USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Ramificación en teoría de números

Javier Guillán Rial

2020/2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Ramificación en teoría de números

Javier Guillán Rial

Julio, 2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álgebra
Título: Ramificación en teoría de números
Breve descrición do contido
En el contexto de la teoría algebraica de números, la teoría de la ramificación juega un papel fundamental. El propósito de este trabajo es estudiar dicha teoría, estudiando previa y paralelamente numerosos aspectos complementarios de la teoría algebraica de números.
Recomendacións
Una buena base de álgebra conmutativa (que el estudiante que propicia este TFG ya posee) será necesaria.
Outras observacións

Índice general

Resumen

Este trabajo trata sobre la noción de ramificación en el contexto de la teoría de números. Para ello se introducirán las herramientas algebraicas y topológicas típicas de la teoría de números algebraica (anillos de valoración discreta, dominios de Dedekind, completación de un cuerpo con un valor absoluto, diferente de una extensión de cuerpos, grupos de ramificación...), así como resultados básicos acerca de la ramificación de una extensión finita de cuerpos, especialmente en el contexto de cuerpos locales.

Abstract

This work falls within the study of the notion of ramification in a number theoretic realm. For that purpose several algebraic and topological tools -namely discrete valuation rings, Dedekind domains, completion of a field with an absolute value, different of a field extension, ramification groups...- are introduced. Furthermore, basic results on ramification, especially in the context of finite extensions of local fields, will be given.

Introducción

En este trabajo se explicará el fenómeno de ramificación en el marco de la teoría de números algebraica. El ejemplo típico de este fenómeno se encuentra al estudiar cómo se comportan los primos de $\mathbb{Z}$ vistos como elementos de $\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$ (que es un dominio euclídeo, y en particular un dominio de ideales principales y de factorización única), anillo de enteros algebraicos de la extensión $\mathbb{Q}(i)|\mathbb{Q}$. Hay números como 3, que se mantienen la propiedad de ser primo una vez visto como elemento de $\mathbb{Z}[i]$. Un primo $p \in \mathbb{Z}$ que cumple la condición anterior se denomina *inerte*. No obstante otros primos, como $2 = -i(1+i)^2$ o $5 = (2+i)(2-i)$, pierden dicha propiedad vistos como elementos de $\mathbb{Z}[i]$. Así, se dice que *ramifican* en el primer caso y que *se descomponen* en el segundo, en función de si los irreducibles que dividen a cada uno son asociados o no). En el caso particular de $\mathbb{Z}[i]$ existe un teorema clásico acerca de qué primos se mantienen inertes y cuáles se descomponen o ramifican en $\mathbb{Z}[i]$:

Teorema 0.1. *Un primo $p \in \mathbb{Z}$ es inerte en $\mathbb{Z}[i]$ si y solo si $p \equiv 3$ (mód 4).*

Un corolario interesante de este teorema está relacionado con los primos representados por la forma cuadrática $X^2 + Y^2$, ya que la ecuación diofántica $X^2 + Y^2 = (X + iY)(X - iY) = p$ tiene solución si y solo si p se descompone o ramifica (por factorización única). De este hecho se puede deducir cuáles son las soluciones de la ecuación diofántica $X^2 + Y^2 = n$:

Corolario 0.2. *Sea $n > 0$ un entero positivo. Entonces, la ecuación diofántica $X^2 + Y^2 = n$ tiene solución si y solo si en la descomposición de n en factores primos los primos congruentes con 3 módulo 4 aparecen un número par de veces.*

Como podemos observar, saber la ramificación de una extensión de cuerpos de números algebraicos no solo nos permite conocer cómo se comportan los primos en los anillos de enteros (si estos son dominios de factorización única), sino que permiten también la resolución de ecuaciones diofánticas. Otro ejemplo ilustrativo, resuelto por Kummer en el siglo XIX, es el de la ecuación $X^p + Y^p = Z^p$ (último teorema de Fermat para el caso $n = p$ primo impar) y el anillo $\mathbb{Z}[\zeta_p]$ (donde ζ_p es la $p-$ésima raíz de la unidad), siempre y cuando este anillo sea de factorización única (por ejemplo, en los casos $p = 3, 5, 7, 11, 13, 17, 19, \dots$), explotando la factorización $X^p + Y^p = (X + Y)(X + \zeta_p Y)(X + \zeta_p^2 Y) \dots (X + \zeta_p^{p-1} Y)$.

No obstante, puede darse la situación en la que la extensión no sea un dominio de factorización única, en cuyo caso, deja de tener sentido hablar de ramificación a nivel de elementos, como

comentamos en el caso de $\mathbb{Z}[i]$. La extensión de la noción de ramificación para abordar estas situaciones aparece cuando hay factorización única no a nivel de elementos, sino de ideales. Los anillos en los que se trabaja en teoría de números (como por ejemplo, los anillos de enteros algebraicos de una extensión finita de $\mathbb{Q}$), no son en general dominios de factorización única, pero sí son *dominios de Dedekind*, donde se cumple la factorización única de ideales

En un marco actual el concepto de ramificación se generaliza más allá de la teoría de números, teniendo significaciones profundas en geometría algebraica, y es fundamental para la demostración de numerosos resultados capitales en teoría de números.

El trabajo está dividido en tres capítulos. En el primero se introducirán y caracterizarán los anillos en los que nos vamos a centrar a lo largo del trabajo: dominios de Dedekind y anillos de valoración discreta (AVD), que son los dominios de Dedekind locales . Tendrán especial relevancia la figura de las *valoraciones discretas*, funciones de un cuerpo a $\mathbb{Z}$ con ciertas propiedades adicionales que nos permitirán definir la estructura de ambos tipos de anillos. En la segunda parte nos centraremos en resultados de extensiones de dominios de Dedekind, es decir inclusiones $A \subset B$ de dominios de Dedekind, generalizando los casos anteriormente comentados $\mathbb{Z} \subset \mathbb{Z}[i], \mathbb{Z} \subset \mathbb{Z}[\zeta_p]$. En particular nos interesará estudiar la factorización de $\mathfrak{p}$ en B cuando $\mathfrak{p}$ es un ideal primo de A.

El segundo capítulo se centrará en la noción de la completación de un cuerpo sobre el que existe un valor absoluto: definiremos y construiremos la completación de un cuerpo y estudiaremos sus propiedades. Esta noción tiene especial importancia cuando tratamos con cuerpos de fracciones de un anillo de valoración discreta, donde podemos relacionar el valor absoluto con la valoración discreta definida previamente sobre el cuerpo. Al igual que sucede en análisis matemático, donde se trabaja con $\mathbb{R}$ (la completación de $\mathbb{Q}$ con respecto al valor absoluto usual), la completación es una herramienta muy útil en teoría de números, y de hecho, en este contexto aparecen de forma natural muchas otras normas distintas de la usual (por ejemplo las normas $p-$ádicas sobre $\mathbb{Q}$), que dan lugar a completaciones distintas del mismo cuerpo, como los cuerpos de los números $p-$ádicos, $\mathbb{Q}_p$. Estos últimos son un ejemplo de lo que denominaremos *cuerpos locales*, de los cuales se dará una caracterización, y que nos resultarán especialmente interesantes.

Finalmente el tercer capítulo se centrará en algunas propiedades de la ramificación, y tiene dos partes bien diferenciadas. En la primera se profundizará en las extensiones de Galois finitas de cuerpos locales, estudiando los llamados *grupos de ramificación* de dichas extensiones, subgrupos del grupo de Galois asociado a la extensión, que aportarán bastante información acerca de su ramificación. En la segunda parte del capítulo se introducirá el *módulo de diferenciales de Kähler* de una extensión de cuerpos, que utilizaremos para caracterizar los ideales primos que no ramifican en extensiones de dominios de Dedekind.

Durante todo el trabajo se ha seguido la estructura de [Ser] a la hora de organizar los resultados, mas en la mayor parte de los casos se ha optado por emplear demostraciones distintas, propias de [Neu] o [Sut] o [Mil], tanto por cuestiones de claridad como de brevedad. Otra razón fundamental es que para el segundo y tercer capítulo, en general trabajaremos con hipótesis ligeramente más fuertes, de modo que no necesitaremos tanta generalidad. Esto último es funda-

mental, pues una de las mayores motivaciones (y dificultades) a la hora de redactar este trabajo ha sido la adaptación de todas las demostraciones a nivel del grado. El resultado ha sido satisfactorio, en el sentido de que se ha conseguido redactar una introducción a la teoría de ramificación, trabajando con hipótesis suficientemente generales para comprender muchos resultados modernos, que toda persona a nivel de grado puede leer y entender, solo siendo necesaria la consulta de algunos conceptos de álgebra conmutativa, para los que nos remitiremos a [AM].

Capítulo 1

AVD y dominios de Dedekind

1.1. Anillos de valoración discreta y dominios de Dedekind

Definición 1.1 (Valoración discreta)**.** Sea K un cuerpo. Una aplicación $v : K^* \to \mathbb{Z}$ que cumple:

1. v es un homomorfismo sobreyectivo de grupos abelianos.
2. $v(x+y) \geq \text{ínf}\{v(x), v(y)\}$.

se dice una *valoración discreta*.[1]

Definición 1.2 (Anillo de valoración discreta)**.** Un anillo A se dice *de valoración discreta* (AVD) si es un dominio de ideales principales con un único ideal primo no nulo $\mathfrak{m} = (\pi)$, donde $\pi \in A$ se denomina *uniformizante* del anillo A. Nótese que este ideal es necesariamente maximal, y por tanto el cociente $A/\mathfrak{m}$ es un cuerpo denominado el *cuerpo residual* del AVD A.

Proposición 1.3. *Todo AVD admite una valoración discreta definida en su cuerpo de fracciones y recíprocamente, si K es un cuerpo y v es una valoración discreta sobre K, entonces $A = \{x \in K \,|\, v(x) \geq 0\}$ (llamado el anillo de valoración de v) es un anillo de valoración discreta que tiene a K como cuerpo de fracciones. Además toda valoración discreta está determinada por su anillo de valoración.*

Demostración. Para la primera parte, es claro que todo elemento no nulo de un AVD A se puede expresar de modo único de la siguiente manera $\pi^n u$, [2] donde $n \in \mathbb{Z}$ y $u \in A^*$. De este modo tenemos que la aplicación $A - \{0\} \to \mathbb{Z}$; $u\pi^n \mapsto n$ está bien definida (podemos extender la aplicación a A tomando $v(0) = \infty$). Además no depende de la elección de π, pues, dado que

[1] En general una valoración es un homomorfismo de grupos abelianos $v : K^* \to \Gamma$, donde Γ es un grupo abeliano ordenado, hacemos esta elección para que v esté determinada por la preimagen del 1, como veremos. Dado que en el resto del trabajo solo trabajaremos con valoraciones discretas nos referiremos a las valoraciones discretas como valoraciones a secas.

[2] Esto se deduce del hecho de que si $\pi^n u = \pi^m v$ entonces, asumiendo sin pérdida de generalidad que $n \geq m$, $\pi^m v(1 - v^{-1}u\pi^{n-m}) = 0$, y dado que estamos trabajando en un dominio, necesariamente $v^{-1}u\pi^{n-m} = 1$ con lo que tenemos que $u = v$ y $n = m$.

en un AVD solo hay un ideal primo, todos los uniformizantes son asociados. Dicha aplicación se extiende de forma natural a una aplicación $v : K^* \to \mathbb{Z}$ $a/b \mapsto v(a) - v(b)$ que cumple las dos propiedades de la definición 1.1. Para comprobar esto basta con ver que se cumple la segunda, porque la primera es inmediata. Podemos suponer sin pérdida de generalidad que $x, y \in A$, pues si $x, y \in K$, reduciendo a común denominador podemos suponer que $x = a/s, y = b/s$ con $a, b, s \in A$, de modo que, por (1):

$$v(x+y) = v(a+b) - v(s) \geq \text{ínf}\{v(a), v(b)\} - v(s) = \text{ínf}\{v(a) - v(s), v(b) - v(s)\} = \text{ínf}\{v(x), v(y)\}$$

Así, sean $x = \pi^n u$ y $y = \pi^m v$, con n, m enteros positivos (asumiremos sin pérdida de generalidad que $n > m$, pues para $n = m$ es trivial que $v(x + y) \geq m = \text{ínf}\{v(x), v(y)\}$), entonces $x + y = \pi^m v(1 + uv^{-1}\pi^{n-m})$. Como estamos trabajando en un anillo local el ideal de Jacobson es $\mathfrak{R}(A) = \mathfrak{m} = (\pi)$, con lo que $1 + uv^{-1}\pi^{n-m}$ es una unidad, de modo que $v(x + y) = m = v(y) = \text{ínf}\{v(x), v(y)\}$.

Para la segunda parte, las propiedades (1) y (2) implican que el conjunto A es cerrado con las operaciones de K, luego es un subanillo de K, veamos que es un AVD. Sea un elemento $\pi \in K^*$ tal que $v(\pi) = 1$ (podemos suponerlo ya que v es sobreyectiva) y $x \in A$. Si $v(x) = n$, entonces $v(x^{-1}\pi^n) = 0$ por (1), con lo que todo elemento de A puede expresarse de modo único como $u\pi^n$ con $u \in A^*$ y $n \in \mathbb{Z}$ (si $x \in A$ es no nulo cumpliendo $v(x) = 0$, entonces $v(x^{-1}) = 0$, es decir, $x^{-1} \in A$ y por tanto $x \in A^*$). Con esto se puede probar que todo ideal $\mathfrak{a}$ de A es igual a (π^n) con $n \geq 0$. Efectivamente, sea $\mathfrak{a}$ un ideal de A, y $n = \text{mín}\{m \,|\, \pi^m \in \mathfrak{a}\}$, por un lado es claro que $(\pi^n) \subset \mathfrak{a}$, y recíprocamente, todo elemento $x \in \mathfrak{a}$ se expresa de modo único como $\pi^m u$, con $m \geq n$ y $u \in A^*$, con lo que $\mathfrak{a} \subset (\pi^n)$. De este modo hemos demostrado que A es un AVD. Para ver que K es su cuerpo de fracciones necesitaremos:

Lema 1.4. *Sea K un cuerpo con una valoración discreta v y sea A su anillo de valoración. Entonces si B es un subanillo de K y $A \subset B$, entonces $B = A$ ó $B = K$ (esto implica que los anillos de valoración discreta son subanillos maximales de su cuerpo de fracciones).*

Demostración. Si $A = B$ el lema ya estaría probado, así que supondremos que la inclusión $A \subset B$ es propia. Por la definición de A debe existir un elemento $b \in B$ cumpliendo $v(b) < 0$. Sea ahora $x \in K$, si $v(x) \geq 0$ entonces $x \in A \subset B$, y si $v(x) = -n < 0$ entonces $v(b^{-n}x) = v(x) - nv(b) \geq 0$ con lo que $b^{-n}x \in A \subset B$, y por tanto $x = b^n(xb^{-n}) \in B$. Esto implica que $K = B$ y el lema estaría probado. □

De este modo, si denotamos como E al cuerpo de fracciones de A, se cumple que $A \subset E \subset K$, con lo que el lema anterior nos asegura que $E = K$, como queríamos probar.

Para demostrar que toda valoración discreta está caracterizada por su anillo de valoración supongamos que v, w son valoraciones sobre un cuerpo K y A_v, A_w sus anillos de valoración. Si $v = w$ es trivial que $A_v = A_w$. Supongamos por otro lado que $A_w = A_v$, como son dominios de valoración discreta entonces sus ideales maximales están generados por elementos $\mathfrak{m}_v = (\pi_v)$, $\mathfrak{m}_w = (\pi_w)$. Como $\mathfrak{m}_v = \mathfrak{m}_w$ entonces π_v y π_w son asociados, de modo que $v(x) = w(x)$ para todo $x \in K^*$ (ya que $v(u) = w(u) = 0$ para todo $u \in A^*$). □

Proposición 1.5. *Sea A un dominio local noetheriano que no es un cuerpo. Son equivalentes:*

1. *A es un AVD.*
2. *El ideal maximal de A es principal.*
3. *A es íntegramente cerrado y $\dim A = 1$.*

Demostración. Para la implicación (2) $\Rightarrow$ (1) primero probaremos que, si $\mathfrak{m}$ es el ideal maximal de A y π un generador de $\mathfrak{m}$, $\bigcap_{n>0} \mathfrak{m}^n = 0$. En efecto, dado que $\mathfrak{m}$ es principal y A es un dominio se cumple $\bigcap_{n>1} \mathfrak{m}^n = \mathfrak{m} \bigcap_{n>0} \mathfrak{m}^n$ (la inclusión hacia la izquierda es clara, para la inclusión hacia la derecha supongamos $x \in \bigcap_{n>1} \mathfrak{m}^n$, de modo que $x = a_n \pi^n$ con $a_n \in A$ para todo $n > 1$, y por tanto, trabajando en el cuerpo de fracciones de A, $x\pi^{-1} \in \bigcap_{n>0} \mathfrak{m}^n \subset A$, con lo que $x = \pi(\pi^{-1}x) \in \mathfrak{m} \bigcap_{n>0} \mathfrak{m}^n$), y esto implica que $\bigcap_{n>0} \mathfrak{m}^n = \bigcap_{n>1} \mathfrak{m}^n = \mathfrak{m} \bigcap_{n>0} \mathfrak{m}^n$, por lo visto anteriormente. Dado que A es noetheriano y $\bigcap_{n>0} \mathfrak{m}^n$ es un ideal de A, $\bigcap_{n>0} \mathfrak{m}^n$ es $A-$módulo finitamente generado. Además, dado que A es local se cumple la igualdad $\mathfrak{m} = \mathfrak{R}(A)$, por lo que el lema de Nakayama [AM, prop. 2.6] nos permite concluir que $\bigcap_{n>0} \mathfrak{m}^n = 0$.

Esto nos garantiza que todo $y \in A$ no nulo se puede escribir de modo único de la forma $y = u\pi^n$ con $u \in A^*$ y $n \in \mathbb{N}$. Efectivamente, $\bigcap_{n>0} \mathfrak{m}^n = 0$ implica que $n_0 = \text{máx}\{n \in \mathbb{N} \,|\, y \in \mathfrak{m}^n = \bigcap_{k=1}^{n} \mathfrak{m}^k\}$ está bien definido, con lo que $y = u\pi^{n_0}$, donde $u \in A^*$(si $u \notin A^*$, dado que A es local, $u \in \mathfrak{m}$ y esto contradeciría la definición de n_0) de modo único, ya que $\mathfrak{m}^{k+1} \subsetneq \mathfrak{m}^k$ para todo $k \in \mathbb{N}$ (al ser A un dominio y $\mathfrak{m}$ es principal).

Para probar la implicación (1) $\Rightarrow$ (3) sea $x \in K$ un elemento del cuerpo de fracciones de A entero sobre A, cumpliendo la relación entera $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, con $a_i \in A$ para todo $i = 0, \ldots, n-1$ (esto en particular quiere decir que $v(a_i) \geq 0$ para todo $i = 1, \ldots, n-1$). Si suponemos que $x \notin A$, entonces $v(x) < 0$, con lo que $v(x^{-1}) > 0$. Pero esto implica que $v(x) = v(-a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0 x^{-(n-1)}) \geq \text{ínf}\{v(a_{n-1}), v(a_{n-2}) + v(x^{-1}), \ldots, v(a_0) + (n-1)v(x^{-1})\} \geq 0$, una contradicción que viene de haber supuesto que $x \notin A$. Además, es claro que si A es un AVD, $\dim A = 1$, pues solo admite la cadena de ideales primos $(0) \subset \mathfrak{m}$.

Finalmente, para demostrar la implicación (3) $\Rightarrow$ (2), como A no es un cuerpo, $\mathfrak{m} \neq 0$, de modo que existe un elemento no nulo $a \in \mathfrak{m}$. Considerando el radical de (a) [AM, def. 1.14], tenemos que, dado que $\dim A = 1$, $rad(a) = \bigcap_{\substack{\mathfrak{p} \text{ primo} \\ a \in \mathfrak{p}}} \mathfrak{p} = \mathfrak{m}$, ya que A tiene solo un ideal primo no nulo (al ser A local de dimensión 1). Por [AM, prop. 7.14] existe un $t \in \mathbb{N}$ tal que $\mathfrak{m}^t \in (a)$, que supondremos el mínimo cumpliendo tal propiedad. Tomando $b \in \mathfrak{m}^{t-1}$ tal que $b \notin (a)$ y K el cuerpo de fracciones de A, el elemento $b/a \in K$ no está en A (ya que $b \notin (a)$), y dado que A es íntegramente cerrado b/a no es entero sobre A. Si $(b/a)\mathfrak{m} \subset \mathfrak{m}$, entonces tenemos que el homomorfismo de $A-$módulos $\varphi : \mathfrak{m} \to \mathfrak{m}$; $x \mapsto (b/a)x$ satisface, por el teorema de Cayley-Hamilton [AM, prop. 2.4] ($\mathfrak{m}$ es finitamente generado pues A es noetheriano) una relación $\varphi^s + a_{s-1}\varphi^{s-1} + \cdots + a_0 = 0$, con $a_i \in A$ para todo $i = 1 \ldots, s-1$, en particular, para $x \in \mathfrak{m}$ no nulo $\varphi(x) = \left((b/a)^s + a_{s-1}(b/a)^{s-1} + \cdots + a_0\right) x = 0$, con lo que $\left((b/a)^s + a_{s-1}(b/a)^{s-1} + \cdots + a_0\right) = 0$ ya que A es un dominio, contradiciendo que b/a no sea un entero sobre A. De este modo concluimos que $(b/a)\mathfrak{m} \not\subset \mathfrak{m}$, pero por otro lado

$(b/a)\mathfrak{m} \subset (1/a)\mathfrak{m}^t \subset A$, con lo que $(b/a)\mathfrak{m}$ es un ideal de A, que ha de ser igual a A por ser $\mathfrak{m}$ el único ideal maximal). Así, $\mathfrak{m} = (a/b)A$ es el ideal principal generado por a/b (que pertenece a $\mathfrak{m} \subset A$ pues $a/b = a/b \cdot 1$), como queríamos probar. □

Proposición 1.6. *Si A es un dominio noetheriano, las dos siguientes condiciones son equivalentes:*

1. *Para todo ideal primo $\mathfrak{p} \neq 0$ de A, $A_\mathfrak{p}$ es un AVD.*
2. *A es íntegramente cerrado de dimensión ≤ 1.*

Demostración. Comencemos con la implicación (1) $\Rightarrow$ (2). Si $0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ es una cadena ascendente de ideales primos de A, por [AM, prop. 3.11] se va a inducir la cadena ascendente $0 \subsetneq \mathfrak{p}_1 A_{\mathfrak{p}_n} \subsetneq \mathfrak{p}_2 A_{\mathfrak{p}_n} \subsetneq \cdots \subsetneq \mathfrak{p}_n A_{\mathfrak{p}_n}$ en $A_{\mathfrak{p}_n}$, y recíprocamente, si $\mathfrak{p}$ es un ideal primo no nulo de A, la cadena ascendente $0 \subsetneq \mathfrak{p}_1 A_\mathfrak{p} \subsetneq \mathfrak{p}_2 A_\mathfrak{p} \subsetneq \cdots \subsetneq \mathfrak{p}_n A_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$ induce una cadena ascendente en A $0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$, de modo que $\dim A = \sup\{\dim A_\mathfrak{p} \mid \mathfrak{p} \text{ ideal primo de } A\}$. Dado que toda localización en un ideal primo no nulo $A_\mathfrak{p}$ es un AVD por hipótesis, es inmediato, por la proposición 1.5 que $\dim A \leq 1$. Por otro lado es claro que A es íntegramente cerrado pues la propiedad de ser íntegramente cerrado es local[AM, prop. 5.13], y todas las localizaciones de A son AVD.

Para la implicación (2) $\Rightarrow$ (1) usamos nuevamente que la propiedad de ser íntegramente cerrado para dominios es local, por lo que toda localización $A_\mathfrak{p}$ de A en un primo $\mathfrak{p}$ es íntegramente cerrada, al serlo A. Por otro lado, dado que $\dim A \leq 1$, es claro que $A_\mathfrak{p}$ solo puede tener un único ideal primo no nulo, ya que de de tener otro, $0 \subsetneq \mathfrak{p}' A_\mathfrak{p} \subsetneq \mathfrak{p} A_\mathfrak{p}$ (al estar trabajando en una localización) tendríamos la cadena ascendente $0 \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p}$, contradiciendo que $\dim A \leq 1$. □

Definición 1.7 (Dominio de Dedekind)**.** Un dominio noetheriano cumpliendo las dos condiciones anteriores se denomina un *Dominio de Dedekind*.

