + ac) \qquad \text{ya que } \sigma^n(c) = c \\
&= \frac{1}{a}(b_0 + \cdots + b_{n-1} + b_0) = \frac{b}{a},
\end{aligned}$$

i.e., $a = b/\sigma(b)$. □

Corolario 2.73. *Sean L/K una extensión finita y $n \geq 1$ un entero coprimo con* car (K). *Supongamos que K contiene al grupo μ_n de raíces n-ésimas de la unidad. Entonces, L/K es cíclica de orden d que divide a n si y sólo si $L = K(\sqrt[d]{a})$ para algún $a \in K^*$ y $d|n$.*

DEMOSTRACIÓN. Si $L = K(\sqrt[d]{a})$ con $d|n$, entonces L es campo de descomposición del polinomio separable (ya que d es coprimo con car (K)) $x^d - a \in K[x]$, y como $d|n$ entonces $\mu_d \subseteq \mu_n \subseteq L$. Sea $\omega \in \mu_d \subseteq L$ una raíz primitiva d-ésima de la unidad. Entonces

$$x^d - a = (x - \alpha)(x - \alpha\omega)\cdots(x - \alpha\omega^{d-1}),$$

donde α es cualquier raíz de $x^d - a$. Se sigue que $L = K(\alpha)$ y claramente todo $\sigma \in \mathrm{Gal}(L/K)$ está determinado por su valor en α; de hecho, $\sigma \in \mathrm{Gal}(L/K)$ está dado por $\sigma(\alpha) := \omega^j\alpha$ para $0 \leq j \leq d-1$; si denotamos esta σ por σ_j se observa que

$$\sigma_i \circ \sigma_j(\alpha) = \sigma_i(\alpha\omega^j) = \omega^j\sigma_i(\alpha) = \omega^j(\omega^i\alpha) = \omega^{i+j}\alpha,$$

donde usamos que $\omega \in K$, por lo que la podemos sacar del morfismo σ_i. Si ahora ponemos $\sigma_1 : \alpha \mapsto \alpha\omega$, de la igualdad anterior se sigue que para todo $\sigma_j \in \mathrm{Gal}(L/K)$ se tiene que

$$\sigma_j = \overbrace{\sigma_1 \circ \cdots \circ \sigma_1}^{j \text{ veces}} = (\sigma_1)^j.$$

Se sigue que $\mathrm{Gal}(L/K)$ es cíclico de orden $d|n$.

Recíprocamente, si $\mathrm{Gal}(L/K)$ es cíclico de orden $d|n$, generado por σ, sea $\omega \in \mu_d \subseteq \mu_n \subseteq K \subseteq L$ una raíz primitiva de la unidad. Como $\omega \in K$ su

norma es

$$N_{L/K}(\omega) = \omega^d = 1$$

y así, por el Teorema 90 de Hilbert, existe un $\alpha \in L^*$ tal que $\omega = \alpha/\sigma(\alpha)$. De esta igualdad se sigue que $\sigma(\alpha) = \alpha\omega^{-1}$, por lo que $\alpha \notin K$ ya que no queda fijo bajo σ y también se sigue que

$$\sigma(\alpha^d) = (\sigma(\alpha))^d = \sigma(\omega^{-1} \cdot \alpha)^d = \omega^{-d} \cdot \alpha^d = 1 \cdot \alpha^d = \alpha^d$$

y por lo tanto $a := \alpha^d \in K^*$. Finalmente, como

$$x^d - a = (x - \alpha)(x - \alpha\omega) \cdots (x - \alpha\omega^{d-1})$$

entonces $K(\alpha)$ es campo de descomposición de $x^d - a$ sobre K. Y como $\sigma^0, \sigma, \ldots, \sigma^{d-1}$ son d automorfismos distintos de $K(\alpha)$ entonces

$$d \leq |\mathrm{Gal}(K(\alpha)/K)| = [K(\alpha) : K] \leq [L : K] = d$$

y por lo tanto $L = K(\alpha) = K(\sqrt[d]{a})$. □

El corolario anterior se generaliza considerando extensiones de la forma siguiente: sea K un campo que contiene al grupo μ_n de las raíces n-ésimas de la unidad, con n primo relativo a la característica de K. Una *extensión de Kummer de exponente n* de K es un campo L de la forma

$$L = K(\sqrt[n]{\Delta})$$

donde Δ es un subgrupo de K^* que contiene al subgrupo $(K^*)^n$ de n-potencias. Así, L está generado por todas las raíces $\sqrt[n]{a}$ con $a \in \Delta$, de tal forma que las extensiones de Kummer generalizan, en efecto, a las extensiones cíclicas. Si $\Delta = K^*$, diremos que la extensión $L = K(\sqrt[n]{K^*})$ es la *extensión de Kummer máxima de exponente n*, de tal forma que $L = K(\sqrt[n]{K^*})$ contiene a todas las raíces n-ésimas de K.

En general, si $D \subseteq K^*$ es cualquier subconjunto y si $\Delta = \langle D \rangle \subseteq K^*$ es el subgrupo que genera, entonces

$$K\left(\sqrt[n]{D}\right) = K\left(\sqrt[n]{\Delta}\right).$$

El resultado principal es:

Teorema 2.74. *Sea K un campo que contiene al grupo μ_n de las raíces n-ésimas de la unidad, con n primo relativo a la característica de K. Entonces:*

(1) *Si L/K es una extensión de Kummer de exponente n, entonces: L/K es normal (Galois, no necesariamente finita) y* Gal(L/K) *es abeliano de exponente n.*

(2) *Recíprocamente, si L/K es una extensión abeliana de exponente n, entonces $L = K(\sqrt[n]{\Delta})$ con $\Delta = L^{*n} \cap K^*$, i.e., L/K es una extensión de Kummer de exponente n.*

DEMOSTRACIÓN. (1): Como L se obtiene de K adjuntando las raíces de los polinomios $x^n - a$, $a \in \Delta \subseteq K^*$, y ninguno de estos polinomios tiene raíces múltiples ya que su derivada nx^{n-1} tiene como única raíz al 0 y así no tiene raíces en común con $x^n - a$, se sigue que los factores irreducibles de $x^n - a$ son separables y por lo tanto L/K es separable.

Para la normalidad, supongamos que M/L es cualquier extensión finita y normal. Entonces para todo K-monomorfismo $\sigma : L \rightarrowtail M$ se tiene que σ está determinado por sus valores en los elementos de la forma $\sqrt[n]{a} \in \sqrt[n]{\Delta}$, y para estos elementos $a \in \Delta$ los polinomios $x^n - a$ se descomponen en L, por lo que $\sigma(\sqrt[n]{a}) \in L$ y consecuentemente σ tiene su imagen en L, i.e., $\sigma : L \to L$ y claramente es un isomorfismo.

Que Gal(L/K) es conmutativo es porque si $\sigma, \tau \in$ Gal(L/K), como L está generado, sobre K, por los elementos $\alpha = \sqrt[n]{a}$, $a \in \Delta$ entonces basta ver la acción de σ y τ en estos elementos. Ahora, claramente σ y τ mandan $\alpha = \sqrt[n]{a}$ a alguna raíz de $x^n - a$, i.e., $\sigma(\alpha) = \alpha \cdot \varepsilon_i$ con $\varepsilon_i \in \mu_n$ y $\tau(\alpha) = \alpha \cdot \varepsilon_j$, con $\varepsilon_j \in \mu_n$. Entonces (como $\varepsilon_i, \varepsilon_j \in \mu_n \subseteq K$ y $\sigma, \tau|_K = id$), se tiene que

$$\tau(\sigma(\alpha)) = \tau(\varepsilon_i \alpha) = \varepsilon_i \tau(\alpha) = \varepsilon_i \varepsilon_j \alpha = \varepsilon_j \varepsilon_i \cdot \alpha = \sigma(\tau(\alpha)).$$

Finalmente, dada $\sigma \in$ Gal(L/K) sea $\alpha = \sqrt[n]{a}$, $a \in \Delta$ un generador de L sobre K. Entonces $\sigma(\alpha) = \varepsilon_i \alpha$, $\sigma^2(\alpha) = \sigma(\varepsilon_i \alpha) = \varepsilon_i \cdot \sigma(\alpha) = \varepsilon_i^2 \cdot \alpha$, $\ldots$, $\sigma^n(\alpha) = \varepsilon_i^n \cdot \alpha = \alpha$, ya que ε_i es raíz n-ésima de 1. Así $\sigma^n = 1$ en todos los $\sqrt[n]{a}$ y como éstos generan L, entonces $\sigma^n = 1$ en L.

(2): Como $\Delta = L^{*n} \cap K^*$, entonces claramente $K(\sqrt[n]{\Delta}) \subseteq L$. Para la otra inclusión observemos que la extensión L/K es la composición de sus *subextensiones finitas* L'/K. Ahora, para cada una de estas L'/K su grupo de Galois Gal(L'/K) es abeliano finito y así es el producto directo de grupos

cíclicos, y cada uno de éstos es, de hecho, el grupo de Galois de una subextensión *cíclica* de L'/K. Así, L'/K es la composición de sus subextensiones cíclicas y por lo tanto L/K es la composición de sus subextensiones cíclicas.

Sea M/K una subextensión cíclica de L/K. Como $\mathrm{Gal}(L/K)$ es de exponente n, entonces $\mathrm{Gal}(M/K)$ también es de exponente n y así el orden $|\mathrm{Gal}(M/K)|$ divide a n. Se sigue que $M = K(\sqrt[n]{a})$ con $a \in L^{*n} \cap K^*$ y así $M \subseteq K(\sqrt[n]{\Delta})$, y por lo tanto $L \subseteq K(\sqrt[n]{\Delta})$. □

Lo que usualmente se conoce como *teoría de Kummer* es el contenido del teorema siguiente:

Teorema 2.75. *Sean K un campo y $n \geq 1$ un entero coprimo con* car (K) *tal que $\mu_n \subseteq K^*$. Si $\Delta \subseteq K^*$ es un subgrupo tal que $(K^*)^n \subseteq \Delta$ y $L = K(\sqrt[n]{\Delta})$ es el campo de Kummer correspondiente, sea $G = \mathrm{Gal}(L/K)$. Entonces se tiene un apareamiento bilineal:*

$$\mathrm{Gal}(L/K) \times \Delta \longrightarrow \mu_n,$$

dado por $(\sigma, a) \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$, tal que:

(1) *El núcleo en la izquierda es* 1.

(2) *El núcleo en la derecha es $(K^*)^n$.*

Demostración. Si $a \in \Delta$ y $\sigma \in G = \mathrm{Gal}(L/K)$, sea $\alpha = \sqrt[n]{a}$ una raíz n-ésima de a. Entonces $\sigma(\alpha) = \omega_\sigma \alpha$ para alguna raíz n-ésima de la unidad $\omega_\sigma \in \mu_n \subseteq K^*$. La función $\sigma \mapsto \omega_\sigma$ es un homomorfismo de G en μ_n ya que si $\tau, \sigma \in G$ entonces $\tau\sigma(\alpha) = \tau(\omega_\sigma \alpha) = \omega_\sigma \tau(\alpha) = \omega_\sigma \omega_\tau \alpha$.

Escribamos $\omega_\sigma = \sigma(\alpha)/\alpha$ y observemos que ω_σ es independiente de la elección de la raíz n-ésima α de a ya que si α' es otra raíz n-ésima de a, entonces $\alpha' = \alpha\zeta$ para alguna $\zeta \in \mu_n$ y por lo tanto

$$\frac{\sigma(\alpha')}{\alpha'} \quad \frac{\sigma(\alpha\zeta)}{} = \frac{\zeta\sigma(\alpha)}{} \quad \frac{\sigma(\alpha)}{\alpha}$$

la penúltima igualdad porque $\zeta \in \mu_n \subseteq K$. Hemos así definido una aplicación $G \times \Delta \longrightarrow \mu_n$ mediante $(\sigma, a) \mapsto \omega_\sigma = \sigma(\alpha)/\alpha$, para $\alpha = \sqrt[n]{a}$ una raíz n-ésima de a. También usaremos la notación $\omega_\sigma = \sigma(\alpha)/\alpha =: \langle \sigma, a \rangle$ para este apareamiento que, de hecho, es bilineal:

Es lineal para la primera variable ya que, como vimos antes

$$\langle \tau\sigma, a\rangle = \frac{\tau\sigma(\alpha)}{\alpha} = \frac{\omega_\tau \omega_\sigma \alpha}{\alpha} = \omega_\sigma \omega_\tau = \langle \tau, a\rangle\langle \sigma, a\rangle.$$

Es lineal en la segunda variable ya que, si $a, b \in \Delta$, sean α, β tales que $\alpha^n = a$ y $\beta^n = b$. Entonces $(\alpha\beta)^n = ab$ y así

$$\langle \sigma, ab\rangle = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)\sigma(\beta)}{\alpha\beta} = \frac{\sigma(\alpha)}{\alpha}\frac{\sigma(\beta)}{\beta} = \langle \sigma, a\rangle\langle \sigma, b\rangle.$$

El núcleo a la derecha es $(K^*)^n$ ya que si $a \in (K^*)^n \subseteq \Delta$, entonces $a = \alpha^n$ con $\alpha \in K$ y por lo tanto $\sigma(\alpha) = \alpha$, por lo que

$$\langle \sigma, a\rangle = \frac{\sigma(\alpha)}{\alpha} = \frac{\alpha}{\alpha} = 1,$$

i.e., a está en el núcleo. Para la otra inclusión, si a está en el núcleo derecho, entonces $\langle \sigma, a\rangle = 1$ para todo $\sigma \in G$. Pongamos $\alpha = \sqrt[n]{a}$ y consideremos el subcampo $K(\sqrt[n]{a})$ de $K(\sqrt[n]{\Delta})$. Si α no estuviera en K entonces existiría un K-automorfismo $K(\alpha)$ que no es la identidad, i.e., $\sigma(\alpha) \neq \alpha$. Extendamos σ a un K-automorfismo de $L = K(\sqrt[n]{\Delta})$ al que seguimos denotando con σ. Para este σ se tiene entonces que

$$\langle \sigma, a\rangle = \frac{\sigma(\alpha)}{\alpha} \neq 1,$$

en contradicción con la hipótesis de que $\langle \sigma, a\rangle = 1$ para todo σ. Se sigue que $\alpha \in K$, i.e., $a = \alpha^n \in (K^*)^n$.

Finalmente, si $\sigma \in G$ está en el núcleo a la izquierda, entonces $\langle \sigma, a\rangle = 1$ para todo $a \in \Delta$ y así, para todo $\alpha \in L$ tal que $\alpha^n = a \in \Delta$, se tiene que $\sigma(\alpha) = \alpha$ y por lo tanto σ es la identidad en $L = K(\sqrt[n]{\Delta})$. □

Observamos ahora que el apareamiento bilineal anterior induce el *apareamiento bilineal no degenerado*:

$$\mathrm{Gal}(L/K) \times \Delta/(K^*)^n \longrightarrow \mu_n.$$

También, el apareamiento bilineal del teorema anterior induce el morfismo $\Delta \longrightarrow \mathrm{Hom}(G, \mu_n)$ mediante $a \mapsto \chi_a := \langle\ ,a\rangle$, i.e., $\chi_a(\sigma) := \langle \sigma, a\rangle = \sigma(\alpha)/\alpha$, cuyo núcleo es $(K^*)^n$, de tal forma que se tiene un monomorfismo natural:

$$\Delta/(K^*)^n \rightarrowtail \mathrm{Hom}(G, \mu_n).$$

En forma análoga se obtiene un monomorfismo

$$G \rightarrowtail \mathrm{Hom}(\Delta/(K^*)^n, \mu_n)$$

mediante $\sigma \mapsto \langle \sigma, \ \rangle$, el cual es inyectivo por la parte (1) del teorema anterior.

De $(*)$ y $(**)$ se sigue que G es finito si y sólo si $\Delta/(K^*)^n$ es finito, y en este caso $(*)$ es un isomorfismo ya que

$$|\Delta/(K^*)^n| \leq |\mathrm{Hom}(G, \mu_n)| = |G| \leq |\mathrm{Hom}(\Delta/(K^*)^n, \mu_n)| = |\Delta/(K^*)^n|,$$

por $(*)$ y $(**)$ y porque un grupo finito es isomorfo a su dual (i.e, si H es un grupo finito, entonces $\mathrm{Hom}(H, \mu_n) \simeq H$). Hemos así probado parte del corolario siguiente:

Corolario 2.76. *Sean K un campo y $n \geq 1$ un entero coprimo con* car (K) *tal que $\mu_n \subseteq K^*$. Si $\Delta \subseteq K^*$ es un subgrupo tal que $(K^*)^n \subseteq \Delta$ y $L = K(\sqrt[n]{\Delta})$ es el campo de Kummer correspondiente, sea $G = \mathrm{Gal}(L/K)$. Entonces el monomorfismo $(*)$ es suprayectivo y así se tiene un isomorfismo canónico:*

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \simeq \Delta/(K^*)^n.$$

DEMOSTRACIÓN. Si L/K es una extensión finita, el monomorfismo $(*)$ es suprayectivo por lo probado en las observaciones previas.

Si L/K es una extensión de grado infinito, sean $\Delta_i/(K^*)^n$ los subgrupos finitos de $\Delta/(K^*)^n$ y pongamos $L_i = K(\sqrt[n]{\Delta_i})$. Entonces $\Delta/(K^*)^n = \bigcup_i \Delta_i/(K^*)^n$ y $L = \bigcup_i L_i$. Se sigue que los grupos $\mathrm{Gal}(L/L_i)$ forman una base de vecindades abiertas del $1 \in \mathrm{Gal}(L/K)$. Ahora, como el núcleo de un homomorfismo continuo $\chi : \mathrm{Gal}(L/K) \to \mu_n$ es abierto, entonces debe contener a algún $\mathrm{Gal}(L/L_i)$. Pasando al cociente, χ induce un morfismo $\overline{\chi} : \mathrm{Gal}(L_i/K) \to \mu_n$ tal que $\chi(\sigma) = \overline{\chi}(\sigma|_{L_i})$. Sin embargo, como L_i/K es una extensión finita, entonces por lo probado en la primera parte de esta demostración se tiene que $\overline{\chi}$ es de la forma $\overline{\chi}_a$ para algún $a \in \Delta_i$. Se sigue que

$$\chi(\sigma) = \overline{\chi}_a(\sigma|_{L_i}) = \sigma(\sqrt[n]{a})/\sqrt[n]{a} = \chi_a(\sigma)$$

y así $\chi = \chi_a$, i.e., el monomorfismo $(*)$ es suprayectivo. □

2.9 Anexo 2: Teoría de Artin-Schreier

Sea K un campo de característica $p \neq 0$. El caso que nos concierne ahora es cuando se tiene una extensión cíclica L/K de grado n tal que $p|n$. El resultado siguiente reduce este caso a una forma más simple:

Lema 2.77. *Sea L/K una extensión cíclica de grado n y supongamos que $n = p^t m$, donde $0 \neq p = \text{car } K$ y $p \nmid m$. Entonces, existe una torre de campos*

$$K = M_t \subseteq \cdots \subseteq M_0 \subseteq L$$

tal que L/M_0 es una extensión cíclica de grado m, y para cada $0 \leq i \leq t$, M_i/M_{i+1} es una extensión cíclica de grado p.

DEMOSTRACIÓN. Como L/K es cíclica, cualquier subgrupo de $\text{Gal}(L/K)$ es normal (de hecho, subgrupos y cocientes de grupos cíclicos son cíclicos). Entonces, del teorema fundamental de la teoría de Galois se sigue que para cualquier campo intermedio $K \subseteq M \subseteq L$ se tiene que tanto M/K como L/M son extensiones cíclicas. Consecuentemente, si $M_1 \subseteq M_2$ son campos intermedios de L/K, entonces M_2/M_1 es cíclica.

Ahora, para $n = p^t m$ con $p \nmid m$, sea H el único subgrupo cíclico de orden m de $\text{Gal}(L/K)$ y sea $M_0 = L^H$ el campo fijo de H. Entonces, L/M_0 es cíclica de grado m (su grupo de Galois es H) y M_0/K es cíclica de grado p^t.

Ahora, como $\text{Gal}(M_0/K)$ es cíclico de orden p^t, entonces es soluble y así existe una sucesión de subgrupos $1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_t = \text{Gal}(M_0/K)$ tales que $|G_i| = p^i$ y los cocientes G_{i+1}/G_i son cíclicos de orden p.

Para cada i sea M_i el campo fijo de G_i en M_0/K. Es claro que $M_0 = M_0^{G_0}$ y $M_t = M_0^{\text{Gal}(M_0/K)} = K$. Por el teorema fundamental de la teoría de Galois, para la sucesión de subgrupos anterior se tiene asociada una torre de campos intermedios: $M_0 \supseteq M_1 \supseteq \cdots \supseteq M_t = K$ tales que los grados $[M_i : M_{i+1}] = [G_{i+1} : G_i] = p$, y además $\text{Gal}(M_i/M_{i+1}) \simeq G_i/G_{i+1}$, que es cíclico de orden p. □

Como consecuencia de este lema, es entonces suficiente considerar ahora el caso de una extensión cíclica L/K de grado $n = p = \text{car } K$.

Para poder probar los análogos de los teoremas (2.73) y (2.74) necesitaremos el análogo del Teorema 90 de Hilbert en una versión aditiva, usando la traza de L/K en lugar de la norma:

Teorema 2.78 (Teorema 90 de Hilbert, forma aditiva). *Sea L/K una extensión cíclica de grado n con grupo de Galois G generado por σ. Entonces, un elemento $a \in L$ tiene traza $\text{Tr}_{L/K}(a) = 0$ si y sólo si $a = b - \sigma(b)$ para algún $b \in L$.*

DEMOSTRACIÓN. Si existe $b \in L$ tal que $a = b - \sigma(b)$, como en (2.72) se tiene que $\text{Tr}_{L/K}(a) = 0$.

Recíprocamente, si $\mathrm{Tr}_{L/K}(a) = 0$, escojamos un elemento $c \in L$ tal que $\mathrm{Tr}_{L/K}(c) = 1$ (ya que la traza es suprayectiva en extensiones separables). Pongamos entonces

$$b := ac + (a + \sigma(a))\sigma(c) + \cdots + (a + \sigma(a) + \cdots + \sigma^{n-2}(a))\sigma^{n-2}(c).$$

Se sigue inmediatamente que $\sigma(b) = b - a$, como se quería probar. □

Consideremos ahora el caso que nos interesa: sea K un campo de característica $p \neq 0$. Pongamos $\wp(x) := x^p - x$; entonces, como $\mathrm{car}(K) = p$, $\wp$ es un endomorfismo del grupo aditivo de K, llamado el morfismo de Artin-Schreier. El resultado análogo a (2.73) es como sigue: si $a \in K$, sea $\alpha \in K_s$ cualquier raíz de la ecuación

$$\wp(x) - a = x^p - x - a = 0$$

y consideremos el campo $K(\wp^{-1}(a)) := K(\alpha)$; entonces:

Corolario 2.79 (Artin-Schreier). *Sean K un campo de característica $p \neq 0$ y L/K una extensión finita. Entonces, L/K es cíclica de grado un divisor de p si y sólo si $L = K(\wp^{-1}(a))$ para algún $a \in K$.*

Demostración. Si L/K es cíclica de grado p con grupo de Galois G generado por σ, entonces como $\mathrm{Tr}_{L/K}(1) = 0$ (ya que es la suma de p unos) entonces, por el corolario anterior, existe un $\alpha \in L$ tal que $\sigma(\alpha) - \alpha = 1$, i.e., $\sigma(\alpha) = \alpha + 1 \neq \alpha$ y por lo tanto $\alpha \notin K$, ya que no queda fijo bajo σ. Observemos ahora que en la torre de campos $K \subset K(\alpha) \subseteq L$, como $[L : K] = p$ es primo entonces no hay campos intermedios propios y como $\alpha \notin K$, entonces $K(\alpha) = L$.

Notemos ahora que

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$$

y por lo tanto $\alpha^p - \alpha$ es invariante bajo $G = \mathrm{Gal}(L/K)$ y así $a := \alpha^p - \alpha \in K$. Se sigue que α es una raíz de $\wp(x) - a = x^p - x - a$.

Observamos ahora que todas las raíces de $x^p - x - a$ son de la forma $\alpha + j$, con $0 \leq j \leq p - 1$ un entero adecuadamente interpretado en K, ya que

$$(\alpha + j)^p - (\alpha + j) - a = \alpha^p + j^p - \alpha - j - a = \alpha^p + j - \alpha - j - a = \alpha^p - \alpha - a,$$

ya que $j^p = j$ en el campo primo $\mathbb{F}_p$ de K. Se sigue que todas las raíces de $x^p - x - a$ están en $K(\alpha)$ y así $L = K(\alpha)$ es campo de descomposición de $x^p - x - a$.