Definición 1.8. Si K es el cuerpo de fracciones de un dominio noetheriano A, un *ideal fraccionario* $\mathfrak{a}$ es un A-submódulo de K finitamente generado. Decimos que $\mathfrak{a}$ es invertible si existe un ideal fraccionario $\mathfrak{b}$ tal que $\mathfrak{ab} = A$, y que es *principal* si existe $s \in K$ tal que $\mathfrak{a} = As$. Denotaremos como $\mathcal{I}_A$ al conjunto de ideales fraccionarios invertibles de un dominio noetheriano.

Proposición 1.9. *Sea A un dominio noetheriano, K su cuerpo de fracciones y $\mathfrak{a}$ un $A-$ submódulo de K. Entonces $\mathfrak{a}$ es un ideal fraccionario si y solo si puede expresarse como $\mathfrak{a} = x^{-1}\mathfrak{b}$, donde $x \in A - \{0\}$ y $\mathfrak{b}$ es un ideal de A.*

Demostración. Para el *solo si*, si $\mathfrak{a}$ es un ideal fraccionario entonces es un $A-$módulo finitamente generado, con lo que (reduciendo a común denominador de ser necesario) podemos suponer que está generado por $y_1/x, \ldots, y_n/x \in K$, de modo que $\mathfrak{a} = x^{-1}\mathfrak{b}$, donde $\mathfrak{b} = (y_1, \ldots, y_n)$. Para el *si* tenemos que al ser $\mathfrak{b}$ un ideal de un anillo noetheriano A es finitamente generado como $A-$módulo, de modo que $x^{-1}\mathfrak{b} \subset K$ es un A-módulo finitamente generado, y por lo tanto un ideal fraccionario. □

Observación 1.10. Si $\mathfrak{a}$,$\mathfrak{b}$ son dos ideales fraccionarios, entonces es claro que $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{ab}$ son ideales fraccionarios. Además podemos definir para un ideal fraccionario $\mathfrak{a}$ no nulo el conjunto $(A:\mathfrak{a}) = \{x \in K \,|\, x\mathfrak{a} \subset A\} \subset K$ que es un $A-$módulo finitamente generado (ya que si $\mathfrak{a} = x^{-1}\mathfrak{b}$, siendo $\mathfrak{b}$ un ideal de A, $(A:\mathfrak{a})x \subset A$ y por tanto $(A:\mathfrak{a}) \subset x^{-1}A$, que es finitamente generado como $A-$módulo, ya que $x^{-1}A$ es un $A-$módulo noetheriano), y por tanto un ideal fraccionario. Otra observación es que la correspondencia $\mathfrak{a} \mapsto (A:\mathfrak{a})$ entre ideales fraccionarios no nulos está bien definida y revierte las inclusiones.

Proposición 1.11. *Sea A un dominio noetheriano. Un ideal fraccionario $\mathfrak{a}$ es invertible si y solo si $\mathfrak{a}(A:\mathfrak{a}) = A$. En tal caso $(A:\mathfrak{a})$ es el único ideal fraccionario que cumple tal condición.*

Demostración. El *si* es evidente. Si $\mathfrak{a}$ es un ideal fraccionario invertible, existe un ideal fraccionario $\mathfrak{b}$ tal que $\mathfrak{ab} = A$, por lo que es claro que $x\mathfrak{a} \subset A$ para todo $x \in \mathfrak{b}$, y por tanto $\mathfrak{b} \subset (A:\mathfrak{a})$. Esto implica que $A = \mathfrak{ab} \subset \mathfrak{a}(A:\mathfrak{a}) \subset A$ con lo que $A(A:\mathfrak{a}) = A$. Para probar la unicidad basta ver que $\mathfrak{b} = A\mathfrak{b} = ((A:\mathfrak{a})\mathfrak{a})\mathfrak{b} = (A:\mathfrak{a})(\mathfrak{ab}) = (A:\mathfrak{a})A = (A:\mathfrak{a})$. □

Corolario 1.12. *Si A es un dominio noetheriano el conjunto $\mathcal{I}_A$, con la multiplicación de ideales fraccionarios admite una estructura de grupo abeliano, en el que los ideales fraccionarios principales no nulos forman un subgrupo.*

Demostración. La primera parte es evidente dada la proposición anterior. Por otro lado es claro que los ideales fraccionarios principales forman un subgrupo, si $\mathfrak{a} = (s)$ es un ideal fraccionario principal su inverso viene dada por $(A:\mathfrak{a}) = (s^{-1})$ y es claro que el producto de ideales fraccionarios principales es un ideal fraccionario principal. □

Observación 1.13. Esto hace que sea coherente la notación $\mathfrak{a}^{-1} = (A:\mathfrak{a})$ para $\mathfrak{a}$ ideal fraccionario invertible.

Definición 1.14. Si denotamos al subgrupo de $\mathcal{I}_A$ de los ideales fraccionarios principales por $\mathcal{P}_A$, llamaremos al cociente $cl(A) = \mathcal{I}_A/\mathcal{P}_A$ el *grupo de clases de ideales*.

Observación 1.15. Es evidente que si A es un dominio de ideales principales noetheriano, $cl(A)$ es trivial, dada la proposición 1.9. Esto implica, por ejemplo que para todo AVD A, $cl(A)$ es trivial.

Proposición 1.16. *[AM, th. 9.3] Sea $\mathfrak{a}$ un ideal fraccionario no nulo de un dominio noetheriano A. Entonces $\mathfrak{a}$ es invertible si y solo si $\mathfrak{a}_\mathfrak{p}$ es invertible para todo ideal primo $\mathfrak{p}$ de A. En otras palabras, la propiedad ser un ideal fraccionario invertible es local.*

Demostración. Supongamos que $\mathfrak{a}$ es un ideal invertible. Esto implica que $\mathfrak{a}(A:\mathfrak{a}) = A$, y por tanto $\mathfrak{a}_\mathfrak{p}(A_\mathfrak{p}:\mathfrak{a}_\mathfrak{p}) = A_\mathfrak{p}$ para todo ideal primo $\mathfrak{p}$, donde hemos aplicado las propiedades de la localización para A-módulos finitamente generados [AM, prop 3.4, prop 3.7, cor. 3.15]. Por otro lado si $\mathfrak{a}_\mathfrak{p}$ es invertible para todo $\mathfrak{p}$ ideal primo, entonces $A_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}(A_\mathfrak{p}:\mathfrak{a}_\mathfrak{p}) = [\mathfrak{a}(A:\mathfrak{a})]_\mathfrak{p}$ (donde se han usado las propiedades de localización de $A-$módulos finitamente generados mencionadas anteriormente), de modo que $A = \mathfrak{a}(A:\mathfrak{a})$, por [AM, prop. 3.9]. □

Corolario 1.17. *En un dominio de Dedekind, todo ideal fraccionario no nulo es invertible.*

Demostración. Es claro que como un AVD es un dominio de ideales principales todos los ideales fraccionarios son principales, por la proposición 1.9. Consecuentemente todos los ideales fraccionarios no nulos de un AVD son invertibles, por lo que también lo serán los de cualquier dominio de Dedekind, por la proposición anterior. □

Observación 1.18. La proposición 1.9 implica que si A es un dominio de Dedekind, $cl(A)$ es trivial si y solo si A es un dominio de ideales principales (para un dominio noetheriano se cumple únicamente el *si*).

Proposición 1.19. *Si $\mathfrak{a}$ es un ideal no nulo de un dominio de Dedekind solo existe un número finito de ideales primos que lo contienen.*

Demostración. Supongamos que $\mathfrak{a} \subset \mathfrak{p}_1, \ldots, \mathfrak{p}_k, \ldots$, siendo $\mathfrak{p}_i$ primo para todo $i = 1, \ldots, k, \ldots$. Podemos construir la cadena descendente de ideales que contienen a $\mathfrak{a}$:

$$\mathfrak{p}_1 \supset \mathfrak{p}_1 \cap \mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \supset \ldots$$

Por la observación 1.10 y por el corolario 1.17 tenemos que tomando inversos obtenemos la cadena ascendente:

$$A \subset (\mathfrak{p}_1)^{-1} \subset (\mathfrak{p}_1 \cap \mathfrak{p}_2)^{-1} \subset \cdots \subset (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k)^{-1} \subset \cdots \subset \mathfrak{a}^{-1} (\subset K)$$

Como A es un dominio de Dedekind, $\mathfrak{a}^{-1}$ es finitamente generado al ser un ideal fraccional, con lo que $\mathfrak{a}^{-1}$ es un $A-$módulo noetheriano, luego la cadena anterior se estabilizará tras k etapas, es decir $(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k)^{-1} \subset (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \cap \mathfrak{p}_{k+1})^{-1}$, o equivalentemente $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \supset \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \cap \mathfrak{p}_{k+1}$. Aplicando lo anterior inductivamente tenemos que en general se tiene que $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \supset \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \cap \mathfrak{p}_i$ para todo $i > k$. Esto en particular implica que:

$$\mathfrak{p}_1 \ldots \mathfrak{p}_k \subset \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \subset \mathfrak{p}_i$$

para todo $i > k$. Como todos los $\mathfrak{p}_i$ son primos no nulos, en particular, todos ellos son coprimos dos a dos, con lo que la expresión anterior implica que todo ideal primo de la cadena es igual a algún $\mathfrak{p}_j$ con $j = 1, \ldots, k$, como queríamos probar. □

Corolario 1.20. *Si $0 \neq x \in A$ entonces existe un número finito de ideales primos que lo contienen.*

Demostración. Basta aplicar la proposición al ideal principal (x), que cumple que $x \in \mathfrak{a}$ si y solo si $(x) \subset \mathfrak{a}$, para todo ideal $\mathfrak{a} \subset A$. □

Observación 1.21 (Extensión de valoraciones a ideales fraccionarios). Consideremos A un dominio de Dedekind y sea K su cuerpo de fracciones, $\mathfrak{p}$ un ideal primo y $v_\mathfrak{p}$ la valoración de $A_\mathfrak{p}$ asociada. Si $\mathfrak{a} \subset K$ es un ideal fraccionario de A, $\mathfrak{a}_\mathfrak{p}$ es un ideal fraccionario de $A_\mathfrak{p}$, con lo que ha de

tener la forma $(\pi_{\mathfrak{p}}^{n_{\mathfrak{p}}})$ donde $n_{\mathfrak{p}} \in \mathbb{Z}$ y $\pi_{\mathfrak{p}}$ es un uniformizante de $\mathfrak{p}$.[3] Esto nos permite extender la valoración $v_{\mathfrak{p}}$ a $\mathcal{I}_A$ como $v_{\mathfrak{p}}(\mathfrak{a}) = n_{\mathfrak{p}}$ (nótese que esta definición es coherente pues si $x \in K$, $v_{\mathfrak{p}}((x)) = v_{\mathfrak{p}}(x)$, con lo que coincide con la definición dada en 1.2).

Proposición 1.22. *Para todo ideal primo $\mathfrak{p}$ la valoración $v_{\mathfrak{p}} : \mathcal{I}_A \to \mathbb{Z}$ definida anteriormente es un homomorfismo de grupos abelianos que revierte los órdenes $(\mathcal{I}_A, \subseteq)$, $(\mathbb{Z}, \leq)$.*

Demostración. Para ver que es un homomorfismo basta con probar que para un ideal primo $\mathfrak{p}$ y dos ideales fraccionarios $\mathfrak{a}$,$\mathfrak{b}$ entonces (tras una elección de uniformizante π de $A_{\mathfrak{p}}$) $\mathfrak{a}_{\mathfrak{p}} = (\pi^{n_{\mathfrak{a}}})$,$\mathfrak{b}_{\mathfrak{p}} = (\pi^{n_{\mathfrak{b}}})$, con lo que $(\mathfrak{ab})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}\mathfrak{b}_{\mathfrak{p}} = (\pi^{n_{\mathfrak{a}}+n_{\mathfrak{b}}})$. Para ver que invierte los órdenes basta con ver que si $\mathfrak{a} \subset \mathfrak{b}$ entonces $n_{\mathfrak{a}} \geq n_{\mathfrak{b}}$. □

Corolario 1.23. *Sea A un dominio de Dedekind con cuerpo de fracciones K y $0 \neq \mathfrak{a} \subset K$ un ideal fraccionario. Entonces $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ para casi todo ideal primo $\mathfrak{p}$ de A.*

Demostración. Si $\mathfrak{a}$ es un ideal fraccionario de A, entonces por la proposición 1.9 tenemos que $\mathfrak{a} = x^{-1}\mathfrak{b}$ siendo $\mathfrak{b}$ un ideal de A, de modo que $v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{b}) - v_{\mathfrak{p}}(x)$ para todo ideal primo $\mathfrak{p}$ de A. Finalmente por 1.19, 1.20 se tiene que dicho valor es cero para casi todo primo $\mathfrak{p}$ de A. □

Proposición 1.24. *Sea A un dominio de Dedekind. Entonces $\mathcal{I}_A$ es isomorfo a $\bigoplus_{SpecA-\{0\}} \mathbb{Z}$ como grupo abeliano.*

Demostración. Si A es un cuerpo la proposición es trivial. Si A no es un cuerpo, definimos la siguiente aplicación $\mathfrak{a} \mapsto (v_{\mathfrak{p}}(\mathfrak{a}))_{\mathfrak{p}\in \mathrm{Spec}(A)-\{0\}}$. Vemos que está bien definida por el corolario 1.23, y que es un homomorfismo de grupos por la proposición 1.22. Comprobar que es inyectiva es inmediato pues $\mathfrak{a} = \mathfrak{b}$ si y solo si $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ para todo $\mathfrak{p} \in \mathrm{Spec}(A) - \{0\}$, con lo que si $\mathfrak{a} \neq \mathfrak{b}$ entonces existe $\mathfrak{p} \in \mathrm{Spec}(A) - \{0\}$ tal que $\mathfrak{a}_{\mathfrak{p}} \neq \mathfrak{b}_{\mathfrak{p}}$, y por lo tanto $v_{\mathfrak{p}}(\mathfrak{a}) \neq v_{\mathfrak{p}}(\mathfrak{b})$. Para ver que es sobreyectiva tenemos que probar antes que si $\mathfrak{p} \neq \mathfrak{q}$ son ideales primos no nulos de A, entonces $v_{\mathfrak{p}}(\mathfrak{q}) = 0$. Efectivamente, dado que estamos trabajando en un dominio de Dedekind, $\dim A \leq 1$, con lo que ningún ideal primo no nulo está propiamente contenido en otro, de modo que para $\mathfrak{p}, \mathfrak{q}$ ideales primos no nulos distintos $\mathfrak{q}A_{\mathfrak{p}} = A_{\mathfrak{p}}$, y consecuentemente $v_{\mathfrak{p}}(\mathfrak{q}) = 0$. Ahora sea $x = (e_{\mathfrak{p}})_{\mathfrak{p}\in \mathrm{SpecA}-\{0\}}$, donde $e_{\mathfrak{p}} \neq 0$ para casi todo $\mathfrak{p} \in \mathrm{Spec}(A) - \{0\}$, entonces tenemos que x es la imagen de $\prod_{\mathfrak{p}\in \mathrm{Spec}(A)-\{0\}} \mathfrak{p}^{e_{\mathfrak{p}}}$ pues si $\mathfrak{q}$ es un ideal primo de A:

$$v_{\mathfrak{q}}\left(\prod_{\mathfrak{p}\in \mathrm{Spec}(A)-\{0\}} \mathfrak{p}^{e_{\mathfrak{p}}}\right) = \sum_{\mathfrak{p}\in \mathrm{Spec}(A)-\{0\}} v_{\mathfrak{q}}(\mathfrak{p}^{e_{\mathfrak{p}}}) = v_{\mathfrak{q}}(\mathfrak{q}^{e_{\mathfrak{q}}}) = e_{\mathfrak{q}}$$

como queríamos probar. □

Corolario 1.25. *Todo ideal fraccionario de un dominio de Dedekind A puede ser escrito de modo único del modo:*

$$\mathfrak{a} = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

donde $v_{\mathfrak{p}}(\mathfrak{a})$ son enteros no nulos para un número finito de ideales primos.

[3] Nótese que este valor no depende del uniformizador elegido, como se comentó en la proposición 1.3

Corolario 1.26. *En un dominio de Dedekind A $cl(A)$ es trivial (o equivalentemente, A es un dominio de ideales principales) si y solo si A es un dominio de factorización única.*

Demostración. Para el *solo si* basta con señalar que todo dominio de ideales principales es un dominio de factorización única. Para el *si* supongamos que A es un dominio de factorización única y veamos que es un dominio de ideales principales. Debido a la factorización única de ideales basta con ver que todos los ideales primos son ideales principales, así que sea $\mathfrak{p}$ un ideal primo. Si $\mathfrak{p} = 0$ ya estaría probado, así que supondremos $\mathfrak{p} \neq 0$ y $0 \neq x \in \mathfrak{p}$. Como A es un dominio de factorización única $x = up_1 \dots p_n$ donde $u \in A^*$ y p_i son elementos irreducibles. Como p es primo, $p_i \in \mathfrak{p}$ para algún $i = 1, \dots, n$, y así $(p_i) = \mathfrak{p}$, ya que el ideal principal generado por un elemento irreducible es un primo (de nuevo por ser A un dominio de factorización única). □

Proposición 1.27. *Sean A un dominio de Dedekind, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ un conjunto de ideales primos no nulos distintos de A y $e_1, \dots, e_n$ números enteros positivos. Entonces $\mathfrak{p}_1^{e_1}$ es coprimo con $\mathfrak{p}_2^{e_2} \dots \mathfrak{p}_n^{e_n}$.*

Demostración. Como los ideales maximales $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ son distintos por hipótesis, $\mathrm{rad}(\mathfrak{p}_1^{e_1} + \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_n^{e_n}) = \mathrm{rad}(\mathrm{rad}(\mathfrak{p}_1^{e_1}) + \mathrm{rad}(\mathfrak{p}_2^{e_2} \dots \mathfrak{p}_n^{e_n})) = \mathrm{rad}(\mathfrak{p}_1 + \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_2) = \mathrm{rad}(\mathfrak{p}_1 + \mathfrak{p}_2 \dots \mathfrak{p}_2) = \mathrm{rad}(A) = A$, donde para la penúltima igualdad se utilizó que $\mathfrak{p}_1$ es maximal y $\mathfrak{p}_1 \subset \mathfrak{p}_1 + \mathfrak{p}_2 \dots \mathfrak{p}_n \subset A$ (si $\mathfrak{p}_2 \dots \mathfrak{p}_n \subset \mathfrak{p}_1$, entonces $\mathfrak{p}_i = \mathfrak{p}_1$ para algún $i = 2, \dots, n$ contradiciendo la hipótesis de que $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ son todos distintos). □

Lema 1.28 (Lema de aproximación)**.** *Sea A un dominio de Dedekind y K su cuerpo de fracciones. Si $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ son ideales primos distintos de A, $x_1, \dots, x_k \in K$ y $n_1, \dots, n_k$ enteros, existe un elemento $x \in K$ tal que $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ para todo $i = 1, \dots, k$ y $v_{\mathfrak{q}}(x) \geq 0$ para todo todo ideal primo $\mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_k$.*

Demostración. Podemos suponer sin pérdida de generalidad que $k > 1$ (si $k = 1$ suponemos que $x_2 = 0$ y $n_2 = 0$ y aplicamos el caso $k = 2$). Lo probaremos suponiendo que $n_1, \dots, n_k$ son enteros positivos (que es un resultado más fuerte). Partimos la prueba en tres casos:

1. *Caso 1*: $x_1, \dots, x_k \in A$, con a lo sumo un único $x_i \neq 0$, y $x_j = 0$ para todo $j = 1, \dots, \hat{i}, \dots, n$. Si todos los x_i son nulos entonces tomando $x \in \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_k^{n_k}$ el lema estaría probado. En caso contrario podemos suponer, reordenando los índices, que $x_1 \neq 0$; en este caso, como los ideales $\mathfrak{p}_1^{n_1}, \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_k^{n_k}$ son coprimos entonces $x_1 = x + y$, con $y \in \mathfrak{p}_1^{n_1}$, $x \in \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_k^{n_k}$. De este modo $x \in A$ cumple que $v_{\mathfrak{p}_1}(x - x_1) = v_{\mathfrak{p}_1}(y) \geq n_1$ y $v_{\mathfrak{p}_i}(x) \geq n_i$ para $i = 2, \dots, n$ y $v_{\mathfrak{q}}(x) \geq 0$ para $\mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_k$, pues $x \in A$, con lo que para este caso el lema estaría probado. Nótese que el x encontrado está en A, utilizaremos este hecho en el *caso 2* a continuación.

2. *Caso 2*: $x_1, \dots, x_k \in A$. Por el caso anterior, para cada $i = 1, \dots, k$ existe un $y_i \in A$ tal que $v_{\mathfrak{p}_i}(y_i - x_i) \geq n_i$ y $v_{\mathfrak{p}_j}(y_i) \geq \mathrm{máx}\{n_1, \dots, n_k\}$. De este modo, el elemento $x = y_1 + \dots + y_k$ cumple que $v_{\mathfrak{p}_i}(x - x_i) = v_{\mathfrak{p}_i}(y_i - x_i + y_1 + \dots + \widehat{y_i} + \dots + y_n) \geq \mathrm{ínf}(\{v_{\mathfrak{p}_i}(y_i - x_i)\} \cup \{v_{\mathfrak{p}_i}(y_j) | j \neq$

$i\}) \geq n_i$. Además, si $\mathfrak{q}$ es un ideal primo no nulo de A diferente de $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, entonces $v_{\mathfrak{q}}(x) \geq 0$, ya que $x \in A$, con lo que el lema estaría probado en este caso.

3. *Caso 3*: $x_1, \ldots, x_k \in K$. En tal caso, reduciendo a común denominador podemos expresar los x_i de la forma $x_i = a_i/s$ con $s \in A$ $a_i \in A$ para todo $i = 1, \ldots, k$. Dado que solo un número finito de ideales primos contienen a s, podemos suponer sin pérdida de generalidad que se encuentran en los $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Así, por el *Caso 2* podemos encontrar, para $a_1, \ldots, a_n \in A$ y $n_1 + v_{\mathfrak{p}_i}(s), \ldots, n_k + v_{\mathfrak{p}_k}(s)$ un elemento $a \in A$ que satisface el lema. De este modo $x = a/s$ cumple que para $i = 1, \ldots, k$:

$$v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(a) - v_{\mathfrak{p}_i}(s) \geq n_i + v_{\mathfrak{p}_i}(s) - v_{\mathfrak{p}_i}(s) = n_i$$

Además, como hemos supuesto que todos los primos que contienen a s están en los $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, tenemos que para $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k$ se cumple $v_{\mathfrak{q}}(x) = v_{\mathfrak{q}}(a) - v_{\mathfrak{q}}(s) = v_{\mathfrak{q}}(a) \geq 0$. De modo que para este caso, que es el más general de todos el lema está probado.

□

Proposición 1.29. *Si un dominio de Dedekind A tiene un número finito de ideales primos entonces $cl(A)$ es trivial.*

Demostración. Si A es un cuerpo entonces el resultado es trivial. Si A no es un cuerpo, demostraremos que A es un dominio de ideales principales. Por la factorización única de ideales basta ver que todo ideal primo es principal, así que supongamos que $\mathrm{Spec}(A) - \{0\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. Sea $\pi_i \in A$ un elemento satisfaciendo $v_{\mathfrak{p}_i}(\pi_i) = 1$ De este modo aplicando el lema anterior (*Caso 2*) para $x_i = \pi_i$, $x_j = 1$ si $j \neq i$ y $n_i = 2$, $n_j = 1$ para $j \neq i$, podemos encontrar un $x \in A$ tal que $v_{\mathfrak{p}_i}(x - \pi_i) \geq 2$ y $v_{\mathfrak{p}_j}(x - 1) \geq 1$ para todo $j \neq i$. Esto implica que $x \notin \mathfrak{p}_j$ (pues si lo estuviese $x - 1 \notin \mathfrak{p}_j$) y $v_{\mathfrak{p}_i}(x) = 1$ (pues si $v_{\mathfrak{p}_i}(x) \geq 2$, entonces $2 \leq v_{\mathfrak{p}_i}(x - \pi_i) =^4 \text{ínf}\{v_{\mathfrak{p}_i}(x), v_{\mathfrak{p}_i}(\pi_i)\} = 1$, lo cual es absurdo, y si $v_{\mathfrak{p}_i}(x) = 0$, entonces $2 \leq v_{\mathfrak{p}_i}(x - \pi_i) = \text{ínf}\{v_{\mathfrak{p}_i}(x), v_{\mathfrak{p}_i}(x)\} = 0$, lo cual también es una contradicción). □

1.2. Extensiones de dominios de Dedekind

Proposición 1.30. *Sea A es un dominio de Dedekind y K su cuerpo de fracciones. Si $L|K$ es una extensión finita de cuerpos y B es la clausura íntegra de A en L ,entonces $L = S^{-1}B$, siendo $S = A - \{0\}$. En particular L es el cuerpo de fracciones de B.*

Demostración. Sea $\alpha \in L$ y $h \in K[X]$ el polinomio irreducible de α sobre K. Como K es el cuerpo de fracciones de A entonces reduciendo los coeficientes de h a común denominador y multiplicando por el mismo obtenemos que α es raíz del polinomio $g(X) = a_0 + a_1X + \cdots + a_nX^n$

[4]Se está utilizando el resultado probado en la demostración de la proposición 1.3, según el cual si v es una valoración discreta, $v(x + y) = \text{ínf}\{v(x), v(y)\}$ si $v(x) \neq v(y)$

con $a_i \in A$ para todo $i = 1 \dots n$, que evidentemente sigue siendo irreducible en $K[X]$. Definimos entonces el polinomio:

$$a_n^{n-1} g(X/a_n) := a_n^{n-1} a_0 + a_n^{n-2} a_1 X + \dots a_{n-2} a_n X^{n-2} + a_{n-1} X^{n-1} + X^n$$

que es un polinomio mónico con coeficientes en A del que $\alpha a_n \in L$ es raíz. Como B es la clausura íntegra de A en L tenemos que todas sus raíces, en particular αa_n están en B. Esto implica que $\alpha = b/a_n$ y por tanto $L = S^{-1}B$, siendo $S = A - \{0\}$. Si ahora denotamos como E el cuerpo de fracciones de B, $L \subset E$. Pero L es un cuerpo conteniendo a B, de modo que la propiedad universal del cuerpo de fracciones implica que $E = L$, como queríamos probar. □

Definición 1.31. Sea $L|K$ una extensión finita de cuerpos y $\alpha \in L$. Se definen la *traza* y la *norma* de la extensión $L|K$ en el elemento α como $\mathrm{Tr}_{L|K}(\alpha) = \mathrm{tr}(T_\alpha) \in K$ y $\mathrm{N}_{L|K}(\alpha) = \det(T_\alpha) \in K$, siendo $T_\alpha : L \to L$ la traslación $x \mapsto \alpha x$, y (T_α) su representación matricial.

Observación 1.32. Nótese que la traza y la norma introducidas anteriormente, al estar definidas en función de la traza y el deteminante, no dependen de la $K-$base de L escogida y definen homomorfismos en los grupos aditivos y multiplicativos de L y K, respectivamente.

Proposición 1.33. *Si $L|K$ es una extensión finita de cuerpos, entonces $Tr_{L|K}(\alpha) = t\, Tr_{K(\alpha)|K}(\alpha)$ y $N_{L|K}(\alpha) = N_{K(\alpha)|K}(\alpha)^t$, donde $t = [L : K(\alpha)]$, para todo $\alpha \in L$.*

Demostración. Sea $\alpha \in L$, consideremos la subextensión (finita, por el teorema del grado) $K(\alpha)|K$. Si el grado del polinomio irreducible de α sobre K es m, $\{1, \alpha, \dots, \alpha^{m-1}\}$ es una $K-$base de $K(\alpha)$. Sea ahora (A) la matriz asociada a la aplicación $K(\alpha) \to K(\alpha)$, $x \mapsto x\alpha$. Dado que la extensión $L|K(\alpha)$ es finita, podemos tomar una $K(\alpha)-$base de L, $\{u_1, \dots, u_t\}$ que nos permitirá una descomposición $L = u_1 K(\alpha) \oplus \cdots \oplus u_t K(\alpha)$. Dado que $T_\alpha(u_i K(\alpha)) \subset u_i K(\alpha)$ es claro que, escogiendo la $K-$base de L $\{u_1, u_1\alpha, \dots, u_1\alpha^{m-1}, u_2, u_2\alpha, \dots, u_2\alpha^{m-1}, \dots, u_t, u_t\alpha, \dots, u_t\alpha^{m-1}\}$ la representación matricial de T_α, (T_α), va a ser diagonal por bloques, conteniendo t copias de (A) a lo largo de la diagonal. De este modo $\mathrm{Tr}_{L|K}(\alpha) = \mathrm{tr}(T_\alpha) = t\,\mathrm{tr}(A) = t\,\mathrm{Tr}_{K(\alpha)|K}(\alpha)$ y $\mathrm{N}_{L|K}(\alpha) = \det(T_\alpha) = \det(A)^t = \mathrm{N}_{K(\alpha)|K}(\alpha)^t$, como queríamos probar. □

Proposición 1.34. *Sea $L|K$ una extensión finita de cuerpos y $\alpha \in L$. Si $f(X) = a_0 + a_1 X + \cdots + a_{m-1}X^{m-1} + X^m$ es el polinomio irreducible de α sobre K, entonces $Tr_{K(\alpha)|K}(\alpha) = -a_{m-1}$ y $N_{K(\alpha)|K}(\alpha) = (-1)^m a_0$.*

Demostración. Consideremos la $K-$base $\{1, \alpha, \dots, \alpha^{m-1}\}$ de $K(\alpha)$. De este modo la matriz de la aplicación $x \mapsto x\alpha$ está compuesta de unos en la diagonal superior, hasta llegar a la última fila, donde se encuentran las coordenadas de α^n en la base anterior. Dado que $f(\alpha) = a_0 + a_1\alpha + \dots a_{m-1}\alpha^{m-1} + \alpha^m = 0$, entonces $\alpha^n = -a_0 - a_1\alpha - \cdots - a_{m-1}\alpha^{m-1}$, con lo que queda claro que la traza de la matriz es $-a_{m-1}$. Para calcular el determinante de la matriz se desarrolla por la primera columna (que solo tiene una única entrada no nula con valor $-a_0$ en la posición $(m, 1)$), obteniendo $-(-1)^{m+1}a_0 = (-1)^m a_0$, como queríamos probar. □

Proposición 1.35. *Sea A un dominio íntegramente cerrado con cuerpo de fracciones K. Sea $L|K$ una extensión finita, $\alpha \in L$ y $f \in K[X]$ su polinomio irreducible. Entonces α es entero sobre A si y solo si $f \in A[X]$.*

Demostración. La inclusión a la izquierda es inmediata (la relación entera viene dada por $f(\alpha) = 0$). Para la aplicación a la derecha supongamos que $\alpha \in L$ es entero sobre A, satisfaciendo $g(\alpha) = 0$ para $g \in A[X]$. Escogiendo una clausura algebraica $\overline{K}$ de la extensión $L|K$ podremos factorizar f como $f(X) = (X - \alpha_1) \dots (X - \alpha_n)$, de modo que para cada $i = 1, \dots, n$ tenemos un $K-$homomorfismo de cuerpos $\sigma_i : K(\alpha) \to \overline{K}$, $\alpha \mapsto \alpha_i$. Así $g(\alpha) = 0$ es equivalente a $\sigma_i(g(\alpha)) = g(\alpha_i) = 0$, luego α_i son enteros sobre A, pertenenciendo a la clausura íntegra $\overline{A}$ de A sobre $\overline{K}$. Dado que los coeficientes de f son sumas y productos de α_i, son elementos de $\overline{A}$, pero como también están en K, son elementos de $\overline{A} \cap K$, pero como A es íntegramente cerrado $\bar{A} \cap K = A$. □

Corolario 1.36. *Sea A un dominio de Dedekind, K su cuerpo de fracciones, $L|K$ es una extensión finita de cuerpos y B la clausura íntegra de A en L. Entonces $Tr_{L|K}(b) \in A$ y $N_{L|K}(b) \in A$ para todo $b \in B$.*

Demostración. Sea $b \in B$. Como B es la clausura íntegra de A en L, b es entero sobre A, y dado que A es un dominio de Dedekind, es íntegramente cerrado, luego el polinomio irreducible f de b sobre K tiene coeficientes en A por la proposición 1.35, con lo que $Tr_{K(b)|K}(b) \in A$, y por lo tanto $Tr_{L|K}(b) \in A$, por las proposiciones 1.34 y 1.33. La demostración para la norma es idéntica. □

Proposición 1.37. *Sea $L|K$ una extensión finita separable de grado n y $\overline{K}$ una clausura algebraica de K conteniendo a L. Sea $\alpha \in L$ y $g \in K[X]$ su polinomio irreducible sobre K (que supondremos de grado m). Entonces se cumple:*

$$\prod_{\sigma \in Hom_K(L,\overline{K})} (X - \sigma(\alpha)) = g^t$$

donde $t = n/m$.

Demostración. Dado que la extensión $L|K$ es finita separable, también lo serán las extensiones $L|K(\alpha)$ y $K(\alpha)|K$, de modo que, por el teorema del elemento primitivo existe un elemento $\gamma \in L$ que genera la extensión $L|K(\alpha)$. Puesto que los $K-$homomorfismos de L en $\overline{K}$ están determinados por su restricción a $K(\alpha)$ y por la imagen de γ, tenemos una aplicación bien definida e inyectiva $\mathrm{Hom}_K(L, \overline{K}) \to \mathrm{Hom}_K(K(\alpha), \overline{K}) \times \mathrm{Hom}_{K(\alpha)}(L, \overline{K})$ dada por $\sigma \mapsto (\sigma_1, \sigma_2)$, donde $\sigma_1(\alpha) = \sigma(\alpha)$ y $\sigma_2(\gamma) = \sigma(\gamma)$. Dicha aplicación además es biyectiva pues como las extensiones $L|K(\alpha)$ y $K(\alpha)|K$ son separables, $\#\mathrm{Hom}_K(K(\alpha), \overline{K}) \#\mathrm{Hom}_{K(\alpha)}(L, \overline{K}) = mt = n = \#\mathrm{Hom}_K(L, \overline{K})$. Componiendo con la proyección canónica obtenemos la aplicación $p : \mathrm{Hom}_K(L, \overline{K}) \to \mathrm{Hom}_K(K(\alpha), \overline{K}) \times \mathrm{Hom}_{K(\alpha)}(L, \overline{K}) \to \mathrm{Hom}_K(K(\alpha), \overline{K})$ dada por $\sigma \mapsto (\sigma_1, \sigma_2) \mapsto \sigma_1$. De esto se deduce que las clases de la relación de equivalencia $\sigma \sim \tau \Leftrightarrow$

$\sigma(\alpha) = \tau(\alpha)$ (donde $\sigma, \tau \in \mathrm{Hom}_K(L, \overline{K})$) son las fibras de la composición anterior. En particular, podemos identificar cada clase con un elemento de $\mathrm{Hom}_K(K(\alpha), \overline{K})$, y cada clase tendrá $\#\mathrm{Hom}_K(\alpha)(L, \overline{K}) = t$ elementos. Así:

$$\prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} (X - \sigma(\alpha)) = \prod_{\overline{\sigma} \in \mathrm{Hom}_K(K(\alpha),\overline{K})} \prod_{\tau \in p^{-1}(\overline{\sigma})} (X - \tau(\alpha)) = \prod_{\overline{\sigma} \in \mathrm{Hom}_K(K(\alpha),\overline{K})} (X - \overline{\sigma}(\alpha))^t = g^t$$

□

Corolario 1.38. *Sea $L|K$ una extensión finita separable de grado n y $\overline{K}$ una clausura algebraica de K conteniendo a L, entonces:*

$$Tr_{L|K} = \sum_{\sigma \in Hom_K(L,\overline{K})} \sigma \quad ; \quad N_{L|K} = \prod_{\sigma \in Hom_K(L,\overline{K})} \sigma$$

En particular, si $L|K$ es una extensión de Galois finita:

$$Tr_{L|K} = \sum_{\sigma \in Gal(L|K)} \sigma \quad ; \quad N_{L|K} = \prod_{\sigma \in Gal(L|K)} \sigma$$

Demostración. Sea $\alpha \in L$ y $g = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m$ su polinomio irreducible sobre K. Dado que la extensión $L|K$ es finita separable, por la proposición anterior:

$$b_0 + b_1 X + \cdots + b_{n-1} X^{n-1} + X^n = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} (X - \sigma(\alpha)) = g^t$$

donde $t = n/m$. Expandiendo el producto obtenemos $b_0 = (-1)^n \prod_\sigma \sigma(\alpha)$ y $b_{n-1} = \sum_\sigma \sigma(\alpha)$, donde σ recorre $\mathrm{Hom}_K(L, \overline{K})$. Repitiendo el mismo procedimiento para el lado derecho de la igualdad obtenemos:

$$X^{mt} + tX^{m(t-1)}(a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}) + \sum_{k=2}^{t} \binom{t}{k} (a_0 + a_1 X + \cdots + a_{m-1} X^{m-1})^k X^{m(t-k)}$$

donde el coeficiente del término independiente es $a_0^t = (-1)^n \mathrm{N}_{L|K}(\alpha)$ y el término en X^{n-1} es $ta_{m-1} = \mathrm{Tr}_{L|K}(\alpha)$ (en la suma en k indicada el grado de los términos del sumando $k-$ésimo es a lo sumo $k(m-1) + m(t-k) = n - k \geq n - 2$, de modo que no tiene términos en X^{n-1}), como queríamos probar. Para el caso particular de que la extensión $L|K$ sea de Galois finita basta con tener en cuenta que $\mathrm{Hom}_K(L, \overline{K}) \simeq \mathrm{Gal}(L|K)$, de modo que las igualdades son consecuencia directa de la demostración anterior. □

Proposición 1.39. *Sea $L|K$ una extensión finita separable de grado n. Se satisface:*

1. *La aplicación $L \times L \to L$, $(x, y) \mapsto Tr_{L|K}(xy)$ es una forma bilineal simétrica, que es no singular, es decir, para todo $0 \neq x \in L$ existe un $y \in L$ tal que $Tr_{L|K}(x, y) \neq 0$.*

2. *Si A es un dominio noetheriano íntegramente cerrado con cuerpo de fracciones K y $L|K$ es una extensión finita separable, la clausura íntegra de A en L, B, es un $A-$módulo de tipo finito (y por tanto un anillo noetheriano).*

Demostración. Para la primera parte de la demostración, es claro por el corolario 1.38, que la aplicación $(x, y) \mapsto \mathrm{Tr}_{L|K}(xy)$ es bilineal y simétrica. Para ver que es no singular sea α un elemento primitivo de la extensión $L|K$. Basta con demostrar que la matriz de Gram asociada a la forma bilineal para la $K-$base de L $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es no singular. Si $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$, por el corolario anterior obtenemos:

$$G_{ij} = \mathrm{Tr}_{L|K}(\alpha^{i-1}\alpha^{j-1}) = \sum_{k=1}^{n} \sigma_k(\alpha^{i-1}\alpha^{j-1}) = \sum_{k=1}^{n} \sigma_k(\alpha)^{i-1}\sigma_k(\alpha)^{j-1} = (AA^T)_{ij}$$

donde $A_{ij} = \sigma_i(\alpha)^{j-1}$. Dado que A es una matriz de Vandermonde, $\det A = \prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha)) \neq 0$, de modo que $\det G \neq 0$, como queríamos probar.

Para la segunda parte de la proposición, por la proposición 1.30, $L = S^{-1}B$ con $S = A - \{0\}$ y por tanto podemos suponer, multiplicando convenientemente por escalares, que existe una $K-$base de L formada por elementos de B, que denotaremos como $\{e_1, \ldots, e_n\}$. De este modo, por el corolario 1.36 la aplicación $\varphi : B \to A^n$, $x \mapsto (\mathrm{Tr}_{L|K}(xe_1), \ldots, \mathrm{Tr}_{L|K}(xe_n))$ está bien definida y es un homomorfismo de $A-$módulos, que además es inyectivo por el apartado anterior (en efecto, si existiese un $x \in B$ tal que $\mathrm{Tr}_{L|K}(xe_i) = 0$ para todo $i = 1, \ldots, n$, entonces, dado que $\{e_1, \ldots, e_n\}$ forman una $K-$ base de L se tendría que $\mathrm{Tr}_{L|K}(xy) = 0$ para todo $y \in L$, contradiciendo que $\mathrm{Tr}_{L|K}$ es no degenerada). Esto implica, por el primer teorema de isomorfía, que $B \simeq \mathrm{Im}(\varphi) \subset A^n$, y como A es noetheriano, B es un $A-$módulo de tipo finito, que además es noetheriano (ya que A^n es un $A-$módulo noetheriano). □

Lema 1.40. *Sean $A \subset B$ anillos, siendo B entero sobre A. Si $\mathfrak{q}_1 \subset \mathfrak{q}_2$ son ideales primos de B tales que $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$, entonces $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Demostración. Dado que $\mathfrak{q}_1 \subset \mathfrak{q}_2$, el teorema de correspondencia para anillos nos asegura que $\mathfrak{q}_2/\mathfrak{q}_1$ es un ideal primo de $B/\mathfrak{q}_1$, que es a su vez entero sobre $A/(\mathfrak{q}_1 \cap A)$ [AM, prop. 5.6], de modo que podemos suponer sin pérdida de generalidad que $\mathfrak{q}_1 = 0$, y que tanto A como B son dominios ($\mathfrak{q}_1 \cap A$ es un ideal primo de A pues es la imagen recíproca del ideal primo $\mathfrak{q}_1$ por el homomorfismo inclusión $A \hookrightarrow B$). Si $\mathfrak{q}_2 \neq \mathfrak{q}_1$ existe un elemento $x \in \mathfrak{q}_2$ no nulo, que ha de satisfacer una relación $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ con $a_i \in A$ para $i = 1, \ldots, n-1$, ya que B es entero sobre A. Supondremos que la relación anterior es la de menor grado entre todas las posibles, esto implica que $a_0 \neq 0$, ya que $x \neq 0$, con lo que $a_0 \in \mathfrak{q}_2 \cap A = \mathfrak{q}_1 \cap A = 0$, lo cual es absurdo. □

Proposición 1.41. *Sea A un dominio de Dedekind, K su cuerpo de fracciones, y $L|K$ una extensión finita de cuerpos tal que la clausura íntegra de A en L, B, es un $A-$módulo finitamente generado. Entonces B es un dominio de Dedekind.*

Demostración. Efectivamente, B es un $A-$módulo noetheriano al ser A un anillo noetheriano y B un $A-$módulo finitamente generado, y es íntegramente cerrado. Lo único que nos queda para probar que es un dominio de Dedekind es que $\dim B \leq 1$. Sea entonces $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ una cadena ascendente de ideales primos de B. El lema anterior nos asegura que $\mathfrak{p}_0 \cap A \subsetneq \mathfrak{p}_1 \cap A \subsetneq \mathfrak{p}_2 \cap A$ es una cadena ascendente de ideales de A, lo cual es absurdo pues A es un dominio de Dedekind, y por tanto $\dim A \leq 1$. □

Observación 1.42. Aunque no lo utilizaremos en este trabajo, para probar esto no es necesario suponer que B sea un $A-$módulo finitamente generado, ni que A es un dominio de Dedekind:

Teorema 1.43 (Krull-Akizuki). *Sea A un dominio noetheriano con $\dim A \leq 1$, cuerpo de fracciones K, $L|K$ una extensión finita y B la clausura íntegra de A en L. Entonces B es un dominio de Dedekind.*

Demostración. Véase [Neu, cap. I, prop. 12.8]. □

Definición 1.44. Sea A un dominio de Dedekind, K su cuerpo de fracciones y $L|K$ una extensión finita de cuerpos. Si la clausura íntegra de A en L (que denotaremos como B y será en particular un dominio de Dedekind) es un $A-$módulo de tipo finito, diremos que el ideal primo no nulo $\mathfrak{q} \subset B$ *divide* (o está *sobre*) al ideal primo no nulo $\mathfrak{p} \subset A$ si $\mathfrak{p} = \mathfrak{q} \cap A$, o equivalentemente cuando $\mathfrak{q}$ contiene al ideal $\mathfrak{p}B$.[5]

Definición 1.45. Que $\mathfrak{q} \subset B$ divida a $\mathfrak{p} \subset A$ implica que el *índice de ramificación* de $\mathfrak{q}$ en la extensión $L|K$, definido como $e_\mathfrak{q} = v_\mathfrak{q}(\mathfrak{p}B)$, sea no nulo. En particular, $\mathfrak{p}B$ admite la siguiente descomposición (por el corolario 1.25):

$$\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$$

Por otro lado sean $\kappa = A/\mathfrak{p}$ y $\lambda = B/\mathfrak{q}$. Dado que B es un $A-$módulo finitamente generado y $\mathfrak{p}B \subset \mathfrak{q}$, λ es un κ- módulo finitamente generado, y como en un dominio de Dedekind todos los ideales primos son maximales, tenemos que ambos $A-$módulos son cuerpos, y en particular, λ es un $\kappa-$espacio vectorial de dimensión finita. Definimos el *grado residual* de $\mathfrak{q}$ en la extensión $L|K$ como:

$$f_\mathfrak{q} = [\lambda : \kappa] = \dim_\kappa \lambda$$

Teorema 1.46. *Sea A un dominio de Dedekind, K su cuerpo de fracciones y $L|K$ una extensión finita de cuerpos de grado n tal que la clausura íntegra de A en L, B, es un $A-$módulo finitamente generado (por ejemplo, si la extensión $L|K$ es separable). Sea $\mathfrak{p}$ un ideal primo no nulo de A y $\kappa = A/\mathfrak{p}$. Entonces:*

[5] En efecto, sea $\mathfrak{q}$ un ideal primo mo nulo de B. Si $\mathfrak{p} = \mathfrak{q} \cap A$, entonces $\mathfrak{p}B = (\mathfrak{q} \cap A)B \subset \mathfrak{q}B = \mathfrak{q}$. Recíprocamente, si $\mathfrak{p} \subset A$ es un ideal primo no nulo, entonces $\mathfrak{p}B \subset \mathfrak{q}$, de modo que $\mathfrak{p} \subset \mathfrak{q} \cap A$, que es un ideal primo de A. Como $\mathfrak{p}$ es un ideal maximal de A, $\mathfrak{p} = \mathfrak{q} \cap A$

1. *El anillo $B/\mathfrak{p}B$ es una κ-álgebra isomorfa al producto $\prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}}$, que como espacio vectorial tiene dimensión $n = [L : K]$.*

2. *Se cumple la relación:*

$$n = \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q}$$

Demostración. Comencemos probando (1). Es claro que $B/\mathfrak{p}B$ es un anillo y un $\kappa-$ módulo finitamente generado (el argumento es el mismo que el dado en la observación 1.45). De modo que el homomorfismo de anillos $A/\mathfrak{p} \to B/\mathfrak{p}B$, inducido por $A \hookrightarrow B \to B/\mathfrak{p}B$, dado por $x \mod \mathfrak{p} \mapsto x \mod \mathfrak{p}B$ hace de $B/\mathfrak{p}B$ un $\kappa-$módulo de tipo finito, es decir, un $\kappa-$ espacio vectorial de dimensión finita, ya que κ es un cuerpo.

Veamos ahora que el grado de $B/\mathfrak{p}B$ es n. Podemos suponer sin pérdida de generalidad que A es un AVD: efectivamente si $\mathfrak{p} \subset A$ es un ideal primo y $S = A - \mathfrak{p}$, sean $A' = S^{-1}A = A_\mathfrak{p}$ y $B' = S^{-1}B$.[6] Es claro entonces que [AM, cor. 3.4]:

$$A'/\mathfrak{p}A' = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq (A/\mathfrak{p})_\mathfrak{p} = A/\mathfrak{p} = \kappa,$$

donde la penúltima igualdad es posible pues, al ser $\mathfrak{p}$ un ideal maximal, $A/\mathfrak{p} = \kappa$ es un cuerpo. Además:

$$B'/\mathfrak{p}B' = S^{-1}B/\mathfrak{p}S^{-1}B = S^{-1}(B/\mathfrak{p}B) \simeq S^{-1}\kappa \otimes_\kappa B/\mathfrak{p}B = \kappa \otimes_\kappa B/\mathfrak{p}B \simeq B/\mathfrak{p}B,$$

donde se han utilizado las propiedades de localización de módulos [AM, prop. 3.5]. Además B' es la clausura íntegra de A' en L (tomar clausuras íntegras conmuta con localizaciones [AM, prop. 5.12]). De este modo podemos suponer que $A' = A_\mathfrak{p}$ es un AVD con cuerpo de fracciones K, $L|K$ una extensión finita de cuerpos y B' la clausura íntegra de A' en L, que es un $A'-$módulo finitamente generado (si B es un $A-$módulo finitamente generado y $S \subset A$ es un conjunto multiplicativo que no contiene a cero, entonces $S^{-1}B$ es un $S^{-1}A-$módulo finitamente generado). Por lo tanto podemos suponer que A es un dominio de ideales principales y B es un $A-$módulo finitamente generado (y libre de torsión, ya que es un dominio que contiene a A), de modo que por el teorema de estructura de módulos de tipo finito sobre un dominio de ideales principales, B es un $A-$módulo libre finitamente generado. Para ver que su rango es $n = [L : K]$ usamos el hecho de que si B es un $A-$módulo libre de rango t, para todo subconjunto multiplicativo $S \subset A$ que no contenga a cero, $S \subset A$, $S^{-1}B$ es un $S^{-1}A-$módulo libre de rango t, de modo que tomando $S = A - \{0\}$, obtenemos por lo visto en la proposición 1.30 que $S^{-1}B = L$. Así, el rango de B como $A-$módulo libre coincide con el rango de L como $K-$módulo (es decir como $K-$espacio vectorial) y vale $n = [L : K]$, como queríamos probar.