Recíprocamente, supongamos ahora que $L = K(\wp^{-1}(a))$ con $a \in K$. Por la observación del párrafo previo, L es campo de descomposición de $x^p - x - a$. Más aún, si una raíz α de $x^p - x - a$ está en K, entonces todas las raíces están y $L = K$. Si ninguna raíz de $x^p - x - a$ está en K, entonces $x^p - x - a$ es irreducible sobre K y por lo tanto L/K es de grado p. Se sigue que $\mathrm{Gal}(L/K)$ es cíclico generado por $\sigma : L \to L$, el automorfismo dado por $\sigma(\alpha) := \alpha + 1$. □

En general, podemos considerar extensiones abelianas de K de exponente $p = \mathrm{car}\,(K)$ de la forma siguiente: sea $\Delta \subseteq K$ un subgrupo del grupo aditivo de K que contiene al subgrupo $\wp(K)$ de K. Una *extensión de Artin-Schreier* de K es un campo L de la forma

$$L = K(\wp^{-1}(\Delta))$$

donde $\wp^{-1}(\Delta) = \{\wp^{-1}(a) \ : \ a \in \Delta\}$ y $\wp^{-1}(a)$ denota a cualquier solución de la ecuación $\wp(x) = x^p - x = a$. En forma completamente análoga a (2.74) se prueba:

Teorema 2.80. *Sea K un campo de característica $p \neq 0$. Entonces, existe una correspondencia biyectiva entre los subgrupos aditivos $\Delta \subseteq K$ que contienen a $\wp(K)$ y las extensiones abelianas L/K de exponente p. La correspondencia está dada por*

$$\Delta \mapsto K(\wp^{-1}(\Delta)).$$

□

La parte de la teoría de Artin-Schreier que nos interesa está en el resultado siguiente, que es completamente análogo a (2.75) y cuya demostración también lo es:

Teorema 2.81. *Sean K un campo de característica $p \neq 0$, $\Delta \subseteq K$ un subgrupo aditivo que contiene a $\wp(K)$ y $L = K(\wp^{-1}(\Delta))$. Entonces, se tiene un apareamiento bilineal*

$$\mathrm{Gal}(L/K) \times \Delta \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

dado por $(\sigma, a) \mapsto \sigma(\alpha) - \alpha$, donde $\alpha \in K_s$ es cualquier solución de la ecuación $\wp(x) - a = x^p - x - a = 0$. Algunas veces denotamos este apareamiento mediante $[\sigma, a\rangle = \sigma(\alpha) - \alpha$.

(1) *El núcleo a la izquierda de este apareamiento es* 1.

(2) *El núcleo a la derecha de este apareamiento es $\wp(K)$.* □

Se sigue que el apareamiento de este teorema induce un apareamiento bilineal no degenerado

$$\mathrm{Gal}(L/K) \times \Delta/\wp(K) \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

y, como en el caso de teoría de Kummer, se tiene un monomorfismo

$$(\dagger) \qquad \Delta/\wp(K) \rightarrowtail \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Z}/p\mathbb{Z})$$

dado por $a \in \Delta \mapsto \chi_a \in \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$, donde $\chi_a := [\ , a\rangle$, el cual es un isomorfismo cuando $\Delta/\wp(K)$ es finito, i.e., cuando L/K es finita.

Corolario 2.82. *Sean K un campo de característica $p \neq 0$, $\Delta \subseteq K$ un subgrupo aditivo que contiene a $\wp(K)$ y $L = K(\wp^{-1}(\Delta))$. Entonces el monomorfismo canónico* $(\dagger)$ *es un isomorfismo:*

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Z}/p\mathbb{Z}) \simeq \Delta/\wp(K).$$

DEMOSTRACIÓN. Similar a la de (2.76). □

2.10 Anexo 3: El residuo de una diferencial

En este anexo se obtienen los resultados sobre residuos, debidos a Hasse, que se usan en la demostración del teorema de Schmid (2.59). Para las propiedades básicas de *derivaciones* y *diferenciales de Kähler* que se usan, véase Lang [26].

Sean k un campo y $K = k((t))$ el campo local de series de Laurent formales en el parámetro local t con coeficientes en k. Entonces, $\mathrm{grtr}(K/k) = 1$ y por lo tanto el K-espacio vectorial de *diferenciales de Kähler* $\Omega_{K/k}$ tiene dimensión 1, generado por la diferencial dt; así, si $\omega \in \Omega_{K/k}$, la podemos escribir como $\omega = f dt$, con $f \in K$. Si $\omega \neq 0$, ponemos $v(\omega) = v(f dt) := v(f)$ y observamos que esta definición de valuación de la diferencial ω no depende de dt. Otro invariante local importante de la diferencial ω es su *residuo*: si $\omega = f dt$, expresando a f en serie de Laurent

$$f = \sum_{n \gg -\infty} a_n t^n, \quad a_n \in k,$$

se define $\mathrm{Res}_t(\omega) := a_{-1} \in k$. Que esta es una buena definición, i.e., que no depende de la elección del parámetro local t, es el contenido de la proposición siguiente, pero antes necesitaremos algunas propiedades del residuo $\mathrm{Res}_t(\omega)$:

Lema 2.83. *Sea k un campo y $K = k((t))$. Entonces*

(1) $\mathrm{Res}_t(\omega)$ *es k-lineal en $\omega \in \Omega_{K/k}$.*

(2) $\mathrm{Res}_t(\omega) = 0$ *si* $v(\omega) \geq 0$, *i.e., si* $\omega \in \mathcal{O}_K \cdot dt$.

(3) $\mathrm{Res}_t(dg) = 0$ *para toda* $g \in K$.

(4) $\mathrm{Res}_t\left(\dfrac{dg}{g}\right) = v(g)$ *para toda* $g \in K^*$.

DEMOSTRACIÓN. (1), (2) y (3) son obvias. Para (4) pongamos $g = t^n u$ con $n = v(g)$ y $u \in U_K$. Entonces

$$\frac{dg}{g} = n\frac{dt}{t} + \frac{du}{u},$$

y por lo tanto

$$\mathrm{Res}_t\left(\frac{dg}{g}\right) = n + \mathrm{Res}_t\left(\frac{du}{u}\right) = n$$

ya que $v(u) = 0$ y así $\mathrm{Res}_t(du/u) = 0$ por (2). □

Proposición 2.84 (Invarianza del residuo). *Si* $K = k((t))$ *y* $\omega \in \Omega_{K/k}$, *entonces* $\mathrm{Res}_t(\omega)$ *no depende de la elección del parámetro local* t, *i.e., si* t, u *son dos parámetros locales de* K, *entonces* $\mathrm{Res}_t(\omega) = \mathrm{Res}_u(\omega)$.

DEMOSTRACIÓN. Escribamos $\omega \in \Omega_{K/k}$ en términos del parámetro local u, digamos $\omega = g\,du$ con $g \in K$. Podemos separar a ω como

$$\omega = \omega_0 + \sum_{n \geq 0} a_n \frac{du}{u^n}$$

(una suma finita) con $v(\omega_0) \geq 0$. Entonces, $\mathrm{Res}_u(\omega) = a_1$ y

$$\mathrm{Res}_t(\omega) = \mathrm{Res}_t(\omega_0) + \sum_{n \geq 0} a_n \mathrm{Res}_t\left(\frac{du}{u^n}\right)$$

ya que Res_t es k-lineal. Por la parte (2) del lema, $\mathrm{Res}_t(\omega_0) = 0$ porque $v(\omega_0) \geq 0$. Ahora, por la parte (4) del lema anterior, $\mathrm{Res}_t(du/u) = v(u) = 1$ ya que u es un parámetro local y así $v(u) = 1$; entonces, debemos probar que

$$(*) \qquad \mathrm{Res}_t\left(\frac{du}{u^n}\right) = 0 \qquad \text{para } n \geq 2.$$

Para esto, consideramos dos casos:

(1): Si car $(k) = 0$, entonces

$$\frac{du}{u^n} = dg \qquad \text{con} \quad g = \frac{-1}{(n-1)u^{n-1}},$$

y así (∗) se sigue de la parte (3) del lema previo.

(2): Si car $(k) = p > 0$, el argumento anterior no funciona porque puede suceder que $n - 1 \equiv 0$ mód p. Sin embargo, este caso se puede reducir al caso de característica 0 de la forma siguiente: escribamos el parámetro u en términos del otro parámetro t:

$$u = \sum_{i \geq 0} a_i t^{i+1} = a_0 t + a_1 t^2 + a_2 t^3 + \cdots = t(a_0 + a_1 t + a_2 t^2 + \cdots)$$

con los $a_i \in k$. Multiplicando por a_0^{-1} si hiciera falta, podemos suponer que $a_0 = 1$ de tal forma que

$$u = t(1 + a_1 t + a_2 t^2 + \cdots) \qquad \text{con los} \quad a_i \in k.$$

Se sigue que

$$\frac{1}{u^n} = \frac{1}{t^n}(1 + a_1 t + a_2 t^2 + \cdots)^{-n} = \frac{1}{t^n}(1 - n a_2 t + \cdots + b_i t^i + \cdots)$$

donde los b_i son polinomios en $a_1, \ldots, a_i$ con coeficientes en $\mathbb{Z}$ y no dependen de la característica de k.

Multiplicando esta última igualdad por $du = dt + 2a_1 t dt + \cdots$, se obtiene

$$\frac{du}{u^n} = \frac{dt}{t^n} \sum_{i=0}^{\infty} c_i t^i$$

donde los c_i son también polinomios en $a_1, \ldots, a_i$ con coeficientes en $\mathbb{Z}$. Se sigue que

$$\operatorname{Res}_t \left(\frac{du}{u^n} \right) = c_{n-1}.$$

Observamos ahora que el polinomio $c_{n-1}(X_1, \ldots, X_{n-1})$ se anula al substituir $X_i = a_i$ con los a_i en un campo de característica 0 ya que

$$c_{n-1} = c_{n-1}(a_1, \ldots, a_{n-1}) = \operatorname{Res}_t \left(\frac{du}{u^n} \right) = 0$$

por el caso (1). Se sigue que el polinomio $c_{n-1}(X_1, \ldots, X_{n-1}) = 0$ es el polinomio idénticamente 0 y así

$$\operatorname{Res}_t \left(\frac{du}{u^n} \right) = c_{n-1} = 0$$

en general. □

El resultado siguiente es usado en la demostración del teorema de Schmid (2.59):

Proposición 2.85. *Si L/K es una extensión finita separable de campos de series formales $L = F((T))$, $K = F((t))$ y $\mathrm{Tr}_{L/K} : L \to K$ es la traza, entonces para todo $f \in L$ se tiene que*

$$\mathrm{Res}_T(f dt) = \mathrm{Res}_t(\mathrm{Tr}_{L/K}(f)dt).$$

DEMOSTRACIÓN. Por la linealidad de Res y Tr, nos podemos restringir al caso cuando f es de la forma T^m con $m \in \mathbb{Z}$.

CASO 1. Supongamos que car $(F) = 0$ y sea $n = [L : K]$. Entonces $v_L(t) = n$ y así $t = w^n$, donde w es un elemento primo de L. Reemplazando T con w podemos suponer que $t = T^n$, y así L/K es una extensión cíclica para la cual el cálculo de la traza no presenta dificultades:

$$\mathrm{Tr}_{L/K}(T^m) = \begin{cases} 0 & \text{si} \quad m \not\equiv 0 \ (\text{mód } n) \\ nt^{m/n} & \text{si} \quad m \equiv 0 \ (\text{mód } n). \end{cases}$$

Se sigue que

$$\mathrm{Res}_t(\mathrm{Tr}_{L/K}(T^m)dt) = \begin{cases} 0 & \text{si} \quad m \neq -n \\ n & \text{si} \quad m = -n, \end{cases}$$

y, por otra parte,

$$\mathrm{Res}_T(T^m dt) = \mathrm{Res}_T(T^m nT^{n-1}dT) = \mathrm{Res}_T(nT^{m+n-1}dT) = \begin{cases} 0 & \text{si} \quad m \neq -n \\ n & \text{si} \quad m = -n, \end{cases}$$

y estas dos últimas igualdades muestran que $\mathrm{Res}_T(f dt) = \mathrm{Res}_t(\mathrm{Tr}_{L/K}(f)dt)$, como se quería.

CASO 2. Consideremos ahora el caso general. Podemos escribir

$$t = T^n + \sum_{i>n} a_i T^i.$$

Se sigue que $1, T, T^2, \ldots, T^{n-1}$ es una base de la extensión $F((T))/F((t))$ y así, para toda $m \in \mathbb{Z}$, podemos escribir

$$T^m T^i = \sum_{j=0}^{n-1} b_{m,i,j}(t)T^j,$$

$0 \leq i \leq n-1$, con los $b_{m,i,j}(t)$ series formales en t:

$$b_{m,i,j}(t) = \sum_k b_{m,i,j,k}\, t^k.$$

Para m fijo los $b_{m,i,j}(t)$ forman una matriz y por definición de traza:

$$\mathrm{Tr}_{L/K}(T^m) = \sum_{i=0}^{n-1} b_{m,i,i}(t) = \sum_{i=0}^{n-1}\sum_k b_{m,i,i,k}t^k = \sum_k \left(\sum_{i=0}^{n-1} b_{m,i,i,k}\right) t^k$$

y por lo tanto su residuo es

$$\begin{aligned} c_m := \mathrm{Res}_t(\mathrm{Tr}_{L/K}(T^m)dt) &= \text{coeficiente de } t^{-1} \text{ en la serie anterior} \\ &= \sum_{i=0}^{n-1} b_{m,i,i,-1} \end{aligned}$$

y, por otra parte,

$$\begin{aligned} \mathrm{Res}_T(T^m\,dt) &= \mathrm{Res}_T(T^m d(T^n + \sum_{i>n} a_i T^i)) \\ &\quad \mathrm{Res}_T(T^m(nT^{n-1}dT + \sum_{i>n} i a_i T^{i-1}dT) \\ &\quad \mathrm{Res}_T\left(nT^{m+n-1}dT + \sum_{i>n} i a_i T^{m+i-1}dT\right) \\ &\quad -ma_{-m}, \end{aligned}$$

para todo $m \in \mathbb{Z}$.

Finalmente, queremos mostrar que

$$-ma_{-m} = c_m = \sum_{i=0}^{n-1} b_{m,i,i,-1}.$$

Para esto, podemos pensar a los $b_{m,i,j,k}$ como polinomios en los a_i con coeficientes en $\mathbb{Z}$ e independientes de la característica del campo. Lo mismo para $c_m + ma_{-m}$. Y para esta última fórmula, substituyendo sus variables observamos que estos polinomios se anulan cada vez que sus argumentos se toman en un campo algebraicamente cerrado de característica 0. Se sigue que el polinomio $c_m + ma_{-m}$ es el polinomio idénticamente nulo, como se quería demostrar. □

2.11 Ejercicios

1. Sea L/K una extensión cíclica de grado primo de campos locales. Demuestre que para i suficientemente grande se tiene que $N_{L/K}(U_L) \supseteq U_K^{(i)}$.
2. Sea L/K una extensión finita de campos locales y sea π_L un primo de L. Si el diferente $\mathcal{D}_{L/K} = \langle \pi_L^d \rangle$ con $d \geq 0$ un entero y $\Delta_{L/K}$ es el discriminante de L/K, demuestre que $|\Delta_{L/K}|_K = |N_{L/K}(\pi_L)|_K^d$.
3. Si $L \supseteq M \supseteq K$ es una torre de extensiones finitas de campos locales y $\mathcal{D}_{L/K} = \langle \pi_L^{d_{L/K}} \rangle$, $\mathcal{D}_{L/M} = \langle \pi_L^{d_{L/M}} \rangle$, $\mathcal{D}_{M/K} = \langle \pi_M^{d_{M/K}} \rangle$, demuestre que
$$d_{L/K} = d_{L/M} + [L : M] d_{M/K}.$$
Sugerencia: Use que $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}(\alpha))$.
4. Sea L/K una extensión finita de campos locales. Demuestre que $\mathcal{D}_{L/K} = \mathcal{O}_L$ si y sólo si L/K es no ramificada.
5. Si $L \supseteq M \supseteq L$ es una torre de extensiones finitas de campos locales, demuestre que $\mathcal{D}_{L/K} = \mathcal{D}_{L/M} \cdot \mathcal{D}_{M/K}$. *Sugerencia*: Use (2.14).
6. Sea L/K una extensión finita de campos locales y sea M un campo intermedio. Pongamos $H = \mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/K) = G$. Demuestre que $v_M(\mathcal{D}_{M/K}) = \dfrac{1}{e(L/M)} \displaystyle\sum_{\sigma \notin H} i_G(\sigma)$. *Sugerencia*: Use (2.13) y la transitividad del diferente (el ejercicio anterior).
7. Sea L/K una extensión finita de Galois de campos locales. Pongamos $L_0 = L \cap K_{nr}$ y supongamos que $\tilde{\phi} \in \mathrm{Frob}(L/K) \subseteq \mathrm{Gal}(L_{nr}/K)$ es un levantamiento de Frobenius del Frobenius $\phi = \mathrm{Fr}_K \in \mathrm{Gal}(K_{nr}/K)$. Demuestre que si $N_{L/L_0}(\tilde{\phi}(u)u^{-1}) = 1$ para $u \in U_L$, entonces $N_{L_{nr}/K_{nr}}(u) \in N_{L/K}U_L$.
8. Sea L/K una extensión abeliana finita de campos locales y M un campo intermedio. Demuestre que: $\alpha \in N_{L/M}L^*$ si y sólo si $N_{M/K}(\alpha) \in N_{L/K}L^*$.
9. Sea L/K una extensión cíclica de grado p^n y M un campo intermedio tal que M/K es de grado p^m.
   (i) Demuestre que $N_{M/K}(M^*) = N_{L/K}(L^*) \cdot (K^*)^{p^m}$.
   (ii) Si además L/K es totalmente ramificada, demuestre que $N_{M/K}U_M = N_{L/K}U_L \cdot (U_K)^{p^m}$.
10. Sean M/K una extensión cíclica con generador $\sigma \in \mathrm{Gal}(M/K)$ y L/M una extensión abeliana finita.
    (i) Demuestre que L/K es Galois si y sólo si $\sigma N_{L/M}L^* = N_{L/M}L^*$.

(ii) Demuestre que L/K es abeliana si y sólo si $\{\alpha^{-1}\sigma(\alpha) \quad \alpha \in M^*\} \subseteq N_{L/M}L^*$.

11. Sean G un grupo y $H \subseteq G$, $H' \subseteq G$ subgrupos de índice finito tales que $H \subseteq H'$. Demuestre que el morfismo de transferencia es tal que el diagrama siguiente conmuta:

$$G^{ab} \xrightarrow{t_{G/H'}} H'^{ab} \xrightarrow{t_{H'/H}} H^{ab}, \qquad t_{G/H} : G^{ab} \to H^{ab}$$

12. Un campo $M \subseteq K^{ab}$ se dice que es un *campo marco* si $M \cap K_{nr} = K$ y $MK_{nr} = K^{ab}$.
    (i) Si $M \subseteq K^{ab}$ es un campo marco, demuestre que
    $$\mathrm{Gal}(K^{ab}/K) \simeq \mathrm{Gal}(K^{ab}/M) \times \mathrm{Gal}(K^{ab}/K_{nr}).$$
    (ii) Sea Fr_K el Frobenius de $\mathrm{Gal}(K_{nr}/K)$ y sea $\phi \in \mathrm{Gal}(K^{ab}/K)$ un levantamiento de Fr_K. Demuestre que el campo fijo de ϕ, denotado K_ϕ, es un campo marco.
    (iii) Demuestre que la correspondencia $\phi \rightsquigarrow K_\phi$ es una biyección entre los levantamientos de Fr_K y los campos marco.
    (iv) Si $\pi \in K$ es un elemento primo, sea $(\pi, K^{ab}/K) \in \mathrm{Gal}(K_{nr}/K)$ el automorfismo dado por la ley de reciprocidad local y sea $\sigma_\pi \in \mathrm{Gal}(K^{ab}/K)$ el levantamiento correspondiente. Demuestre que la correspondencia $\pi \rightsquigarrow \sigma_\pi$ es una biyección entre el conjunto de primos de K y los levantamientos de Fr_K.
    (v) Usando el ejercicio anterior, concluya que la correspondencia $\pi \rightsquigarrow K_{\sigma_\pi}$ es una biyección entre los primos de K y los campos marco.
    (vi) Demuestre que $\pi \in N_{K_{\sigma_\pi}/K}(K_{\sigma_\pi})^*$.
    (vii) Si π es un primo de K, demuestre que $\pi \in N_{L/K}L^*$ si y sólo si $L \cap K_{nr} = K$.

13. Sea K un campo local de característica 0. Un elemento $w \in K$ se dice que es p^n-*primario* si la extensión $K(\sqrt[p^n]{w})/K$ es no ramificada de grado p^n.
    (i) Demuestre que si w es p^n-primario, entonces es p^m-primario para toda $m \leq n$.
    (ii) Usando teoría de Kummer, demuestre que el conjunto de elementos p^n-primarios visto en el conjunto $K^*/(K^*)^{p^n}$ es un subgrupo cíclico de orden p^n.

14. Sea $(\ ,\ )_n : K^* \times K^* \to \mu_n$ el símbolo de Hilbert.

(i) Si n es impar, demuestre que $(\alpha, \alpha)_n = (-1, \alpha)_n = 1$ para $\alpha \in K^*$.
(ii) Si $\omega \in \mu_{q-1}$ y $\beta \in K^*$, demuestre que $(\omega, \beta)_{p^n} = 1$.

15. Sea ζ_p una raíz primitiva p-ésima de la unidad. Demuestre que $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$.
16. Sea ζ_1 una raíz $(p^n - 1)$-ésima primitiva de la unidad y pongamos $L_1 = \mathbb{Q}_p(\zeta_1)$. Demuestre que
$$N_{L_1/\mathbb{Q}_p} L_1^* = \langle p^n \rangle \times U_{\mathbb{Q}_p}.$$
17. Supongamos que $L \subseteq \mathbb{Q}_p(\zeta_{p^k})$ para algún k. Demuestre que $\alpha \in L$ está en la intersección de todos los grupos de norma $N_{\mathbb{Q}_p(\zeta_{p^i})/L}(\mathbb{Q}_p(\zeta_{p^i})^*)$ para $i \geq k$ si y sólo si $N_{L/\mathbb{Q}_p}(\alpha) = p^m$, para algún entero m.
18. Sean K un campo local, K_s una cerradura separable de K y K_{nr}/K su máxima subextensión no ramificada. Considere el subgrupo discreto $\langle \mathrm{Fr}_K^n \quad n \in \mathbb{Z} \rangle$ de $\mathrm{Gal}(K_{nr}/K) \simeq \widehat{\mathbb{Z}}$ y el epimorfismo canónico $\rho_K : \mathrm{Gal}(K_s/K) \twoheadrightarrow \mathrm{Gal}(K_{nr}/K)$, (véase §2.2). El *grupo de Weil* de K es la imagen inversa $W_K := \rho_K^{-1}(\langle \mathrm{Fr}_K^n : n \in \mathbb{Z} \rangle)$. Se tiene así el epimorfismo $\rho_K : W_K \twoheadrightarrow \langle \mathrm{Fr}_K^n : n \in \mathbb{Z} \rangle \simeq \mathbb{Z}$. Demuestre que el núcleo de este epimorfismo es el grupo de inercia de K_s/K.
19. Sea $r \geq 0$ un entero. Un campo K se dice que tiene la propiedad C_r si todo polinomio $f \in K[x_1, \ldots, x_n]$ homogéneo de grado $d \neq 0$ tiene un cero no trivial en K^n siempre que $n > d^r$.
(i) Demuestre que K es algebraicamente cerrado si y sólo si K es C_0.
(ii) Muestre que un campo finito $\mathbb{F}_q$ es C_1.
(iii) Demuestre que si K es C_r, entonces K es C_s para toda $s \geq r$.
(iv) Demuestre que si K es C_1 y L/K es una extensión finita, entonces
$$N_{L/K} L^* = K^*.$$
(v) Si K es algebraicamente cerrado, entonces el campo de funciones $K(t)$ es C_1.
(vi) Demuestre que si K es un campo de característica p y es C_1, entonces K es perfecto ó $[K : K^p] = p$.

Capítulo 3

Grupos formales y extensiones abelianas de campos locales

En este capítulo, siguiendo a Lubin-Tate [28], consideramos la introducción de la teoría de grupos formales en la teoría de campos de clases locales, para al final obtener una fórmula explícita para el símbolo de norma residual de las extensiones construidas usando grupos formales y que generalizan a las extensiones ciclotómicas de $\mathbb{Q}_p$. Como una consecuencia importante, se demuestra que los campos de clases de los grupos de norma $(\pi) \times U_K^{(n)} \subseteq K^*$ son los campos de Lubin-Tate $K_{\pi,n}$ obtenidos adjuntando a K puntos de torsión de ciertos grupos formales, y como corolario se obtiene una descripción explícita de la máxima extensión abeliana K^{ab} de un campo local K arbitrario generalizando el teorema de Kronecker-Weber local (2.71), probando en (3.27) que $K^{ab} = K_\pi K_{nr}$, donde K_{nr} es la máxima extensión no ramificada de K y K_π es la unión de todas las extensiones de Lubin-Tate $K_{\pi,n}$.

3.1 Grupos formales

El objetivo de introducir grupos formales en la teoría de campos de clases local es obtener una generalización de la teoría de extensiones ciclotómicas de $\mathbb{Q}_p$ para cualquier campo local K. Se comienza observando que las extensiones ciclotómicas se obtienen adjuntando el grupo de raíces n-ésimas de la unidad μ_n a $\mathbb{Q}_p$ y que el grupo μ_n es el núcleo del morfismo $K^* \xrightarrow{n} K^*$ (elevar a la n potencia); la idea es modificar el concepto de grupo multiplicativo de un campo para obtener el equivalente del grupo de raíces de la unidad, el grupo de *puntos de división*, que también es el núcleo de un morfismo $[n]$ que equivale a elevar a la n-potencia.

Comencemos con una analogía: sea G un grupo de Lie real de dimensión 1. Escogiendo cartas adecuadas en G podemos identificar una vecindad del neutro $e \in G$ con una vecindad del $0 \in \mathbb{R}$, de tal forma que e corresponda al 0. Entonces, el producto μ de G está dado por una serie de potencias

$$\mu(x, y) = \sum_{i,j \geq 0} a_{ij} x^i y^j;$$

esta serie converge para x, y pequeños y satisface

$$\begin{aligned} \mu(x, 0) &= x, \\ \mu(0, y) &= y, \\ \mu(x, \mu(y, z)) &= \mu(\mu(x, y), z). \end{aligned}$$

Series de potencias formales. En lo que sigue, A denotará un anillo conmutativo con unidad. Consideraremos *series de potencias formales* con coeficientes en A:

$$\sum_{n \geq 0} a_n x^n,$$

con la suma y producto de series definidos en la forma usual:

$$\sum_{i \geq 0} a_i x^i + \sum_{i \geq 0} b_i x^i := \sum_{i \geq 0} (a_i + b_i) x^i$$

$$\sum_{i \geq 0} a_i x^i \cdot \sum_{j \geq 0} b_j x^j := \sum_{i+j \geq 0} a_i b_j x^{i+j}.$$

El conjunto de series de potencias con coeficientes en A forma un anillo conmutativo al que denotamos por $A[[x]]$. Nótese que, a diferencia de los polinomios, para series de potencias, en general no se puede substituir un elemento $c \in A$ en una serie $\sum_{i \geq 0} a_i x^i$ ya que la suma $\sum_{i \geq 0} a_i c^i$ tiene un número infinito de sumandos de A y esto, en general, no está definido en A. Por la misma razón no podemos substituir una serie de potencias $g(x) = \sum_{i \geq 0} b_i x^i$ en otra serie de potencias $f(x) = \sum_{i \geq 0} a_i x^i$ si la serie de potencias $g(x)$ tiene término constante $\neq 0$. Sin embargo, si el término constante de $g(x)$ es 0, entonces $f(g(x))$ es de nuevo una serie formal a la cual algunas veces se le denota por $f \circ g$.

Similarmente se definen series de potencias en dos o más variables y usamos la notación natural: $A[[x, y]]$, etc.

Definición 3.1. Sean x, y, z indeterminadas. Un *grupo formal* (uniparamétrico) $\mathcal{F}$ definido sobre A es una serie de potencias $\mathcal{F}(x, y) \in A[[x, y]]$ que satisface:

(i) $\mathcal{F}(x, 0) = x$ y $\mathcal{F}(0, y) = y$.

(ii) $\mathcal{F}(x, \mathcal{F}(y, z)) = \mathcal{F}(\mathcal{F}(x, y), z)$.

Si además se cumple que

(iii) $\mathcal{F}(x, y) = \mathcal{F}(y, x)$,

diremos que $\mathcal{F}$ es un *grupo formal conmutativo*. A la serie $\mathcal{F}$ la llamamos la *ley de grupo formal* del grupo formal $\mathcal{F}$.

Nótese que (i) implica que $\mathcal{F}(0, 0) = 0$, i.e., que su término constante es 0 y así ambos lados de (ii) tienen sentido, es decir, son series formales en $A[[x, y, z]]$. Por otro lado, puesto que $\mathcal{F}(0, 0) = 0$, entonces

$$\mathcal{F}(x, y) = x + y + \text{términos de grado} \geq 2 =: x + y \quad \text{mód (gr 2)},$$

donde (mod gr d) quiere decir que los términos restantes son de grado $\geq d$.

Ejemplo 1. $F(x, y) = x + y$ define una ley de grupo formal. El grupo formal asociado se llama el *grupo formal aditivo* y se denota por $\mathbb{G}_a$.

Ejemplo 2. $F(x, y) = x + y + xy = (1 + x)(1 + y) - 1$ define una ley de grupo formal. El grupo formal asociado se llama el *grupo formal multiplicativo* y se denota por $\mathbb{G}_m$.

Observe que este segundo ejemplo proviene de considerar al grupo de Lie $G = (\mathbb{R}^+, \cdot)$ y usar la carta bajo la cual $x \in \mathbb{R}$ (x pequeño) va a dar a $1 + x \in \mathbb{R}^+$. El producto de $\mathbb{R}$ se vuelve entonces el producto formal del ejemplo 2.

El lema siguiente, de la teoría de series formales, nos servirá para mostrar la existencia de inversos para un grupo formal:

Lema 3.2. *Sea A un anillo conmutativo con $1 \neq 0$. Sea*

$$f(x) = \sum_{n=1}^{\infty} a_n x^n \in A[[x]]$$

una serie formal con término constante $= 0$. Si $a_1 \in A^*$ (es una unidad), entonces $f(x)$ es invertible en $A[[x]]$, es decir, existe una serie $i(x) \in A[[x]]$ tal que

$$i(f(x)) = x \quad \text{y} \quad f(i(x)) = x.$$

DEMOSTRACIÓN. La idea es construir una sucesión de polinomios $i_n(X) \in A[x]$ tales que

$$f(i_n(x)) \equiv x \pmod{x^{n+1}}$$

e

$$i_{n+1}(x) \equiv i_n(x) \pmod{x^{n+1}},$$

de modo que si elegimos $i(x) := \lim_{n\to\infty} i_n(x) \in A[[x]]$ se tendrá que

$$\begin{aligned} f(i(x)) \quad & f(\lim_{n\to\infty} i_n(x)) \\ & \lim_{n\to\infty} f(i_n(x)) \\ & \lim_{n\to\infty} x \pmod{x^{n+1}} \\ & x. \end{aligned}$$

Construiremos inductivamente los polinomios $i_n(x)$: para $n = 1$, sea $i_1(x) := a_1^{-1}x$. Entonces

$$\begin{aligned} f(i_1(x)) \quad & a_1(a_1^{-1}x) + \text{términos de grado } \geq 2 \\ = \quad & x + \text{términos de grado } \geq 2 \\ \equiv \quad & x \pmod{x^2}. \end{aligned}$$

Supongamos que hemos construido i_{n-1} de tal modo que

$$f(i_{n-1}(x)) \equiv x \pmod{x^n}.$$

Queremos construir i_n tal que

$$i_n(x) \equiv i_{n-1}(x) \pmod{x^n},$$

es decir, queremos encontrar $\lambda \in A$ tal que

(1) $$i_n(x) = i_{n-1}(x) + \lambda x^n$$

y también

(2) $$f(i_n(x)) \equiv x \pmod{x^{n+1}}.$$

Substituyendo (1) en (2) y calculando, obtenemos

$$\begin{aligned} f(i_n(x)) \quad & f(i_{n-1}(x) + \lambda x^n) \\ - \quad & f(i_{n-1}(x)) + a_1 \lambda x^n \ (\text{mód } x^{n+1}) \\ - \quad & x + \gamma x^n + a_1 \lambda x^n \ (\text{mód } x^{n+1}) \\ - \quad & x + (\gamma + a_1 \lambda) x^n \ (\text{mód } x^{n+1}) \end{aligned}$$

para algún $\gamma \in A$, por hipótesis de inducción. Tomando $\lambda = -\gamma/a_1 \in A$ (recuérdese que a_1 es invertible) se tiene que

$$f(i_n(x)) \equiv x \ (\text{mód } x^{n+1}).$$

Finalmente, como $f(i(x)) = x$, entonces $i(f(i(x))) = i(x)$, la cual es una identidad en el anillo $A[[x]]$, y por lo tanto $i(f(x)) = x$.

Para mostrar la unicidad de $i(x)$ tal que

$$i(f(x)) = x \qquad \text{y} \qquad f(i(x)) = x,$$

sea $h \in A[[x]]$ tal que $f(h(x)) = x$ y $h(f(x)) = x$. Entonces,

$$i(x) = i(f(h(x))) = if(h(x)) = h(x)$$

ya que $if(x) = x$. □

Proposición 3.3 (Existencia de inversa formal). *Si $\mathcal{F} \in A[[x, y]]$ es un grupo formal, entonces existe una única serie $i_{\mathcal{F}}(x) \in A[[x]]$ tal que*

$$\mathcal{F}(x, i_{\mathcal{F}}(x)) = 0 = \mathcal{F}(i_{\mathcal{F}}(x), x).$$

DEMOSTRACIÓN. Sea $g(x, y) := x - \mathcal{F}(x, y)$ y veamos a g como una serie de potencias en y. Obsérvese que g tiene término constante igual a cero (aun como serie de potencias en y, pues hemos eliminado a la x que estaba sola). La serie $g(y) = \sum_{n=1} a_n y^n$, con $a_n \in A[[x]]$, tiene término $a_1 = -1 \in A^*$ y así, y por el lema previo, g es invertible, esto es, existe una única $h(x, y) \in A[[x, y]]$ tal que $g(x, h(x, y)) = y = h(x, g(x, y))$; puesto que $g(x, y) = x - \mathcal{F}(x, y)$, la identidad anterior se trasforma en

$$\mathcal{F}(x, h(x, y)) = x - y,$$

de donde, al tomar $y = x$, obtenemos

$$\mathcal{F}(x, h(x, x)) = 0,$$

con lo que la proposición queda demostrada si definimos

$$i_{\mathcal{F}}(x) = h(x, x).$$

□

Ejemplo 3. Sea $\mathcal{F}(x, y) = x + y$ el grupo formal aditivo $\mathbb{G}_a$. En este caso, su inversa formal claramente es

$$i_{\mathbb{G}_a}(x) := -x.$$

Ejemplo 4. Sea $\mathcal{F}(x, y) = x + y + xy = (1 + x)(1 + y) - 1$ el grupo formal multiplicativo $\mathbb{G}_m$. Su inversa formal es

$$i_{\mathbb{G}_m}(x) := -x + x^2 - x^3 + x^4 - x^5 + \cdots$$

Definición 3.4. Sean $\mathcal{F}$, $\mathcal{G}$ grupos formales sobre A. Un *morfismo de grupos formales* $f : \mathcal{F} \to \mathcal{G}$ es una serie de potencias $f \in A[[x]]$ con término constante igual a cero y tal que

$$f(\mathcal{F}(x, y)) = \mathcal{G}(f(x), f(y)).$$

Denotemos por $\mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ al conjunto de morfismos $f : \mathcal{F} \to \mathcal{G}$. Más adelante demostraremos que, con una operación natural, este conjunto es un grupo abeliano.

Ejemplo 5. Sea $\mathcal{F}$ un grupo formal sobre A. Podemos definir homomorfismos

$$[m] : \mathcal{F} \longrightarrow \mathcal{F}$$

para $m \in \mathbb{Z}$ mediante

$$[0]T = 0$$

$$[m + 1]T = \mathcal{F}([m]T, T)$$

$$[m - 1]T = \mathcal{F}([m]T, i(T)).$$

Demostraremos por inducción que $[m]$ es un homomorfismo para toda $m \in \mathbb{Z}$ (llamado *multiplicación por m*): en primer lugar, observemos que el término constante de la serie $[m]$ es cero para toda $m \in \mathbb{Z}$. Claramente, $[0]$ es un morfismo de grupos pues

$$[0](\mathcal{F}(x, y)) := 0 = \mathcal{F}(0, 0) = \mathcal{F}([0]x, [0]y).$$

Sea $m \geq 0$ y supongamos que $[m]$ es un morfismo de grupos formales, es decir, supongamos que

$$[m](\mathcal{F}(x, y)) = \mathcal{F}([m]x, [m]y).$$

Entonces,

$$\begin{aligned}
[m+1](\mathcal{F}(x,y)) \ &.\!- \ \mathcal{F}([m](\mathcal{F}(x,y)), \mathcal{F}(x,y)) \quad \text{por definición de } [m+1] \\
&\quad \mathcal{F}(\mathcal{F}([m]x, [m]y), \mathcal{F}(x,y)) \quad \text{por hipótesis de inducción} \\
&= \ \mathcal{F}([m]x, \mathcal{F}([m]y, \mathcal{F}(x,y))) \quad \text{asociatividad de } \mathcal{F} \\
&\quad \mathcal{F}([m]x, \mathcal{F}([m]y, \mathcal{F}(y,x))) \quad \text{conmutatividad de } \mathcal{F} \\
&= \ \mathcal{F}([m]x, \mathcal{F}(\mathcal{F}([m]y, y), x)) \quad \text{asociatividad} \\
&\quad \mathcal{F}([m]x, \mathcal{F}([m+1]y, x)) \quad \text{definición de } [m+1] \\
&\quad \mathcal{F}([m]x, \mathcal{F}(x, [m+1]y)) \quad \text{conmutatividad} \\
&\quad \mathcal{F}(\mathcal{F}([m]x, x), [m+1]y)) \quad \text{asociatividad} \\
&.\!- \ \mathcal{F}([m+1]x, [m+1]y) \quad \text{definición de } [m+1]
\end{aligned}$$

Si $m \leq 0$, se procede de manera análoga.

Obsérvese que

$$[m]T = mT + \text{ elementos de orden superior,}$$

ya que para $m \geq 0$ es trivial usando inducción sobre m y el hecho de que $F(x, y) = x + y + \cdots$. Ahora, como $i(T) = -T + \cdots$, entonces la afirmación es cierta para $m < 0$ por inducción descendente. También, si $m \in A^*$, entonces $[m]$ es un isomorfismo por (3.2) con inversa $[m^{-1}]$.

A continuación mostraremos que el conjunto $\mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ de morfismos entre dos grupos formales es un grupo abeliano, y en el caso particular cuando $\mathcal{F} = \mathcal{G}$ mostraremos que $\mathrm{End}_A(\mathcal{F}) := \mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ es un anillo, llamado el *anillo de endomorfismos* del grupo formal $\mathcal{F}$. La operación de grupo en $\mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ se define como sigue: sean $f, g \in \mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ (recuérdese que entonces tienen término constante 0); ponemos

$$f +_{\mathcal{G}} g := \mathcal{G}(f(x), g(x)).$$

Ahora, si $f, g \in \mathrm{End}_A(\mathcal{F}) := \mathrm{Hom}_A(\mathcal{F}, \mathcal{F})$, entonces definimos

$$f \circ g := f(g(x)).$$

Proposición 3.5. *Sean $\mathcal{F}$, $\mathcal{G}$ dos grupos formales sobre un anillo A. Entonces:*

(1) $\mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ *es un grupo abeliano con la operación* $+_{\mathcal{G}}$ *definida arriba.*

(2) $\mathrm{End}_A(\mathcal{F})$ *es un anillo con las operaciones* $+_{\mathcal{G}}$ *y* $\circ$.

DEMOSTRACIÓN. (1): Observemos para comenzar que, por las propiedades que definen el grupo formal $\mathcal{G}$, la operación $+_{\mathcal{G}}$ vuelve al conjunto de series formales en una indeterminada con término constante cero $xA[[x]]$ un grupo abeliano. En particular,

$$f +_{\mathcal{G}} (i_{\mathcal{G}} \circ f) = 0.$$

Mostraremos que $\mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ es un subgrupo de $(xA[[x]], +_{\mathcal{G}})$. Debemos entonces mostrar que dados $f, g \in \mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ entonces $f +_{\mathcal{G}} g \in \mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$. Para esto, pongamos $h := f +_{\mathcal{G}} g$. Entonces

$$\begin{aligned} h(\mathcal{F}(x, y)) \quad .- \quad & \mathcal{G}(f(\mathcal{F}(x, y)), g(\mathcal{F}(x, y))) \\ & \mathcal{G}(\mathcal{G}(f(x), f(y)), \mathcal{G}(g(x), g(y))). \end{aligned}$$

Y (simbólicamente) esta última serie se puede escribir como

$$(f(x) +_{\mathcal{G}} f(x)) +_{\mathcal{G}} (g(y) +_{\mathcal{G}} g(y))$$

y la asociatividad y conmutatividad de $(xA[[x]], +_{\mathcal{G}})$ nos permiten escribir esta última serie como

$$(\dagger) \qquad (f(x) +_{\mathcal{G}} g(x)) +_{\mathcal{G}} (f(y) +_{\mathcal{G}} g(y)),$$

es decir, como $\mathcal{G}(h(x), h(y))$. Formalmente, lo que queremos decir es que las operaciones que llevan $(*)$ en $(\dagger)$ también llevan $\mathcal{G}(\mathcal{G}(f(x), f(y)), \mathcal{G}(g(x), g(y)))$ en $\mathcal{G}(h(x), h(y))$. Esto prueba que $h \in \mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$.

Similarmente se demuestra que $i_{\mathcal{G}} \circ f \in \mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ y como $0 \in \mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$, esto termina la demostración de que $\mathrm{Hom}_A(\mathcal{F}, \mathcal{G})$ es un subgrupo de $(xA[[x]], +_{\mathcal{G}})$.

(2): El *neutro multiplicativo* de $\mathrm{End}_A(\mathcal{F})$ es la serie x.

Asociatividad: En general, $(f_1 f_2) \circ g = (f_1 \circ g)(f_2 \circ g)$ y así $f^n \circ g = (f \circ g)^n$. Se sigue que, cuando $f = x^n$,

$$f \circ (g \circ h) = (g \circ h)^n = (f \circ g) \circ h.$$

Entonces, para $f = \sum a_i x^i$ se tiene que

$$f \circ (g \circ h) = \sum a_i (g \circ h)^i = (f \circ g) \circ h.$$

Distributividad: Dados $f, g, h \in \mathrm{End}_A(\mathcal{F})$:

$$\begin{aligned} f \circ (g +_{\mathcal{F}} h) &\cdots f(\mathcal{F}(g(x), h(y))) \\ &\quad \mathcal{F}((f \circ g)(x), (f \circ h)(y)) \\ &= f \circ g +_{\mathcal{F}} f \circ h. \end{aligned}$$

□

3.2 Grupos asociados a grupos formales

Hasta ahora, un grupo formal es como una sonrisa sin un gato de Cheshire, esto es, hasta aquí un grupo formal es simplemente una operación de grupo, sin grupo subyacente alguno. Pero si el anillo A es el *anillo de enteros* $\mathcal{O}_K$ de un *campo valuado discreto completo* K, y si las variables x y y toman valores en el ideal máximo $\mathfrak{p}_K$ de $\mathcal{O}_K$, entonces la serie de potencias

$$\mathcal{F}(x, y) = \sum_{i,j \geq 0} a_{ij} x^i y^j, \quad a_{ij} \in \mathcal{O}_K,$$

de la ley de grupo formal, converge en $\mathcal{O}_K$, ya que como $|a_{ij}|_v \leq 1$ (donde v es la valuación asociada al campo K) y como $x, y \in \mathfrak{p}_K$ (y por lo tanto $|x|_v < 1$ y $|y|_v < 1$), entonces $|a_{ij} x^i y^j|_v \leq |x^i y^j|_v < 1$ y por lo tanto $a_{ij} x^i y^j \to 0$ cuando $i, j \to \infty$. Como la valuación es no arquimediana, esto implica que la serie $(*)$ converge y como $\mathcal{O}_K$ es completo,

$$\sum_{i,j \geq 0} a_{ij} x^i y^j \in \mathcal{O}_K$$

(de hecho en $\mathfrak{p}_K$). De manera análoga, la serie formal $i_{\mathcal{F}}(x) \in \mathcal{O}_K[[x]]$ converge en $\mathcal{O}_K$ (de hecho en $\mathfrak{p}_K$) si $x \in \mathfrak{p}_K$. En esta sección estudiaremos algunos grupos que se obtienen de este modo.

Definición 3.6. Sea $\mathcal{O}_K$ el anillo de enteros de un campo valuado discreto completo K, $\mathfrak{p}_K$ su ideal máximo y K su campo residual $\mathcal{O}_K/\mathfrak{p}_K$. Sea $\mathcal{F}$ un grupo formal conmutativo. El *grupo asociado* a $\mathcal{F}$, denotado $\mathcal{F}(\mathfrak{p}_K)$, es el conjunto $\mathfrak{p}_K$ con las operaciones de grupo:

(i) $x +_{\mathcal{F}} y := \mathcal{F}(x, y)$ para $x, y \in \mathfrak{p}_K$.

(ii) $-_{\mathcal{F}} x := i_{\mathcal{F}}(x)$ para $x \in \mathfrak{p}_K$.

Observe que, como $(\mathcal{O}_K, \mathfrak{p}_K)$ es completo y $x, y \in \mathfrak{p}_K$, entonces $x +_{\mathcal{F}} y \in \mathcal{O}_K$ y $-_{\mathcal{F}} x \in \mathcal{O}_K$, y de hecho $x +_{\mathcal{F}} y \in \mathfrak{p}_K$ y $-_{\mathcal{F}} x \in \mathfrak{p}_K$ ya que, por ejemplo, $v(x+_{\mathcal{F}} y) = v(\mathcal{F}(x, y)) < 1$. La asociatividad de $+_{\mathcal{F}}$ se sigue de la asociatividad de $\mathcal{F}$. El neutro de $+_{\mathcal{F}}$ es la serie $0 \in \mathcal{O}_K[[x, y]]$, $\mathcal{F}(x, 0) = \mathcal{F}(0, x) = 0$, por lo que $x +_{\mathcal{F}} 0 = 0 +_{\mathcal{F}} x = 0$. El inverso de $x \in \mathcal{F}(\mathfrak{p}_K)$ es $-_{\mathcal{F}} x \in \mathcal{F}(\mathfrak{p}_K)$, ya que $x +_{\mathcal{F}} (-_{\mathcal{F}} x) = F(x, i(x)) = 0$.

Si $\mathcal{F}$ es conmutativo, entonces $\mathcal{F}(\mathfrak{p}_K)$ también lo es.

Del mismo modo, para $n \geq 1$, $\mathcal{F}(\mathfrak{p}_K^n)$ es el subgrupo de $\mathcal{F}(\mathfrak{p}_K)$ que se obtiene al restringir las operaciones al conjunto $\mathfrak{p}_K^n$.

Ejemplo 6. El grupo aditivo $\mathbb{G}_a(\mathfrak{p}_K)$ es simplemente $\mathfrak{p}_K$ con la ley de adición usual. Se tiene la sucesión exacta de grupos aditivos $(K = \mathcal{O}_K/\mathfrak{p}_K)$:

$$0 \longrightarrow \mathbb{G}_a(\mathfrak{p}_K) \longrightarrow \mathcal{O}_K \longrightarrow K \longrightarrow 0.$$

Ejemplo 7. El grupo multiplicativo $\mathbb{G}_m(\mathfrak{p}_K)$ es el grupo de 1-unidades, es decir

$$\mathbb{G}_m(\mathfrak{p}_K) = \mathfrak{p}_K \simeq 1 + \mathfrak{p}_K = U_K^{(1)}$$
$$x \mapsto 1 + x,$$

con la multiplicación usual, es decir, si $x, y \in \mathbb{G}_m(\mathfrak{p}_K) = \mathfrak{p}_K \simeq 1+\mathfrak{p}_K$, entonces

$$\begin{aligned} x +_{\mathcal{F}} y &:= F(x, y) = (1 + x)(1 + y) - 1 = x + y + xy \in \mathfrak{p}_K \\ &= (1 + x)(1 + y) \in 1 + \mathfrak{p}_K \end{aligned}$$

con neutro $0 \mapsto 1 + 0 \in 1 + \mathfrak{p}_K$. Se tiene la sucesión exacta de grupos multiplicativos:

$$0 \longrightarrow \mathbb{G}_m(\mathfrak{p}_K) \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \longrightarrow 0.$$

Proposición 3.7. *Sean $\mathcal{O}_K$ el anillo de enteros de un campo valuado discreto completo K y $\mathcal{F}$ un grupo formal sobre $\mathcal{O}_K$. Entonces,*

(1)*: Para toda $n \geq 1$, la función*

$$\mathcal{F}(\mathfrak{p}_K^n)/\mathcal{F}(\mathfrak{p}_K^{n+1}) \longrightarrow \mathfrak{p}_K^n/\mathfrak{p}_K^{n+1},$$

inducida por la identidad en los conjuntos subyacentes, es un isomorfismo de grupos.