Para la segunda parte, usaremos la propiedad de que si $\mathfrak{q}_1, \mathfrak{q}_2$ son ideales primos no nulos de B, entonces $\mathfrak{q}_1^n$ y $\mathfrak{q}_2^m$ son coprimos para cualquier par de enteros positivos n, m, ya que sus ideales radicales son ideales maximales distintos. Esto implica que $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}} = \bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$.

[6] Nótese que S es multiplicativamente cerrado visto como subconjunto de B, luego tiene sentido

De este modo, el teorema chino de los restos nos permite asegurar que:

$$B/\mathfrak{p}B = B/\bigcap_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}}$$

La expresión anterior nos da un isomorfismo de κ-espacios vectoriales, de modo que igualando dimensiones:

$$n = \dim_\kappa(B/\mathfrak{p}B) = \sum_{\mathfrak{q}|\mathfrak{p}} \dim_\kappa(B/\mathfrak{q}^{e_\mathfrak{q}})$$

Solo queda probar que $\dim_\kappa(B/\mathfrak{q}^{e_\mathfrak{q}}) = e_\mathfrak{q} f_\mathfrak{q}$ para todo $\mathfrak{q}|\mathfrak{p}$. Esto se prueba en el siguiente lema:

Lema 1.47. *En las condiciones del teorema,* $\dim_\kappa(B/\mathfrak{q}^{e_\mathfrak{q}}) = e_\mathfrak{q} f_\mathfrak{q}$.

Demostración. Dado que $B_\mathfrak{q}/\mathfrak{q}^{e_\mathfrak{q}} B_\mathfrak{q} \simeq B/\mathfrak{q}^{e_\mathfrak{q}} B$, podemos suponer sin pérdida de generalidad que B es un AVD. Tenemos la siguiente sucesión exacta de $\kappa-$espacios vectoriales:

$$0 \to \mathfrak{q}^{e_\mathfrak{q}-1}/\mathfrak{q}^{e_\mathfrak{q}} \hookrightarrow B/\mathfrak{q}^{e_\mathfrak{q}} \to (B/\mathfrak{q}^{e_\mathfrak{q}})/(\mathfrak{q}^{e_\mathfrak{q}-1}/\mathfrak{q}^{e_\mathfrak{q}}) \simeq B/\mathfrak{q}^{e_\mathfrak{q}-1} \to 0,$$

de modo que $\dim_\kappa(B/\mathfrak{q}^{\mathfrak{e}_\mathfrak{q}}) = \dim_\kappa(\mathfrak{q}^{e_\mathfrak{q}-1}/\mathfrak{q}^{e_\mathfrak{q}}) + \dim_\kappa(B/\mathfrak{q}^{e_\mathfrak{q}-1})$. Aplicando inductivamente el razonamiento se deduce que $\dim_\kappa(B/\mathfrak{q}^{e_\mathfrak{q}}) = \dim_\kappa(\mathfrak{q}^{e_\mathfrak{q}-1}/\mathfrak{q}^{e_\mathfrak{q}}) + \dim_\kappa(\mathfrak{q}^{e_\mathfrak{q}-2}/\mathfrak{q}^{e_\mathfrak{q}-1}) + \cdots + \dim_\kappa(\mathfrak{q}/\mathfrak{q}^2) + \dim_\kappa(B/\mathfrak{q})$, con lo que para concluir basta con demostrar que $\dim_\kappa(\mathfrak{q}^n/\mathfrak{q}^{n+1}) = f_\mathfrak{q}$ para $n \geq 1$. Sea pues π un uniformizante de $\mathfrak{q}$, entonces la aplicación $B \to \mathfrak{q}^n/\mathfrak{q}^{n+1}$ dada por $x \mapsto x\pi^n$ mód $\mathfrak{q}^{n+1}$ es un homomorfismo de $A-$módulos sobreyectivo que tiene a $\mathfrak{q}$ como núcleo (efectivamente, $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ no es nulo, como se vio en la demostración de la proposición 1.5 y su núcleo es un ideal propio de B que contiene al ideal maximal $\mathfrak{q}$, de modo que ambos ideales tienen que ser iguales). Este homomorfismo induce el isomorfismo de $\kappa-$módulos $B/\mathfrak{q} \to \mathfrak{q}^n/\mathfrak{q}^{n+1}$, y así, $\dim_\kappa(\mathfrak{q}^n/\mathfrak{q}^{n+1}) = \dim_\kappa(B/\mathfrak{q}) = f_\mathfrak{q}$, como queríamos probar.

□

La demostración del teorema 1.46 está entonces terminada. □

Corolario 1.48. *Sea A un dominio de Dedekind, K su cuerpo de fracciones y $L|K$ una extensión finita de cuerpos de grado n tal que la clausura íntegra de A en L, B, es un $A-$módulo finitamente generado. El número de ideales primos $\mathfrak{q}$ de B que dividen a un ideal primo $\mathfrak{p}$ de A es, como mínimo 1 y como máximo n. Si A tiene un número finito de ideales primos, también lo tendrá B (con lo que será un dominio de ideales principales).*

Definición 1.49. Sea A un dominio de Dedekind, K su cuerpo de fracciones y $L|K$ una extensión finita de cuerpos tal que la clausura íntegra de A en L, B, es un $A-$módulo finitamente generado. Sea también $\mathfrak{p}$ un ideal primo de A y $\kappa = A/\mathfrak{p}$. Si solo hay un ideal primo $\mathfrak{q}$ de B tal que $\mathfrak{q}|\mathfrak{p}$ y $f_\mathfrak{q} = 1$ diremos que la extensión $L|K$ está *totalmente ramificada* en $\mathfrak{p}$. Si $\mathfrak{q}$ es un ideal primo sobre $\mathfrak{p}$ tal que $e_\mathfrak{q} = 1$ y $\lambda := B/\mathfrak{q}|\kappa$ es una extensión separable, diremos que $L|K$ es *no ramificada* en $\mathfrak{q}$. Finalmente, si la extensión $L|K$ es no ramificada sobre todos los primos $\mathfrak{q} \subset B$ sobre $\mathfrak{p}$ diremos que la extensión $L|K$ es *no ramificada* en $\mathfrak{p}$.

Definición 1.50. Sea A un dominio de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita de cuerpos y B la clausura íntegra de A en L. Una valoración w de L se dice que *extiende* una valoración v de K (con índice $e > 0$ entero positivo) si $w(x) = ev(x)$ para todo $x \in K$.

Proposición 1.51. *Sea A un dominio de Dedekind, K su cuerpo de fracciones y $L|K$ una extensión finita de cuerpos tal que la clausura íntegra de A en L, B, es un $A-$módulo finitamente generado. Sea también $\mathfrak{p}$ un ideal primo no nulo de A. Para cada primo $\mathfrak{q}$ de B dividiendo a $\mathfrak{p}$, la valoración $v_\mathfrak{q}$ extiende la valoración $v_\mathfrak{p}$ con índice $e_\mathfrak{q}$. Además la aplicación $\mathfrak{q} \mapsto v_\mathfrak{q}$ es una biyección del conjunto de los ideales primos de B que dividen a $\mathfrak{p}$ y el conjunto de valoraciones que extienden $v_\mathfrak{p}$.*

Demostración. Para la primera parte de la proposición, sea $\mathfrak{q}$ un ideal primo de B que divide a $\mathfrak{p}$ y $\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$ la factorización de $\mathfrak{p}B$. Por lo visto en la demostración 1.24, $(\mathfrak{p}B)_\mathfrak{q} = \mathfrak{q}^{e_\mathfrak{q}} B_\mathfrak{q}$ por lo que para cada $n \in \mathbb{Z}$, $(\mathfrak{p}^n B)_\mathfrak{q} = (\mathfrak{p}B_\mathfrak{q})^n = (\mathfrak{q}^{e_\mathfrak{q}} B_\mathfrak{q})^n$ (ya que la localización conmuta con los productos), con lo que $v_\mathfrak{q}(\mathfrak{p}^n B_\mathfrak{q}) = ne_\mathfrak{q} = e_\mathfrak{q} v_\mathfrak{p}(\mathfrak{p}^n A_\mathfrak{p})$. Por factorización única de ideales esto implica que para todo ideal fraccionario $\mathfrak{a} \subset L$ se tiene que $v_\mathfrak{q}(\mathfrak{a}B_\mathfrak{q}) = e_\mathfrak{q} v_\mathfrak{p}(\mathfrak{a}A_\mathfrak{p})$, y en particular para todo ideal fraccionario principal xB con $x \in K$, lo que nos permite concluir.

Para ver que la correspondencia $\mathfrak{q} \mapsto v_\mathfrak{q}$ es inyectiva, tenemos que si $\mathfrak{q}_1, \mathfrak{q}_2$ son ideales primos de B distintos que dividen a $\mathfrak{p}$, entonces, como son maximales, uno no puede contener propiamente al otro, de modo que tomando $0 \neq x \in \mathfrak{q}_1 - \mathfrak{q}_2$, tenemos que $v_{\mathfrak{q}_1}(x) > 0 \geq v_{\mathfrak{q}_2}(x)$, con lo que $v_{\mathfrak{q}_1} \neq v_{\mathfrak{q}_2}$.

Para ver que la correspondencia es sobreyectiva, sea w una valoración discreta de L que extiende $v_\mathfrak{p}$, C su anillo de valoración y $\mathfrak{m}$ su ideal maximal. Como w extiende $v_\mathfrak{p}$, entonces la valoración w es no negativa en A, de modo que $A \subset C$, y dado que C es un AVD, es íntegramente cerrado en L, con lo que $B \subset C$ (ya que B es la clausura íntegra de A en L). Definiendo $\mathfrak{n} = \mathfrak{m} \cap B$, tenemos que es un ideal primo (ya que $\mathfrak{m}$ lo es) y que $\mathfrak{p} = \mathfrak{n} \cap A$, de modo que $\mathfrak{n}$ divide a $\mathfrak{p}$. Esto implica que C contiene a $B_\mathfrak{n}$ (esto puede verse ya que si $x = a/b \in B_\mathfrak{n}$, $w(x) = w(a) - w(b) \geq 0$ ya que $b \notin \mathfrak{n}$, con lo que $b \notin \mathfrak{m}$). Como $B_\mathfrak{n}$ es un anillo de valoración discreta (ya que B es un dominio de Dedekind), el lema 1.4 nos permite deducir que $C = B_\mathfrak{n}$, pero como los AVD están únicamente determinados por su valoración (proposición 1.3), $w = v_\mathfrak{n}$. □

Capítulo 2

Cuerpos locales

Definición 2.1. Sea K un cuerpo. Un *valor absoluto* sobre K es una aplicación $|\cdot| : K \to \mathbb{R}$ que verifica:

(1) $|x| \geq 0$, para todo $x \in K$

(2) $|x| = 0 \iff x = 0$

(3) $|xy| = |x||y|$, para todo $x, y \in K$

(4) $|x + y| \leq |x| + |y|$

Un valor absoluto $|\cdot|$ se dice *no arquimediano* si verifica $|x + y| \leq \text{máx}\{|x|, |y|\}$ para todo $x, y \in K$, y *arquimediano*, en otro caso.

Observación 2.2. Sea K un cuerpo, la aplicación que lleva todo elemento no nulo de K a 1 y el cero a 0 es un valor absoluto, que denominaremos valor absoluto *trivial*. Todo valor absoluto sobre un cuerpo finito F es trivial, ya que, denotando $q = \#F$, si $x \in F$ es no nulo, $|x| = |x^q| = |x|^q$, y entonces necesariamente $|x| = 1$ (pues $|x|$ es real y positivo).

Proposición 2.3. *Sea K un cuerpo y $|\cdot|$ un valor absoluto. Entonces $|\cdot|$ es no arquimediano si y solo si existe una constante $M \in \mathbb{R}$ tal que $|n| = |\overbrace{1 + \cdots + 1}^{n}| < M$ para todo $n \in \mathbb{N}$.*

Demostración. Para el *solo si* basta con ver que $|n| \leq \text{máx}\{|1|, \cdots, |1|\} = |1| = 1$. Para el *si*, supongamos que $|n| \leq M$ para todo $n \in \mathbb{N}$ y sean $x, y \in K$ tales que $|x| \geq |y|$. Esto implica que $|x|^m |y|^{n-m} \leq |x|^n$ para todo $m \geq 1$. Por el binomio de Newton:

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

por tanto $|x + y| \leq (M(n + 1))^{1/n}|x|$, de modo que tomando el límite $n \to \infty$ obtenemos que $|x + y| \leq |x|$, y en consecuencia, el valor absoluto $|\cdot|$ es no arquimediano. □

Observación 2.4. Un valor absoluto induce una topología sobre K, generada por las bolas abiertas $B(x_0, r) = \{x \in K \,|\, |x - x_0| < r\}$ con $r \in (0, \infty)$ y $x_0 \in K$, que hacen de K un *cuerpo topológico*. Esto implica que los grupos aditivos y multiplicativos de K tienen estructura de grupos topológicos, y por tanto las traslaciones $x \mapsto a + x$ (si $a \in K$), $a \mapsto ax$ (si $a \in K^*$), son homeomorfismos, con lo que para estudiar las propiedades topológicas locales de K nos restringiremos sistemáticamente a estudiarlas en entornos del cero. Es claro que la topología generada

por el valor absoluto trivial es discreta. Necesitamos introducir un criterio para distinguir valores absolutos en función de su topología:

Proposición 2.5. *Sea K un cuerpo y $|\cdot|_1$, $|\cdot|_2$ dos valores absolutos sobre K. Entonces $|\cdot|_1$, $|\cdot|_2$ definen la misma topología sobre K si y solo si existe un $s > 0$ tal que $|x|_2 = |x|_1^s$ para todo $x \in K$.*

Demostración. Es claro que si $|x|_2 = |x|_1^s$ para todo $x \in K$ entonces el sistema de entornos abiertos de cero en $|\cdot|_1$ $\{B(0, 1/n)\}_{n>0}$, es un sistema de entornos abiertos de cero de $|\cdot|_2$, luego, por homogeneidad, ambos valores absolutos tienen una misma base de topología. Por otro lado, si ambos valores absolutos generan la misma topología, entonces $|x|_1 < 1$ implica $|x|_2 < 1$. Efectivamente, la condición $|x|_1 < 1$ equivale a que la sucesión $\{x^n\}_{n\in\mathbb{N}}$ converja a cero para la topología definida por $|\cdot|_1$, y esto implica que converge a cero en la topología de $|\cdot|_2$, por lo que $|x|_2 < 1$. Si $|x|_1 = 1$ para todo $x \neq 0$, entonces $|x|_2 = 1$ para todo $x \neq 0$ ya que si algún $x \neq 0$ verifica $|x|_2 \neq 1$, entonces $|x|_2 < 1$ o $|x|_2 > 1$ (y por tanto, la topología generada por $|\cdot|_2$ no sería la discreta). En caso contrario tomemos un elemento $z \in K$ tal que $|z|_1 > 1$ para todo $x \in K$ no nulo, entonces $|x|_1 = |z|_1^\alpha$ para algún $\alpha \in \mathbb{R}$, de modo que tomando una sucesión de elementos de $\mathbb{Q}$, $\{k_n/m_n\}_{n\in\mathbb{N}}$ acotada inferiormente por α y convergiendo a α, $|x|_1 = |z|_1^\alpha < |z|^{k_n/m_n}$, y por tanto $|z^{m_n}/x^{k_n}|_1 < 1$ para todo $n \in \mathbb{N}$; esto implica por lo anterior que $|z^{m_n}/x^{k_n}|_2 < 1$, con lo que $|x|_2 \leq |z|_2^\alpha$. Si ahora tomamos una sucesión acotada superiormente por α convergiendo a α obtenemos que $|x|_2 = |y|_2^\alpha$, de modo que el valor de $s = \log|x|_2/\log|x|_1$ es una constante para todo $x \in K$, y por tanto $|x|_2 = |x|_1^s$ para todo $x \in K$, como queríamos probar. □

Observación 2.6. Si K es un cuerpo y $|\cdot|$ un valor absoluto no arquimediano, entonces el conjunto $A = \{x \in K \,|\, |x| \leq 1\}$ tiene estructura de dominio local con las operaciones de K, cuyo único ideal maximal es $\mathfrak{m} = \{x \in K \,|\, |x| < 1\}$ (en efecto, la propiedad no arquimediana implica que $\mathfrak{m}$ es un ideal de A y si $|x| = 1$, x no es nulo y por tanto $|1/x| = 1$, con lo que $1/x \in A$). La proposición anterior equivale a que el anillo A de un valor absoluto no arquimediano $|\cdot|$ se mantiene bajo equivalencia, de hecho caracteriza la topología del valor absoluto.

Proposición 2.7. *Sea K un cuerpo y $|\cdot|$ un valor absoluto no arquimediano:*

1. *Todo punto de una bola abierta o cerrada es un centro.*
2. *Cualquier par de bolas abiertas son disjuntas o concéntricas.*
3. *Toda bola abierta es cerrada y toda bola cerrada es abierta.*

Demostración. Para (1) sea $x \in K$ y $r > 0$. Si $y, z \in B(x, r)$ (respectivamente, $B[x, r]$), entonces $|y - z| \leq \max\{|y - x|, |x - z|\} < r$ (respectivamente $\leq r$), con lo que $B(x, r) = B(y, r)$ (respectivamente $B[x, r] = B[y, r]$). Claramente, (2) se deduce de (1). Para (3), probar que toda bola cerrada es un abierto se deduce de (1). En efecto, sean $x, y \in K$ y $r \geq 0$, si $y \in B[x, r]$, entonces $y \in B(y, r) \subset B[y, r] = B[x, r]$. Esto implica también que toda bola abierta es cerrada, ya que para $x, y \in K$ y $r > 0$, si $y \neq B(x, r)$, por (2) se cumple que $B(y, r) \cap B(x, r) = \varnothing$, y por

tanto el complementario de $B(y,r)$ es abierto. De este modo $B(y,r)$ es cerrado, como queríamos probar. □

2.1. Completación de un cuerpo para un valor absoluto

Sea K un cuerpo con un valor absoluto $|\cdot|$. Sea $\mathcal{C}_K$ el conjunto de sucesiones de Cauchy de K, sobre el que definimos la relación de equivalencia $\{x_n\}_{n\in\mathbb{N}} \sim \{y_n\}_{n\in\mathbb{N}} \iff \{x_n - y_n\}_{n\in\mathbb{N}} \to 0$. Llamaremos al conjunto cociente $\hat{K} = \mathcal{C}_K/\sim$ la *completación topológica* de K respecto de $|\cdot|$.

Proposición 2.8. *Sea K un cuerpo con un valor absoluto $|\cdot|$. Su completación topológica $\hat{K}$ tiene estructura de cuerpo completo con un valor absoluto $|\cdot|'$ que además cumple la siguiente propiedad universal: todo homomorfismo de cuerpos topológicos (es decir, un homomorfismo de cuerpos continuo) de K a un cuerpo completo para un valor absoluto $f : K \to L$ puede extenderse de modo único a un homomorfismo continuo $f : \hat{K} \to L$. Además, f es un isomorfismo de cuerpos topológicos si y solo si f es un embebimiento y la imagen de f es densa en L.*

Demostración.

Lema 2.9. *$\hat{K}$ tiene estructura de cuerpo.*

Demostración. Sean $\mathbf{x} = [\{x_n\}_{n\in\mathbb{N}}], \mathbf{y} = [\{y_n\}_{n\in\mathbb{N}}] \in \hat{K}$. Definimos su suma y producto como $\mathbf{x}+\mathbf{y} = [\{x_n+y_n\}_{n\in\mathbb{N}}]$, $\mathbf{xy} = [\{x_n y_n\}_{n\in\mathbb{N}}]$. Dichas operaciones están bien definidas porque si $\{x_n\}_{n\in\mathbb{N}}, \{y_n\}_{n\in\mathbb{N}}$ son sucesiones de Cauchy, $\{x_n+y_n\}_{n\in\mathbb{N}}$ y $\{x_n y_n\}_{n\in\mathbb{N}}$ son sucesiones de Cauchy, y no dependen del representante pues si $\{x_n\}_{n\in\mathbb{N}} \sim \{\bar{x}_n\}_{n\in\mathbb{N}}$, $\{y_n\}_{n\in\mathbb{N}} \sim \{\bar{y}_n\}_{n\in\mathbb{N}}$, entonces:

$$|(x_n+y_n) - (\bar{x}_n+\bar{y}_n)| \le |x_n-\bar{x}_n| + |y_n-\bar{y}_n| \to 0$$

$$|x_n y_n - \bar{x}_n\bar{y}_n| = |x_n y_n - \bar{x}_n y_n + \bar{x}_n y_n - \bar{x}_n\bar{y}_n| \le |y_n||x_n-\bar{x}_n| + |\bar{x}_n||y_n-\bar{y}_n| \to 0$$

donde se ha utilizado que las sucesiones de Cauchy son acotadas. Los neutros para la suma y el producto son $\mathbf{0} = [\{0\}_{n\in\mathbb{N}}]$ y $\mathbf{1} = [\{1\}_{n\in\mathbb{N}}]$. Construyamos los inversos, sea $\mathbf{x} = [\{x_n\}_{n\in\mathbb{N}}] \in \hat{K}$ una clase no nula, de modo que $|x_n| \not\to 0$. Como toda sucesión de Cauchy es acotada existen $\varepsilon_0, N_0 > 0$ con $|x_n| > \varepsilon_0 > 0$ para $n > N_0$, y en particular $x_n \neq 0$ para $n > N_0$. La sucesión $\{z_n\}_{n\in\mathbb{N}} = \{x_{n+N_0}\}_{n\in\mathbb{N}}$ es de Cauchy y $\{z_n\}_{n\in\mathbb{N}} \in \mathbf{x}$ por la propia definición de sucesión de Cauchy. La sucesión $\{z_n^{-1}\}_{n\in\mathbb{N}}$ es de Cauchy, efectivamente, sea $\varepsilon > 0$ fijado, como $\{z_n\}_{n\in\mathbb{N}}$ es de Cauchy, existe $M > 0$ tal que $|z_n - z_m| < \varepsilon_0^2\varepsilon$ para $n, m > M$, de modo que para tales $n, m > M$ se cumple:

$$|z_n^{-1} - z_m^{-1}| = \left|\frac{z_n - z_m}{z_n z_m}\right| = \frac{|z_n - z_m|}{|z_n||z_m|} \le \frac{\varepsilon_0^2\varepsilon}{\varepsilon_0^2} = \varepsilon,$$

y por lo tanto $\{z_n^{-1}\}_{n\in\mathbb{N}}$ es de Cauchy. Definimos entonces $\mathbf{x}^{-1} = [\{z_n^{-1}\}_{n\in\mathbb{N}}]$, que cumple $\mathbf{x}^{-1}\mathbf{x} = [\{z_n^{-1}\}_{n\in\mathbb{N}}][\{z_n\}_{n\in\mathbb{N}}] = \mathbf{1}$.

□

Observación 2.10. Se puede demostrar igual que en la proposición anterior que $\mathcal{C}_K$ tiene estructura de anillo y $\mathfrak{m} = \{\{x_n\}_{n\in\mathbb{N}} \,|\, |x_n| \to 0\}$ (llamado el conjunto de las *nilsucesiones* de K) es un ideal maximal de $\mathcal{C}_K$, con lo que $\hat{K} = \mathcal{C}_K/\mathfrak{m}$ es un cuerpo.

Lema 2.11. *Sea* $\mathbf{x} = [\{x_n\}_{n\in\mathbb{N}}] \in \hat{K}$. *La aplicación* $|\cdot|' : \mathbf{x} \mapsto \lim_n |x_n|$ *es un valor absoluto.*

Demostración. Por la desigualdad triangular, dichos límites son límites de sucesiones de Cauchy en $\mathbb{R}$ y por lo tanto existen. Además, la aplicación $|\cdot|'$ está bien definida, pues por la definición de la relación de equivalencia $\{x_n\}_{n\in\mathbb{N}} \sim \{y_n\}_{n\in\mathbb{N}}$, $\lim_n |x_n| = \lim_n |y_n|$. Si $\mathbf{x} = [\{x_n\}_{n\in\mathbb{N}}] \in \hat{K}$, es claro que $|\mathbf{x}|' \geq 0$ pues $|x_n| \geq 0$ para todo $n \in \mathbb{N}$, así como $|\mathbf{x}|' = 0 \iff \mathbf{x} = \mathbf{0}$. Si $\mathbf{x} = [\{x_n\}_{n\in\mathbb{N}}]$, $\mathbf{y} = [\{y_n\}_{n\in\mathbb{N}}] \in \hat{K}$, entonces:

$$|\mathbf{xy}|' = \lim_n |x_n y_n| = \lim_n |x_n||y_n| = \lim_n |x_n| \lim_n |y_n| = |\mathbf{x}|'|\mathbf{y}|'$$

$$|\mathbf{x}+\mathbf{y}|' = \lim_n |x_n + y_n| \leq \lim_n |x_n| + \lim_n |y_n| = |\mathbf{x}|' + |\mathbf{y}|'$$

□

Observación 2.12. El homomorfismo $i : K \to \hat{K}$ $x \mapsto [\{x\}_{n\in\mathbb{N}}]$ nos permite identificar K con $i(K) \subset \hat{K}$ (como cuerpo).