(2): *Sea* $p = \text{car}\,(K)$ *(posiblemente* $= 0$*). Entonces todo elemento de torsión de* $\mathcal{F}(\mathfrak{p}_K)$ *tiene orden una potencia de* p.

DEMOSTRACIÓN. (1): Como los conjuntos subyacentes son iguales y la función es biyectiva, basta demostrar que f es un homomorfismo. Pero dados $x, y \in \mathfrak{p}_K^n$ se tiene

$$x +_{\mathcal{F}} y = \mathcal{F}(x, y) = x + y + xy\, g(x, y) \equiv x + y \,(\text{mód } \mathfrak{p}_K^{2n}),$$

y por lo tanto

$$x +_{\mathcal{F}} y \equiv x + y \,(\text{mód } \mathfrak{p}_K^{n+1}).$$

(2): Basta demostrar que no hay elementos de torsión $x \neq 0$ de orden primo a p, porque si $\text{ord}(x) = bp^q$ con $\text{mcd}(b, p) = 1$, entonces $\text{ord}(x^{p^q}) = b$ implica que $x^{p^q} = 0$.

Ahora, sea $m \geq 1$ primo relativo a p (m es arbitrario si $p = 0$) y $x \in \mathcal{F}(\mathfrak{p}_K)$ un elemento tal que $[m](x) = 0$. Como m es primo a p, entonces $m \notin \mathfrak{p}_K$ y por lo tanto $[m]$ es un isomorfismo de $\mathcal{F}$ en sí mismo, y así induce un isomorfismo

$$[m] : \mathcal{F}(\mathfrak{p}_K) \xrightarrow{\simeq} \mathcal{F}(\mathfrak{p}_K),$$

en particular $x \in \text{Ker}\,[m] = 0$. □

3.3 Grupos formales de Lubin-Tate

En esta sección, $A = \mathcal{O}_K$ es el anillo de enteros de un campo local K, π es un elemento primo de $\mathcal{O}_K$ y $q = |K|$ es el cardinal del campo residual correspondiente. Consideremos el subconjunto $\mathcal{F}_\pi \subseteq \mathcal{O}_K[[x]]$ de series $f(x)$ que satisfacen:

(i) $f(x) = \pi x +$ términos de grado ≥ 2

y

(ii) $f(x) \equiv x^q \,(\text{mód } \pi)$.

Ejemplo 8. El polinomio $f(x) = \pi x + x^q$ está en $\mathcal{F}_\pi$.

Ejemplo 9. Si $K = \mathbb{Q}_p$ y $\pi = p$, entonces el polinomio

$$f(x) = (1 + x)^p - 1 = px + \binom{p}{2} x^2 + \cdots + px^{p-1} + x^p$$

está en $\mathcal{F}_p$.

Mostraremos que para cualquier $f \in \mathcal{F}_\pi$ existe una ley de grupo formal $\mathcal{F}_f$ sobre $\mathcal{O}_K$ que admite a f como un endomorfismo; estos grupos formales $\mathcal{F}_f$ se llaman los *grupos formales de Lubin-Tate*. Antes necesitaremos el resultado siguiente:

Lema 3.8. *Sean $f, g \in \mathcal{F}_\pi$ y sea $L(x_1, \ldots, x_n) = \sum_{i=1} a_i x_i$ una forma lineal con coeficientes en $\mathcal{O}_K$. Entonces, existe una única serie de potencias $F(x_1, \ldots, x_n)$ en $\mathcal{O}_K[[x_1, \ldots, x_n]]$ tal que*

$$F(x_1, \ldots, x_n) = L(x_1, \ldots, x_n) + \text{términos de grado} \geq 2$$

y

$$f(F(x_1, \ldots, x_n)) = F(g(x_1), \ldots, g(x_n)).$$

DEMOSTRACIÓN. La serie que queremos se puede escribir como

$$F(x_1, \ldots, x_n) = \sum_{j=1}^{\infty} E_j(x_1, \ldots, x_n) \in \mathcal{O}_K[x_1, \ldots, x_n],$$

donde los $E_j(x_1, \ldots, x_n)$ son polinomios homogéneos de grado j. Poniendo

$$F_r(x_1, \ldots, x_n) := \sum_{j=1}^{r} E_j(x_1, \ldots, x_n),$$

la serie $F(x_1, \ldots, x_n)$ será la que deseamos si satisface que

$$\begin{aligned} F_1(x_1, \ldots, x_n) &= L(x_1, \ldots, x_n) \\ f(F_r(x_1, \ldots, x_n) &\equiv F_r(g(x_1), \ldots, g(x_n)) + \text{términos de grado} \geq r+1. \end{aligned}$$

Probaremos por inducción sobre r la existencia y unicidad de los polinomios E_r. Para $r = 1$, el único candidato es el polinomio $E_1 = L$; ciertamente satisface la primera condición y escribiendo $L = \sum a_i x_i$, la segunda condición pide que

$$\pi(\sum a_i x_i) = \sum a_i(\pi x_i) + \text{términos de grado} \geq 2,$$

lo cual es verdadero. Supongamos que hemos encontrado los polinomios únicos $E_1, \ldots, E_r$ de tal forma que satisfagan las dos condiciones anteriores. Como

$$F_{r+1} = F_r + E_{r+1}$$

donde E_{r+1} es un polinomio homogéneo de grado $r+1$ que estamos buscando, y como se debe satisfacer la condición

$$(*) \qquad f(F_{r+1}(x_1, \ldots, x_n)) \equiv F_{r+1}(g(x_1), \ldots, g(x_n)) \text{ mód gr } (r+2)$$

para $F_{r+1} = F_r + E_{r+1}$, si notamos que el lado izquierdo de $(*)$ es

$$f(F_{r+1}(x_1, \ldots, x_n)) \equiv f(F_r(x_1, \ldots, x_n)) + \pi(E_{r+1}(x_1, \ldots, x_n)) \text{ mód } \mathrm{gr}(r+2),$$

mientras que el lado derecho de $(*)$ es

$$\begin{aligned} F_{r+1}(g(x_1), \ldots, g(x_n)) \equiv\ & F_r(g(x_1), \ldots, g(x_n)) \\ & + E_{r+1}(\pi x_1, \ldots, \pi x_n) \text{ mód gr } (r+2) \\ & - F_r(g(x_1), \ldots, g(x_n)) \\ & + \pi^{r+1} E_{r+1}(x_1, \ldots, x_n) \text{ mód gr } (r+2) \end{aligned}$$

(la última igualdad porque E_{r+1} es homogéneo de grado $r+1$). Se sigue que lo que queremos en la igualdad $(*)$ es

$$\begin{aligned} f(F_r(x_1, \ldots, x_n)) + \pi(E_{r+1}(x_1, \ldots, x_n)) = {} & F_r(g(x_1), \ldots, g(x_n)) \\ & + \pi^{r+1} E_{r+1}(x_1, \ldots, x_n) \\ & + \text{términos de grado } \geq (r+2), \end{aligned}$$

i.e., que

$$\begin{aligned} (\pi^{r+1} - \pi) E_{r+1}(x_1, \ldots, x_n) \qquad & f(F_r(x_1, \ldots, x_n)) \\ & - F_r(g(x_1), \ldots, g(x_n)) \text{ mód gr } (r+2), \end{aligned}$$

y por lo tanto E_{r+1} debe ser el único polinomio que satisface

$$E_{r+1}(x_1, \ldots, x_n) \equiv \frac{f(F_r(x_1, \ldots, x_n)) - F_r(g(x_1), \ldots, g(x_n))}{\pi(\pi^r - 1)} \text{ mód gr } (r+2).$$

Notemos ahora que, como la característica del campo residual K es p y como q es una potencia de p, entonces

$$f \circ F_r - F_r \circ g \equiv F_r(x_1, \ldots, x_n)^q - F_r(x_1^q, \ldots, x_n^q) \equiv 0 \text{ mód } (\pi).$$

Ahora, como π divide a $f \circ F_r - F_r \circ g$ y $\pi^r - 1 \in U_K^{(r)}$ es una unidad de $\mathcal{O}_K$, entonces E_{r+1} tiene coeficientes en $\mathcal{O}_K$ y como F_r satisface la hipótesis de inducción, entonces E_{r+1} debe ser un polinomio de grado $r+1$ y así este E_{r+1} nos sirve. □

Teorema 3.9. *Sean K un campo local, $\mathcal{O}_K$ su anillo de enteros y π un elemento primo de K. Para cualquier $f \in \mathcal{F}_\pi$ existe un único grupo formal conmutativo $\mathcal{F}_f$ sobre $\mathcal{O}_K$ que admite a f como un endomorfismo.*

DEMOSTRACIÓN. Por el lema anterior existe una única serie de potencias $\mathcal{F}_f(x, y)$ tal que

$$\begin{aligned} \mathcal{F}_f(x, y) &= x + y \mod (x^2) \\ f(\mathcal{F}_f(x, y)) &= \mathcal{F}_f(f(x), f(y)). \end{aligned}$$

Resta demostrar que $\mathcal{F}_f(x, y)$ es un grupo formal conmutativo:

Conmutatividad: Pongamos $G(x, y) := \mathcal{F}_f(y, x)$; entonces claramente G satisface las conclusiones del lema anterior y así, por unicidad, $G = \mathcal{F}_f$, es decir

$$\mathcal{F}_f(x, y) = \mathcal{F}_f(y, x).$$

Asociatividad: Consideremos las series siguientes $G_1(x, y, z) := \mathcal{F}_f(x, \mathcal{F}_f(y, z))$ y $G_2(x, y, z) := \mathcal{F}_f(\mathcal{F}_f(x, y), z)$; entonces los G_i satisfacen el lema anterior y así, por unicidad, deben ser iguales, i.e.,

$$\mathcal{F}_f(x, \mathcal{F}_f(y, z)) = \mathcal{F}_f(\mathcal{F}_f(x, y), z).$$

□

Definición 3.10. Sean K un campo local, $\mathcal{O}_K$ su anillo de enteros y π un elemento primo de K. Sea $f \in \mathcal{F}_\pi$. El grupo formal $\mathcal{F}_f$ del teorema anterior se llama el *grupo formal de Lubin-Tate* con endomorfismo f.

Nótese que los grupos formales de Lubin-Tate son los grupos formales que admiten un endomorfismo el cual al reducirlo módulo el primo $\mathfrak{p}_K = \pi\mathcal{O}_K$ es el Frobenius $x \mapsto x^q$ y además su derivada en el origen es el primo π de K.

Ejemplo 10. Sean $K = \mathbb{Q}_p$ y $\pi = p$; entonces $f(x) = (1 + x)^p - 1 \in \mathcal{F}_p$ y el grupo formal de Lubin-Tate asociado es $\mathcal{F}(x, y) = \mathbb{G}_m(x, y)$, ya que f es un endomorfismo de $\mathbb{G}_m$ porque

$$\mathbb{G}_m(f(x), f(y)) = (1 + x)^p(1 + y)^p - 1 = f(\mathbb{G}_m(x, y)).$$

Proposición 3.11. *Sean $f, g \in \mathcal{F}_\pi$ y $a \in \mathcal{O}_K$. Sea $[a]_{g,f}$ el único elemento de $\mathcal{O}_K[[x]]$ determinado por* (3.8) *tal que:*

$$\begin{aligned} [a]_{g,f}(x) &= ax \mod (x^2) \\ g \circ [a]_{g,f} &= [a]_{g,f} \circ f. \end{aligned}$$

Entonces $[a]_{g,f} \in \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{F}_f, \mathcal{F}_g)$.

DEMOSTRACIÓN. El lema (3.8) garantiza la existencia de la serie $h =: [a]_{g,f}$. Debemos mostrar que

$$h(\mathcal{F}_f(x, y)) = \mathcal{F}_g(h(x), h(y)).$$

Claramente, para el término lineal de cada uno de los lados de esta supuesta igualdad se tiene en efecto la igualdad. Más aún,

$$h(\mathcal{F}_f(f(x), f(y)) = (h \circ f)(\mathcal{F}_f(x, y)) = g(h(\mathcal{F}(x, y)))$$

y

$$\mathcal{F}_g((h(f(x)), h(f(y)) = \mathcal{F}_g(g(h(x)), g(h(y))) = g((\mathcal{F}_g(h(x), h(y)));$$

por lo tanto, podemos aplicar la unicidad del lema previo. □

Proposición 3.12. *Para toda $a, b \in \mathcal{O}_K$ se tiene que*

$$[a + b]_{g,f} = [a]_{g,f} + [b]_{g,f}$$

y

$$[ab]_{g,f} = [a]_{g,f}[b]_{g,f}.$$

DEMOSTRACIÓN. En cada caso la serie de potencias de la derecha satisface las condiciones que caracterizan la serie de la izquierda. El resultado se sigue del lema (3.8) previo. □

Corolario 3.13. *Sean $f, g \in \mathcal{F}_\pi$. Entonces $\mathcal{F}_f \simeq \mathcal{F}_g$.*

DEMOSTRACIÓN. Para cualquier $u \in \mathcal{O}_K^*$ se tiene que $[u]_{f,g}$ y $[u^{-1}]_{g,f}$ son isomorfismos inversos uno del otro, i.e.,

$$[u]_{f,g} \circ [u^{-1}]_{g,f} = [1]_{g,f} = [u^{-1}]_{g,f} \circ [u]_{f,g}.$$

□

Corolario 3.14. *Sea $f \in \mathcal{F}_\pi$. Para cada $a \in \mathcal{O}_K$ existe un único endomorfismo $[a]_f := [a]_{f,f} : \mathcal{F}_\pi \to \mathcal{F}_\pi$ tal que*

$$[a]_f(x) = ax \text{ mód } (x^2)$$

y $[a]_f$ conmuta con el endomorfismo $f : \mathcal{F}_\pi \to \mathcal{F}_\pi$, i.e.,

$$[a]_f(f(x)) = f([a]_f(x)).$$

Más aún, la función

$$\mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K}(\mathcal{F}_f) \qquad a \mapsto [a]_f(x)$$

es un morfismo de anillos.

En el caso cuando $a = \pi \in \mathcal{O}_K$ *es el elemento primo, se tiene que* $[\pi]_f = f$. *En particular* $[\pi]_f(x) \equiv x^q$ mód (π), *donde* q *es el orden del campo residual* K.

DEMOSTRACIÓN. Para $a \in \mathcal{O}_K$, la serie $[a]_f(x) := [a]_{f,f}(x) = ax + \cdots$ es la única serie que conmuta con f y es un endomorfismo de $\mathcal{F}_f$. Que la función $a \mapsto [a]_f(x)$ es un morfismo de anillos se sigue del lema previo y del hecho de que $[1]_f(x) = x$. La última afirmación se sigue de la observación de que $[\pi]_f(x) = \pi x$ mód $(x^2) = f(x)$ y la unicidad del endomorfismo de $\mathcal{F}_f$ que satisface esto. □

Ejemplo 11. Si $K = \mathbb{Q}_p$ y $f(x) = (1+x)^p - 1 \in \mathcal{F}_p$, entonces $\mathcal{F}_f(x, y) = x + y + xy$ como vimos antes. Ahora, para cualquier $a \in \mathbb{Z}_p$, definimos

$$(1+x)^a := \sum_{n \geq 0} \binom{a}{n} x^n$$

donde

$$\binom{a}{n} := \frac{a!}{n!(a-n)!}$$

si $a \geq 0$ en $\mathbb{Z}$. Y si $\{s_i\}_{i \geq 1}$ es una sucesión de enteros que converge a $a \in \mathbb{Z}_p$ (por (1.16)(1) y el ejemplo 11 después de (1.16), $a \in \mathbb{Z}_p$ es límite de una sucesión de sumas parciales $\{s_i\}_{i \geq 1}$ de enteros no negativos), entonces

$$\lim_{i \to \infty} \binom{s_i}{n} =: \binom{a}{n}$$

y por lo tanto $\binom{a}{n} \in \mathbb{Z}_p$. Mostraremos ahora que

$$[a]_f(x) = (1+x)^a - 1.$$

En efecto, $(1+x)^a - 1 = ax + \cdots$ y por lo tanto, cuando $a \in \mathbb{Z}$,

$$f \circ ((1+x)^a - 1) = (1+x)^{pa} - 1 = ((1+x)^a - 1) \circ f$$

y así, por continuidad, la igualdad anterior es válida para todo $a \in \mathbb{Z}_p$.

Definición 3.15. Sea $f \in \mathcal{F}_\pi$. El morfismo de anillos del corolario (3.14)

$$\mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K}(\mathcal{F}_f) \qquad a \mapsto [a]_f(x)$$

decimos que da al grupo formal de Lubin-Tate $\mathcal{F}_f$ la estructura de $\mathcal{O}_K$-*módulo formal* y decimos que $\mathcal{F}_f$ es un $\mathcal{O}_K$-*módulo formal de Lubin-Tate*. Nótese que este morfismo satisface que

$$[\pi]_f(x) \equiv x^q \text{ mód } (\pi),$$

donde q es el cardinal del campo residual de K.

3.4 Campos de Lubin-Tate

Si $\mathcal{F}$ es un $\mathcal{O}_K$-módulo formal, escogiendo un dominio donde las series converjan, por ejemplo tomando $\mathfrak{p}_K$, se obtiene un $\mathcal{O}_K$-módulo $\mathcal{F}(\mathfrak{p}_K)$ en el sentido usual. En particular, elegiremos como dominio de convergencia de la serie $\mathcal{F}$ al ideal máximo $\mathfrak{p}_{K^{al}}$ del anillo de enteros $\mathcal{O}_{K^{al}}$ de una cerradura algebraica K^{al} de K. Nótese que la valuación v_K de K se extiende de manera única a cualquier subcampo $L \subseteq K^{al}$ de grado finito sobre K y por lo tanto, usando el lema de Zorn, se extiende a K^{al} y es así como consideramos su ideal máximo $\mathfrak{p}_{K^{al}}$ anterior. Se tiene entonces que:

Proposición 3.16. *Si $\mathcal{F}$ es un $\mathcal{O}_K$-módulo formal entonces $\mathcal{F}(\mathfrak{p}_{K^{al}})$ es un $\mathcal{O}_K$-módulo, en el sentido usual, con las operaciones*

$$x +_{\mathcal{F}} y := \mathcal{F}(x, y) \qquad \text{y} \qquad a \cdot x := [a]_{\mathcal{F}}(x),$$

para $x, y \in \mathfrak{p}_{K^{al}}$.

Similarmente, si $f : \mathcal{F} \to \mathcal{G}$ es un morfismo (isomorfismo) de $\mathcal{O}_K$-módulos formales, entonces

$$f : \mathcal{F}(\mathfrak{p}_{K^{al}}) \longrightarrow \mathcal{G}(\mathfrak{p}_{K^{al}})$$

es un morfismo (isomorfismo) de $\mathcal{O}_K$-módulos.

□

Definición 3.17. Sea $\mathcal{F} \in \mathcal{F}_\pi$ un módulo de Lubin-Tate para un elemento primo π de $\mathcal{O}_K$. El *grupo de puntos de división π^n-ésimos* es el grupo

$$\mathcal{F}(n) := \{\alpha \in \mathfrak{p}_{K^{al}} \ : \ \pi^n \cdot \alpha = 0\} = \text{Ker}\,([\pi^n]).$$

Claramente, $\mathcal{F}(n)$ es un $\mathcal{O}_K$-submódulo de $\mathcal{F}(\mathfrak{p}_{K^{al}})$ y como es aniquilado por $\pi^n\mathcal{O}_K$, entonces es un $\mathcal{O}_K/\pi^n\mathcal{O}_K$-módulo.

Proposición 3.18. *El $\mathcal{O}_K$-módulo $\mathcal{F}(n)$ es isomorfo a $\mathcal{O}_K/\pi^n\mathcal{O}_K$.*

DEMOSTRACIÓN. Como todos los módulos de Lubin-Tate para π son isomorfos, podemos suponer que $\mathcal{F}_f = \mathcal{F}_e$ donde $e(x) := x^q + \pi x = [\pi]_{\mathcal{F}}(x)$. Entonces $\mathcal{F}(n)$ es el conjunto de raíces en K^{al} del polinomio iterado:

$$e^{(n)} := \overbrace{e \circ \cdots \circ e}^{n},$$

ya que

$$\begin{aligned} e \circ e(x) &= e(e(x)) = e(\pi x + x^q) \\ &\quad \pi(\pi x + x^q) + (\pi x + x^q)^q \\ &\quad \pi^2 x + \pi x^q + \pi^q x^q + x^{q^2} \\ &\quad [\pi^2]_{\mathcal{F}}(x), \end{aligned}$$

y por inducción se prueba que

$$e^{(n)} := \overbrace{e \circ \cdots \circ e}^{} = [\pi^n]_{\mathcal{F}}(x).$$

El polinomio $e(x) = \pi x + x^q$ es un polinomio de Eisenstein y así tiene exactamente q raíces distintas y consecuentemente es separable. Por inducción se demuestra que el polinomio iterado $e^{(n)}(x)$ es separable y tiene q^n raíces.

Ahora, si $\alpha_n \in \mathcal{F}(n) - \mathcal{F}(n-1)$, entonces la acción de $\mathcal{O}_K$ en $\mathcal{F}(n)$

$$\mathcal{O}_K \longrightarrow \mathcal{F}(n)$$

dada por $a \mapsto a \cdot \alpha_n$ es un morfismo de $\mathcal{O}_K$-módulos con núcleo $\pi^n \mathcal{O}_K$ por definición de $\mathcal{F}(n)$. Se sigue que esta función induce un monomorfismo

$$\mathcal{O}_K/\pi^n \mathcal{O}_K \rightarrowtail \mathcal{F}(n),$$

el cual es un isomorfismo ya que ambos lados son finitos de orden q^n. □

Corolario 3.19. *Se tienen isomorfismos*

$$\mathcal{O}_K/\pi^n \mathcal{O}_K \xrightarrow{\simeq} \mathrm{End}_{\mathcal{O}_K}(\mathcal{F}(n))$$

y

$$U_K/U_K^{(n)} \xrightarrow{\simeq} \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{F}(n))$$

dados por $a \mapsto [a]_{\mathcal{F}}$.

DEMOSTRACIÓN. El primer isomorfismo es directo de la proposición previa y el segundo isomorfismo se obtiene tomando el grupo de unidades en el primer isomorfismo. □

Definición 3.20. Si $\mathcal{F}$ es un módulo de Lubin-Tate para el elemento primo π de $\mathcal{O}_K$, se define el *campo de puntos de división π^n-ésimos* o *campo de Lubin-Tate n-ésimo* mediante

$$K_{\pi,n} := K(\mathcal{F}(n)).$$

Observación. Se tienen inclusiones $\mathcal{F}(n) \subseteq \mathcal{F}(n+1)$ y así se tiene una torre de campos:

$$K \subseteq K_{\pi,1} \subseteq K_{\pi,2} \subseteq \cdots \subseteq K_{\pi,n} \subseteq \cdots \subseteq K_\pi := \bigcup_{n=1}^{\infty} K_{\pi,n}.$$

Algunas veces diremos que éstas son *extensiones de Lubin-Tate*.

Nótese que estas extensiones dependen sólo del primo π y no del módulo de Lubin-Tate $\mathcal{F}$ para π, ya que si $\mathcal{G}$ es otro módulo de Lubin-Tate para π por (3.13), existe un isomorfismo $f : \mathcal{F} \to \mathcal{G}$ con $f \in \mathcal{O}_K[[x]]$ y por lo tanto

$$\mathcal{G}(n) = f(\mathcal{F}(n)) \subseteq K(\mathcal{F}(n));$$

consecuentemente, $K(\mathcal{G}(n)) \subseteq K(\mathcal{F}(n))$. La otra inclusión se sigue por simetría.

Ahora, como vimos en la demostración de la proposición (3.18), $\mathcal{F}(n)$ es el conjunto de raíces en K^{al} del polinomio iterado:

$$e^{(n)} := \overbrace{e \circ \cdots \circ e}^{n}$$

por lo que la extensión $K_{\pi,n}/K$ es el campo de descomposición del polinomio $e^{(n)}(x) = [\pi^n]_{\mathcal{F}}(x)$.