Lema 2.13. $\hat{K}$ *es un cuerpo completo, y* $K \subset \hat{K}$ *es denso.*

Demostración. Veamos que $\hat{K}$ es completo, sea $\{\mathbf{x}_n\}_{n\in\mathbb{N}}$ una sucesión de Cauchy en $\hat{K}$, para cada $n \in \mathbb{N}$ denotaremos $\mathbf{x}_n = [\{x_k^{(n)}\}_{k\in\mathbb{N}}]$.

Como $\{x_k^{(n)}\}_{k\in\mathbb{N}}$ es de Cauchy, existe $k_n \in \mathbb{N}$ tal que $|x_k^{(n)} - x_{k_n}^{(n)}| \leq 1/n$ para todo $k \geq k_n$, y por lo tanto $\lim_k |x_k^{(n)} - x_{k_n}^{(n)}| \leq 1/n$. Probemos que $\{z_n\}_{n\in\mathbb{N}} := \{x_{k_n}^{(n)}\}_{n\in\mathbb{N}}$ es de Cauchy. Sea pues $\varepsilon > 0$ fijado. Como la sucesión $\{\mathbf{x}_n\}_{n\in\mathbb{N}}$ es de Cauchy, existe $N_\varepsilon > 0$ tal que $|\mathbf{x}_n - \mathbf{x}_m|' = \lim_k |x_k^{(n)} - x_k^{(m)}| < \varepsilon/3$, para todo $n, m > N_\varepsilon$. Además sea $M_\varepsilon = \min\{n \in \mathbb{N} \,|\, 1/n \leq \varepsilon/3\}$.

Para $N_0 \geq \max\{N_\varepsilon, M_\varepsilon\}$ tenemos que si $n, m > N_0$ y $l > \max\{k_n, k_m\}$:

$$|x_{k_n}^{(n)} - x_{k_m}^{(m)}| \leq |x_{k_n}^{(n)} - x_l^{(n)}| + |x_l^{(n)} - x_l^{(m)}| + |x_l^{(m)} - x_{k_m}^{(m)}| < 1/n + \varepsilon/3 + 1/m \leq \varepsilon$$

como queríamos probar. Además, $\lim_n \mathbf{x}_n = [\{z_n\}_{n\in\mathbb{N}}]$, pues si fijamos un $\varepsilon > 0$ y $N = \min\{n \in \mathbb{N} \,|\, 1/n < \varepsilon/2\}$. Como $\{z_n\}_{n\in\mathbb{N}}$ es de Cauchy, existe un $M > 0$ tal que $|z_n - z_m| = |x_{k_n}^{(n)} - x_{k_m}^{(m)}| \leq \varepsilon/2$ para $n, m > M$ lo que implica que $\lim_l |x_{k_n}^{(n)} - x_{k_l}^{(l)}| \leq \varepsilon/2$. Con esto tenemos que para $n > \max\{N, M\}$:

$$|\mathbf{x}_n - [\{z_n\}_{n\in\mathbb{N}}]|' = \lim_l |x_l^{(n)} - x_{k_l}^{(l)}| \leq \lim_l |x_l^{(n)} - x_{k_n}^{(n)}| + \lim_l |x_{k_n}^{(n)} - x_{k_l}^{(l)}| \leq \varepsilon/2 + \varepsilon/2 = \varepsilon$$

Con esto probamos que toda sucesión de Cauchy en $\hat{K}$ converge a un elemento de $\hat{K}$, con lo que $\hat{K}$ es completo. Para ver que la inclusión $K \subset \hat{K}$ es densa basta ver que todo elemento de $\hat{K}$ es límite de una sucesión de elementos de K, pero esto es claro pues si $\mathbf{x}_n = [\{x_n\}_{n\in\mathbb{N}}]$ es un elemento de $\hat{K}$ es el límite de la sucesión $\{x_n\}_{n\in\mathbb{N}}$ de elementos de K. □

Observación 2.14. La prueba de la proposición anterior también implica que la aplicación i definida antes es continua (pues lleva sucesiones de Cauchy en K con sucesiones de Cauchy en $\hat{K}$) y un embebimiento topológico (pues lleva sucesiones de Cauchy en $i(K)$ en sucesiones de Cauchy en K).

Proposición 2.15. *Sea K un cuerpo con un valor absoluto $|\cdot|$ y $\hat{K}$ su completación. Todo homomorfismo de cuerpos topológicos $f : K \to L$ de K a un cuerpo completo para un valor absoluto $(L, |\cdot|'')$ puede extenderse de modo único a un homomorfismo de cuerpos topológicos $\hat{f} : \hat{K} \to L$. Además, si f es un embebimiento con imagen densa $\hat{f}$ es un isomorfismo y un homeomorfismo.*

Demostración. Como K es denso en $\hat{K}$ la función f puede extenderse de modo único a una aplicación continua $\hat{f} : \hat{K} \to L$ dada por $\hat{f}([\{x_n\}]) = \lim_n f(x_n)$, que está bien definida pues L es completo y f es continua (como $\hat{K}$ es completo es Cauchy-continua, con lo que $\{f(x_n)\}_{n\in\mathbb{N}}$ es de Cauchy). Tenemos que ver que esta aplicación es un homomorfismo de cuerpos, pero eso es inmediato pues f lo es:

$$\hat{f}([\{x_n\}_{n\in\mathbb{N}}][\{y_n\}_{n\in\mathbb{N}}]) = \lim_n f(x_n y_n) = \lim_n f(x_n)f(y_n) = \hat{f}([\{x_n\}_{n\in\mathbb{N}}])\hat{f}([\{y_n\}_{n\in\mathbb{N}}])$$

$$\hat{f}([\{x_n\}_{n\in\mathbb{N}}] + [\{y_n\}_{n\in\mathbb{N}}]) = \lim_n f(x_n + y_n) = \lim_n (f(x_n) + f(y_n)) = \hat{f}([\{x_n\}_{n\in\mathbb{N}}]) + \hat{f}([\{y_n\}_{n\in\mathbb{N}}])$$

Si f es un embebimiento topológico veamos que $\hat{f}$ es un embebimiento. Consideremos la restricción de rango $\bar{f} = \hat{K} \to \hat{f}(\hat{K})$, que es una aplicación biyectiva ya que $\hat{f}$ es un homomorfismo de cuerpos, de modo que tenemos que probar que $\bar{f}^{-1} : \hat{f}(\hat{K}) \to \hat{K}$ es continua. Sea $\{\hat{f}(\mathbf{x}_n)\}_{n\in\mathbb{N}}$ una sucesión de Cauchy en $\hat{f}(\hat{K})$. Denotando $\hat{f}(\mathbf{x}_n) = \lim_k f(x_k^{(n)})$, con $\{x_k^{(n)}\}_{k\in\mathbb{N}} \in \mathbf{x}_n$ para todo $n \in \mathbb{N}$ podemos construir, mediante un procedimiento diagonal como en el del lema 2.13 una sucesión $\{f(x_{k_n}^{(n)})\}_{n\in\mathbb{N}}$ tal que $\lim_n f(x_{k_n}^{(n)}) = \lim_n f(\mathbf{x}_n)$, veamos que $\{\mathbf{x}_n\}_{n\in\mathbb{N}}$ es de Cauchy. Sea $\varepsilon > 0$ fijado, como f es un embebimiento topológico, su restricción de rango g es un homeomorfismo y un isomorfismo, de modo que tanto g como su inversa son Cauchy-continuas (la inversa es un homomorfismo continuo, de modo que es uniformemente continua, y por tanto Cauchy-continua), por lo que $\{x_{k_n}^{(n)}\}_{n\in\mathbb{N}} = \{f^{-1}(f(x_{k_n}^{(n)}))\}$ es de Cauchy. Probemos que $\lim_n \mathbf{x}_n = [\{x_{k_n}^{(n)}\}_{n\in\mathbb{N}}]$, sea pues $\varepsilon > 0$ fijado. Como f^{-1} es Cauchy-continua para toda sucesión de Cauchy $\{x_n\}_{n\in\mathbb{N}}$ existe un $N_0 > 0$ tal que $|f^{-1}(x_n) - f^{-1}(x_m)|'' < \varepsilon$, para todo $n, m > N_0$. Sea entonces $\delta > 0$ tal que $\delta + 1/N_0 < \varepsilon$. Dado que $\{f(x_{k_n}^{(n)})\}_{n\in\mathbb{N}}$ es de Cauchy en L, existe un $M > 0$ tal que $|f(x_{k_n}^{(n)}) - f(x_{k_l}^{(l)})|' < \delta$, para todo $n, l > M$. Tomando $n > \max N, M$ se tiene que:

$$|f(x_l^{(n)}) - f(x_{k_l}^{(l)})|' \leq |f(x_l^{(n)}) - f(x_{k_n}^{(n)})|' + |f(x_{k_n}^{(n)}) - f(x_{k_l}^{(l)})|' \leq \frac{1}{N_0} + \delta \leq \varepsilon \quad , \forall l > k_n$$

por construcción de la sucesión $\{f(x_{k_n}^{(n)})\}_{n\in\mathbb{N}}$. De este modo, para dicho n y $l > k_n$ se cumple:

$$|x_l^{(n)} - x_{k_l}^{(l)}| = |f^{-1}(f(x_l^{(n)})) - f^{-1}(f(x_{k_l}^{(l)}))| < \varepsilon$$

de modo que $|\mathbf{x}_n - [\{x_{k_l}^{(l)}\}_{n\in\mathbb{N}}]|' = \lim_l |x_l^{(n)} - x_{k_l}^{(l)}| \leq \varepsilon$, como se quería probar. De este modo tenemos que $\bar{f}^{-1}$ es continua, y por tanto un homeomorfismo e isomorfismo $\hat{K} \cong \bar{f}(\hat{K}) = \hat{f}(\hat{K})$, de modo que $\hat{f}(\hat{K})$ es completo. Esto implica que $\hat{f}(\hat{K})$ es un cerrado denso en L (pues $f(K) \subset \hat{f}(\hat{K}) \subset L$), de modo que $\hat{f}(\hat{K}) = L$. Así $\hat{f}$ es sobreyectiva, y por tanto, un homeomorfismo y un isomorfismo. □

Observación 2.16. La proposición anterior implica que una completación de un cuerpo es única salvo isomorfismo topológico, y que si un cuerpo completo L para un valor absoluto contiene a un cuerpo K, contiene también a su completación $\hat{K}$. Esto en particular implica que la completación de un cuerpo completo es idéntica al propio cuerpo.

La demostración de la proposición 2.8 está entonces terminada. □

Proposición 2.17. *Sea K un cuerpo con una valoración discreta v. Entonces para $a \in (0,1)$ la aplicación $x \mapsto |x|_{v,a} = a^{v(x)}$ es un valor absoluto no arquimediano sobre K.*

Demostración. Las propiedades $|x|_{v,a} \geq 0$ y la multiplicatividad son inmediatas. La propiedad $|x|_{v,a} = 0 \iff x = 0$ se sigue de que $v(0) = \infty$ para toda valoración discreta (tal y como se vio en la proposición 1.3) y para la aditividad basta con comprobar que:

$$|x+y|_{v,a} = a^{v(x+y)} \leq a^{\text{ínf}\{v(x),v(y)\}} = \sup\{a^{v(x)}, a^{v(y)}\} = \sup\{|x|_{v,a}, |y|_{v,a}\}$$

□

Observación 2.18. La topología de K como espacio métrico no depende del valor de a escogido, en efecto, si $a, b \in (0,1)$, entonces $|x|_{v,a} = b^{\log_b(a)v(x)} = |x|_{v,b}^{\log_b(a)}$, y dado que $\log_b(a) > 0$, $|\cdot|_{v,a}$ y $|\cdot|_{v,b}$ son equivalentes. Esto en particular implica que inducen la misma completación de K, y por tanto justifica que en resto del trabajo omitamos cuando sea posible la dependencia en $a \in (0,1)$ al referirnos a los valores absolutos inducidos por una valoración discreta v y escribamos solamente $|\cdot|_v$.

Proposición 2.19. *Sea K un cuerpo con una valoración discreta v. Entonces la completación de K con respecto a $|\cdot|_v$ admite una valoración discreta que extiende v.*

Demostración. Por el lema 2.11, para $a \in (0,1)$, el valor absoluto de la completación de K es:

$$|\,[\{x_n\}_{n\in\mathbb{N}}]\,|' = \lim_n |x|_{v,a} = \lim_n a^{v(x_n)} = a^{\lim_n v(x_n)}$$

Al ser $\{v(x_n)\}_{n\in\mathbb{N}}$ una sucesión de números enteros, la existencia de $a^{\lim_n v(x_n)}$ implica que $\lim_n v(x_n)$ existe. De este modo tiene sentido definir para $\mathbf{x} = [\{x_n\}_{n\in\mathbb{N}}] \in \hat{K}$ $\hat{v}(\mathbf{x}) = \lim_n v(x_n)$, que naturalmente coincide con v para $x \in K$. □

Proposición 2.20. *Sea K un cuerpo con una valoración discreta v y $\hat{K}$ su completación. Si denotamos como A, $\hat{A}$ los anillos de valoración de K y $\hat{K}$ y π es un uniformizante de A, entonces $A/\pi^n A$ y $\hat{A}/\pi^n\hat{A}$ son isomorfos como anillos topológicos.*

Demostración. La aplicación $\varphi_n : A \to \hat{A}/\pi^n\hat{A}$ dada por $x \mapsto x \mod \pi^n\hat{A}$ es un homomorfismo de anillos, dado que se trata de la composición $A \hookrightarrow \hat{A} \to \hat{A}/\pi^n\hat{A}$, cuyo núcleo es $\ker(\varphi_n) = A \cap \pi^n\hat{A} = \pi^n A$. La inclusión hacia la izquierda es inmediata, y para la inclusión hacia la derecha sea $x \in A \cap \pi^n\hat{A}$. Como la valoración de $\hat{A}$ extiende la de A por la proposición 2.19, tenemos que $v(x) = \hat{v}(x) \geq n$, pues $x \in \pi^n\hat{A}$ ($\hat{v}$ denota la extensión de la valoración discreta v a la completación), de modo que $x \in \pi^n A$. Además φ_n es sobreyectiva pues, para $a \in (0,1)$ y $x \in \hat{A}$ fijados, como $\hat{A} \subset \hat{K}$ es cerrado, $\hat{A}$ es completo, y como $A \subset \hat{A}$ es denso (dado que $A = B_K[0,1]$, la clausura de A en $\hat{K}$, $\overline{A}^{\hat{K}} = \overline{B_K[0,1]}^{\hat{K}} = B_{\hat{K}}[0,1] = \hat{A}$), existe un $y \in A$ tal que $|x-y|_{v,a} \leq a^{-n}$, o equivalentemente, $x + \pi^n\hat{A} = y + \pi^n\hat{A}$, como queríamos probar. Por el primer teorema de isomorfía tenemos el isomorfismo $A/\pi^n A \simeq \hat{A}/\pi^n\hat{A}$ que es también un homeomorfismo al ser una aplicación biyectiva entre espacios discretos. [1] □

Proposición 2.21. *Sea K un cuerpo con una valoración v, A su anillo de valoración, π un uniformizante de A y $\mathcal{S} \subset A$ un conjunto de representantes de $\kappa = A/\pi A$ conteniendo a 0. La sucesión de sumas parciales $\{s_k\}_{k\in\mathbb{N}} = \{\sum_{i=n}^{k} a_i\pi^i\}_{k\in\mathbb{N}}$, con $n \in \mathbb{Z}$ y $a_i \in \mathcal{S}$ para todo $i \geq n$, es de Cauchy, y toda sucesión de Cauchy en K es equivalente a una única sucesión de ese tipo.*

Demostración. Sea la sucesión de sumas parciales $s_k = a_n\pi^n + \cdots + a_k\pi^k$, con $n \in \mathbb{Z}$ fijado y $k \in \mathbb{N}$. Tomando $a \in (0,1)$ y $\varepsilon > 0$, sean además $k > l > \text{mín}\{n \in \mathbb{N} \,|\, a^n < \varepsilon\}$. Podemos suponer sin pérdida de generalidad que $a_l \neq 0$ (si no fuese posible, la sucesión sería constante a partir de un índice y por tanto de Cauchy), de modo que obtenemos:

$$|s_k - s_l|_{v,a} = |a_l\pi^l + \cdots + a_k\pi^k|_{v,a} \leq \text{ínf}\{|a_i\pi^i|_{v,a}, i = l \ldots k\} = |a_l\pi^l|_{v,a} = a^{-l} < \varepsilon,$$

donde hemos usado que $v(a_l) = 0$ (ya que $0 \neq a_l \notin \pi A$ por la propia definición de $\mathcal{S}$). Sea ahora $x \in \hat{K}$, que podemos expresar $x = x_0\pi^n$, con $n \in \mathbb{Z}$ y $x_0 \in \hat{A}$ (ya que π es un uniformizante de $\hat{A}$). Por definición de $\mathcal{S}$ existe un único $a_0 \in \mathcal{S}$ tal que $x_0 - a_0 \in \pi\hat{A}$ (como $A/\pi A \simeq \hat{A}/\pi\hat{A}$ por la proposición anterior $\mathcal{S}$ es un conjunto de representantes de $\hat{A}/\pi\hat{A}$). De este modo $x_1 = \pi^{-1}(x_0 - a_0) \in \hat{A}$ y por tanto existe un $a_1 \in \mathcal{S}$ tal que $x_1 - a_1 \in \pi\hat{A}$. Inductivamente construimos la sucesión $\pi^n(a_0 + a_1\pi + a_2\pi^2 + \ldots)$, que es de Cauchy y converge a x por construcción. Para comprobar la unicidad veamos que si $a_n\pi^n + a_{n+1}\pi^{n+1} + \cdots = 0$, entonces $a_i = 0$, para todo $i \geq n \in \mathbb{Z}$ (recordemos que $0 \in \mathcal{S}$). En efecto, supongamos que una serie no nula cumpliese $a_n\pi^n + a_{n+1}\pi^{n+1} + \cdots = 0$ con $n \in \mathbb{Z}$ y $a_n \neq 0$, entonces para $c \in (0,1)$ fijado:

$$|a_n\pi^n + a_{n+1}\pi^{n+1} + \ldots|_{v,c} = \text{ínf}\{|a_i\pi^i|_{v,c}, i \geq n\} = |a_n\pi^n|_{v,c} = |\pi^n|_{v,c} \neq |0|_{v,c}$$

lo cual es una contradicción. Esto implica la unicidad de la representación pues si dos series $\mathbf{x} = a_n\pi^n + a_{n+1}\pi^{n+1} + \ldots$ e $\mathbf{y} = b_n\pi^n + b_{n+1}\pi^{n+1} + \ldots$, con $n \in \mathbb{Z}$ fuesen equivalentes y distintas, tomando $m = \text{mín}\{k \in \mathbb{N} \,|\, a_k \neq b_k\}$, entonces $\hat{v}(\mathbf{x} - \mathbf{y}) = \hat{v}(c_m\pi^m + c_{m+1}\pi^{m+1} + \ldots) = m$

[1] Dado que el conjunto $\pi^n A$ (y por tanto $x + \pi^n A$ para todo $x \in A$) es un abierto en A, el espacio $A/\pi^n A$ es un espacio discreto, ya que la proyección canónica $A \to A/\pi^n A$ es una aplicación abierta al ser una aplicación de paso al cociente. El mismo argumento se aplica para probar que $\hat{A}/\pi^n\hat{A}$ es un espacio discreto.

por definición de m, siendo para cada $k \geq m$, c_k el representante de $a_k - b_k \mod \pi A$ en $\mathcal{S}$, contradiciendo que $\mathbf{x} - \mathbf{y} = 0$. □

Observación 2.22. La proposición anterior hace coherente la notación alternativa $\mathbf{x} = a_n\pi^n + a_{n+1}\pi^{n+1} + \ldots$, con $n \in \mathbb{Z}$ para un elemento $\mathbf{x} \in \hat{K}$, fijado un conjunto de representantes en A del cuerpo residual de A. Otra consideración interesante es que para todo elemento $\pi_m \in A$ tal que $v(\pi_m) = m$ se cumple que $\pi_m A = \pi^m A$, de modo que en la demostración anterior podemos sustituir todas las apariciones de π^m, con $m \in \mathbb{Z}$, por un elemento $\pi_m \in K$ tal que $v(\pi_m) = m$.

Corolario 2.23. *Sea K un cuerpo con una valoración discreta v y A su anillo de valoración. Toda sucesión de Cauchy $\{x_n\}_{n\in\mathbb{N}}$ de elementos de A se estabiliza en $A/\pi^n A$ para todo $n \in \mathbb{N}$.*

Definición 2.24. Sea I un conjunto dirigido inferiormente (es decir con un *preorden* $\leq$, que cumple la propiedad reflexiva y transitiva; y dados $i, j \in I$ existe un elemento $k \in I$ tal que $k \leq i$ y $k \leq j$), $\{X_i\}_{i\in I}$ una familia de espacios topológicos y $\{f_{ij}\}_{\substack{i,j\in I\\ i\leq j}}$ un conjunto de aplicaciones continuas que cumplen que $f_{ij} : X_j \to X_i$ y $f_{ij} \circ f_{jk} = f_{ik}$, para todo $i, j, k \in I$ que satisfagan $i \leq j \leq k$. El par $(\{X_i\}_{i\in I}, \{f_{ij}\}_{\substack{i,j\in I\\ i\leq j}})$ se denomina *sistema inverso de espacios topológicos*. Se define el *límite inverso* de un sistema inverso de espacios topológicos $(\{X_i\}_{i\in I}, \{f_{ij}\}_{\substack{i,j\in I\\ i\leq j}})$ como:

$$\varprojlim_{i\in I} X_i = \bigcap_{i\leq j} \{(x_i)_{i\in I} \in \prod_{i\in I} X_i \,|\, x_i = f_{ij}(x_j)\} \subset \prod_{i\in I} X_i$$

dotado de la topología inducida por la topología producto.

Observación 2.25. La construcción del límite inverso también existe en sistemas inversos de anillos (donde X_i es un anillo para todo $i \in I$ y f_{ij} son homomorfismos para todo $i \geq j$). El límite inverso de un sistema inverso de espacios topológicos (resp. anillos) $(\{X_i\}_{i\in I}, \{f_{ij}\}_{\substack{i,j\in I\\ i\leq j}})$ satisface la siguiente propiedad universal. Para todo sistema inverso de espacios topológicos (resp. de anillos), si existe un espacio topológico (resp. anillo) Y y un conjunto de aplicaciones de $\psi_i : Y \to X_i$ tales que $\psi_i = f_{ij} \circ \psi_j$ para todo $i \leq j$ (se dice que las aplicaciones ψ_i son *compatibles* con el sistema inverso $(\{X_i\}_{i\in I}, \{f_{ij}\}_{\substack{i,j\in I\\ i\leq j}})$), entonces existe una única función continua (resp. homomorfismo) $\psi : Y \to \varprojlim_{i\in I} X_i$ tal que $\psi_i = \psi \circ \pi_i$, donde π_i es la restricción de la proyección canónica a $\varprojlim_{i\in I} X_i$.

Corolario 2.26. *Sea K un cuerpo con una valoración discreta v y A su anillo de valoración. Entonces el anillo de valoración $\hat{A}$ de $\hat{K}$ es isomorfo y homeomorfo a la completación π-ádica de A (en el sentido de [AM, cap. 10]), donde π es un uniformizante de A.*

Demostración. Para cada $n \in \mathbb{N} - \{0\}$ se define el homomorfismo sobreyectivo $\varphi_n : \hat{A} \to A/\pi^n A$ como $[\{x_k\}_{k\in\mathbb{N}}] \mapsto \lim_k(x_k + \pi^n A)$. φ_n, que está bien definida por el corolario anterior, y cumple que $\ker\varphi_n = \pi^n\hat{A}$.[2] Además es compatible con las proyecciones canónicas $\pi_{nm} : A/\pi^m A \to A/\pi^n A$, para $m \geq n$.

[2]La inclusión hacia la izquierda es inmediata, para la inclusión hacia la derecha basta con ver que si $\varphi_n(a_0 + a_1\pi + a_2\pi^2 + \ldots) = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \mod \pi^n = 0$, entonces $a_0 = \cdots = a_{n-1} = 0$

Por la propiedad universal del límite inverso, esto induce el homomorfismo $\varphi : \hat{A} \to \varprojlim_n A/\pi^n A$ definido como $[\{x_k\}_{k\in\mathbb{N}}] \mapsto (\varphi_n([\{x_k\}_{k\in\mathbb{N}}]))_{n\in\mathbb{N}}$, que es inyectivo pues $\ker\varphi = \bigcap_n \varphi_n = \bigcap_n \pi^n\hat{A} = 0$ y además es sobreyectivo. Para probar esto último sea $x = (x_0 \mod \pi, x_1 \mod \pi^2, \dots, x_n \mod \pi^{n+1}, \dots) \in \varprojlim_n A/\pi^n A$. Por la definición de límite inverso podemos construir una sucesión de Cauchy $\mathbf{x} = a_0 + a_1\pi + a_2\pi^2 + \cdots \in \hat{A}$, con $n \in \mathbb{N}$ y $a_i \in A$ para todo $i \geq 0$ tal que $x = \varphi(\mathbf{x})$. Efectivamente, como $x_1 \equiv x_0 \mod \pi$ existe un $a_1 \in A$ tal que $x_1 = x_0 + a_1\pi$, y como $x_2 \equiv x_1 \mod \pi^2$ existe un $a_2 \in A$ tal que $x_2 = x_1 + a_2\pi^2 = x_0 + a_1\pi + a_2\pi^2$. De modo general, para $n > 1$ se cumple que $x_{n+1} \equiv x_n \mod \pi^{n+1}$, con lo que existe un $a_{n+1} \in A$ tal que $x_{n+1} = x_n + a_{n+1}\pi^{n+1} = x_0 + a_1\pi + \cdots + a_{n+1}\pi^{n+1}$. Inductivamente podemos construir una sucesión de Cauchy $\mathbf{x} = x_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \dots$ que cumple por construcción que $x = \varphi(\mathbf{x})$.

Para ver que es un homeomorfismo veremos que φ lleva una base de la topología de $\hat{A}$ en una base de la topología de la completación $\pi-$ádica, pero por un argumento de homogeneidad podemos restringirnos a una base de abiertos de 0. Por construcción de la completación $\pi-$ádica de A, la familia $\{P_n \cap \varprojlim_k A/\pi^k A\}_{n\in\mathbb{N}-\{0\}}$ (donde $P_n = \psi_1^{-1}(0) \cap \cdots \cap \psi_n^{-1}(0)$, siendo $\psi_k : \prod_n A/\pi^n A \to A/\pi^k A$ la $k-$ésima proyección canónica) es una base de entornos abiertos de 0 en $\varprojlim_k A/\pi^k A$. De este modo si probamos que $\varphi(\pi^n\hat{A}) = P_n \cap \varprojlim_k A/\pi^k A$ para todo $n \in \mathbb{N} - \{0\}$ habremos terminado (pues para $a \in (0,1)$, $\{\pi^k\hat{A}\}_{k\geq 0} = \{B(0, a^{-k})\}_{k\geq 0}$ es una base de abiertos de 0 en $\hat{A}$ por la proposición 2.7). Para la inclusión hacia la derecha basta con ver que si $\mathbf{x} \in \pi^n\hat{A}$, entonces $\varphi(\mathbf{x}) = \varphi(a_n\pi^n + a_{n+1}\pi^{n+1} + \dots) = (0, \dots, 0, a_n\pi^n \mod \pi^{n+1}, a_n\pi^n + a_{n+1}\pi^{n+1} \mod \pi^{n+2}, \dots) \in P_n \cap \varprojlim_k A/\pi^k A$, mientras que para la inclusión hacia la izquierda, si $x = (0, \dots, 0, x_{n+1} \mod \pi^{n+1}, x_{n+2} \mod \pi^{n+2}, \dots) \in P_n \cap \varprojlim_k A/\pi^k A$, entonces por un razonamiento idéntico al que usamos antes para probar que la aplicación φ es sobreyectiva, existe un elemento $\mathbf{x} = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n + \cdots \in \hat{A}$, que cumple por construcción que $\varphi(\mathbf{x}) = x$. No obstante, dado que $x_n \equiv 0 \mod \pi^n$, se cumple que $a_0 = a_1 = \cdots = a_{n-1} = 0$, con lo que $\mathbf{x} \in \pi\hat{A}^n$. Esto prueba que φ es un homeomorfismo. □

Observación 2.27. Esto implica que para todo cuerpo K con una valoración discreta v y uniformizante π, tomar la completación topológica de K por el valor absoluto inducido por la valoración v es equivalente a tomar el cuerpo de fracciones de la completación $\pi-$ádica de su anillo de valoración.

2.2. Extensiones de un AVD completo. Cuerpos locales

Lema 2.28. *Sea $\{X_i, f_{ij}\}_{i\in I, j\geq i}$ un sistema inverso de espacios topológicos Hausdorff. Entonces $\varprojlim_i X_i$ es un cerrado de $\prod_i X_i$, y si además X_i es compacto para todo $i \in I$, $\varprojlim_i X_i$ es compacto.*

Demostración. Por la definición de límite inverso:

$$\varprojlim_{i\in I} X_i = \bigcap_{i\leq j} \{(x_i)_{i\in I} \in \prod_{i\in I} X_i | x_i = f_{ij}(x_j)\} = \bigcap_{i\leq j} (\mathrm{id}_{\prod_{i\in I} X_i} \times f_{ij})^{-1}(\Delta_i)$$

donde Δ_i es la diagonal de $X_i \times X_i$. Como f_{ij} es continua para todo $i \leq j$ y Δ_i es un cerrado en $X_i \times X_i$, ya que X_i es Hausdorff, se sigue que $\varprojlim_i X_i$ es cerrado. Si además X_i es compacto para

todo $i \in I$, el producto $\prod_i X_i$ es compacto por el teorema de Tychonov, de modo que $\varprojlim_{i\in I} X_i$ es compacto al ser cerrado en $\prod_i X_i$. □

Teorema 2.29. *Sea K un cuerpo con una valoración discreta v, A su anillo de valoración y π un uniformizante. K es localmente compacto si y solo si K es completo y su cuerpo residual $A/\pi A$ es finito.*

Demostración. Por un lado, si K es localmente compacto es completo. En efecto, si K es localmente compacto, entonces $K \subset \hat{K}$ es abierto en $\hat{K}$, y por lo tanto cerrado, al ser un subgrupo, de modo que K es completo al ser un subconjunto cerrado de un espacio completo. Veamos que es un abierto. Sea $x \in K$, como K es localmente compacto existe un entorno de x relativo a K, V, cuya clausura $\bar{V}$ en K es compacta. Sea U un entorno de x en $\hat{K}$ tal que $V = U \cap \hat{K}$. Como $\bar{V}$ es compacto y $\hat{K}$ es Hausdorff (es un espacio métrico), $\bar{V}$ es cerrado en $\hat{K}$, y por tanto $U - \bar{V}$ es abierto en $\hat{K}$. Pero $U - \hat{V}$ no interseca a K (pues como $U \cap K = V \subset \bar{V}$, $\varnothing = (U \cap K) - \bar{V} = K \cap (U - \bar{V})$) y K es un subconjunto denso de $\hat{K}$, $U - V = \varnothing$ y por tanto $x \in U \subset \bar{V} \subset K$. De modo que para todo punto $x \in K$ existe un entorno abierto de x en $\hat{K}$ contenido en K, de modo que K es abierto en $\hat{K}$.

Además, como $\{\pi^n A\}_{n\in\mathbb{Z}}$ es un sistema de entornos cerrados de 0, al menos uno de ellos va a ser compacto (pues si U es un entorno abierto con clausura $\bar{U}$ compacta existe un $n \in \mathbb{Z}$ tal que $\pi^n A \subset U \subset \bar{U}$). Sea $\pi^n A$ con $n \in \mathbb{Z}$, un entorno que cumple la propiedad anterior. Dado que $A = \pi^{-n}(\pi^n A)$, A es compacto, por lo que $A/\pi A$ es compacto y por tanto finito, al ser un espacio discreto.

Por otro lado, si $A/\pi A$ es finito entonces $A/\pi^n A$ es finito para todo $n \in \mathbb{N}$. En efecto, aplicando inducción en n, el caso $n = 1$ se cumple por hipótesis, y suponiendo que la propiedad se cumple para el caso $n-1$, dada la sucesión exacta $0 \to \pi^{n-1}A/\pi^n A \to A/\pi^n A \to A/\pi^{n-1} \to 0$, se deduce que $(A/\pi^n A)$ es finito pues $(A/\pi^n A)/(\pi^{n-1}A/\pi^n A) \simeq A/\pi^{n-1}A$ y $\pi^{n-1}A/\pi^n A$ es finito, dado que es isomorfo a $A/\pi A$, como se vio en la demostración del lema 1.47. Luego $\hat{A}$ es el límite proyectivo de espacios finitos (y por tanto compactos), y por esta razón es compacto por el lema 2.28. Si K es completo, entonces $K = \hat{K}$ y así, $A = \hat{A}$, con lo que $\{\pi^n A\}_{n\in\mathbb{Z}}$ forma una base de entornos compactos del origen, y consecuentemente K es localmente compacto (el sistema de entornos de cero se puede trasladar homeomórficamente a una base de entornos compactos de cualquier punto de K). □

Definición 2.30 (Cuerpo local)**.** Un cuerpo K completo para una valoración discreta v se dice *local* si es localmente compacto (es decir, su cuerpo residual es finito).

Observación 2.31. Si K es un cuerpo local para una valoración discreta v con anillo de valoración A de uniformizante π y cuerpo residual κ, tenemos una elección natural de tomar el valor $a \in (0,1)$ dado en la proposición 1.1, $a = (\#\kappa)^{-1}$. Dichos valores absolutos se denominan *normalizados*, y poseen propiedades analíticas deseables (relacionadas con la medida de Haar de K).

Ejemplo 2.32. El anillo $\mathbb{Z}$ es el ejemplo típico de dominio de Dedekind: sus ideales maximales son los generados por los números primos. De modo que para cada primo p tenemos la aplicación que lleva a cada entero n al exponente de p en su descomposición en primos, que induce una valoración $v_p : \mathbb{Q} \to \mathbb{Z}$ cuyo anillo de valoración es $\mathbb{Z}_{(p)}$. Dicha valoración induce un valor absoluto $|\cdot|_{v_p} : \mathbb{Q} \to \mathbb{R}$. La completación de $\mathbb{Q}$ con respecto a este valor absoluto se denomina el cuerpo de los números p-ádicos, $\mathbb{Q}_p$, que es el cuerpo de fracciones del anillo de los números p-ádicos $\mathbb{Z}_p$. Como el cuerpo residual de $\mathbb{Q}_p$ con respecto a la valoración v_p es finito (pues $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$ es finito), $\mathbb{Q}_p$ es un cuerpo local. Definimos entonces el valor absoluto $p-$ádico sobre $\mathbb{Q}_p$ como el valor absoluto normalizado inducido por v_p que naturalmente, restringido a $x \in \mathbb{Q}$ tiene la forma $|x|_p = p^{-v_p(x)}$. Es claro que $|\cdot|_p$ es un valor absoluto discreto no arquimediano, y en el caso de $\mathbb{Q}$ también se da el recíproco:

Teorema 2.33 (Ostrowski)**.** *Todo valor absoluto definido no trivial sobre $\mathbb{Q}$ es equivalente a algún $|\cdot|_p$, para algún primo p o al valor absoluto usual.*

Demostración. Sea $|\cdot|$ un valor absoluto definido sobre $\mathbb{Q}$. Si $|\cdot|$ es no arquimediano, entonces sean $A = \{x \in \mathbb{Q} \,|\, |x| \leq 1\}$ y $\mathfrak{m} = \{x \in \mathbb{Q} \,|\, |x| < 1\}$ (que son un subanillo local de $\mathbb{Q}$ y su ideal maximal respectivamente, por la observación 2.6), de modo que $\mathfrak{p} = \mathbb{Z} \cap \mathfrak{m}$ es un ideal primo de $\mathbb{Z}$. El ideal $\mathfrak{p}$ es no nulo pues de serlo, por definición de A, se cumpliría que $|x| = 1$ para todo $x \in \mathbb{Q}^*$ (ya que todo elemento de $\mathbb{Q}$ es de la forma a/b, con $a, b \in \mathbb{Z}$, $b \neq 0$), lo cual contradice que $|\cdot|$ es no trivial; de este modo $\mathfrak{p} = p\mathbb{Z}$ para algún primo $p \in \mathbb{Z}$. Si $x = a/b \in \mathbb{Q}^*$, entonces se expresa de modo único como $x = p^k c/d$, con $k \in \mathbb{Z}$ y $c, d \in \mathbb{Z}$ cumpliendo $(p, cd) = 1$ (donde en este caso, $(\cdot,\cdot)$ representa el máximo común divisor), por lo que:

$$|x| = |p^k||c/d| = |p^k||c|/|d| = |p^k| = |p|^k = p^{-ks} = |x|_p^s$$

donde $s = -\log_p(|p|) > 0$ (pues $p \in \mathfrak{m}$). De este modo $|\cdot|$ es equivalente a $|\cdot|_p$. Si $|\cdot|$ es arquimediano, entonces para todo par de números enteros positivos n, m se cumple $|m|^{-\log(m)} = |n|^{-\log(n)}$. En efecto, m admite una expresión única de la forma $m = b_0 + b_1 n + \cdots + b_r n^r$, donde $r \in \mathbb{N}$, $b_i \in \{0, 1, \ldots, n-1\}$ para todo $i \in \{0, \ldots, r\}$ y $n^r \leq m$. Así, $\log_n(m) \geq r$ y $|b_i| = |\overbrace{1 + \cdots + 1}^{b_i}| \leq b_i|1| = b_i < n$ para todo $i \in \{0, \ldots, r\}$. De este modo obtenemos la siguiente cadena de desigualdades:

$$|m| \leq \sum_{i=0}^{r} |b_i||n|^i \leq \sum_{i=0}^{r} |b_i||n|^i \leq \sum_{i=0}^{r} |b_i||n|^r \leq (1+r)n|n|^r \leq (1+\log_n(m))\, n|n|^{\log_n(m)},$$

donde para la tercera desigualdad se usó que $|\cdot|$ es arquimediano. En efecto, por la multiplicatividad del valor absoluto basta demostrar que $|n| \geq 1$ para todo $n > 1$, pero es inmediato comprobar que si $|n| < 1$, entonces $|n+1| \leq 1$. Inductivamente se tendría que la sucesión $\{n, n+1, n+2, \ldots\}$ es acotada, violando que $|\cdot|$ es un valor absoluto arquimediano por la proposición 2.3. En consecuencia para todo $k \in \mathbb{Z}$ se cumple $|m|^k = |m^k| \leq (1 + k\log_n(m))n|n|^{k\log_n(m)}$, y por tanto $|m| \leq (1 + k\log_n(m))^{1/k} n^{1/k} |n|^{\log_n(m)}$. Tomando entonces el límite en k obtenemos

$|m| \leq |n|^{\log_n(m)}$, y por tanto $|n|^{1/\log(n)} = |m|^{1/\log(m)}$, como queríamos probar. De este modo, existe una constante real $c > 1$ tal que $|n| = c^{\log n}$ para todo entero positivo n. Dado que $|-1| = 1$ (Pues $|-1|^2 = |1| = 1$ y la ecuación $X^2 = 1$ solo tiene a 1 como raíz positiva en $\mathbb{R}$), podemos extender el resultado anterior a $|n| = c^{\log|n|_\infty}$ para todo entero n, siendo $|\cdot|_\infty$ el valor absoluto usual de $\mathbb{Q}$. Así, para $x = a/b \in \mathbb{Q}$:

$$|x| = |a|/|b| = c^{\log\left|\frac{a}{b}\right|_\infty} = e^{s\log\left|\frac{a}{b}\right|_\infty} = \left|\frac{a}{b}\right|_\infty^s,$$

siendo $s = \log c > 0$. De este modo $|\cdot|$ y $|\cdot|_\infty$ son equivalentes, como queríamos probar. □

Ejemplo 2.34. Sea $\mathbb{F}_p$ el cuerpo finito de p elementos. El anillo de polinomios $\mathbb{F}_p[X]$ es un dominio de Dedekind (efectivamente es dominio de ideales principales). Si f es un polinomio irreducible de $\mathbb{F}_p[X]$, va a inducir, del mismo modo que estudiamos en el ejemplo anterior, una valoración $v_f : \mathbb{F}_p(X) \to \mathbb{Z}$ y un valor absoluto $|\cdot|_{v_f} : \mathbb{F}_p(X) \to \mathbb{R}$, cuyo cuerpo residual es $\mathbb{F}_p[X]/(f)$, una extensión finita de $\mathbb{F}_p$ y por lo tanto isomorfa a $\mathbb{F}_q$ con $q = p^n$ para algún $n \geq 1$. La completación de $\mathbb{F}_q(X)$ con respecto a la valoración v_f, como se verá en el corolario 2.42, es isomorfa al cuerpo de las series de Laurent con coeficientes en $\mathbb{F}_q$, denotado como $\mathbb{F}_q((X)) := \{\sum_{k\geq n} a_k X^k | n \in \mathbb{Z}, a_k \in \mathbb{F}_q, \forall k \geq n\}$. Dado que su cuerpo residual con respecto a la valoración v_f coincide con $\mathbb{F}_q$, $\mathbb{F}_q((X))$ es un cuerpo local. Consideremos entonces el valor absoluto normalizado equivalente a $|\cdot|_{v_f}$, que denotaremos como $|\cdot|_f$.

A mayores sobre $\mathbb{F}_p(X)$ podemos definir un valor absoluto más, inducido por la valoración discreta $v_\infty : f/g \mapsto \deg g - \deg f$, con anillo de valoración $\mathbb{F}_p^{pol} = \{f/g \in \mathbb{F}_p(X) | \deg g \geq \deg f\}$, con ideal primo $\mathfrak{p}^{pol} = \{f/g \in \mathbb{F}_p(X) | \deg g > \deg f\}$ y uniformizante X^{-1}. Probaremos que $\mathbb{F}_p^{pol}[X]/\mathfrak{p}^{pol} \simeq \mathbb{F}_p$, sea pues $f/g \in \mathbb{F}_p^{pol}(X)$. Podemos suponer sin pérdida de generalidad, multiplicando numerador y denominador por un elemento de $\mathbb{F}_p$, que el coeficiente principal de g es uno, de modo que, si $f(X) = a_0 + a_1X + \cdots + a_nX^n$ (a_n puede valer cero), y $g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + X^n$, tenemos que, reordenando términos, f/g puede expresarse de la forma:

$$a_n - a_n\frac{b_{n-1}X^{n-1} + \cdots + b_1X + b_0}{X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0} + \frac{a_{n-1}X^{n-1} + \cdots + a_0}{X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0} \equiv a_n \mod \mathfrak{p}^{pol}$$

con lo que la aplicación $f/g \mod \mathfrak{p}^{pol} \mapsto a_n$ es un isomorfismo de $\mathbb{F}_p^{pol}$ a $\mathbb{F}_p$. Así, la completación de $\mathbb{F}_p(X)$ con respecto a v_∞ es un cuerpo local, cuyo valor absoluto normalizado denotaremos como $|x|_\infty = p^{-v_\infty(x)}$. Al igual que el ejemplo anterior, tenemos un teorema de clasificación de los valores absolutos en $\mathbb{F}_p(X)$:

Teorema 2.35. *Todo valor absoluto no trivial sobre $\mathbb{F}_p(X)$ es equivalente a $|\cdot|_f$ para algún polinomio irreducible $f \in \mathbb{F}_p[X]$ o a $|\cdot|_\infty$*

Demostración. Sea $|\cdot|$ un valor absoluto definido sobre $\mathbb{F}_p(X)$. Dado que todos los valores absolutos sobre un cuerpo finito son triviales (por la observación 2.2), entonces $|n| = 1$ para todo $n \in \mathbb{N} - \{0\}$, de modo que el valor absoluto $|\cdot|$ es no arquimediano por la proposición 2.3. Sea $A = \{f \in \mathbb{F}_p(X) \,|\, |f| \leq 1\}$ el anillo de $|\cdot|$ y $\mathfrak{m} = \{f \in \mathbb{F}_p(X) \,|\, |f| < 1\}$ su ideal maximal.

Supongamos que $|X| \leq 1$. Dado que el conjunto $\mathfrak{m} \cap \mathbb{F}_p[X]$ contiene un polinomio no constante (si no lo hiciese, entonces para todo $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{F}_p[X]$, $1 \leq |f| \leq$ máx$\{|a_0|, |a_1||X|, \ldots, |a_n||X|^n\} =$ máx$\{1, |X|, \ldots, |X|^n\} = 1$, por lo que $|f/g| = 1$ para todo $f/g \in \mathbb{F}_p(X)^*$, contradiciendo que $|\cdot|$ es no trivial), de modo que, como $\mathfrak{m} \cap \mathbb{F}_p[X]$ es primo (pues $\mathfrak{m}$ es maximal, y por tanto primo) , $\mathfrak{m} \cap \mathbb{F}_p[X] = (f)$, siendo $f \in \mathbb{F}_p[X]$ un polinomio irreducible. Sea pues $h/g \in \mathbb{F}_p(X)$; si $h/g = 0$ no hay nada que probar, de modo que supondremos que $h \neq 0$, entonces h/g puede expresarse de la forma $h/g = f^k\overline{h}/\overline{g}$, donde $k \in \mathbb{Z}$ y $(f, \overline{h}\overline{g}) = 1$. De este modo $|\overline{h}/\overline{g}| = 1$, y si q es el cardinal del cuerpo residual de v_f se cumple:

$$|h/g| = |f^k| = |f|^k = q^{-k(-\log_q |f|)} = (q^{-k})^s = |h/g|_f^s$$

donde $s = -\log_q |f|$, que es positivo pues $f \in \mathfrak{m}$, y por tanto $|f| < 1$. De este modo hemos probado que $|\cdot|$ es equivalente a $|\cdot|_f$, para un polinomio irreducible f.

Por otro lado supongamos que $|X| > 1$. Esto implica que si $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{F}_p[X]$, $(a_nX^n)^{-1}f = b_0X^{-n} + b_1X^{-n+1} + \cdots + b_{n-1}X^{-1} + 1 := g + 1$, siendo $b_i = a_i/a_n$, para todo $i \in \{1, \ldots, n-1\}$. Ya que $|g| = |b_0X^{-n} + b_1X^{-n+1} + \cdots + b_{n-1}X^{-1}| \leq$ máx$\{|X|^{-n}, |X|^{1-n}, \ldots, |X|^{-1}\}$ $= |X|^{-1} < 1$, $g \in \mathfrak{m}$, y por tanto $1 + g$ es una unidad de A (ya que es local). Como consecuencia tenemos que $|1 + g| = 1$, y así, $|f| = |a_nX^n||1 + g| = |a_nX^n| = |X|^n = |X|^{\deg f}$, de modo que si $f/g \in \mathbb{F}_p(X)^*$ (si f fuese nulo no habría nada que demostrar):

$$|f/g| = |X|^{\deg f - \deg g} = p^{\log_p |X|(\deg f - \deg g)} = (p^{-(\deg g - \deg f)})^{\log_p |X|} = |f/g|_\infty^s,$$

donde por hipótesis, $s := \log_p |X| > 0$. De este modo hemos probado que $|\cdot|$ es equivalente a $|\cdot|_\infty$.