Ejemplo 12. Sea $K = \mathbb{Q}_p$; entonces $\mathcal{O}_K = \mathbb{Z}_p$. Para el módulo de Lubin-Tate $\mathbb{G}_m$ se tiene que

$$e^{(n)}(x) = [p^n]_{\mathbb{G}_m}(x) = (1+x)^{p^n} - 1$$

y así el grupo de puntos de división p^n-ésimos $\mathbb{G}_m(n)$ es el grupo de raíces del polinomio $(1+x)^{p^n} - 1$, y por lo tanto, si $\lambda \in \mu_{p^n}$ es una raíz p^n-ésima de la unidad, entonces $\lambda - 1$ es una raíz de $(1+x)^{p^n} - 1$, y éstas son todas las p^n raíces de este polinomio. Se sigue que $\mathbb{G}_m(n)$ consiste de los elementos $\lambda - 1$, donde $\lambda \in \mu_{p^n}$ y por lo tanto la extensión de Lubin-Tate correspondiente $K_{\pi,n}/\mathbb{Q}_p$ es la extensión ciclotómica $K_{\pi,n} = \mathbb{Q}_p(\mathbb{G}_m(n)) = \mathbb{Q}_p(\mu_{p^n})$. El teorema siguiente muestra la analogía estrecha entre las extensiones de Lubin-Tate y las extensiones ciclotómicas (véase (2.68)). Antes necesitamos un lema:

Lema 3.21. *Sea L/K una extensión finita de Galois de campos locales con grupo de Galois $G = \mathrm{Gal}(L/K)$. Para cualquier $F \in \mathcal{O}_K[[x_1, \ldots, x_n]]$ y cualesquiera $\alpha_1, \ldots, \alpha_n$ en $\mathfrak{p}_L$ se tiene que*

$$F(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = \sigma F(\alpha_1, \ldots, \alpha_n)$$

para todo $\sigma \in G$.

DEMOSTRACIÓN. Si F es un polinomio, el resultado se sigue del hecho de que σ es un K-automorfismo de L y por lo tanto fija a $\mathcal{O}_K$.

Por otra parte, sabemos que en general σ preserva la valuación de L, i.e., $|\sigma(a)|_L = |a|_L$ para todo $a \in L$ y por lo tanto $\sigma : L \to L$ es continua y así preserva límites:

$$\lim_{m\to\infty}(a_m) = \ell \quad \text{implica} \quad \lim_{m\to\infty}(\sigma a_m) = \sigma(\ell).$$

Entonces, si escribimos la serie F como

$$F = F_m + \text{términos de grado} \geq m+1,$$

se tiene que

$$\begin{aligned}\sigma(F(a_1, \ldots, a_n)) &= \sigma(\lim_{m\to\infty} F_m(a_1, \ldots, a_n)) = \lim_{m\to\infty} \sigma F_m(a_1, \ldots, a_n) \\ &= \lim_{m\to\infty} F_m(\sigma(a_1), \ldots, \sigma(a_n)) = F(\sigma(a_1), \ldots, \sigma(a_n)),\end{aligned}$$

que es lo que queríamos probar. □

Teorema 3.22. *Sea $K_{\pi,n} = K(\mathcal{F}(n))$ el campo de Lubin-Tate generado por los puntos de división π^n-ésimos. Entonces:*

(1) *$K_{\pi,n}/K$ es una extensión totalmente ramificada de grado $q^{n-1}(q-1)$.*

(2) *La acción de $\mathcal{O}_K$ en $\mathcal{F}(n)$ induce un isomorfismo*

$$\mathrm{Gal}(K_{\pi,n}/K) \simeq \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{F}(n)) \simeq U_K/U_K^{(n)},$$

i.e., para cada $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$ existe una única clase $\overline{u} = u \bmod U_K^{(n)}$ con $u \in U_K$, tal que

$$\sigma(\lambda) = [u]_F(\lambda) \qquad \text{para } \lambda \in \mathcal{F}(n).$$

En particular, $K_{\pi,n}/K$ es una extensión abeliana.

(3) *El primo π de K es una norma de $K_{\pi,n}$. Más aún, si F es el módulo de Lubin-Tate asociado a $e(x) \in \mathcal{F}_\pi$ y si $\lambda_n \in \mathcal{F}(n) - \mathcal{F}(n-1)$, entonces λ_n es un elemento primo de $K_{\pi,n}$, i.e., $K_{\pi,n} = K(\lambda_n)$ y*

$$\phi_n(x) := \frac{e^n(x)}{e^{n-1}(x)} = x^{q^{n-1}(q-1)} + \cdots + \pi \in \mathcal{O}_K[x]$$

es su polinomio mínimo. En particular, $N_{K_{\pi,n}/K}(-\lambda_n) = \pi$.

DEMOSTRACIÓN. Podemos suponer que F es el módulo de Lubin-Tate asociado al polinomio $e \in \mathcal{F}_\pi$ de la forma

$$e(x) = x^q + \pi(a_{q-1}x^{q-1} + \cdots + a_2x^2) + \pi x,$$

y por lo tanto

$$\phi_n(x) := \frac{e^n(x)}{e^{n-1}(x)} = e^{n-1}(x)^{q-1} + \pi(a_{q-1}e^{n-1}(x)^{q-2} + \cdots + a_2e^{n-1}(x)) + \pi$$

es un polinomio de Eisenstein de grado $q^{n-1}(q-1)$. Ahora, si $\lambda_n \in \mathcal{F}(n) - \mathcal{F}(n-1)$, entonces λ_n es una raíz de este polinomio $\phi_n(x)$ y así, por (1.54), λ_n es un elemento primo de $K_{\pi,n}$ y la extensión $K(\lambda_n)/K$ es totalmente ramificada de grado $q^{n-1}(q-1)$. Mostraremos ahora que $K_{\pi,n} = K(\mathcal{F}(n)) = K(\lambda_n)$. En efecto, como $\mathcal{F}(n)$ es el conjunto de raíces del polinomio iterado $e^{(n)}$ en K^{al}, entonces $K_{\pi,n} = K(\mathcal{F}(n))$ es el campo de descomposición del polinomio $e^{(n)}$ y por lo tanto $\mathrm{Gal}(K_{\pi,n}/K)$ se puede identificar con un subgrupo del grupo de permutaciones del conjunto $\mathcal{F}(n)$. Pero el lema previo implica que cada elemento de $\mathrm{Gal}(K_{\pi,n}/K)$ actúa en $\mathcal{F}(n)$ como un isomorfismo de $\mathcal{O}_K$-módulos y así la imagen de $\mathrm{Gal}(K_{\pi,n}/K)$ en el grupo de permutaciones de $\mathcal{F}(n)$ está contenida en

$$\mathrm{End}_{\mathcal{O}_K}(\mathcal{F}(n)) \simeq (\mathcal{O}_K/\pi\mathcal{O}_K)^* = U_K/U_K^{(n)}.$$

Se sigue que

$$(q-1)q^{n-1} = |\mathrm{Gal}(K_{\pi,n}/K)| = [K_{\pi,n} : K] \leq [K(\lambda_n) : K] = (q-1)q^{n-1}$$

y por lo tanto las desigualdades deben ser igualdades, en particular $K(\lambda_n) = K(\mathcal{F}(n)) = K_{\pi,n}$ y así $K_{\pi,n}/K$ es totalmente ramificada de grado $(q-1)q^{n-1}$, lo cual prueba (1).

Para (2), de las mismas igualdades obtenidas antes se tiene que

$$\mathrm{Gal}(K(\mathcal{F}(n))/K) \simeq \mathrm{Gal}(K(\lambda_n)/K)$$

y ya vimos que este grupo se encuentra contenido en

$$\mathrm{End}_{\mathcal{O}_K}(\mathcal{F}(n)) \simeq (\mathcal{O}_K/\pi\mathcal{O}_K)^*,$$

y como ambos grupos finitos tienen el mismo orden $(q-1)q^{n-1}$, entonces deben ser isomorfos. Esto prueba (2).

Para (3), observemos que $K_{\pi,n} = K(\lambda_n)$ y que ϕ_n es el polinomio mínimo de λ_n sobre K y por lo tanto

$$N_{K_{\pi,n}/K}(\lambda_n) = (-1)^{(q-1)q^{n-2}}(\pi);$$

y este último término es $= \pi$, a menos que $q = 2$ y $n = 1$. En el caso excepcional se tiene que $K_{\pi,1} = K$ y así π ciertamente es una norma. □

A continuación obtenemos una fórmula explícita para el símbolo de norma residual de las extensiones de Lubin-Tate $K_{\pi,n}/K$, pero antes necesitaremos dos lemas:

Lema 3.23. *Sean K un campo local y $\widehat{K}_{nr}$ la completación de la máxima extensión no ramificada K_{nr} de K. Sea $\mathrm{Fr}_{\widehat{K}_{nr}}$ la extensión continua del Frobenius de K_{nr} a $\widehat{K}_{nr}$. Entonces:*

(1) *El morfismo $\mathcal{O}_{\widehat{K}_{nr}} \to \mathcal{O}_{\widehat{K}_{nr}}$ dado por $a \mapsto \mathrm{Fr}_{\widehat{K}_{nr}}(a) - a$ es suprayectivo con núcleo $\mathcal{O}_K$.*

(2) *El morfismo $U_{\widehat{K}_{nr}} \to U_{\widehat{K}_{nr}}$ dado por $a \mapsto \mathrm{Fr}_{\widehat{K}_{nr}}(a)/a$ es suprayectivo con núcleo U_K.*

DEMOSTRACIÓN. Si π es un primo de K, entonces π es primo de K_{nr} y por lo tanto también es primo de $\widehat{K}_{nr}$, de tal forma que los isomorfismos de (1.65)

$$U_{\widehat{K}_{nr}}/U^{(1)}_{\widehat{K}_{nr}} \simeq \overline{\widehat{K}}^*_{nr}, \qquad U^{(n)}_{\widehat{K}_{nr}}/U^{(n+1)}_{\widehat{K}_{nr}} \simeq \overline{\widehat{K}}_{nr}$$

son invariantes bajo $\mathrm{Fr}_{\widehat{K}_{nr}}$. Ahora, sea $c \in U_{\widehat{K}_{nr}}$ y consideremos su reducción $\overline{c}$ módulo $\mathfrak{p}_{\widehat{K}_{nr}}$. Por (1.51) el campo residual $\overline{\widehat{K}}_{nr}$ es algebraicamente cerrado y por lo tanto la ecuación

$$\frac{\mathrm{Fr}_{\widehat{K}_{nr}}(\overline{x})}{\overline{x}} = \frac{\overline{x}^q}{\overline{x}} = \overline{c},$$

donde $q = q_k = |K|$ es el orden del campo residual de K, tiene una solución $\neq 0$ en $\widehat{K}_{nr} = \mathcal{O}_{\widehat{K}_{nr}}/\mathfrak{p}_{\widehat{K}_{nr}}$, i.e., existe un $0 \neq x_1 \in \widehat{K}_{nr} \simeq U_{\widehat{K}_{nr}}/U^{(1)}_{\widehat{K}_{nr}}$ que es

solución de la ecuación anterior; escribiendo entonces $x_1 = x_1 a_1$ con $x_1 \in U_{\widehat{K}_{nr}}$ y $a_1 \in U^{(1)}_{\widehat{K}_{nr}}$ se tiene que

$$c = (\mathrm{Fr}_{\widehat{K}_{nr}}(x_1)/x_1)a_1.$$

Ahora, usando a_1, por la misma razón que antes podemos encontrar un $x_2 \in U^{(1)}_{\widehat{K}_{nr}}$ y un $a_2 \in U^{(2)}_{\widehat{K}_{nr}}$ tales que

$$c = (\mathrm{Fr}_{\widehat{K}_{nr}}(x_1x_2)/x_1x_2)a_2.$$

Inductivamente, podemos encontrar un $x_n \in U^{(n-1)}_{\widehat{K}_{nr}}$ y un $a_n \in U^{(n)}_{\widehat{K}_{nr}}$ tales que

$$c = (\mathrm{Fr}_{\widehat{K}_{nr}}(x_1x_2\cdots x_n)/x_1x_2\cdots x_n)a_n.$$

Pasando al límite obtenemos que

$$c = (\mathrm{Fr}_{\widehat{K}_{nr}}(x)/x \quad \text{con} \quad x = \prod_{n=1}^{\infty} x_n \in U_{\widehat{K}_{nr}}.$$

Esto prueba la solubilidad de la ecuación $(\mathrm{Fr}_{\widehat{K}_{nr}})(x)/x = c$. Para la solubilidad de la ecuación $\mathrm{Fr}_{\widehat{K}_{nr}}(x) - x = c$ en $\mathcal{O}_{\widehat{K}_{nr}}$ se procede análogamente usando los isomorfismos

$$\mathfrak{p}^n_{\widehat{K}_{nr}}/\mathfrak{p}^{n+1}_{\widehat{K}_{nr}} \simeq \widehat{K}_{nr}.$$

Esto prueba las primeras partes de (1) y (2).

Finalmente, si $x \in \mathcal{O}_{\widehat{K}_{nr}}$ satisface que $\mathrm{Fr}_{\widehat{K}_{nr}}(x) = x$, entonces para todo $n \geq 1$ se tiene que

$$x = x_n + \pi^n y_n \quad \text{con} \quad x_n \in \mathcal{O}_K \quad \text{y} \quad y_n \in \mathcal{O}_{\widehat{K}_{nr}}$$

ya que, para $n = 1$ se tiene que $x = a + \pi b$ con $a \in \mathcal{O}_{K_{nr}}$ y $b \in \mathcal{O}_{\widehat{K}_{nr}}$; ahora, como $\mathrm{Fr}_{\widehat{K}_{nr}}(x) = x$ se sigue que $\mathrm{Fr}_{\widehat{K}_{nr}}(a) \equiv a \pmod{\pi}$, de tal forma que $a = x_1 + \pi c$ con $x_1 \in \mathcal{O}_K$ y $c \in \mathcal{O}_{K_{nr}}$; consecuentemente

$$x = x_1 + \pi(b + c) = x_1 + \pi y_1 \quad \text{con} \quad x_1 \in \mathcal{O}_K \quad \text{y} \quad y_1 \in \mathcal{O}_{K_{nr}}.$$

Inductivamente, si ya obtuvimos la igualdad $(*)$ para n, entonces de $(*)$ se sigue que $\mathrm{Fr}_{\widehat{K}_{nr}}(y_n) = y_n$ y así, procediendo como en el caso $n = 1$, se sigue que

$$y_n = c_n + \pi d_n \quad \text{con} \quad c_n \in \mathcal{O}_K \quad \text{y} \quad d_n \in \mathcal{O}_{K_{nr}},$$

de tal forma que

$$x = (x_n + c_n\pi^n) + \pi^{n+1}d_n = x_{n+1} + \pi^{n+1}y_{n+1}$$

con $x_{n+1} \in \mathcal{O}_K$ y $y_{n+1} \in \mathcal{O}_{K_{nr}}$. Hemos probado así $(*)$ para $n+1$. Finalmente, pasando al límite en $(*)$ se obtiene que

$$x = \lim_{n\to\infty} x_n \in \mathcal{O}_K$$

ya que K es completo. Esto prueba la segunda parte de (1). La segunda parte de (2) es similar. □

Si K es un campo local y π es un elemento primo de K, dada $g \in \mathcal{F}_\pi \subseteq \mathcal{O}_K[[x]]$ recordemos que $g(x) = \pi x +$ términos de grado ≥ 2 y así su derivada $g'(x)$ es tal que $g'(0) = \pi$.

Lema 3.24. *Sean K un campo local y π un primo de K. Sean $e(x), f(x) \in \mathcal{F}_\pi \subseteq \mathcal{O}_K[[x]]$. Pongamos $f'(0) = ue'(0)$ con $u \in U_K$. Si $[u](x) = ux + \cdots \in \mathcal{O}_K[[x]]$ es una serie de potencias tal que*

$$e \circ [u] = [u] \circ e,$$

entonces existe una serie de potencias $\theta(x) = \varepsilon x + \cdots \in \mathcal{O}_{\widehat{K}_{nr}}[[x]]$, $\varepsilon \in U_{\widehat{K}_{nr}}$, tal que

$$\mathrm{Fr}_{\widehat{K}_{nr}}(\theta) = \theta \circ [u] \qquad \text{y} \qquad \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e = f \circ \theta.$$

DEMOSTRACIÓN. Construiremos inductivamente una sucesión de polinomios $\theta_r(x) = \sum a_i x^i \in \mathcal{O}_{\widehat{K}_{nr}}[x]$ tales que, para toda $r \geq 1$,

$$\begin{aligned} \theta_r(x) &= \theta_{r-1}(x) + bx^r \quad \text{para algún } b \in \mathcal{O}_{\widehat{K}_{nr}} \\ \mathrm{Fr}_{\widehat{K}_{nr}}(\theta_r) &= \theta_r \circ [u] + \text{términos de grado} \geq r+1. \end{aligned}$$

Comenzamos con $r = 1$ observando que por el lema anterior existe un $\varepsilon \in U_{\widehat{K}_{nr}}$ tal que $\mathrm{Fr}_{\widehat{K}_{nr}}(\varepsilon) = \varepsilon u$. Se define entonces $\theta_1(x) := \varepsilon x$ notando que la segunda condición anterior se cumple ya que

$$\mathrm{Fr}_{\widehat{K}_{nr}}(\theta_1)(x) = \mathrm{Fr}_{\widehat{K}_{nr}}(\varepsilon x) = \mathrm{Fr}_{\widehat{K}_{nr}}(\varepsilon)x = \varepsilon ux = \varepsilon[u](x) = (\theta_1 \circ [u])(x).$$

Supongamos que ya encontramos θ_r; queremos definir θ_{r+1} tal que satisfaga la primera condición anterior, i.e., tal que

$$\theta_{r+1}(x) = \theta_r(x) + bx^{r+1} \quad \text{para algún } b \in \mathcal{O}_{\widehat{K}_{nr}}.$$

Para esto, escribamos $b = a\varepsilon^{r+1}$ con $a \in \mathcal{O}_{\widehat{K}_{nr}}$. Entonces, para $\theta_{r+1}(x) = \theta_r(x) + a\varepsilon^{r+1}x^{r+1}$ la segunda igualdad anterior debe ser de la forma

$$\begin{aligned}(\mathrm{Fr}_{\widehat{K}_{nr}} \circ \theta_r)(x) + (\mathrm{Fr}_{\widehat{K}_{nr}}(a)(\mathrm{Fr}_{\widehat{K}_{nr}}(\varepsilon))^{r+1}x^{r+1} &= \theta_r([u](x)) + a\varepsilon^{r+1}[u](x^{r+1}) \\ &= \theta_r([u](x)) + a\varepsilon^{r+1}(ux)^{r+1} \\ &\quad \text{mód } (x^{r+2}),\end{aligned}$$

donde por inducción podemos cancelar los primeros términos de cada lado de la anterior igualdad, obteniendo

$$(\mathrm{Fr}_{\widehat{K}_{nr}}(a)(\mathrm{Fr}_{\widehat{K}_{nr}}(\varepsilon))^{r+1}x^{r+1} \equiv a\varepsilon^{r+1}(ux)^{r+1} \text{ mód } (x^{r+2}),$$

i.e.,

$$(\mathrm{Fr}_{\widehat{K}_{nr}}(a))(\varepsilon u)^{r+1}x^{r+1} \equiv a(\varepsilon u)^{r+1}x^{r+1} \text{ mód } (x^{r+2}),$$

i.e., $a \in \mathcal{O}_{\widehat{K}_{nr}}$ debe ser una solución de la ecuación

$$(\mathrm{Fr}_{\widehat{K}_{nr}}(a) - a) = c/(\varepsilon u)^{r+1}$$

donde c es el coeficiente de x^{r+1} en $\theta_r \circ [u] - \mathrm{Fr}_{\widehat{K}_{nr}}(\theta_r)$. Este elemento $a \in \mathcal{O}_{\widehat{K}_{nr}}$ existe por el lema previo, y así la igualdad deseada para $r+1$ es cierta. Se sigue que la serie

$$\theta(x) := \sum_{i=1} a_i x^i \in \mathcal{O}_{\widehat{K}_{nr}}[[x]]$$

satisface que $\theta(x) \equiv \varepsilon x$ mód x^2 y además

$$\mathrm{Fr}_{\widehat{K}_{nr}}(\theta)(x) = \theta \circ [u](x),$$

lo cual prueba la primera igualdad del lema. Para la segunda igualdad, pongamos

$$h := \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e \circ \theta^{-1} = \theta \circ [u] \circ e \circ \theta^{-1} = \theta \circ e \circ [u] \circ \theta^{-1}$$

(donde la segunda igualdad es por la primera propiedad de la serie θ, que ya probamos, y la tercera igualdad es por la hipótesis sobre e y $[u]$). Ahora, como e y $[u]$ tienen coeficientes en $\mathcal{O}_K$, entonces quedan invariantes bajo $\mathrm{Fr}_{\widehat{K}_{nr}}$ y por

lo tanto

$$\begin{aligned}
\mathrm{Fr}_{\widehat{K}_{nr}}(h) \qquad & \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e \circ [u] \circ \mathrm{Fr}_{\widehat{K}_{nr}}(\theta^{-1}) \\
& \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e \circ [u] \circ (\theta \circ [u])^{-1} \\
& \text{por la primera parte del lema.} \\
& \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e \circ [u] \circ [u]^{-1} \circ \theta^{-1} \\
= \; & \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e \circ \theta^{-1} \\
= \; & h,
\end{aligned}$$

i.e., $\mathrm{Fr}_{\widehat{K}_{nr}}(h) = h$, lo cual por el lema previo implica que $h \in \mathcal{O}_K[[x]]$. Más aún,

$$\begin{aligned}
h(x) \qquad & (\mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e \circ \theta^{-1})(x) = (\mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e)(\varepsilon^{-1}x + \cdots) \\
& (\mathrm{Fr}_{\widehat{K}_{nr}}(\theta)(\pi\varepsilon^{-1}x + \cdots) = \mathrm{Fr}_{\widehat{K}_{nr}}(\varepsilon) \cdot \pi\varepsilon^{-1}x + \cdots \\
& \varepsilon u \pi \varepsilon^{-1} x + \cdots = u\pi x + \cdots \\
& \varpi x + \cdots \quad \text{donde } \varpi := f'(0) = ue'(0) = u\pi,
\end{aligned}$$

i.e., $h(x) \equiv \varpi x$ mód (x^2), y como

$$\begin{aligned}
h(x) \; = \; & \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e \circ \theta^{-1}(x) \\
& \mathrm{Fr}_{\widehat{K}_{nr}}(\theta)(e(\theta^{-1}(x))) \text{ mód } \pi \\
& \mathrm{Fr}_{\widehat{K}_{nr}}(\theta)(\theta^{-1}(x))^q \text{ mód } \pi \\
& \text{ya que } e(x) \equiv x^q \text{ mód } \pi \\
= \; & \mathrm{Fr}_{\widehat{K}_{nr}}(\theta)\mathrm{Fr}_{\widehat{K}_{nr}}(\theta)^{-1}(x^q) \text{ mód } \pi \\
= \; & x^q \text{ mód } \pi,
\end{aligned}$$

entonces $h(x) \equiv x^q$ mód π. Las tres propiedades de $h(x)$ que hemos probado implican que $h \in \mathcal{F}_{\varpi}$.

Pongamos ahora $\psi := [1]_{f,h} \circ \theta$. Entonces claramente ψ satisface que

$$\psi(x) \equiv \varepsilon x \text{ mód } (x^2)$$

(porque θ satisface esta condición) y además cumple que

$$\mathrm{Fr}_{\widehat{K}_{nr}}(\psi) = \psi \circ [u]$$

ya que $[1]_{f,h} \in \mathcal{O}_K[[x]]$ y por lo tanto queda invariante bajo el Frobenius. Más aún,

$$\mathrm{Fr}_{\widehat{K}_{nr}}(\psi) \circ e \circ \psi^{-1} = [1]_{f,h} \circ h \circ [1]_{f,h}^{-1} = f,$$

i.e.

$$\mathrm{Fr}_{\widehat{K}_{nr}}(\psi) \circ e = f \circ \psi,$$

que es lo que faltaba probar. □

El resultado principal es el cálculo explícito del símbolo de norma residual:

Teorema 3.25. *Si $K_{\pi,n}/K$ es una extensión de Lubin-Tate y $a = u\pi^{v_K(a)} \in K^*$ con $u \in U_K$, entonces*

$$(a, K_{\pi,n}/K)(\lambda) = [u^{-1}]_F(\lambda)$$

para $\lambda \in \mathcal{F}(n)$.

DEMOSTRACIÓN. Por el teorema (3.22)(2) sea $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$ el automorfismo definido por

$$\sigma(\lambda) = [u^{-1}]_F(\lambda) \qquad \text{para} \quad \lambda \in \mathcal{F}(n).$$

Como $K_{\pi,n}/K$ es totalmente ramificada por (3.22)(1), entonces por (1.53)(3) se tiene que $\mathrm{Gal}(K_{\pi,n}/K) \simeq \mathrm{Gal}(K_{\pi,n}^{nr}/K^{nr})$ y así $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$ se puede ver como un elemento del grupo $\mathrm{Gal}(K_{\pi,n}^{nr}/K^{nr})$. Consideremos entonces un levantamiento $\widetilde{\sigma} \in \mathrm{Gal}(K_{\pi,n}^{nr}/K)$ de σ, véase §2.2. Por (2.20) y (1.52) se sigue que el campo fijo Σ de $\widetilde{\sigma}$ es una extensión finita totalmente ramificada Σ/K y por (1.52) se tiene entonces que

$$\Sigma \cap K_{nr} = K \qquad \text{y} \qquad \Sigma_{nr} = \Sigma K_{nr} = K_{\pi,n}^{nr}$$

de tal forma que

$$[\Sigma : K] = [K_{\pi,n}^{nr} : K_{nr}] = [K_{\pi,n} : K] = q^{n-1}(q-1),$$

la última igualdad por (3.22).