□

Proposición 2.36 (Lema de Hensel)**.** *Sea K un cuerpo completo para una valoración discreta v, A su anillo de valoración y π un uniformizante de A. Si un polinomio primitivo $f \in A[X]$ (es decir, que cumple $f \not\equiv 0 \mod \pi$) admite una factorización módulo π, $\bar{f} = \bar{g}\bar{h}$, siendo $\bar{g}, \bar{h} \in \kappa[X]$ dos polinomios coprimos, entonces f admite una factorización $f = gh$ con polinomios $f, g \in A[X]$ con* $\deg g = \deg \bar{g}$*, siendo g y h representantes en $A[X]$ de $\bar{g}$ y $\bar{h}$.*

Demostración. Sea $d = \deg f$ y $m = \deg \bar{g}$, luego $d = \deg f \geq \deg \bar{f} = \deg \bar{h} + \deg \bar{g}$ (ya que κ es un cuerpo), por lo que $d - m \geq \deg \bar{h}$. Sean $g_0, h_0 \in A[X]$ representantes de $\bar{g}, \bar{h}$ respectívamente cumpliendo que $\deg g_0 = m$ y $\deg h_0 \leq d - m$. Como $\bar{g}$ y $\bar{h}$ son coprimos existen $a, b \in A[X]$ tales que $ag_0 + bh_0 \equiv 1 \mod \pi$. Necesitamos demostrar el siguiente lema:

Lema 2.37. *Para todo $i \in \mathbb{N} - \{0\}$ existen polinomios $p_i, q_i \in A[X]$ de grados $\leq m$ y $\leq d - m$ respectivamente tales que para $n \geq 1$ los polinomios:*

$$g_{n-1} = g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1} \quad , \quad h_{n-1} = h_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1}$$

satisfacen $f \equiv g_{n-1}h_{n-1} \mod \pi^n$

Demostración. El resultado se probará por inducción en n. Para $n = 1$ el resultado estaría probado (por la elección de g_0 y h_0). Supongamos que el resultado está probado para el caso n, y veamos que se cumple para el caso $n+1$. Para ello basta con construir los polinomios $p_n, q_n \in A[X]$, con los grados adecuados que cumplan $f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n$ mód π^{n+1}. Esto es claro, pues si $g_n = g_{n-1} + p_n\pi^n$ y $h_n = h_{n-1} + q_n\pi^n$, entonces la congruencia $f \equiv g_n h_n \mod \pi^{n+1}$ equivale a $f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n \mod \pi^{n+1}$. Sea pues $f_n = \pi^{-n}(f - g_{n-1}h_{n-1})$, que pertenece a $A[X]$ por la hipótesis de inducción, de modo que $f_n \equiv g_0 a f_n + h_0 b f_n \mod \pi$. Si $\deg(bf_n) < m$ ya estaría, pues tomando como p_n y q_n los polinomios con los términos de bf_n y af_n cuyos coeficientes no están en πA, se cumple que $\deg q_n \leq d-m$. En efecto, $\deg q_n + m = \deg q_n + \deg g_0 = \deg(q_n g_0) = \deg(q_n g_0 \mod \pi) = \deg(f_n - bf_n \mod \pi) \leq d$ (ya que $\deg(f_n \mod \pi) \leq \deg f_n \leq \max\{\deg f, \deg g_{n-1}h_{n-1}\} \leq d$ y el coeficiente principal de g_0 es una unidad, ya que no está en πA A es local y $\deg g_0 = \deg(\bar{g})$. Si $\deg(bf_n) \geq m = \deg g_0$, dado que el coeficiente principal de g_0 es una unidad, por el algoritmo de la división obtenemos $bf_n = r_n g_0 + p_n$ con $\deg p_n < m$, de modo que $f_n \equiv g_0(af_n + h_0 r_n) + h_0 p_n \mod \pi$ con $\deg p_n < m$ (y estaría probado, por el caso anterior). □

Por el lema anterior, tenemos que los coeficientes de $g_{n+t} - g_n$, para $n, t \in \mathbb{N}$ están en $\pi^{n+1}A$. Como A es completo, $g = \lim_n g_n$ y $h = \lim_n h_n$ están bien definidos y cumplen $\deg g = \deg g_0 = m$ y $\deg h \leq d - m$ por construcción. Además la relación $f \equiv g_{n-1}h_{n-1} \mod \pi^n$ para todo $n \geq 1$ implica la igualdad $f = gh$ en A ya que, como $g_{n+t} \equiv g_n \mod \pi^{n+1}$ para todo $t \in \mathbb{N}$, tenemos que $g \equiv g_n \mod \pi^{n+1}$ (y análogamente para h), y por tanto $f - gh \equiv f - g_n h_n \equiv 0 \mod \pi^{n+1}$ para todo $n \in \mathbb{N}$. De modo que, usando que $\cap_n \pi^n A[X] = (0)$ [AM, cor. 10.18], tenemos que $f = gh$, como queríamos probar. □

Corolario 2.38. *Sea A un AVD completo con uniformizante π y K su cuerpo de fracciones. Si el término independiente de un polinomio mónico irreducible $f \in K[X]$ pertenece a A, entonces $f \in A[X]$.*

Demostración. Sea $f = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n \in K[X]$, como K es el cuerpo de fracciones de A, el coeficiente a_i admite una expresión $a_i = u_i \pi^{-m_i}$ con $u_i \in A^*$ y $m_i \in \mathbb{Z}$ para todo $i = 1, \ldots, n-1$, de modo que $m = \max\{-m_i, i = 1 \ldots, n-1\}$ (y cero, en caso de que todos los coeficientes estén en A) es el menor número natural que verifica que $\pi^m f \in A$. Supongamos ahora que $a_0 \in A$ y $f \notin A[X]$, entonces si a_r es el primer coeficiente que verifica que $m_r = m$ para la descomposición anterior, es claro que $r \neq 0$ y $m > 0$. Además, esto implica que $\pi^m f(X) \equiv X^r(\pi^m a_r + \cdots + \pi^m X^{n-r}) \mod \pi$. De la minimalidad de m se deduce que $X^r \mod \pi$ y $\pi^m a_r + \cdots + \pi^m X^{n-r} \mod \pi$ son coprimos, pero eso contradice que f es irreducible como polinomio de $K[X]$, por el lema de Hensel. De este modo concluimos que $f \in A[X]$. □

Corolario 2.39. *Sea A un AVD completo con valoración v, K su cuerpo de fracciones, $L|K$ una extensión finita de grado n y B la clausura íntegra de A en L. Entonces $B = \{\alpha \in L | N_{L|K}(\alpha) \in A\}$.*

Demostración. Para la primera parte, la inclusión hacia la derecha está probada en el corolario 1.36. Sea pues $\alpha \in L$ tal que $N_{L|K}(\alpha) \in A$ y sea $f = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m$ su polinomio irreducible. Entonces $N_{L|K}(\alpha) = (-1)^n a_0^t \in A$ para $t = [L : K(\alpha)]$, de modo que $a_0 \in K$ es solución del polinomio $X^t \pm N_{L|K}(\alpha) \in A[X]$ (signo en función de $(-1)^n$) por lo que $a_0 \in A$, ya que A es íntegramente cerrado. Dado que $a_0 \in A$, por el corolario anterior $f \in A[X]$, de modo que $\alpha \in B$, al ser una raíz de f.

□

Observación 2.40. El lema de Hensel implica que como el polinomio $X^{p-1} - 1 \in \mathbb{Z}_p[X]$ escinde en $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$ con raíces distintas, $X^{p-1} - 1 \in \mathbb{Z}_p$ escinde en $\mathbb{Z}_p$, de modo que $\mathbb{Z}_p$ contiene a las $p-1$-ésimas raíces de la unidad que pueden tomarse, junto con el cero, para formar un conjunto de representantes $\mathcal{S}$ en $\mathbb{Z}_p$ de $\mathbb{Z}_p/p\mathbb{Z}_p$ multiplicativamente cerrado. Un conjunto de representantes con dicha propiedad se dice *de Teichmüller*. En general se puede probar que todo AVD completo admite un único conjunto de representantes de Teichmüller [Ser, cap. II, prop.8], nosotros probaremos su existencia para un caso particular:

Proposición 2.41. *Sea K un cuerpo local de caracteristica p para una valoración discreta v y A su anillo de valoración con uniformizante π. Entonces A contiene un conjunto de representantes $\mathcal{S}$ de $\kappa = A/\pi A$ con estructura de cuerpo.*

Demostración. Como K es local, su cuerpo residual κ es finito, luego, dado que A tiene característica p (al tenerlo K), $\kappa \simeq \mathbb{F}_{p^n}$ para un $n \in \mathbb{N} - \{0\}$. Como $\mathbb{F}_p \subset A$, denotemos como F_0 a un subcuerpo maximal de A (con respecto a la inclusión) conteniendo a $\mathbb{F}_p$ (existe pues todo subcuerpo F de A induce un homomorfismo inyectivo $F \hookrightarrow \kappa$, y así el cardinal de F es como mucho p^n, siendo $n \in \mathbb{N} - \{0\}$). Sea $q : A \to \kappa$ el homomorfismo canónico, demostraremos que F_0 es un conjunto de representantes de κ. En primer lugar $|F_0| \leq |\kappa|$ pues la restricción de q a F_0 es inyectiva, veamos que $F_0 = \kappa$, sea entonces $\alpha \in \kappa$ tal que $\alpha \notin q(F_0)$. Como todo elemento de κ es raíz del polinomio $\bar{f}(X) = X^{p^n-1} - 1 \in \kappa[X]$, $\bar{f}$ escinde con raíces distintas en κ y, por el lema de Hensel, $f(X) = X^{p^n-1} - 1$ escinde en A con raíces distintas. En particular existe un $a \in A$ tal que $f(a) = 0$ y $q(a) = \alpha$ que cumplirá que $a \notin F_0$ (ya que $\alpha \notin q(F_0)$), con lo que $F_0[a]$ es un cuerpo (ya que a es algebraico sobre F_0) que contiene estrictamente a F_0 y está contenido en A, lo que viola la maximalidad de F_0. □

Corolario 2.42. *Para p primo la completación de $\mathbb{F}_p(X)$ para un valor absoluto es isomorfa al cuerpo de las series de Laurent $\mathbb{F}_{p^n}((X))$ para algún $n \geq 1$*

Demostración. Sea $|\cdot|$ un valor absoluto en $\mathbb{F}_p(X)$. Por el teorema 2.35 es equivalente a $|\cdot|_f$ para un polinomio irreducible $f \in \mathbb{F}_p[X]$ o bien a $|\cdot|_\infty$. Para el primer caso sea p^n con $n \geq 1$ el cardinal del cuerpo residual de $|\cdot|$. Por las proposiciones 2.21 y 2.41 la completación de $\mathbb{F}_p(X)$ con respecto a $|\cdot|$ es isomorfa a $\mathbb{F}_{p^n}((X))$ (ya que $f \in \mathbb{F}_p[X]$ es trascendente sobre $\mathbb{F}_p$). Para el segundo caso, por un razonamiento similar, la completación de $\mathbb{F}_p(X)$ con respecto a $|\cdot|$ es isomorfa a $\mathbb{F}_p((X))$ (ya que $X^{-1} \in \mathbb{F}_p^{pol}(X)$, con la notación del ejemplo 2.34, es trascendente sobre $\mathbb{F}_p$). □

Proposición 2.43. *Sea K un cuerpo completo para una valoración discreta v con anillo de valoración A y $L|K$ una extensión finita de grado n. Entonces la clausura íntegra de A en L es es un anillo de valoración discreta completo finitamente generado como $A-$módulo.*

Demostración. Dado que v y $N_{L|K}$ son multiplicativas, la composición $v \circ N_{L|K} : L^* \to \mathbb{Z}$ es un homomorfismo de grupos, de modo que su imagen es un subgrupo de $\mathbb{Z}$ (no nulo, ya que si π es un uniformizante de A, $v(N_{L|K}(\pi)) = n \neq 0$), y por tanto, generado por un $m \in \mathbb{Z}$, con $m > 0$. De este modo la aplicación $w : L^* \to \mathbb{Z}$ dada por $w(x) = \frac{1}{m} v(N_{L|K}(x))$ está bien definida, veamos que es una valoración discreta. En primer lugar, dado que $v \circ N_{L|K}(x)$ es un homomorfismo de grupos, w es un homomorfismo de grupos, que además es sobreyectivo (pues $1 \in w(L)$ por construcción). Si $x, y \in L$ (supondremos sin pérdida de generalidad que $w(x) \geq w(y)$), entonces $w(x+y) \geq \text{ínf}\{w(x), w(y)\}$ es equivalente, restando a ambos lados de la ecuación $w(y)$, a que si $w(z) \geq 0$, entonces $w(1+z) \geq 0$. Sea pues B la clausura íntegra de A en L y $z \in L$ tal que $w(z) \geq 0$, entonces por definición de w, $N_{L|K}(z) \in A$, por lo que por el corolario 2.39, $z \in B$ y por tanto $1 + z \in B$ de nuevo por el corolario 2.39, y en consecuencia $w(1+z) \geq 0$. Concluimos que w es una valoración discreta, y que B es su anillo de valoración. Consideremos ahora un valor absoluto inducido por w, $|\cdot|_w$, veamos que L es completo para dicho valor absoluto. Usaremos el siguiente resultado conocido:

Lema 2.44. *Sea K un cuerpo completo para un valor absoluto $|\cdot|$ y V un $K-$espacio vectorial de dimensión finita n con una norma $\|\cdot\|$. Para cualquier base $\{v_1, \ldots, v_n\}$ de V la norma del máximo $\|\lambda_1 v_1 + \cdots + \lambda_n v_n\|_0 = \text{máx}\{|\lambda_1|, \cdots, |\lambda_n|\}$ es equivalente a $\|\cdot\|$. En particular V es completo y homeomorfo a K^n.*

Demostración. Véase [Neu, cap II, prop. 4.9]. □

Como la restricción de w a K coincide con v, $|\cdot|_w$ es una norma de L (visto como espacio vectorial $n-$dimensional sobre K), L es completo para la topología definida por $|\cdot|_w$. Además, hecha una elección de $c \in (0,1)$, $|\cdot|_{w,c}$ está unívocamente determinado por $|\cdot|_{v,c}$. En efecto, si hubiese otro valor absoluto $|\cdot|$ que extendiese $|\cdot|_{w,c}$, ha de ser necesariamente equivalente a $|\cdot|_{w,c}$ (ya que ambos, como normas, inducirían la misma topología de L, por el lema anterior), y por tanto $|x| = |x|_{w,c}^s$ para todo $x \in L$ y $s > 0$, pero como ambos valores absolutos coinciden en K, $s = 1$.

Veamos que B es un $A-$módulo finitamente generado. Sea π un uniformizante de A y $\overline{B} = B/\pi B$ (que es un $\kappa-$espacio vectorial, siendo $\kappa = A/\pi A$), tomando m elementos $b_1, \ldots, b_m \in B$ cuyas imágenes $\overline{b}_i$ en $\overline{B}$ son linealmente independientes sobre κ entonces son linealmente independientes sobre A, en efecto, si $\sum_{i=1}^m a_i b_i = 0$ con $a_i \in A$ (podemos suponer sin pérdida de generalidad que existe un a_i no divisible por π, ya que A es un dominio), entonces módulo πB tendríamos una relación $\sum_{i=1}^m \overline{a_i}\overline{b_i} = 0$, contradiciendo que los $\overline{b}_i$ son linealmente independientes. Como $[L : K] = n$ existen a lo sumo n elementos de $\overline{B}$ linealmente independientes sobre κ (pues si $\overline{b}_1, \ldots, \overline{b}_m$ con $m > n$ es un conjunto de elementos de $\overline{B}$ linealmente independiente sobre κ entonces un conjunto de representantes $b_1, \ldots, b_m$ son linealmente independientes sobre A y por

tanto, dado que K es el cuerpo de fracciones de A, linealmente independientes sobre K como elementos de L, lo cual contradice que $[L:K]=n$). Supongamos sin pérdida de generalidad entonces que existen elementos de B $b_1,\dots,b_m$, con $m\leq n$ cuyas imágenes $\overline{b}_1,\dots,\overline{b}_m$ forman una $\kappa-$base de $\overline{B}$. Definimos entonces M como el $A-$módulo generado por $b_1,\dots,b_m$, probemos que $M=B$. Sea pues $b\in B$, entonces (dado que $\overline{b}_1,\dots,\overline{b}_m$ es una base de $\overline{B}$), $b=c_0+\pi c$, donde c_0 es igual a una $A-$combinación lineal de los b_i y $c\in B$. Repitiendo este paso para c y aplicándolo inductivamente obtenemos que $b=c_0+c_1\pi+c_2\pi^2+\dots$, donde $a_i\in A$ y cada c_i es igual a una $A-$combinación lineal de los b_i (como $w(\pi)\geq 1$ y B es completo para el valor absoluto $|\cdot|_L$ la expresión anterior tiene sentido), de modo que agrupando términos en cada b_i (que tiene sentido pues A es completo) obtenemos que $B=M$, como queríamos probar.

Como B es un anillo de valoración discreta y un $A-$módulo finitamente generado, por la proposición 1.46, $[L:K]=n=ef$ (ya que B es un anillo de valoración discreta y por lo tanto contiene un único ideal primo), y como $e=w(\pi)=\frac{1}{m}v(\mathrm{N}_{L|K}(\pi))=\frac{1}{m}v(\pi^n)=n/m$, obtenemos que $m=f$.

□

Proposición 2.45. *[Iwa, lem. 1.4] Sean K,L dos cuerpos completos para dos valoraciones v,w respectivamente, con anillos de valoración A, B, uniformizantes π, Π y cuerpos residuales κ, λ. Entonces si la valoración w extiende v con grado $e=w(\pi)$ y la extensión $\lambda|\kappa$ es finita de grado f, entonces la extensión $L|K$ es finita de grado ef.*

Demostración. Sea $\{\overline{\alpha}_1,\dots,\overline{\alpha}_f\}$ una base de λ como $\kappa-$espacio vectorial y $\alpha_1,\dots,\alpha_f$ un conjunto de representantes en B. Probemos que el conjunto $\{\alpha_j\Pi^i | j=1,\dots,f; i=0,\dots,e-1\}$ es linealmente independiente sobre K, sea pues una combinación lineal $\sum_{i,j}a_{ij}\alpha_j\Pi^i=0$, $a_{ij}\in K$, con algún coeficiente a_{ij} distinto de cero, de modo que existe una suma $s_{i_0}=\sum_j a_{i_0j}\alpha_j$ no nula. Dividiendo s_{i_0} entre un $a_{i_0j_0}$ tal que $v(a_{i_0j_0})=\mín\{v(a_{i_0j}), j=1\dots,f\}$ obtenemos que $\bar{s}_{i_0}=s_{i_0}/a_{i_0j_0}$ es una combinación lineal de elementos de A, uno de ellos igual a 1. Dado que los $\alpha_1,\dots,\alpha_f$ son unidades de B (al no pertenecer a ΠB y ser B local), de modo que s_{i_0}, no puede pertenecer a ΠB, efectivamente, si perteneciese a ΠB, tendríamos módulo ΠB una combinación lineal de los $\bar{\alpha}_1,\dots,\bar{\alpha}_f$ igualadas a cero con al menos un sumando no nulo, lo cual viola su independencia lineal. De modo que $w(\bar{s}_{i_0})=0$ y por tanto $w(s_{i_0})=w(a_{i_0j_0})=ev(a_{i_0j_0})$. Por otro lado, en $\sum_i s_i\Pi^i=0$ (eliminando de ser necesario los términos nulos), dos sumandos deben tener la misma valoración w, porque si todas fuesen estrictamente distintas, entonces $w(\sum_i s_i\Pi^i)=\mín\{w(s_i\Pi^i)\}\neq w(0)$, donde i recorre los términos no nulos de la suma (esto se sigue de que $w(x)\neq w(y)$ implica $w(x+y)=\ínf\{w(x),w(y)\}$, como se vio en la proposición 1.3) y por tanto, la suma no podría anularse. Pero esto es absurdo, pues si i,j representan los dos sumandos de igual valoración, por lo visto antes, $w(s_i\Pi^i)=w(s_j\Pi^j)$, o equivalentemente $i-j=w(\Pi^i)-w(\Pi^j)=w(s_j)-w(s_i)\in e\mathbb{Z}$, lo cual contradice nuestra hipótesis iniciales de que $0<i-j<e$. Esto prueba la independencia lineal y por tanto $\dim_K L=[L:K]\geq ef$.

Para probar la igualdad, sea $\mathcal{S}_\kappa$ un conjunto de representantes de κ. Como $\lambda|\kappa$ es finita todo elemento $\overline{\omega}\in\lambda$ puede expresarse de modo único como $\overline{\omega}=\sum_{j=1}^f\overline{a}_j\overline{\alpha}_j$, donde $\overline{a}_j$ es imagen por

la proyección canónica de un $a_j \in \mathcal{S}_\kappa$, de modo que $\mathcal{S}_\lambda = \{\sum_{j=1}^f a_j\alpha_j | a_j \in \mathcal{S}_\kappa\}$ es un conjunto de representantes de λ. Escribiendo cada entero m de la forma $m = et+j$, con $t \in \mathbb{Z}$, $j = 0, \ldots, 1-e$, sea $\Pi_m = \pi^t\Pi^j$, que satisface que $w(\Pi_m) = w(\pi^t)+w(\Pi^j) = ev(\pi^t)+w(\Pi^j) = et+j = m$, y por tanto, si $z \in L$, dado que L es completo para la valoración discreta w, z tiene una representación única de la forma $z = \sum_{k\geq n} a'_k\Pi_k$, donde $n \in \mathbb{Z}$ y $a'_k \in \mathcal{S}_\lambda$, reescribiendo convenientemente:

$$z = \sum_{k\geq n}\left(\sum_{i=1}^f a_{im}\alpha_i\right)\Pi_m = \sum_{t\geq n'}\sum_{j=0}^{e-1}\sum_{i=1}^f a_{i,te+j}\pi^t\Pi^j = \sum_{j=1}^{e-1}\sum_{i=1}^f\left(\sum_{t\geq n'} a_{i,te+j}\pi^t\right)\alpha_i\Pi^j,$$

donde n' es la parte entera por defecto de n/e. La última igualdad tiene sentido pues $a_{i,te+j} \in \mathcal{S}_\kappa$, y por tanto $\sum_{t\geq n'} a_{i,te+j}\pi^t \in K$ ya que K es completo para la valoración v. Con esto hemos probado que $\{\alpha_j\Pi^i\}$ es un conjunto de generadores de L como K espacio vectorial, y dado que son linealmente independientes, forman una base, y por tanto $[L : K] = ef$.

□

Observación 2.46. En la prueba anterior, si la extensión $L|K$ es separable, entonces por la proposición 1.46 $[L : K] = ef$, de modo que la propiedad anterior se puede demostrar sin la necesidad de que A y B sean completos. Otra puntualización es que si $z \in A$, entonces $z = \sum_{k\geq 0} a'_k\Pi_k$, y por lo tanto $n' \geq 0$. Esto prueba que el conjunto $\{\alpha_j\Pi^i\} \subset B$ genera B como $A-$módulo. Pero como dicho conjunto es linealmente independiente sobre K, lo será también sobre A, de modo que también forma una base de B como $A-$módulo.

Lema 2.47. *Sea A un anillo, $f \in A[X]$ y $a \in A$. Entonces $f(X) = f(a) + f'(a)(X-a) + g(X)(X-a)^2$, donde f' denota la derivada de f y $g \in A[X]$.*

Demostración. En efecto, si $f(X) = \sum_{i=0}^n b_iX^i$, entonces $f'(a) = \sum_{i=0}^n ib_ia^{i-1}$, luego:

$$f(X) = \sum_{i=0}^n b_i(a+(X-a))^i = \sum_{i=0}^n b_i\sum_{j\leq i}\binom{i}{j}a^i(X-a)^{i-j} =$$
$$= \sum_{i=0}^n b_i\left(a^i + ia^{i-1}(X-a) + \sum_{j\leq i-2}\binom{i}{j}a^i(X-a)^{i-j}\right),$$

que no es otro que $f(a) + f'(a) + g(X)(X-a)^2$, donde $g(X) = \sum_{i=0}^n\sum_{j\leq i-2} b_i\binom{i}{j}a^i(X-a)^{i-j-2}$. □

Proposición 2.48. *Sea K un cuerpo completo para una valoración discreta v, A su anillo de valoración y κ su cuerpo residual. Sea además $L|K$ una extensión finita de cuerpos y B la clausura íntegra de A en L (que será un anillo de valoración discreta por la proposición 2.43) y λ su cuerpo residual. Entonces si la extensión $\lambda|\kappa$ es separable, existe un elemento $x \in B$ tal que $B = A[x]$.*

Demostración. Como la extensión $\lambda|\kappa$ es finita (al serlo $L|K$) y separable, por el teorema del elemento primitivo existe un elemento $\overline{x_0} \in \lambda$ tal que $\lambda = \kappa[\overline{x_0}]$, sea $\overline{f}$ su polinomio irreducible sobre κ. Sea ahora $f \in A[X]$ es un representante mónico de $\overline{f}$ y x_0 un representante de $\overline{x_0}$ sobre A, que cumplirá que $w(f(x_0)) \geq 1$ (ya que su reducción módulo λ es nula). Si $w(f(x_0)) = 1$, entonces denotamos $x = x_0$. Por otro lado, si $w(f(x_0)) \geq 2$, sea Π un uniformizante de B y $x = x_0 + \Pi$, que cumplirá que $w(f(x)) = 1$. En efecto, por el lema 2.47, $f(x) = f(x_0) + \Pi f'(x_0) + b\Pi^2$, con $b \in B$, y como la extensión $\lambda|\kappa$ es separable, $\overline{x_0}$ no es raíz de la derivada de $\overline{f}$, $\overline{f}'$. Dado que la derivada de f, f', es un representante de $\overline{f}'$, se deduce que $w(f'(x_0)) = 0$, de modo que que $w(f(x)) = w(\Pi f'(x_0)) = 1$ (ya que $w(f(x_0)) \geq 2$ por hipótesis y $w(b\Pi^2) \geq 2$), y por tanto, $f(x)$ es un uniformizante de B. Dado que la imagen de x en λ genera la extensión $\lambda|\kappa$ y $f(x)$ es un uniformizante de B, por la proposición 2.45, $\{x^i f(x)^j\} \subset B$, donde $i = 0, \ldots, e-1$ y $j = 1, \ldots, f$, donde e, f representan los índices de extensión y residual de la extensión $L|K$ respectivamente, forma una $A-$base de B sobre A. Esto en particular implica que $B = A[x]$, como queríamos probar. □

Proposición 2.49. *Un cuerpo K es local si y solo si es una extensión finita de $\mathbb{Q}_p$ o de $\mathbb{F}_p((X))$, con p primo.*

Demostración. Por un lado es claro que toda extensión finita de $\mathbb{Q}_p$ (completo para la valoración $p-$ádica, como se vio en el ejemplo 2.32) y de $\mathbb{F}_p((X))$ (completa para la valoración inducida por el polinomio irreducible $f(X) = X \in \mathbb{F}_p[X]$) es un cuerpo local, pues por la proposición 2.43, la valoración considerada en $\mathbb{Q}_p$ o $\mathbb{F}_p((X))$ se extiende de modo único a una valoración sobre K, cuyo cuerpo residual es finito al ser una extensión finita del cuerpo residual finito de $\mathbb{Q}_p$ o $\mathbb{F}_p((X))$, al ser estos cuerpos locales. Esto prueba que K es un cuerpo local.