Ahora, sean $e \in \mathcal{F}_\pi$ y $f \in \mathcal{F}_\varpi$ donde $\varpi = u\pi$, y sea $F = F_e$. Por el lema (3.24) existe una serie $\theta(x) = \varepsilon x + \cdots \in \mathcal{O}_{\widehat{K}_{nr}}[[x]]$ con $\varepsilon \in U_{\widehat{K}_{nr}}$ tal que

$$\mathrm{Fr}_{\widehat{K}_{nr}}(\theta) = \theta \circ [u]_F \quad \text{y} \quad \mathrm{Fr}_{\widehat{K}_{nr}}(\theta) \circ e = f \circ \theta.$$

Sea $\lambda_n \in \mathcal{F}(n) - \mathcal{F}(n-1)$; por (3.22) λ_n es un elemento primo de $K_{\pi,n}$ y $\pi_\Sigma = \theta(\lambda_n) \in \mathcal{O}_{\widehat{K}_{\pi,n}}$ es un elemento primo de Σ ya que

$$[u^{-1}](\sigma(\lambda_n)) = \sigma(\lambda_n^{u^{-1}}) = \lambda_n$$

y por lo tanto

$$\tilde{\sigma}(\pi_\Sigma) = \mathrm{Fr}_{\widehat{K}_{nr}}(\theta)(\sigma(\lambda_n)) = \theta([u^{-1}]_F(\sigma(\lambda_n))) = \theta(\lambda_n) = \pi_\Sigma$$

(la segunda igualdad por el lema (3.24)) y así $\pi_\Sigma \in \Sigma$ por definición de Σ.

Ahora, como por (3.24)

$$f^i(\theta(\lambda_n)) = \mathrm{Fr}^i_{\widehat{K}_{nr}}(\theta)(e^i(\lambda_n)) = \begin{cases} 0 & \text{para} \quad i = n \\ \neq 0 & \text{para} \quad i = n-1 \end{cases}$$

y como

$$f^i(\pi_\Sigma) = f^i(\theta(\lambda_n)) = \mathrm{Fr}^i_{\widehat{K}_{nr}}(\theta)(e^i(\lambda_n)),$$

entonces

$$f^i(\pi_\Sigma) = \begin{cases} 0 & \text{para} \quad i = n \\ \neq 0 & \text{para} \quad i = n-1, \end{cases}$$

y por lo tanto $\pi_\Sigma \in \mathcal{F}_f(n) - \mathcal{F}_f(n-1)$. Se sigue que $\Sigma = K(\pi_\Sigma)$ es el campo de Lubin-Tate n-ésimo para el primo ϖ. Por el teorema (3.22), se tiene entonces que $N_{\Sigma/K}(-\pi_\Sigma) = \varpi = u\pi$ y como, por (3.22), $\pi \in N_{K_{\pi,n}}(K^*_{\pi,n})$ entonces por definición el inverso del morfismo de reciprocidad $\Upsilon_{K_{\pi,n}/K}$ actúa como

$$\Upsilon_{K_{\pi,n}/K}(\sigma) = N_{\Sigma/K}(-\pi_\Sigma) = \varpi \equiv u \text{ mód } N_{K_{\pi,n}/K}(K^*_{\pi,n})$$

y consecuentemente su inverso aplicado a $a = \pi^{v_K(a)}u$ es

$$(a, K_{\pi,n}/K) = (\pi^{v_K(a)}, K_{\pi,n}/K)(u, K_{\pi,n}/K) = (u, K_{\pi,n}/K) = \sigma$$

(la penúltima igualdad porque π es una norma, como recordamos antes, y la última igualdad porque el símbolo de norma residual es el inverso del morfismo $\Upsilon_{K_{\pi,n}/K}$), i.e.,

$$(a, K_{\pi,n}/K)(\lambda) = \sigma(\lambda) = [u^{-1}]_F(\lambda)$$

para $\lambda \in \mathcal{F}(n)$, como se quería probar. □

Tenemos entonces la generalización siguiente del teorema (2.69) de extensiones ciclotómicas a extensiones de Lubin-Tate:

Corolario 3.26. *La extensión de Lubin-Tate $K_{\pi,n}/K$ de puntos de división π^n-ésimos es el campo de clases del grupo de normas $\langle\pi\rangle \times U_K^{(n)} \subseteq K^*$.*

DEMOSTRACIÓN. Sea $a = u\pi^{v_K(a)} \in K^*$ con $u \in U_K$. Entonces

$$\begin{aligned} a \in N_{K_{\pi,n}/K}(K^*_{\pi,n}) &\Leftrightarrow (a, K_{\pi,n}/K) = 1 \\ &\Leftrightarrow [u^{-1}]_F(\lambda) = \lambda \quad \text{para toda } \lambda \in \mathcal{F}(n) \\ &\Leftrightarrow [u^{-1}]_F = id_{\mathcal{F}(n)} \\ &\Leftrightarrow u^{-1} \in U_K^{(n)} \\ &\Leftrightarrow u \in U_K^{(n)} \\ &\Leftrightarrow a \in (\pi) \times U_K^{(n)} \end{aligned}$$

y por lo tanto $N_{K_{\pi,n}/K}(K^*_{\pi,n}) = (\pi) \times U_K^{(n)}$. □

Para la máxima extensión abeliana K^{ab}/K de un campo local arbitrario K tenemos la generalización siguiente del teorema de Kronecker-Weber local que nos da una descripción explícita de K^{ab}, ya que K_{nr} está descrita explícitamente en (1.64)(3):

Corolario 3.27. *Sea K un campo local. Entonces K^{ab} es el campo compuesto*

$$K^{ab} = K_{nr} \cdot K_\pi,$$

donde K_{nr} es la máxima extensión no ramificada de K y K_π es la unión de los campos de Lubin-Tate $K_{\pi,n}$, i.e., $K_\pi = \bigcup_{n=1} K_{\pi,n}$.

DEMOSTRACIÓN. Sea L/K cualquier extensión finita. Sabemos (véase la observación después de (2.67)) que $(\pi^f) \times U_K^{(n)} \subseteq N_{L/K}L^*$ para algunos enteros f y n, i.e., L está contenido en el campo de clases del grupo

$$(\pi^f) \times U_K^{(n)} = ((\pi^f) \times U_K) \cap ((\pi) \times U_K^{(n)})$$

y el campo de clases de este último grupo de normas es la composición del campo de clases de $(\pi^f) \times U_K$, que es la extensión no ramificada K_f de K de grado f y el campo de clases de $(\pi) \times U_K^{(n)}$, que es el campo de Lubin-Tate $K_{\pi,n}$; se sigue que $L \subseteq K_f \cdot K_{\pi,n}$. Pasando al límite sobre las extensiones abelianas finitas de K se obtiene el resultado deseado. □

El símbolo de norma residual sobre $\mathbb{Q}_p$. El teorema (3.25) anterior aplicado a las extensiones ciclotómicas de $\mathbb{Q}_p$, que son de Lubin-Tate como ya sabemos, se traduce en el siguiente corolario:

Corolario 3.28. *Sea $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ una extensión ciclotómica con ζ una raíz primitiva p^n-ésima de la unidad. Si $a = u \cdot p^{v_p(a)} \in \mathbb{Q}_p^*$, entonces*

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)(\zeta) = \zeta^{u^{-1}}$$

donde $\zeta^{u^{-1}}$ quiere decir ζ^r con $r \in \mathbb{Z}$ tal que $r \equiv u^{-1}$ (mód p^n).

DEMOSTRACIÓN. Sólo tenemos que observar que $K_{\pi,n} = \mathbb{Q}_p(\zeta)$ es una extensión de Lubin-Tate de $\mathbb{Q}_p$ para el grupo multiplicativo $\mathbb{G}_m$, y que para $\zeta \in \mathbb{G}_m(n) = \mu_{p^n}$ se tiene que $\lambda = \zeta - 1 \in \mathbb{G}_m(n)$ y así

$$[u^{-1}]_{\mathbb{G}_m}(\zeta) = (1+\zeta)^{u^{-1}} - 1 = \zeta^{u^{-1}}.$$

□

3.5 Ejercicios

1. Sea K un campo local y $p = \text{car}\,(K)$.
   (i) Si $f(x) = \sum_{n\geq 0} x^n$ y $g(x) = p^{-2}x - p^{-3}x^2$, demuestre que $g(x)$ converge para $x = p$, $f(x)$ converge para $x = g(p)$ pero $f \circ g$ no converge en $x = p$.
   (ii) Si $p = 2$, $f(x) = \exp(x)$, $g(x) = \log(1+x)$, demuestre que g y $f \circ g$ convergen en $x = \sqrt{2}$, pero f no converge en $g(\sqrt{2})$.
   (iii) Si $f(x) = \exp(x)$, $g(x) = \log(1+x)$ y ζ es una raíz primitiva p-ésima de la unidad, demuestre que $g(\zeta - 1) = 0$ y $f(g(\zeta - 1)) = 1$ pero $(f \circ g)(\zeta - 1) = \zeta$.
   (iv) Si $f_n(x) = a_n(\log(1+x))^n$, donde los coeficientes a_n están dados por $\exp(x) = \prod_{n\geq 1}(1 + a_n x^n)$.
      (a) Demuestre que $\prod_{n\geq 1}(1 + f_n(x)) = 1 + x$.
      (b) Si $x = \zeta - 1$ con ζ una raíz primitiva p-ésima de la unidad, demuestre que $f_n(\zeta - 1) = 0$ y que $\prod_{n\geq 1}(1 + f_n(\zeta - 1)) \neq \zeta$.
2. Sea A un anillo conmutativo con uno y supongamos que $1/2 \in A$. Demuestre que para cada $\alpha \in A$ la serie:
$$F_\alpha(x, y) := \frac{x\sqrt{(1-y^2)(1-\alpha^2y^2)} + y\sqrt{(1-x^2)(1-\alpha^2x^2)}}{1 + \alpha^2x^2y^2}$$
determina una ley de grupo formal en A. (Ésta es la fórmula de adición para las funciones de Jacobi en curvas elípticas).
3. Sea K un *campo cualquiera*. Demuestre que todo grupo formal conmutativo $\mathcal{F}$ en K es isomorfo al grupo formal aditivo $\mathbb{G}_a$ en K, i.e., demuestre que existe una serie de potencias formal sin término constante $\lambda(x) \in K[[x]]$ (por lo tanto invertible) tal que $\lambda(x) \equiv x$ mód (x^2) y
$$\mathcal{F}(x, y) = \lambda^{-1}(\lambda(x), \lambda(y)).$$
Nota: La serie $\lambda(x)$ se llama el *logaritmo* del grupo formal $\mathcal{F}$ y se denota por $\log_{\mathcal{F}}(x)$. Su inversa, con respecto a la composición, se llama la *exponencial* del grupo formal $\mathcal{F}$ y se denota por $\exp_{\mathcal{F}}$. Así, el ejercicio nos dice que
$$\mathcal{F}(x, y) = \exp_{\mathcal{F}}(\log_{\mathcal{F}}(x), \log_{\mathcal{F}}(y)).$$

4. Si L/K es una extensión finita de campos locales con ideales máximos $\mathfrak{p}_L$ y $\mathfrak{p}_K$ respectivamente y si $\mathcal{F}(x, y)$ es un grupo formal sobre el anillo $\mathcal{O}_K$, demuestre que la inclusión
$$(\mathcal{F}(\mathfrak{p}_K), +_{\mathcal{F}}) \hookrightarrow (\mathcal{F}(\mathfrak{p}_L), +_{\mathcal{F}})$$
es un homomorfismo de grupos.
5. Si K es un campo local, demuestre que el morfismo de anillos del corolario (3.14), $\mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(\mathcal{F}_f)$ es inyectivo.
6. Sean K un campo local y π un elemento primo de K. Si L/K es una extensión abeliana totalmente ramificada tal que $L \supseteq K_\pi$, demuestre que $L = K_\pi$.
7. Sean K un campo local y π un elemento primo de K. Demuestre que toda extensión no ramificada de K_π está contenida en el campo compuesto $K_\pi K_{nr}$.
8. Sea L/K una extensión abeliana finita de campos locales de exponente m y sea K_m la extensión no ramificada de K de grado m.

   Demuestre que existe una extensión abeliana totalmente ramificada L_t de K tal que $L \subseteq L_t K_m = L K_m$. *Sugerencias*: Muestre primero que $\mathrm{Gal}(LK_m/K)$ es un grupo abeliano de exponente m. Luego, muestre que si $\tau \in \mathrm{Gal}(LK_m/K)$ es tal que $\tau|_{K_m}$ es el Frobenius de K_m/K, entonces τ es de orden m y $\mathrm{Gal}(L/K) \simeq \langle\tau\rangle \times H$ (producto directo), para algún subgrupo H. Finalmente ponga $L_t = L^{\langle\tau\rangle}$ (el campo fijo de $\langle\tau\rangle$).
9. Usando los dos ejercicios anteriores, dé otra demostración de (3.27): si K es un campo local y π es un elemento primo de K, entonces $K^{ab} = K_{nr} K_\pi$.

Capítulo 4

Ramificación superior

En (2.33) demostramos que si L/K es una extensión abeliana de campos locales, entonces el símbolo de norma residual $(\ ,L/K) : K^* \to \mathrm{Gal}(L/K)$ manda al grupo de unidades U_K en el grupo de inercia $G_0(L/K)$ de $\mathrm{Gal}(L/K)$. En este capítulo se generalizará lo anterior probando que el símbolo de norma residual manda al grupo de unidades superiores $U_K^{(n)}$ en el n-ésimo grupo de ramificación superior G^n de $\mathrm{Gal}(L/K)$ para toda $n \geq 0$. Para esto recordamos algunas propiedades de los grupos de ramificación superior G_n (en la notación con subíndices) y después introducimos la renumeración con supraíndices G^n de los grupos de ramificación superior; mostramos entonces que la ventaja de la numeración superior es que no cambia cuando se pasa a subextensiones de L/K. Después calculamos los grupos de ramificación superior de la extensión ciclotómica $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ usando algunos cálculos, (2.68), del capítulo 2. Esto nos servirá de motivación para estudiar la ramificación superior de las extensiones abelianas de campos locales L/K en general y para esto usaremos el enfoque de Lubin-Tate [28] del capítulo anterior. Al final del capítulo demostramos el teorema clásico de Hasse-Arf que afirma que los *saltos* en los grupos de ramificación superior son *enteros*.

4.1 Grupos de ramificación superior

Si L/K es una extensión finita de campos locales con grupo de Galois $G = \mathrm{Gal}(L/K)$, recordemos de §1.8 que para cada número real $s \geq -1$ se define el *s-ésimo grupo de ramificación* de L/K mediante

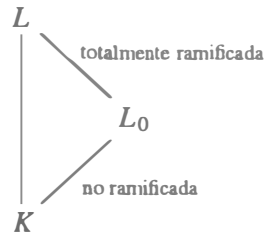
$$G_s = G_s(L/K) := \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(a)-a) \geq s+1 \text{ para todo } a \in \mathcal{O}_L\}.$$

Recordemos que como $v_L : L^* \twoheadrightarrow \mathbb{Z}$ tiene valores enteros, entonces para todo número real $s \geq -1$ se tiene que

$$G_s = G_{j(s)}$$

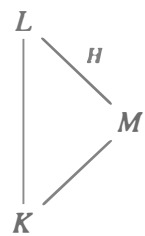
donde $j(s)$ es el menor entero $\geq s$.

En (1.76) mostramos que si L/K es una extensión finita de campos locales y $G = \mathrm{Gal}(L/K)$, entonces el campo fijo L_0 del grupo de inercia G_0 es la máxima extensión no ramificada de K contenida en L y los grupos de ramificación de G coinciden con los de su grupo de inercia $G_0 = \mathrm{Gal}(L/L_0)$. En la situación anterior,



la extensión L/L_0 con grupo de Galois H es totalmente ramificada de tal forma que la proposición (1.76) reduce el estudio de los grupos de ramificación superior de índice $s \geq 0$ al caso totalmente ramificado.

Ahora, si H es cualquier subgrupo de $G = \mathrm{Gal}(L/K)$ y $M = L^H$ es el campo fijo de H,



entonces $\mathrm{Gal}(L/M) = H$ y veremos a continuación que los grupos de ramificación de G determinan los de H:

Proposición 4.1. *Con la notación anterior, sea $i_G :\to \mathbb{Z}$ la función de* (1.80)*; entonces, para todo $\sigma \in H$ se tiene que $i_H(\sigma) = i_G(\sigma)$ y $H_s = G_s \cap H$.*

DEMOSTRACIÓN. Si $\sigma \in H_s$ entonces $v_L(\sigma x - x) \geq s + 1$ y así $x \in G_s$ y por lo tanto $H_s \subseteq G_s \cap H$. La otra inclusión es similar. □

Supongamos ahora además que $H \lhd G = \mathrm{Gal}(L/K)$ es un subgrupo normal y sea L^H el campo fijo de H de tal forma que $G/H \simeq \mathrm{Gal}(L^H/K)$. Veremos

a continuación que los grupos de ramificación de G determinan los de G/H y expresaremos el resultado en términos de las funciones i_G e $i_{G/H}$; esto será consecuencia de la proposición siguiente:

Proposición 4.2. *Sea L/K una extensión finita de campos locales y supongamos que $H \lhd G = \mathrm{Gal}(L/K)$ es un subgrupo normal. Sea L^H el campo fijo de H. Entonces, para todo $\overline{\sigma} \in G/H = \mathrm{Gal}(L^H/K)$ se tiene que*

$$i_{G/H}(\overline{\sigma}) = \frac{1}{e'} \sum_{\sigma \in G,\ \sigma \to \overline{\sigma}} i_G(\sigma),$$

donde $e' = e(L/L^H)$ es el índice de ramificación de L/L^H y $\sigma \to \overline{\sigma}$ quiere decir que σ es un representante de la clase $\overline{\sigma}$.

DEMOSTRACIÓN. (Tate). Para $\overline{\sigma} = 1$ ambos lados son iguales a $+\infty$. Supongamos entonces que $\overline{\sigma} \neq 1$. Usando (1.40) sea $\alpha \in \mathcal{O}_L$ tal que $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ y sea $\beta \in \mathcal{O}_{L^H}$ tal que $\mathcal{O}_{L^H} = \mathcal{O}_K[\beta]$. Por definición,

$$e' i_{G/H}(\overline{\sigma}) = e' i_{\mathrm{Gal}(L^H/K)}(\overline{\sigma}) = e' v_{L^H}(\overline{\sigma}\beta - \beta) = v_L(\sigma\beta - \beta)$$

ya que $v_L = e' v_{L^H}$. También

$$i_G(\sigma) = i_{\mathrm{Gal}(L/K)}(\sigma) = v_L(\sigma\alpha - \alpha).$$

Escojamos un $\sigma \in G = \mathrm{Gal}(L/K)$ fijo tal que su clase lateral sea σ. Entonces, los otros elementos de G que representan a σ son de la forma $\varrho\sigma$ con $\varrho \in H = \mathrm{Gal}(L/L^H)$. Se sigue que

$$\sum_{\varrho \in G,\ \varrho\sigma = \overline{\sigma}} i_G(\varrho) = \sum_{\varrho \in H} i_G(\varrho\sigma) = \sum_{\varrho \in H} v_L(\varrho\sigma\alpha - \alpha),$$

lo cual queremos que sea igual a

$$e' i_{G/H}(\overline{\sigma}) = v_L(\overline{\sigma}\beta - \beta) = v_L(\sigma\beta - \beta)$$

y así basta probar que los siguientes elementos de $\mathcal{O}_L$:

$$a := \prod_{\varrho \in H} (\varrho\sigma\alpha - \alpha) \quad \text{y} \quad b := \sigma\beta - \beta$$

al aplicarles v_L dan el mismo valor, i.e., basta ver que generan el mismo ideal en $\mathcal{O}_L$. Para esto, sea $f(x) = \mathrm{Irr}(\alpha, L^H) \in \mathcal{O}_{L^H}[x]$. Entonces

$$f(x) = \prod_{\varrho \in H} (x - \varrho(\alpha)) \quad \text{y} \quad (\sigma f)(x) = \prod_{\varrho \in H} (x - \sigma\varrho(\alpha)).$$

Ahora, como todos los coeficientes de $\sigma(f) - f$ son divisibles por $\sigma\beta - \beta$,entonces $b := \sigma\beta - \beta$ divide, en $\mathcal{O}_L$, a

$$(\sigma f)(\alpha) - f(\alpha) = (\sigma f)(\alpha) = \prod_{\varrho \in H} (\alpha - \sigma\varrho(\alpha)) =: a,$$

(la segunda igualdad es porque $f(\alpha) = 0$); i.e., b divide a a. Para probar que $a|b$, escribamos a $\beta \in \mathcal{O}_{L^H} \subseteq \mathcal{O}_L = \mathcal{O}_K[\alpha]$ como un polinomio en α con coeficientes en $\mathcal{O}_K$: $\beta = g(\alpha)$. Observemos ahora que el polinomio $g(x) - \beta$ tiene todos sus coeficientes en $\mathcal{O}_{L^H}$ y α es una de sus raíces. Se sigue que el polinomio mínimo de α, $f(x) = \mathrm{Irr}(\alpha, L^H)$ divide al polinomio $g(x) - \beta$:

$$g(x) - \beta = f(x)h(x)$$

con $h(x) \in \mathcal{O}_{L^H}[x]$. Aplicando σ a los coeficientes de ambos lados de esta igualdad, observando que $\sigma g = g$ porque $g(x) \in \mathcal{O}_K[x]$, obtenemos

$$g(x) - \sigma(\beta) = \sigma f(x)\sigma h(x)$$

y substituyendo $x = \alpha$ se obtiene

$$\beta - \sigma\beta = g(\alpha) - \sigma\beta = \sigma f(\alpha)\sigma h(\alpha),$$

i.e., $a = \sigma f(\alpha)$ divide a $\beta - \sigma\beta = a$ en $\mathcal{O}_L$. □

Una consecuencia de la proposición anterior es que los grupos de ramificación de G determinan los del cociente G/H en un caso especial:

Corolario 4.3. *Con las mismas hipótesis de la proposición anterior, si además* $H = G_j$ *para algún* $j \geq 0$, *entonces* $(G/H)_i = G_i/H$ *para* $i \leq j$ *y* $(G/H)_i = \{1\}$ *para* $i \geq j$.

DEMOSTRACIÓN. Los G_i/H para $i \leq j$ forman una filtración decreciente de G/H; mostraremos que esta filtración coincide con la dada por los grupos de ramificación $(G/H)_i$ para $i \leq j$. En efecto, si $\overline{\sigma} \in G/H$ y $\overline{\sigma} \neq 1$, entonces existe un único índice $i < j$ tal que $\overline{\sigma} \in G_i/H$ y $\overline{\sigma} \notin G_{i+1}/H$. Si $s \in G$ representa a $\overline{\sigma}$ entonces claramente $s \in G_i$ pero $s \notin G_{i+1}$; se sigue que $i_G(s) = i + 1$.

Ahora, como $H = G_j$ para algún $j \geq 0$, entonces $H \subseteq G_0$ y así los campos fijos satisfacen $L^H \supseteq L^{G_0} = L_0$ y por lo tanto, la extensión L/L^H

es totalmente ramificada y así $e(L/L^H) = |H|$. Por la proposición anterior se sigue que

$$i_{G/H}(\sigma) = \frac{1}{|H|} \sum_{s \in G} i_G(s) = \frac{1}{|H|} \sum_{s \in G} (i+1) = \frac{1}{|H|} |H|(i+1) = i+1,$$

donde las sumas son sobre los elementos $s \in G$ que representan a las clases $\overline{\sigma}$. Por lo tanto, la filtración $(G/H)_i$ coincide con la filtración G_i/H para $i \leq j$.

Finalmente, como para $i = j$ ya vimos que $(G/H)_j = G_j/H = \{1\}$ (la última igualdad porque $H = G_j$), se sigue que si $i \geq j$ entonces $(G/H)_i = \{1\}$ ya que son subgrupos de $(G/H)_j = \{1\}$. □

Observación. El corolario anterior requiere que el subgrupo normal $H \lhd G$ sea de la forma $H = G_j$ para algún $j \geq 0$. En realidad, para cualquier subgrupo normal $H \lhd G$ es cierto que los grupos de ramificación de G/H son imágenes de los grupos de ramificación de G, pero es necesario modificar la numeración. Este cambio de numeración lo da la función $\phi_{L/K} : [-1, \infty\rangle \longrightarrow [-1, \infty\rangle$ definida mediante

$$\phi(u) := \int_0^u \frac{dt}{(G_0 : G_t)'}$$

donde $(G_0 : G_t) = [G_0 : G_t]$ es el índice de G_t en G_0 si $t > 0$ y si $t \leq 0$ ponemos $(G_0 : G_t) = [G_t : G_0]^{-1}$, el recíproco del índice de G_0 en G_t. Obsérvese que para $u \in [-1, 0]$ se tiene que $\phi(u) = u$ ya que para $t \in (-1, 0]$ se tiene que $(G_t : G_0)^{-1} = (G_0 : G_0)^{-1} = 1$.

La función $\phi_{L/K}$ se puede hacer explícita como sigue: si $u \in \mathbb{R}$ se pone en el intervalo "entero" $m \leq u \leq m+1$, donde m es un entero positivo, entonces

$$\begin{aligned}
\phi_{L/K}(u) &= \int_0^u \frac{dt}{(G_0 : G_t)} \\
&- \int_0^1 \frac{dt}{|G_0/G_1|} + \cdots + \int_{m-1}^m \frac{dt}{|G_0/G_m|} + \int_m^u \frac{dt}{|G_0/G_{m+1}|} \\
&- \frac{1}{|G_0|} \left(|G_1| + |G_2| + \cdots + |G_m| + (u-m)|G_{m+1}| \right) \\
&= \frac{1}{g_0} (g_1 + g_2 + \cdots + g_m + (u-m) g_{m+1})
\end{aligned}$$

donde $g_i := |G_i|$. En particular, si $u = m$,

$$\phi_{L/K}(m) = \frac{1}{g_0}(g_1 + g_2 + \cdots + g_m).$$

Es claro que la función $\phi_{L/K}$ es continua, lineal a tramos, creciente, cóncava y además $\phi_{L/K}(0) = 0$.

En términos de los números $i_{L/K}(\sigma)$, para $\sigma \in \mathrm{Gal}(L/K)$, la función $\phi_{L/K}$ se puede expresar como sigue:

Proposición 4.4. *Si $G = \mathrm{Gal}(L/K)$, entonces*

$$\phi_{L/K}(u) = \frac{1}{g_0} \sum_{\sigma \in G} \min\{i_{L/K}(\sigma), u+1\} - 1.$$

DEMOSTRACIÓN. Sea $\theta(u)$ la función definida por el lado derecho; claramente θ es una función continua, es lineal a tramos y se anula en $u = 0$. Si elegimos u tal que existe un entero $m \geq -1$ que satisface $m < u < m+1$, entonces la derivada

$$\begin{aligned} \theta'(u) &= \frac{1}{g_0}|\{\sigma \in G \,:\, i_{L/K}(\sigma) \geq m+2\}| \\ &\frac{1}{|G_0|}|G_{m+1}| = \frac{1}{(G_0 : G_{m+1})} \\ &\phi'_{L/K}(u) \end{aligned}$$

por definición de $\phi_{L/K}$. Hemos así probado que $\theta'(u) = \phi'_{L/K}(u)$ y como también $\theta(0) = 0 = \phi_{L/K}(0)$, entonces $\theta(u) = \phi_{L/K}(u)$. □

Teorema 4.5 (Herbrand). *Sea L/K una extensión finita de Galois y M/K una subextensión de Galois. Sean $G = \mathrm{Gal}(L/K)$ y $H = \mathrm{Gal}(L/M)$. Si $t = \phi_{L/K}(s)$, entonces $G_s H/H = (G/H)_t$.*

DEMOSTRACIÓN. Para cada $\sigma' \in G/H = \mathrm{Gal}(M/K)$ escojamos una preimagen $\sigma \in G$ de σ' cuyo valor $i_{L/K}(\sigma)$ sea máximo entre todas las preimágenes de σ'. Mostraremos primero que

$$i_{M/K}(\sigma') - 1 = \phi_{L/M}(i_{L/K}(\sigma) - 1).$$

Para esto, pongamos $m = i_{L/K}(\sigma)$. Si $\tau \in H$ está en H_{m-1}, entonces $i_{L/K}(\tau) \geq m$ y así $i_{L/K}(\tau\sigma) \geq m$, y por la forma en que elegimos σ se debe

entonces tener que $i_{L/K}(\tau\sigma) = m$. Por otra parte, si τ no está en H_{m-1} entonces $i_{L/K}(\tau) < m$ y así $i_{L/K}(\tau\sigma) = i_{L/K}(\tau)$. Así, en ambos casos se tiene que

$$i_{L/K}(\tau\sigma) = \min\{i_{L/K}(\tau), m\}$$

y consecuentemente, por (4.2) y (4.4), obtenemos

$$i_{M/K}(\sigma') = \frac{1}{e(L/M)} \sum_{\tau \in H} \min\{i_{L/K}(\tau), m\}.$$

Ahora, como $i_{L/K}(\tau) = i_{L/M}(\tau)$ por (4.1) ya que $\mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/K)$ y como $e' = e(L/M) = |H_0|$, entonces por (4.2) y (4.4) se tiene que

$$i_{M/K}(\sigma') = \frac{1}{|H_0|} \sum_{\tau \in H} \min\{i_{L/M}(\tau), m\} - 1 = \phi_{L/M}(m-1),$$

y como $m = i_{L/K}(\sigma)$, esto demuestra $(*)$.

Ahora, usando la fórmula $(*)$ obtenemos

$$\begin{aligned}
\sigma' \in G_s H/H &\Leftrightarrow i_{L/K}(\sigma) - 1 \geq s \quad \text{por definición de } G_s \\
&\Leftrightarrow \phi_{L/M}(i_{L/K}(\sigma) - 1) \geq \phi_{L/M}(s) \text{ porque } \phi_{L/M} \text{ es creciente} \\
&\Leftrightarrow i_{M/K}(\sigma') - 1 \geq \phi_{L/M}(s) \quad \text{por } (*) \\
&\Leftrightarrow \sigma' \in (G/H)_{\phi_{L/M}(s)} \quad \text{por definición de } (G/H)_t \\
&\Leftrightarrow \sigma' \in (G/H)_t \quad \text{ya que } t = \phi_{L/M}(s)
\end{aligned}$$

□

Consideremos ahora la inversa $\psi_{L/K} : [-1, \infty) \to [-1, \infty)$ de la función $\phi_{L/K}$. Entonces $\psi_{L/K}$ es continua, lineal a tramos, creciente, convexa y además $\psi_{L/K}(0) = 0$.

Lema 4.6. *Si v es un entero, entonces $\psi_{L/K}(v)$ también lo es.*

DEMOSTRACIÓN. Pongamos $u = \psi_{L/K}(v)$ y sea m un entero tal que $m \leq \psi(v) \leq m+1$. Como $v = \phi(\psi(v)) = \phi(u)$, usando el cálculo antes de (4.4):

$$v = \phi(u) = \frac{1}{g_0}(g_1 + \cdots + g_m + (u-m)g_{m+1},$$

se tiene que

$$g_0 v = g_1 + \cdots + g_m + (u-m)g_{m+1}$$

y como G_{m+1} está contenido en $G_0, \ldots, G_m$, entonces su orden g_{m+1} divide a los órdenes $g_0, \ldots, g_m$ y así

$$(u-m) = \frac{1}{g_{m+1}}(g_0 v - g_1 - \cdots - g_m)$$

es un entero; y como $m \in \mathbb{Z}$, entonces $u = \psi(v)$ también es un entero. □

Podemos ahora definir la *numeración superior* de los grupos de ramificación mediante

$$G^v := G_{\psi_{L/K}(v)}$$

o, en forma equivalente,

$$G^{\phi_{L/K}(u)} := G_u.$$

Claramente, $G^{-1} = G$, $G^0 = G_0$ y $G^t = \{1\}$ para t suficientemente grande. Nótese que el conocimiento de los G^v es equivalente al conocimiento de los G_u ya que

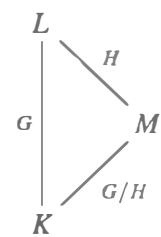
$$\psi_{L/K}(v) = \int_0^v (G^0 : G^t)dt.$$

Usando la numeración de supraíndices de los grupos de ramificación y el teorema de Herbrand determinaremos los grupos de ramificación del cociente G/H en términos de los grupos de ramificación de G, pero antes necesitamos la propiedad de transitividad de las funciones $\phi_{L/K}$ y $\psi_{L/K}$:

Proposición 4.7. *Sea L/K una extensión finita de Galois de campos locales y sea M/K una subextensión. Entonces, las funciones ϕ y ψ satisfacen las siguientes fórmulas de transitividad:*

$$\phi_{L/K} = \phi_{M/K} \circ \phi_{L/M} \qquad \text{y} \qquad \psi_{L/K} = \psi_{L/M} \circ \psi_{M/K}.$$

DEMOSTRACIÓN. Para las extensiones



los índices de ramificación satisfacen $e(L/K) = e(L/M)e(M/K)$ y sabemos que $e(L/K) = |G_0|$, $e(L/M) = |H_0|$ y $e(M/K) = |(G/H)_0|$.

Del teorema de Herbrand y del teorema de isomorfismo de Noether obtenemos que

$$(G/H)_v = G_u H/H = \frac{G_u H/H_u}{H/H_u} = G_u/H_u$$

con $v = \phi_{L/K}(u)$.

Ahora, si $u > -1$ no es un entero, la derivada de la composición $\phi_{M/K} \circ \phi_{L/M}$ en u es

$$(*) \qquad \phi'_{M/K}(\phi_{L/M}(u)) \cdot \phi'_{L/M}(u) = \phi'_{M/K}(v) \cdot \phi'_{L/M}(u)$$

con $v = \phi_{L/M}(u)$. Y como, por definición de ϕ, sus derivadas son

$$\phi'_{L/M}(u) = \frac{1}{(H_0 : H_u)} \frac{H_u}{H_0} = \frac{1}{e(L/M)} |H_u|$$

$$\phi'_{M/K}(v) = \frac{1}{((G/H)_0 : (G/H)_v)} \frac{1}{e(M/K)} |(G/H)_v|$$

entonces la derivada $(*)$ se puede escribir como

$$\begin{aligned} \phi'_{M/K}(v) \cdot \phi'_{L/M}(u) &= \frac{1}{e(L/M)} |H_u| \cdot \frac{1}{e(M/K)} |(G/H)_v| \\ &- \frac{1}{e(L/K)} |H_u||(G/H)_v| \\ &= \frac{1}{e(L/K)} |H_u| \cdot \frac{G_u}{H_u} \quad \text{ya que } (G/H)_v = G_u/H_u \\ &\quad \frac{1}{e(L/K)} |G_u| \\ &= \phi'_{L/K}(u). \end{aligned}$$

Así, $\phi_{L/K}(u) = \phi_{M/K} \circ \phi_{L/M}(u) + \textit{constante}$ y como $\phi_{L/K}(0) = 0 = \phi_{M/K} \circ \phi_{L/M}(0)$, entonces $\phi_{L/K} = \phi_{M/K} \circ \phi_{L/M}$ como se quería. Tomando inversas se sigue la correspondiente fórmula para las ψ. □

De esta proposición y del teorema de Herbrand obtenemos los grupos de ramificación del cociente G/H, i.e., de las subextensiones M/K de L/K, mostrando que con la notación de supraíndices, la numeración se mantiene:

Teorema 4.8. *Si L/K es una extensión finita de Galois de campos locales y M/K es una subextensión de Galois y si $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/M)$ y $G/H = \mathrm{Gal}(M/K)$, entonces para todo v se tiene que*

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

DEMOSTRACIÓN. Sea $u = \psi_{M/K}(v)$. Entonces

$$\begin{aligned} (G/H)^v &= (G/H)_u && \text{por definición de numeración superior} \\ &= G_w H/H && \text{por el teorema de Herbrand con } w = \psi_{L/M}(u) \\ &= G^v H/H, \end{aligned}$$

la última igualdad porque $w = \psi_{L/M}(u) = \psi_{L/M}(\psi_{M/K}(v)) = \psi_{L/K}(v)$ por la proposición anterior, y así, por definición de numeración superior, $G^v = G_w$ ya que $w = \psi_{L/K}(v)$. □

4.2 Ramificación en el caso ciclotómico

Como un ejemplo, determinamos los grupos de ramificación superior de las extensiones ciclotómicas de $\mathbb{Q}_p$. Recordemos primero, (1.64) o (2.70), que si n es coprimo con p entonces la extensión $\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p$ es no ramificada, de tal forma que en este caso los grupos de ramificación son triviales. En el caso restante, cuando $n = p^m$, $m \geq 1$, sabemos por (2.68) que la extensión $\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p$ es totalmente ramificada de grado $\varphi(p^m) = (p-1)p^{m-1}$ con grupo de Galois $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^m\mathbb{Z})^*$, al que denotaremos por $G(m)$. Para determinar los grupos de ramificación de $G(m)$, si v es un entero tal que $0 \leq v \leq m$, denotemos por $G(m)^v$ al subgrupo de $G(m)$ dado por

$$G(m)^v := \{a \in G(m) \ : \ a \equiv 1 \text{ mód } p^v\}.$$

Observamos que se tiene un isomorfismo $G(m)/G(m)^v \simeq G(v)$ que manda $x \in G(m)$ a su reducción módulo p^v. Ahora, como $G(v) = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^v})/\mathbb{Q}_p)$ entonces se tiene un isomorfismo

$$G(m)^v \simeq \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p(\mu_{p^v})).$$

Teorema 4.9. *Los grupos de ramificación G_u de $G(m) \simeq \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p)$ son*

$$\begin{array}{lll} G_0 & G(m) & \\ G_u = & G(m)^1 & \text{si } 1 \leq u \leq p-1 \\ G_u = & G(m)^2 & \text{si } p \leq u \leq p^2-1 \end{array}$$

$$G_u \quad G(m)^m = \{1\} \quad \text{si } p^{m-1} \leq u.$$

DEMOSTRACIÓN. Sea $1 \neq a \in G(m)$ y sea $\sigma_a \in \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^v})/\mathbb{Q}_p)$ el elemento correspondiente. Sea v el mayor entero tal que $a \equiv 1$ mód p^v; entonces $a \in G(m)^v$ y $a \notin G(m)^{v+1}$. Por otro lado,

$$i_G(\sigma_a) = v_{\mathbb{Q}_p(\mu_{p^m})}(\sigma_a(\zeta) - \zeta) = v_{\mathbb{Q}_p(\mu_{p^m})}(\zeta^q - \zeta) = v_{\mathbb{Q}_p(\zeta\mu_{p^m})}(\zeta^{q-1} - 1)$$

(factorizando a ζ y observando que $v_{\mathbb{Q}_p(\mu_{p^m})}(\zeta) = 0$).

Ahora, como ζ^{q-1} es una raíz primitiva p^{m-v}-ésima de la unidad, por (2.68)(2) el elemento $\zeta^{q-1} - 1$ es un primo del campo ciclotómico $\mathbb{Q}_p(\mu_{p^{m-v}})$. Se sigue que

$$\begin{array}{lll} i_G(\sigma_a) & v_{\mathbb{Q}_p(\mu_{p^m})}(\zeta^{q-1} - 1) & \\ - & [\mathbb{Q}_p(\mu_{p^m}) : \mathbb{Q}_p(\mu_{p^{m-v}})] \cdot v_{\mathbb{Q}_p(\mu_{p^m})}(\zeta) & \\ = & [\mathbb{Q}_p(\mu_{p^m}) : \mathbb{Q}_p(\mu_{p^{m-v}})] & \text{ya que } v_{\mathbb{Q}_p(\mu_{p^m})}(\zeta) = 1 \\ & |\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p(\mu_{p^{m-v}})| & \\ & p^v. & \end{array}$$

Con este cálculo a la mano observamos que si $p^{k-1} \leq u \leq p^k - 1$, entonces $\sigma_a \in G_u$ si y sólo si $v \geq k$ y por lo tanto $G_u = G(m)^v$. □

Habiendo definido los grupos de ramificación G^v para todo número real $v \geq -1$, es natural preguntarse para cuáles de estos números v los grupos de ramificación cambian; a estos números se les llama *saltos* de la filtración $\{G^v\}$ de $G = \mathrm{Gal}(L/K)$. Es decir, v es un *salto* de la filtración $\{G^u\}$ si para todo $\varepsilon > 0$ se tiene que

$$G^v \neq G^{v+\varepsilon}.$$

En el caso cuando L/K es abeliana, el teorema de Hasse-Arf que probaremos en (4.13) nos dice que estos saltos son *enteros*. En el caso ciclotómico (que por supuesto es abeliano), donde los grupos de ramificación ya los hemos calculado, esto se puede probar directamente:

Corolario 4.10 (Hasse-Arf en el caso ciclotómico). *Si G es el grupo de Galois de $\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p$, entonces los saltos en la filtración $\{G^v\}$ de G son enteros. Más aún,*

$$G^v = G(m)^v \quad \text{para } 0 \leq v \leq m$$

y

$$G^v = \{1\} \qquad \text{para } v \geq m.$$

DEMOSTRACIÓN. Los saltos de la filtración $\{G_u\}$ ocurren cuando $u = p^k - 1$ con $0 \leq k \leq m-1$ (el caso $p = 2$ es excepcional porque 0 no es un salto; esto es porque para $p = 2$,

$$G(m) = \mathrm{Gal}(\mathbb{Q}_2(\mu_{2^m})/\mathbb{Q}_2) \simeq (\mathbb{Z}/2^m\mathbb{Z})^* \simeq \{a \in \mathbb{Z} : a \text{ es impar y } 1 \leq a \leq 2^m\}$$
$$= \{a \in G(m) \ : \ a \equiv 1 \bmod 2\} = G(m)^1).$$

Ahora, como los cocientes $G(m)/G(m)^v \simeq G(v)$ entonces el orden

$$(*) \qquad |G(m)^v| = |G(m)/G(v)| = \frac{(p-1)p^{m-1}}{(p-1)p^{v-1}} = p^{m-v}.$$

Sin embargo, por el cálculo de los grupos de ramificación del teorema anterior, $G_j = G(m)^1$ si $1 \leq j \leq p-1$ y hay $p-1$ de estos grupos con órdenes $|G_j| = p^{m-1}$ por $(*)$. Para $G_j = G(m)^2$, i.e., cuando $p \leq j \leq p^2 - 1$, hay $p^2 - p$ de estos grupos de órdenes $|G_j| = p^{m-2}$ por $(*)$. Continuando recursivamente, para los grupos $G_j = G(m)^k$, i.e., cuando $p^{k-1} \leq j \leq p^k - 1$, hay $p^k - p^{k-1}$ de estos grupos, de órdenes $G_j = p^{m-k}$ por $(*)$. Finalmente, mostraremos que $\phi(p^k - 1) = k$. En efecto, usando la fórmula antes de (4.4),

$$\begin{aligned}
\phi(p^k - 1) &= \frac{1}{g_0}(g_1 + \cdots + g_{p^k-1}) \\
&\quad \frac{1}{(p-1)p^{m-1}}[p^{m-1}(p-1) + \cdots + p^{m-k}(p^k - p^{k-1})] \\
&= \frac{1}{(p-1)p^{m-1}}[p^{m-1}(p-1) + \cdots + p^{m-k}p^{k-1}(p-1)] \\
&= \frac{1}{(p-1)p^{m-1}}[p^{m-1}(p-1) + \cdots + p^{m-1}(p-1)] \\
&\quad \frac{1}{(p-1)p^{m-1}}[p^{m-1}(p-1)\overbrace{(1 + \cdots + 1)}^{k \text{ veces}}] = k,
\end{aligned}$$

que es lo queríamos probar. □

4.3 El teorema de Hasse-Arf

Antes de considerar el caso general de una extenión finita de Galois de campos locales, consideraremos las extensiones de Lubin-Tate, para las cuales se tiene la siguiente generalización del cálculo de los grupos de ramificación de las extensiones ciclotómicas (4.9):

Teorema 4.11. *Sea $K_{\pi,n}/K$ una extensión de Lubin-Tate. Entonces los grupos de ramificación G_i de $G = \mathrm{Gal}(K_{\pi,n}/K)$ son*

$$G_i = \mathrm{Gal}(K_{\pi,n}/K_{\pi,j})$$

para $q^{j-1} \leq i \leq q^j - 1$.

DEMOSTRACIÓN. Por (3.22) se tiene un isomorfismo

$$\mathrm{Gal}(K_{\pi,j}/K) \simeq U_K/U_K^{(j)}$$

para cada j, y este isomorfismo está dado asociando a una clase $u \in U_K$ mód $U_K^{(j)}$ el automorfismo $\sigma \in \mathrm{Gal}(K_{\pi,j}/K)$ tal que $\sigma(\lambda) = [u^{-1}]_F(\lambda)$ para $\lambda \in F(j)$.

Por (3.25), el isomorfismo anterior es precisamente el símbolo de norma residual $(\ ,\ K_{\pi,j}/K)$ y por lo tanto,

$$\mathrm{Gal}(K_{\pi,j}/K) \simeq (U_K^{(j)},\ K_{\pi,j}/K).$$

Así, si consideramos la torre de campos $K \subseteq K_{\pi,j} \subseteq K_{\pi,n}$, la sucesión exacta corta dada por teoría de Galois:

$$1 \to \mathrm{Gal}(K_{\pi,n}/K_{\pi,j}) \rightarrowtail \mathrm{Gal}(K_{\pi,n}/K) \twoheadrightarrow \mathrm{Gal}(K_{\pi,j}/K) \to 1$$

implica que el grupo $\mathrm{Gal}(K_{\pi,n}/K_{\pi,j})$ consiste de los elementos del grupo $U_K/U_K^{(n)}$ $\mathrm{Gal}(K_{\pi,n}/K)$ que van a dar al 1 de $U_K/U_K^{(j)} \simeq \mathrm{Gal}(K_{\pi,j}/K)$, i.e.,

$$\mathrm{Gal}(K_{\pi,n}/K_{\pi,j}) = U_K^{(j)}/U_K^{(n)} = (U_K^{(j)},\ K_{\pi,n}/K). \tag{1}$$

Debemos entonces probar que

$$G_i(K_{\pi,n}/K) = (U_K^{(j)},\ K_{\pi,n}/K)$$

para $q^{j-1} \leq i \leq q^j - 1$.

Para esto, observemos que, por (3.22), el grupo $U_K/U_K^{(1)} \simeq \mathrm{Gal}(K_{\pi,1}/K)$ tiene orden $q^{1-1}(q-1) = q-1$ y el grupo $U_K/U_K^{(n)} \simeq \mathrm{Gal}(K_{\pi,n}/K)$ tiene orden $q^{n-1}(q-1)$, donde $q = |K|$. De estas observaciones y de (1) se sigue

que el grupo $U_K^{(1)}/U_K^{(n)}$ tiene orden q^{n-1} y además tiene índice $q-1$ (coprimo con p) en $U_K/U_K^{(n)}$; se sigue que $U_K^{(1)}/U_K^{(n)}$ es un p-subgrupo de Sylow de $U_K/U_K^{(n)}$. Por otra parte, $G_1(K_{\pi,n}/K)$ también es un p-subgrupo de Sylow de $\mathrm{Gal}(K_{\pi,n}/K)$ por (1.77)(3).

Ahora, sea $\sigma \in G_1(K_{\pi,n}/K)$ y sea $u \in U_K$ tal que $\sigma = (u^{-1}, K_{\pi,n}/K)$. Como el isomorfismo $(\ , K_{\pi,n}/K) : U_K/U_K^{(n)} \simeq \mathrm{Gal}(K_{\pi,n}/K)$ manda el p-subgrupo de Sylow en el p-subgrupo de Sylow, entonces manda a $U_K^{(1)}/U_K^{(n)}$ en $G_1(K_{\pi,n}/K)$, y como $\sigma \in G_1(K_{\pi,n}/K)$, entonces se debe tener que $\sigma \in U_K^{(1)}$.

Ahora, pongamos $u = 1 + \varepsilon\pi^m$ con $\varepsilon \in U_K$ y sea $\lambda \in F(n) - F(n-1)$. Por (3.22) λ es un elemento primo de $K_{\pi,n}$ y por (3.25) se tiene que

$$\sigma(\lambda) = [u]_F(\lambda) = F(\lambda, [\varepsilon\pi^m]_F(\lambda)).$$

Si $m \geq n$, entonces

$$\sigma(\lambda) = F(\lambda, [\varepsilon\pi^m]_F(\lambda)) = F(\lambda, 0) = 0,$$

porque $[\pi^m]_F(\lambda) = 0$ ya que $\lambda \in F(n) \subseteq F(m)$. Se sigue que $\sigma = 1$ y así

$$v_{K_{\pi,n}}(\sigma(\lambda) - \lambda) = v_{K_{\pi,n}}(0) = \infty.$$

Si $m < n$, entonces $\lambda_{n-m} := [\pi^m]_F(\lambda)$ es un elemento primo de $K_{\pi,n-m}$ por (3.22) y así también $[\varepsilon\pi^m]_F(\lambda) = [\varepsilon]_F(\lambda_{n-m})$ es un primo de $K_{\pi,n-m}$. Ahora, como $K_{\pi,n}/K_{,\pi,n-m}$ es totalmente ramificada de grado q^m por (3.22), podemos escribir $[\varepsilon\pi^m]_F(\lambda) = \varepsilon_0\lambda^{q^m}$ con $\varepsilon_0 \in U_{K_{\pi,n}}$. De las igualdades $F(x, 0) = x$ y $F(0, y) = y$ se sigue que

$$F(x, y) = x + y + xyG(x, y)$$

con $G(x, y) \in \mathcal{O}_K[[x]]$ y por lo tanto

$$\begin{aligned}
\sigma(\lambda) - \lambda &= F(\lambda, \varepsilon_0\lambda^{q^m}) - \lambda \\
&= \varepsilon_0\lambda^{q^m} + \lambda + \varepsilon_0\lambda^{q^m+1}b - \lambda \quad \text{para algún } b \in \mathcal{O}_{K_{\pi,n}} \\
&= \varepsilon_0\lambda^{q^m} + a\lambda^{q^m+1} \qquad \text{con } a = \varepsilon_0 b \in \mathcal{O}_{K_{\pi,n}}.
\end{aligned}$$

Se sigue que

$$\begin{aligned}
v_{K_{\pi,n}}(\sigma(\lambda) - \lambda) &= v_{K_{\pi,n}}(\varepsilon_0\lambda^{q^m} + a\lambda^{q^m+1}) \\
&= v_{K_{\pi,n}}(\lambda^{q^m}(\varepsilon_0 + a\lambda))
\end{aligned}$$

ya que $v_{K_{\pi,n}}(\varepsilon_0+a\lambda) = 0$ porque $\varepsilon_0+a\lambda = \varepsilon_0(1+a\lambda/\varepsilon_0)$ con $1+a\lambda/\varepsilon_0 \in U_K^{(1)}$, y así los dos factores del lado derecho de la igualdad anterior son unidades.

Por lo tanto,

$$(*)\quad i_{K_{\pi,n}/K}(\sigma) = v_{K_{\pi,n}}(\sigma(\lambda)-\lambda) = v_{K_{\pi,n}}(\lambda^{q^m}(\varepsilon_0+a\lambda) = \begin{cases} q^m & \text{si } m < n \\ \infty & \text{si } m \geq n. \end{cases}$$

Supongamos que i es tal que $q^{j-1} \leq i \leq q^j - 1$. Para $u = 1+\varepsilon\pi^m \in U_K^{(m)}$ con $\varepsilon \in U_K$, si sucediera que $u \in U_K^{(j)}$ entonces $m \geq j$, i.e., $i_{K_{\pi,n}}(\sigma) \geq q^j \geq i+1$ (la primera desigualdad por $(*)$ y la segunda desigualdad porque $i \leq q^j - 1$) y por lo tanto $\sigma \in G_j(K_{\pi,n}/K)$. Esto muestra que

$$(U_K^{(j)}, K_{\pi,n}/K) \subseteq G_i(K_{\pi,n}/K).$$

Recíprocamente, si $\sigma \in G_i(K_{\pi,n}/K)$ y $\sigma \neq 1$ entonces $i_{K_{\pi,n}/K}(\sigma) = q^m > i \geq q^{j-1}$ (la igualdad por $(*)$ y las desigualdades por la elección de i); se sigue que $m \geq j$ y así $u \in U_K^{(j)}$; por lo tanto,

$$G_i(K_{\pi,n}/K) \subseteq (U_K^{(j)}, K_{\pi,n}/K).$$

□

Así, en completa analogía con el caso ciclotómico los grupos de ramificación de $G = \mathrm{Gal}(K_{\pi,n}/K)$ son

$$\begin{array}{lcl} G_0 & = & G \\ G_{q-1} & & G_{q-2} \quad = \quad G_1 \\ G_{q^2-1} & = & G_{q^2-2} \quad\quad G_q \\ & \vdots & \\ G_{q^n-1} & = & \{1\}. \end{array}$$

Podemos ahora probar otro caso especial del teorema de Hasse-Arf, para las extensiones de Lubin-Tate, como consecuencia directa del cálculo de los grupos de ramificación anterior:

Corolario 4.12 (Hasse-Arf para extensiones de Lubin-Tate). *Si G es el grupo de Galois de $K_{\pi,m}/K$, entonces los saltos en la filtración $\{G^v(K_{\pi,m}/K)\}$ de G son enteros.*

DEMOSTRACIÓN. Por el teorema previo, los saltos de la filtración $\{G_u(K_{\pi,m}/K)\}$ son los enteros $q^n - 1$ para $n = 0, 1, \ldots, m-1$ ($q = 2$ es una excepción ya que 0 no es un salto, por un argumento similar al del caso ciclotómico en (4.10)), y por lo tanto los saltos de la filtración $\{G^u(K_{\pi,m}/K)\}$ son los números $\phi_{K_{\pi,m}/K}(q^n - 1)$, y éstos se calculan como en (4.10), usando el hecho de que sus grupos de ramificación son $G_i(K_{\pi,m}/K) = \mathrm{Gal}(K_{\pi,m}/K_{\pi,j})$ para $q^{j-1} \leq i \leq q^j - 1$, y por lo tanto sus órdenes son

$$g_i := |G_i(K_{\pi,m}/K)| = |\mathrm{Gal}(K_{\pi,m}/K_{\pi,j})| = q^{m-j},$$

la última igualdad por (3.22), habiendo $q^j - q^{j-1}$ de estos grupos. Al igual que en la parte final de la demostración de (4.10) (usando la fórmula antes de (4.4)), se sigue que $\phi(q^n - 1) = n$, para $0 \leq n \leq m-1$. □

El caso general del teorema de Hasse-Arf se reduce al anterior, como veremos a continuación:

Teorema 4.13 (Hasse-Arf). *Sea L/K una extensión abeliana finita de campos locales. Entonces, los saltos en la filtración $\{G^u\}_{u \geq -1}$ de $G = \mathrm{Gal}(L/K)$ son enteros. En otras palabras, si $G_j \neq G_{j+1}$ entonces $\phi_{L/K}(j)$ es un entero.*

DEMOSTRACIÓN. Por (1.76) podemos suponer que L/K es totalmente ramificada ya que $G^u(L/K) = G^u(L/L_0)$ para $u > -1$, donde L_0 es la máxima extensión no ramificada de K contenida en L.

Ahora, si L/K es totalmente ramificada y si π_L es un elemento primo de L, entonces el polinomio mínimo de π_L, $f(x) = \mathrm{Irr}(\pi_L, K)$ es de Eisenstein por (1.54) y así su término independiente es un primo π de K; pero este término independiente π es precisamente $N_{L/K}(\pi_L)$, y así $\pi = N_{L/K}(\pi_L)$ es un primo de K y por lo tanto $(\pi) \times U_K^{(m)} \subseteq N_{L/K}(L^*)$ para m suficientemente grande. Se sigue que L está contenido en el campo de clases de $(\pi) \times U_K^{(m)}$ el cual, por (3.26), es el campo de Lubin-Tate $K_{\pi,m}$; se tiene así una torre de campos $K \subseteq L \subseteq K_{\pi,m}$ y por el teorema de Herbrand (4.5) se tiene que

$$G^u(L/K) = \frac{G^u(K_{\pi,m}/K)\mathrm{Gal}(K_{\pi,m}/L)}{\mathrm{Gal}(K_{\pi,m}/L)}.$$

Así, si u es un salto de la filtración $\{G^u(L/K)\}$ entonces u es un salto de la filtración $\{G^u(K_{\pi,m}/K)\}$. Por lo tanto, podemos suponer que $L = K_{\pi,m}$, y este es caso del corolario anterior. □

El resultado principal de la teoría de ramificación es:

Teorema 4.14. *Si L/K es una extensión abeliana finita de campos locales, entonces el símbolo de norma residual*

$$(\ ,L/K) : K^* \longrightarrow \mathrm{Gal}(L/K)$$

lleva el grupo de unidades $U_K^{(n)}$ en el grupo de ramificación $G^n(L/K)$ de $\mathrm{Gal}(L/K)$ *para toda $n \geq 0$.*

DEMOSTRACIÓN. Si L_0/K es la máxima extensión no ramificada de K contenida en L entonces, por (1.76), para $t \geq -1$ los grupos de ramificación son iguales: $G^t(L/K) = G^t(L/L_0)$. Y por otra parte, por la funtorialidad (2.34)(1)(i) del morfismo de reciprocidad, para la torre de campos $K \subseteq L_0 \subseteq L$ se tiene un diagrama conmutativo:

$$\begin{array}{ccc} L_0^* & \xrightarrow{(\ ,L/L_0)} & \mathrm{Gal}(L/L_0) \\ {\scriptstyle N_{L_0/K}}\downarrow & & \downarrow \\ K^* & \xrightarrow[(\ ,L/K)]{} & \mathrm{Gal}(L/K) \end{array}$$

y por lo tanto, para $U_{L_0}^{(n)} \subseteq L^*$, se tiene que

$$(U_{L_0}^{(n)}, L/L_0) = (N_{L_0/K} U_{L_0}^{(n)}, L/K)$$

y como L_0/K es no ramificada, por (2.5) se tiene que $N_{L_0/K} U_{L_0}^{(n)} = U_K^{(n)}$ y así

$$(U_{L_0}^{(n)}, L/L_0) = (U_K^{(n)}, L/K);$$

y por lo tanto, podemos reemplazar la extensión L/K por L/L_0, i.e., podemos suponer que L/K es abeliana totalmente ramificada. En este caso, por (1.54), si π_L es un primo de L entonces $\pi_K = N_{L/K}(\pi_L)$ es un primo de K y así $\pi_K \in N_{L/K} L^*$ y por lo tanto, $(\pi_K) \times U_K^{(m)} \subseteq N_{L/K} L^*$ para algún m y consecuentemente el campo L está contenido en el campo de clases del grupo de normas $(\pi_K) \times U_K^{(m)} \subseteq K^*$ que, por (3.26), es el campo de Lubin-Tate $K_{\pi_K,m}$, i.e., $L \subseteq K_{\pi_K,m}$ para algún m. Ahora, para la torre de campos $K \subseteq L \subseteq K_{\pi_K,m}$, por (4.8), se tiene que

$$(1) \qquad G^t(K_{\pi_K,m}/K) \cdot \mathrm{Gal}(K_{\pi_K,m}/L)/\mathrm{Gal}(K_{\pi_K,m}/L) = G^t(L/K)$$

y por la funtorialidad (2.34)(1)(ii) del morfismo de reciprocidad aplicada a la torre $K \subseteq L \subseteq K_{\pi_K,m}$,

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,K_{\pi_K,m}/K)} & \mathrm{Gal}(K_{\pi_K,m}/K) \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ K^* & \xrightarrow[(\ ,L/K)]{} & \mathrm{Gal}(L/K) \end{array}$$

para $U_K^{(n)} \subseteq K^*$ se tiene que

$$(U_K^{(n)}, K_{\pi_K,m}/K) = (U_K^{(n)}, L/K) \tag{2}$$

de tal forma que, de (1) y (2), para probar que

$$(U_K^{(n)}, L/K) = G^n(L/K) \qquad \text{para } n \geq 0$$

basta mostrar que

$$(U_K^{(n)}, K_{\pi_K,m}/K) = G^n(K_{\pi_K,m}/K),$$

es decir, podemos reemplazar L por el campo de Lubin-Tate $K_{\pi_K,m}$.

Ahora, por (3.22) (ver la demostración de (4.11)), el símbolo de norma residual es un isomorfismo de $U_K/U_K^{(n)}$ en $\mathrm{Gal}(K_{\pi_K,m}/K)$ de tal forma que

$$G_i(K_{\pi_K,m}/K) = \mathrm{Gal}(K_{\pi_K,m}/K) = (U_K^{(n)}, K_{\pi_K,m}/K)$$

para $q^{n-1} \leq i \leq q^n - 1$. Finalmente, como vimos en la parte final de la demostración de (4.12), $\phi_{K_{\pi_K,m}/K}(q^n - 1) = n$ y por lo tanto para $i = q^n - 1$ se tiene que

$$(U_K^{(n)}, K_{\pi_K,m}/K) = G_{q^n-1}(K_{\pi_K,m}/K) = G^n(K_{\pi_K,m}/K),$$

como se quería demostrar. □

4.4 Ejercicios

1. Sean L/K una extensión finita de Galois de campos locales y $G = \mathrm{Gal}(L/K)$. Sea $f = f_{L/K}$ el *conductor* de L/K, i.e., el menor entero f tal que $(U_K^{(f)}, L/K) = 0$. Demuestre que $f_{L/K} = \phi_{L/K}(c) + 1$, donde c es el mayor entero tal que el grupo de ramificación G_c es $\neq 0$.
2. Sean L/K una extensión finita de Galois de campos locales y $G = \mathrm{Gal}(L/K)$. Sea $\chi : G \to \mathbb{C}^*$ un carácter y sea $L_\chi := L^{\mathrm{Ker}(\chi)}$ el campo fijo de $\mathrm{Ker}\,(\chi) \subseteq G$.
   (i) Demuestre que L_χ/K es una extensión cíclica.
   (ii) Si $f(\chi)$ es el conductor de L_χ/K y G_i son los grupos de ramificación de G de órdenes $g_i = |G_i|$, demuestre que

$$f(\chi) = \sum_{i=0} \frac{g_i}{g_0}(1 - \chi(G_i)),$$

   donde $\chi(G_i) = \dfrac{1}{g_i} \displaystyle\sum_{\sigma \in G_i} \chi(\sigma)$ es el *promedio* de χ en G_i.
3. Sea L/K una extensión separable de campos valuados discretos completos tal que $\overline{L}/K$ es separable. Sean $G = \mathrm{Gal}(L/K)$ y G_i los grupos de ramificación de L/K.
   (i) Demuestre que el grupo G_0 actúa sobre los cocientes G_i/G_{i+1} por medio de conjugaciones.
   (ii) Determine estas acciones en términos de los isomorfismos λ_i de (1.65) y ϑ_i de (1.82). Específicamente:
      (a) Si $\sigma \in G_0$ y $\tau \in G_i/G_{i+1}$, $i \geq 1$, demuestre que

$$\lambda_i(\sigma\tau\sigma^{-1}) = \lambda_0(\sigma)^i \lambda_i(\tau).$$

      (b) Si $\sigma \in G_0$ y $\tau \in G_i$, $i \geq 1$, demuestre que $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+1}$ si y sólo si $\sigma^i \in G_1$ ó $\tau \in G_{i+1}$.
      (c) Si G es abeliano y e_0 es el orden del cociente G_0/G_1, demuestre que para todo entero i no divisible por e_0 se tiene que $G_i = G_{i=1}$.
4. Usando el último inciso del problema anterior y el teorema de Herbrand, demuestre que si el teorema de Hasse-Arf es verdadero para toda extensión cíclica de orden una potencia de un primo, entonces es verdadera en general.
5. Sean L/K una extensión finita de Galois de campos locales, $G = \mathrm{Gal}(L/K)$ y $p = \mathrm{car}\,(K)$. Demuestre que si los enteros $i \geq 1$ tales que $G_i \neq G_{i+1}$ son

todos divisibles por p, entonces son de la forma $i = p^k i_0$ con $1 \leq k \leq h$, donde $p^h i_0 = e/(p-1)$, $e = e(L/K)$ y el grupo G_1 es cíclico de orden p^h.

6. Si L/K es una extensión abeliana finita de campos locales, $G = \mathrm{Gal}(L/K)$ y G_i son sus grupos de ramificación, muestre que

$$[L : K] = \prod_{i=0}^{\infty} [G_i : G_{i+1}].$$

7. Sea $\psi_{L/K}$ la función inversa de $\phi_{L/K}$. Si L/K es cíclica totalmente ramificada de grado primo ℓ y $\sigma \in \mathrm{Gal}(L/K)$ es un generador, sea $t := i_G(\sigma) - 1$ (véase §2.1.1).
   (i) Si $\ell = p = \mathrm{car}\,(K)$, demuestre que

$$\psi_{L/K}(x) = \begin{cases} x & \text{si } x \leq t \\ t + \ell(x - t) & \text{si } x \geq t, \end{cases}$$

   es decir, $\psi_{L/K}$ es la función ψ de (2.17).
   (ii) Si L/K es mansa, i.e., si $\ell \neq p = \mathrm{car}\,(K)$, entonces $\psi_{L/K}$ es la función $i \mapsto \ell i$.

8. Si L/K es cíclica totalmente ramificada de grado primo ℓ, $G = \mathrm{Gal}(L/K)$ y t es como en el problema anterior, demuestre que la sucesión siguiente es exacta:

$$0 \to G \xrightarrow{\vartheta_t} U_L^{(t)}/U_L^{(t+1)} \xrightarrow{N_t} U_K^{(t)}/U_K^{(t+1)},$$

donde ϑ_t es el morfismo dado en (1.82) y N_t es el morfismo inducido por el paso al cociente de la norma $N_{L/K}$ (véase §2.1, especialmente (2.6), (2.7), (2.17) y (2.18)).

Bibliografía

[1] Artin, E. *Collected Papers*. Addison-Wesley, Reading MA (1965).

[2] Artin, E. *Galois Theory*. 2nd. Ed. Notre Dame Lecture Notes, University of Notre Dame Press, South Bend, IN (1971).

[3] Artin, E. *Algebraic Numbers and Algebraic Functions*. Gordon and Breach, New York (1967).

[4] Artin, E. *Theory of Algebraic Numbers*. Notes by G. Würgues. Götingen (1956).

[5] Artin, E., Tate, J. *Class Field Theory*. Addison-Wesley, Reading MA (1989).

[6] Cassels, J.W.S. *Local Fields*. Cambridge University Press, London (1986).

[7] Cassels, J.W.S., Fröhlich, A. (Eds.) *Algebraic Number Theory*. Academic Press, London (1990).

[8] Chevalley, C. *Sur la théorie du corps de classes dans les corps finis et les corps locaux*. J. Fac. Sci. Tokyo Imp. Univ. Ser. Math. **2** (1933), 363-476.

[9] Chevalley, C. *Class field theory*. Nagoya University, Nagoya, (1954).

[10] Cohn, P.M. *Algebraic Numbers and Algebraic Functions*. Chapman & Hall, London (1991).

[11] Curtis, C., Reiner, I. *Representation Theory of Finite Groups and Associative Algebras*. Wiley, New York (1962).

[12] de Shalit, E. *The explicit reciprocity law in local field theory*. Duke Math. J. **53** (1986), 163-176.

[13] Dwork, B. *Norm residue symbol in local number fields*. Abh. Math. Sem. Univ. Hamburg **22** (1958), 180-190.

[14] Fesenko, I.B.; Vostokov, S.V. *Local Fields and their Extensions: A constructive approach*. American Mathematical Society, Trans. of Mathematical Monographs **121**, (1993), Providence, RI.

[15] Hasse, H. *Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper*. J. Fac. Sci. Tokyo, **2** (1934), 477-498.

[16] Hasse, H. *Theorie der relativ-zyklischen algebraischen Funktionenkörper inbesondere bei endlichen Konstantenkörper*. Crelle's Journal **172** (1934), 37-54.

[17] Hasse, H. *Theorie der Differentiale in algebraischen Funktionenkörper mit vollkommenen Konstantenkörper*. Crelle's Journal **172** (1934), 55-64.

[18] Hasse, H. *Zahlentheorie*. Akademie-Verlag, Berlin (1949).

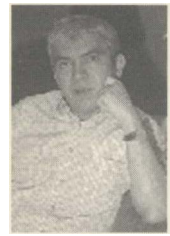
[19] Hazewinkel, M. *Abelian extensions of local fields*. Doctoral Dissertation, Universiteit van Amsterdam, Amsterdam (1969).

[20] Hazewinkel, M. *Local class-field theory is easy*. Adv. Math. **18** (1975), 148-181.

[21] Herbrand, J. *Sur la théorie des groupes de decomposition, d'inertie et de ramification.* J. Math. Pures et Appl. **10** (1931), 481-498.
[22] Huppert, B. *Endliche Gruppen I.* Springer-Verlag, Berlin (1983).
[23] Iwasawa, K. *Explicit formulas for the norm residue symbol.* J. Math. Soc. Japan **20** (1968), 151-164.
[24] Iwasawa, K. *Local Class Field Theory.* Oxford University Press, Oxford (1986).
[25] Kürschák, J. *Über Limesbildung und allgemeine Körpertheorie.* Crelle's Journal **142** (1913), 211-253.
[26] Lang, S. *Algebra.* 3rd. Ed. Addison Wesley, Reading, MA (1993).
[27] Lorenz, F. *Algebraische Zahlentheorie.* B.I. Wissenschaftsverlag, Mannheim (1993).
[28] Lubin, J.; Tate, J. *Formal complex multiplication in local fields.* Ann. of Math. **81** (1965), 380-387.
[29] Matsumura, H. *Commutative Algebra.* 2nd. Ed. Benjamin, Reading, MA (1981).
[30] Neukirch, J. *Neubegründung der Klassenkörpertheorie*, Math. Zeit. **186** (1984), 557-574.
[31] Neukirch, J. *Class Field Theory.* Springer-Verlag, Berlin (1986).
[32] Neukirch, J. *Algebraische Zahlentheorie.* Springer-Verlag, Berlin (1992).
[33] Ostrowski, A. *Über einige Lösungen der Funktionalgleichung* $\varphi(x) \cdot \varphi(y) = \varphi(xy)$. Acta Math. **41** (1918), 271-284.
[34] Rotman, J.J. *Notes on Homological Algebra.* Van Nostrand, New York (1970).
[35] Schmid, H. L. *Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichen Konstantkörper.* Math. Zeit. **40** (1936), 94-109.
[36] Serre, J.-P. *Local Fields.* Springer-Verlag, Berlin (1979).
[37] Serre, J.-P. *Algebraic Groups and Class Fields.* Springer-Verlag, Berlin (1988).
[38] Serre, J.-P. *Linear Representations of Finite Groups.* Springer-Verlag, Berlin (1979).
[39] Shatz, S. *Profinite Groups, Arithmetic and Geometry.* Princeton University Press, Princeton (1972).
[40] Weil, A. *Basic Number Theory*, 3rd. Ed., Springer-Verlag, Berlin (1974).
[41] Wiles, A. *Higher explicit reciprocity laws.* Ann. of Math., **107** (1978), 235-254.
[42] Zaldívar, F. *Teoría de Galois.* Anthropos, Barcelona (1996).
[43] Zariski, O., Samuel, P. *Commutative Algebra, Vol. I.* Springer-Verlag, Berlin (1979).

Índice alfabético

Campos locales se terminó de imprimir en julio del 2001
en la Sección de Impresiones y Diseño Gráfico de la
UAM-I. La edición consta de 1,000 ejemplares.



Felipe Zaldívar estudió la licenciatura y maestría en matemáticas en la Facultad de Ciencias de la Universidad Nacional Autonóma de México y obtuvo el grado de Doctor en Filosofía (Matemáticas) de la University of Western Ontario, en Canadá. Ha sido profesor visitante en la George Washington University, en Washington, D.C., y actuamente es profesor titular de matemáticas en la Universidad Autonóma Metropolitana-Iztapalapa.

En la aritmética de campos, los campos finitos, los campos de números, y los campos de funciones aparecen tempranamente. Un lugar intermedio ocupan los campos locales, que son estructuralmente más complejos que los campos finitos y se obtienen completando campos de números o campos de funciones con campo de constantes finito.

En este libro se estudian los conceptos básicos sobre campos con una valuación no arquimediana, enfocándose al caso de campos completos con respecto a una valuación discreta y con campo residual finito, es decir, al caso de campos locales.

Después de un estudio preliminar exhaustivo de las propiedades elementales de estos campos, se hace un análisis de la norma relativa para extensiones de campos locales y se estudia en detalle el automorfismo de Frobenius de ciertas extensiones. Usando lo anterior, se estudian los grupos de Galois de las extensiones abelianas de campos locales obteniendo la ley de reciprocidad local correspondiente, junto con sus propiedades.

Finalmente se describe en forma explícita el morfismo de reciprocidad local en el caso de extensiones de Lubin-Tate y luego se aplica esto al estudio de los grupos de ramificación superior.

El libro se puede estudiar en dos cursos con requisitos mínimos: teoría de Galois y elementos de teoría de módulos, de análisis matemático y de topología general, usualmente estudiados en la licenciatura.

Los temas desarrollados en el texto conforman un buen lugar de encuentro de diversas ramas de la matemática, dando al estudiante interesado una visión de conjunto de nuestra ciencia.

ISBN: 970-654-868-8