Recíprocamente sea K un cuerpo local y v su valoración discreta. Si la característica de K es cero, entonces K es una extensión de $\mathbb{Q}$, y la restricción del valor absoluto inducido por v a $\mathbb{Q}$ ha ser equivalente a algún $|\cdot|_p$ con p primo por el teorema de Ostrowski (no puede ser equivalente al valor absoluto usual pues el valor absoluto inducido por una valoración discreta es no arquimediano), de modo que como K es completo (al ser local), por la propiedad universal de las completaciones $\mathbb{Q}_p \subset K$, y la valoración v extiende la valoración v_p de $\mathbb{Q}_p$. Para ver que dicha extensión es finita basta con tener en cuenta que como K es local su cuerpo residual es finito, de modo que es una extensión finita del cuerpo residual de $\mathbb{Q}_p$, $\mathbb{F}_p$, por lo que que la extensión $K|\mathbb{Q}_p$ es finita por la proposición 2.45.

Por otro lado, si la característica de K es p entonces K debe contener un elemento trascendente sobre $\mathbb{F}_p$. En efecto, si todos los elementos de K fuesen algebraicos sobre $\mathbb{F}_p$, entonces para $\alpha \in K$ la extensión $\mathbb{F}_p(\alpha)|\mathbb{F}_p$ sería finita, y por tanto $|\alpha| = 1$ por la observación 2.2. Por lo tanto $\mathbb{F}_p(X) \subset K$, de modo que por un razonamiento análogo al anterior y por el corolario 2.41, $\mathbb{F}_{p^n}((X)) \subset K$, y consecuentemente $\mathbb{F}_p((X)) \subset K$, (ya que la extensión $\mathbb{F}_{p^n}|\mathbb{F}_p$ induce naturalmente la extensión $\mathbb{F}_{p^n}((X))|\mathbb{F}_p((X))$). De modo que por el mismo razonamiento que antes, el cuerpo residual de K es una extensión finita del cuerpo residual de $\mathbb{F}_p((X))$, y por tanto la extensión $K|\mathbb{F}_p((X))$ es finita, como queríamos probar. □

Proposición 2.50. *Sea $L|K$ una extensión finita y separable de grado n, v una valoración discreta de K con anillo de valoración A y B la clausura íntegra de A en L. Sean w_i las diferentes prolongaciones de v en L (dadas por la proposición 1.51); e_i, f_i los índices de ramificación y residuales de sus ideales maximales, y $\hat{K}$, $\hat{L}_i$ las completaciones de K y L para las topologías dadas por las valoraciones v y w_i respectivamente (con extensiones a sus completaciones $\hat{v}$, $\hat{w}_i$ respectivamente). Se cumple:*

1. *El cuerpo $\hat{L}_i$ es una extensión finita de $\hat{K}$ de grado $e_i f_i$. Además la valoración w_i es la única de $\hat{L}_i$ prolongando v, y se cumple que $e_{w_i} = e_{\hat{w}_i}$ y $f_{w_i} = f_{\hat{w}_i}$.*

2. *Las extensiones $\hat{L}_i|K$ son separables, y se tiene el isomorfismo de $\hat{K}-$álgebras $L \otimes_K \hat{K} \simeq \prod_i \hat{L}_i$.*

Demostración. El apartado (1) es sencillo teniendo en cuenta que la valoración $\hat{w}_i$ sobre $\hat{L}_i$ coincide con w_i, y si π es un uniformizante de K, es también un uniformizante de $\hat{K}$. De este modo $e_{w_i} = w_i(\pi) = \hat{w}_i(\pi) = e_{\hat{w}_i}$. Además, si A denota el anillo de valoración de K y B_i el anillo de valoración de L para w_i (con uniformizante Π_i) y $\hat{A}$, $\hat{B}_i$ sus completaciones, $\lambda_i = B_i/\Pi_i B_i = \hat{B}_i/\Pi_i \hat{B}_i$; $\kappa = A/\pi A = \hat{A}/\pi\hat{A}$, de modo que es claro que $f_{w_i} = f_{\hat{w}_i}$. La igualdad $[\hat{L}_i : \hat{K}] = e_i f_i$ se sigue entonces de lo anterior y de la proposición 2.45.

Para el apartado (2), al ser $L|K$ finita y separable, por el teorema del elemento primitivo $L \simeq K[X]/(f) \simeq K[\alpha]$, donde $f \in K[X]$ es un polinomio mónico, irreducible y separable y α uno de sus ceros. Probaremos que el conjunto de divisores irreducibles de f en $\hat{K}[X]$ está en correspondencia biyectiva con las extensiones w_i de la valoración v a L. Sea g un divisor irreducible de f en $\hat{K}[X]$, entonces $\hat{K}[\alpha] = \hat{K}[X]/(g)$ es una extensión finita de $\hat{K}$, y por tanto $\hat{v}$ se extiende de forma única a una valoración $\hat{w}_g$ de $\hat{K}[X]/(g)$ por la proposición 2.43, esto prueba que la correspondencia está bien definida y es inyectiva. Para demostrar la sobreyectividad sea w_i una valoración sobre L que extiende a v, probemos que la completación de L con respecto a w_i, $\widehat{K[\alpha]} = \hat{K}[\alpha]$. Por un lado es claro que como $K[\alpha]|K$ es finita $\hat{K}[\alpha]|\hat{K}$ también lo es, de modo que por 2.43 $\hat{K}[\alpha]$ es completo, y además contiene a $K[\alpha]$, de modo que $\hat{L}_i \subset \hat{K}[\alpha]$. Por otro lado $\hat{K} \subset \hat{L}_i$ (ya que $\hat{L}_i$ es completo y contiene a K) y $\alpha \in \hat{L}_i$, de modo que $\hat{L}_i = \hat{K}[\alpha]$. Como $\hat{K}[\alpha]|\hat{K}$ es finito existe un polinomio mónico irreducible que se anula en α $g_i \in \hat{K}[X]$ tal que $\hat{K}[\alpha] \simeq \hat{K}/(g_i)$, y como $f(\alpha) = 0$, $g|f$. Esto prueba la sobreyectividad de la correspondencia.

El apartado (2) se de deduce de este resultado, pues canónicamente $L \otimes_K \hat{K} \simeq K[X]/(f) \otimes_K \hat{K} \simeq \hat{K}[X]/(f) \simeq \prod_g K[X]/(g) = \prod_i \hat{L}_i$ donde g recorre los polinomios mónicos irreducibles que dividen a $f \in \hat{K}[X]$ e i el conjunto de las valoraciones discretas que extienden v. La segunda igualdad se sigue de [AM, ej. 2.6], la tercera del teorema chino de los restos, y la última de la correspondencia que probamos anteriormente. Esta descomposición prueba también que $\hat{L}_i$ es separable (al estar generada por un divisor de f, que es separable), y que el grado de $L \otimes_K \hat{K}$ como $\hat{K}$-álgebra es n (pues coincide con las sumas de los grados de los $\hat{L}_i$, que valen $e_i f_i$ por el apartado anterior, y estos suman n por la proposición 1.46). □

Capítulo 3

Ramificación

Lema 3.1. *Sea $L|K$ una extensión de Galois finita de cuerpos locales. Si w denota la valoración de L, B su anillo de valoración, $\mathfrak{q}$ su ideal maximal e $i \geq 0$ es un entero; si $\alpha \in \mathfrak{q}^i$ para $i \geq 0$, entonces $\sigma(\alpha) \in \mathfrak{q}^i$ (entendiendo $\mathfrak{q}^0 = B$).*

Demostración. Sea $\alpha \in B$. Por lo visto en la proposición 2.43, $w(\alpha) = \frac{1}{f} v(N_{L|K}(\alpha))$, de modo que es claro que $w(\alpha) = w(\sigma(\alpha))$ para todo $\alpha \in B$ y todo $\sigma \in \mathrm{Gal}(L|K)$, de donde se sigue el resultado. □

Proposición 3.2. *Sea $L|K$ es una extensión de Galois finita de cuerpos locales. Entonces su extensión de cuerpos residuales asociada $\lambda|\kappa$ es de Galois.*

Demostración. Basta probar que, en las hipótesis de la proposición, la extensión $\lambda|\kappa$ es normal. Sea $\overline{\alpha} \in \lambda$ y $\alpha \in B$ un representante. Como $L|K$ es de Galois el polinomio irreducible de α sobre K escindirá en factores lineales $f(X) = \prod_\sigma (X - \sigma(\alpha))$, donde σ recorre todo $\mathrm{Gal}(L|K)$. Por el lema anterior $\sigma(\alpha) \in B$, de modo que, la imagen de f en $\lambda[X]$ escindirá también en factores lineales. Esto prueba que $\lambda|\kappa$ es normal. □

Observación 3.3. Sea $L|K$ una extensión finita de Galois de cuerpos locales y $\lambda|\kappa$ la extensión inducida en los cuerpos residuales. Por lo visto en la demostración anterior existe un homomorfismo de grupos bien definido y sobreyectivo $\mathrm{Gal}(L|K) \to \mathrm{Gal}(\lambda|\kappa)$ dado por reducción $\sigma \mapsto \overline{\sigma}$, donde $\overline{\sigma}$ está dada por $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)}$.

Lema 3.4. *Sea K un cuerpo completo para una valoración discreta y $L|K$, $K'|K$ dos extensiones dentro de una misma clausura algebraica y $L' = LK'$ su extensión compuesta. Entonces:*

1. *si $L|K$ es no ramificada $L'|K'$ es no ramificada. Si $L|K$ y $K'|K$ son no ramificadas, $L'|K$ es no ramificada.*

2. *si $L|K$ es no ramificada y $E|K$ es una subextensión, $E|K$ y $L|E$ son no ramificadas.*

Demostración. Comencemos probando el apartado (1). Como $L|K$ es finita, la extensión de sus cuerpos residuales $\lambda|\kappa$ es también finita por la proposición 2.43, y separable, al ser $L|K$

no ramificada (por la proposición 1.46, (2)), de modo que por el teorema del elemento primitivo existe un elemento $\overline{\alpha} \in \lambda$ tal que $\kappa(\overline{\alpha}) = \lambda$. Sea α un representante de $\overline{\alpha}$ en el anillo de valoración de L, que denotaremos como B, f su polinomio irreducible sobre K (que pertenecerá a $A[X]$ por la proposición 1.35) y $\overline{f} = f \mod \mathfrak{p} \in \kappa[X]$, siendo $\mathfrak{p}$ el ideal maximal de A. Si denotamos como g el polinomio irreducible de $\overline{\alpha}$ sobre κ es claro que $g|\overline{f}$, ya que $\overline{f}(\alpha) = 0$, de modo que se tiene la cadena de desigualdades:

$$[\lambda : \kappa] \leq \deg(\overline{f}) \leq \deg f = [K(\alpha) : K] \leq [L : K] = [\lambda : \kappa]$$

donde la última igualdad se deduce de que la extensión $L|K$ es no ramificada. Por lo tanto se obtiene que $L = K(\alpha)$ y que $\overline{f}$ es el polinomio característico de $\overline{\alpha}$ sobre κ (ya que divide a g y tiene su mismo grado).

Sean ahora A', B' los anillos de valoración de K' y L' $\mathfrak{p}'$, $\mathfrak{q}'$ sus ideales maximales y κ', λ' sus cuerpos residuales. Por lo visto anteriormente para la extensión $L|K$, $L' = LK' = K'K(\alpha) = K'(\alpha)$, de modo que sea $h \in A'[X]$ el polinomio irreducible de α sobre K' (bien definido ya que tanto K' como L están en la misma clausura algebraica) y $\bar{h} \in \kappa'[X]$ su reducción módulo $\mathfrak{q}'$. El polinomio $\bar{h}$ es separable, al ser un divisor de $\bar{f}$, y por tanto irreducible, por el lema de Hensel (si fuese reducible entonces sus componentes serían coprimas por ser $\bar{h}$ separable, y eso induciría una descomposición del polinomio h, que contradiría que h es irreducible). De este modo llegamos a la cadena de desigualdades:

$$[\lambda' : \kappa'] \leq [L' : K'] = \deg h = \deg \bar{h} = [\kappa'(\alpha) : \kappa'] \leq [\lambda' : \kappa'],$$

con lo que $[L' : K'] = [\lambda' : \kappa']$, como queríamos probar. Si además la extensión $K'|K$ es no ramificada, $[L' : K] = [L' : K'][K' : K] = [\lambda' : \kappa'][\kappa' : \kappa] = [\lambda' : \kappa]$ por lo visto anteriormente, de modo que la extensión $L'|K$ es no ramificada en virtud de la proposición 1.46, (2). Para el apartado (2), basta con ver que, por el apartado anterior, la extensión $L|E$ es no ramificada (pues es la extensión compuesta de $L|K$ y $E|K$), de modo que si κ_E representa el cuerpo residual de E, por la fórmula del grado:

$$[\kappa_E : \kappa] = \frac{[\lambda : \kappa]}{[\lambda : \kappa_E]} = \frac{[L : K]}{[L : E]} = [E : K]$$

□

Teorema 3.5. *Sea K un cuerpo completo para una valoración discreta v y κ su cuerpo residual. Si $L|K$ es una extensión finita de cuerpos con cuerpo residual λ, la aplicación $K' \mapsto \kappa'$, que lleva a cada subextensión a su cuerpo residual define una biyección entre las subextensiones no ramificadas de $L|K$ y las subextensiones separables de $\lambda|\kappa$ que preserva las inclusiones. Además, $K'|K$ es de Galois si y solo si lo es $\kappa'|\kappa$, en cuyo caso se tiene el isomorfismo $Gal(K'|K) \simeq Gal(\kappa'|\kappa)$.*

Demostración. Sea $\kappa'|\kappa$ una subextensión separable de $\lambda|\kappa$. Como es finita, existe un elemento $\overline{\alpha} \in \lambda$ tal que $\kappa' = \kappa(\overline{\alpha})$. Sea $\overline{f}$ el polinomio irreducible de $\overline{\alpha}$ sobre κ y $f \in A[X]$ un representante

mónico de $\overline{f}$. Como se vio en la demostración del lema anterior, la subextensión $K' = K(\alpha)|K$ de $L|K$ es no ramificada, de modo que la correspondencia $K' \mapsto \kappa'$ es sobreyectiva.

Por otro lado, si K' y K'' son dos subextensiones no ramificadas con anillos de valoración A'' y A' e igual cuerpo residual κ', por el lema anterior $K'K''|K'$ es una extensión no ramificada cuyo cuerpo residual es κ'. En efecto, si $K''|K$ está generado por un elemento $\alpha'' \in A''$, como se vio en la prueba del lema anterior $[K'K'' : K'] = \deg(\overline{g})$, donde $\overline{g}$ es el polinomio irreducible de $\overline{\alpha''}$ sobre κ', siendo $\overline{\alpha''}$ el representante de α'' en κ', pero $\kappa(\overline{\alpha''}) = \kappa'$, de modo que $\kappa' = \kappa'(\overline{\alpha''})$, y por tanto $\deg \overline{g} = 1$. Esto implica que $\kappa' = \kappa$, y así, la correspondencia es inyectiva. Que preserva las inclusiones es inmediato, dado el lema anterior.

La implicación $K'|K$ de Galois $\Rightarrow \kappa'|\kappa$ de Galois se ha probado de modo general en 3.2. Por otro lado, si $\kappa'|\kappa$ es de Galois, en particular es separable, y por el teorema del elemento primitivo $\kappa' = \kappa(\overline{\alpha})$ para $\overline{\alpha} \in \kappa$. Como $\kappa'|\kappa$ es de Galois, si $\overline{g}$ es el polinomio irreducible de $\overline{\alpha}$ sobre κ y $g \in A[X]$ es un representante mónico (que genera la extensión $K'|K$, por el lema anterior), $\overline{g}$ escinde en factores lineales distintos, de modo que por el lema de Hensel g escinde en factores lineales distintos, como queríamos probar.

De este modo si $K'|K$ es una extensión de Galois finita no ramificada y $\kappa'|\kappa$ denota la extensión de los cuerpos residuales tenemos, por la observación 3.3 un homomorfismo de grupos bien definido y sobreyectivo $\mathrm{Gal}(K'|K) \to \mathrm{Gal}(\kappa'|\kappa)$. Como $K'|K$ es no ramificada, $\mathrm{Gal}(K'|K) = [K' : K] = [\kappa' : \kappa] = \mathrm{Gal}(\kappa'|\kappa)$, de modo que el homomorfismo anterior es biyectivo, por tanto un isomorfismo de grupos.

□

Corolario 3.6. *Si K es un cuerpo completo para una valoración discreta y $L|K$ es una extensión finita que induce la extensión $\lambda|\kappa$ en los cuerpos residuales, entonces la mayor subextensión no ramificada (denotada como K^{nr}) tiene como cuerpo residual la clausura separable de la extensión $\lambda|\kappa$.*

Observación 3.7. Esto implica en particular que, en las hipótesis del corolario anterior, la extensión $L|K^{nr}$ es totalmente ramificada.

3.1. Grupos de ramificación

Durante toda la sección siempre se supondrá que K es un cuerpo local para una valoración v, con anillo de valoración A, ideal maximal $\mathfrak{p}$, uniformizante π y cuerpo residual λ; y que $L|K$ es una extensión finita separable. Por la proposición 2.49, L es un cuerpo local para una única valoración w que extiende v. Se denotará como B al anillo de valoración de L, $\mathfrak{q}$ a su ideal maximal, Π a su uniformizante y λ a su cuerpo residual. Por la observación 2.48 existe un elemento $x \in B$ tal que $B = A[x]$.

Proposición 3.8. *Sea K un cuerpo local y $L|K$ una extensión de Galois finita. Si $\sigma \in G = Gal(L|K)$, la aplicación $i_G : G \to \mathbb{Z}$ dada por $\sigma \mapsto w(\sigma(x) - x)$, donde x es un generador de B como $A-$álgebra, satisface:*

1. $w(\sigma(\alpha)-\alpha) \geq i_G(s)$, *para todo* $\alpha \in B$, *y en particular la definición de* i_G *no depende de la elección de* x.

2. $i_G(\sigma\tau^{-1}) \geq \min\{i_G(\sigma), i_G(\tau)\}$ *para todo* $\sigma, \tau \in G$.

3. $i_G(\tau\sigma\tau^{-1}) = i_G(\sigma)$, *para todo* $\sigma, \tau \in G$.

Demostración. Para el primer apartado, sea $\alpha \in B$, como $B = A[x]$, entonces $\alpha = a_0 + a_1 x + \cdots + a_n x^n$, con $a_i \in A$ y $n \in \mathbb{N}$, de modo que para $\sigma \in G$:

$$w(\sigma(\alpha)-\alpha) = w\left(\sigma\left(\sum_{i=0}^{n} a_i x^i\right) - \sum_{i=0}^{n} a_i x^i\right) = w\left(\sum_{i=1}^{n} a_i(\sigma(x)^i - x^i)\right) \geq w(\sigma(x)-x)$$

donde, para la desigualdad se utilizó que $\sigma(x)-x$ divide a $\sigma(x)^i - x^i$ para todo $i \geq 1$. Para el segundo apartado sean $\sigma, \tau \in G$, entonces:

$$w(\sigma\tau^{-1}(x)-x) = w((\sigma\tau^{-1}(x)-\tau^{-1}(x)) - (\tau\tau^{-1}(x)-\tau^{-1}(x))) \geq \min\{i_G(\sigma), i_G(\tau)\}$$

donde se utilizó el primer apartado para la desigualdad. El tercer apartado es inmediato teniendo en cuenta la proposición 3.1 :

$$i_G(\tau\sigma\tau^{-1}) = w(\tau\sigma\tau^{-1}(x)-x) = w(\tau^{-1}(\tau\sigma\tau^{-1}(x)-x)) = w(\sigma(\tau^{-1}(x))-\tau^{-1}(x)) \geq i_G(\sigma)$$

la otra desigualdad se deriva de que $i_G(\sigma) = i_G(\tau^{-1}(\tau\sigma\tau^{-1})(\tau^{-1})^{-1}) \geq i_G(\tau\sigma\tau^{-1})$. □

Lema 3.9. *Sea* $L|K$ *una extensión de Galois y* $G = Gal(L|K)$. *Los subconjuntos* $G_i = \{\sigma \in G \,|\, i_G(\sigma) \geq i+1\}$ *para* $i \geq -1$ *forman una sucesión decreciente de subgrupos normales de* G, *que se estabiliza en* $\{1\}$.

Demostración. El hecho de que los G_i forman una sucesión decreciente de subgrupos normales de G es consecuencia directa de 3.8. Para comprobar que se estabiliza en $\{1\}$, es claro que para $i \geq \max_{\sigma \in G-\{1\}}\{w(\sigma(x)-x)\}$ G_i es trivial, de modo que el resultado se deriva de que la sucesión G_i es decreciente. □

Definición 3.10. El subgrupo $G_i \subset G$ definido en la proposición anterior se denomina el $i-$*ésimo grupo de ramificación de la extensión* $L|K$.

Observación 3.11. Por la proposición 3.1 se deduce que $G = G_{-1}$. Es claro por definición que si H es un subgrupo de G y K' es el subcuerpo de L fijado por H, $i_H(x) = w_L(\sigma(x)-x) = i_G(x)$ para $x \in L$ y $\sigma \in \mathrm{Gal}(L|K') \subset G$, con lo que si H_i representa el $i-$ésimo grupo de ramificación de la extensión $L|K'$, $H_i = G_i \cap H$.

Proposición 3.12. *Si* K *es un cuerpo completo para una valoración discreta y* $L|K$ *es una extensión finita,* $G_0 = Gal(L|K^{nr})$, *donde* K^{nr} *representa la máxima subextensión no ramificada de* $L|K$.

Demostración. En las condiciones de la proposición $\lambda|\kappa$ es de Galois al serlo $L|K$, por la proposición 3.2, de modo que la extensión $K^{nr}|K$ es de Galois, al ser no ramificada por la proposición 3.5. Sea $\overline{\alpha}$ un generador de la extensión $\lambda|\kappa$, B la clausura íntegra de A en K^{nr} y $\alpha \in B$ un representante de $\overline{\alpha}$, de modo que $K^{nr} = K[\alpha]$. Es claro que si $\sigma \in \mathrm{Gal}(L|K^{nr})$, entonces $\sigma(\alpha) = \alpha$, por lo que, $\overline{\sigma}(\overline{\alpha}) = \overline{\alpha}$, vía el homomorfismo definido en 3.2 (de modo que $\overline{\sigma} = 1 \in \mathrm{Gal}(\lambda|\kappa)$). Sea pues $x \in B$, pasando al cuerpo residual λ se obtiene $\overline{\sigma(x) - x} = \overline{\sigma}(\overline{x}) - \overline{x} = 0$, de donde se deduce que $\sigma \in G_0$. Por otro lado, si $\sigma \in G_0$, para ver que $\sigma \in Gal(L|K^{nr})$ basta con comprobar que $\sigma(\alpha) = \alpha$, pero esto es inmediato pues si $\sigma' = \sigma|_{K^{nr}} \in Gal(K^{nr}|K)$, $0 = \overline{\sigma'(\alpha) - \alpha} = \overline{\sigma'}(\overline{\alpha}) - \overline{\alpha}$, con lo que $\overline{\sigma'}(\bar{\alpha}) = \overline{\alpha}$, de modo que $\sigma' = 1 \in \mathrm{Gal}(K^{nr}|K)$, porque como $K^{nr}|K$ es no ramificada, el homomorfismo $\sigma \mapsto \overline{\sigma}$ es un isomorfismo. Consecuentemente $\sigma(\alpha) = \alpha$, y por tanto $\sigma \in \mathrm{Gal}(L|K^{nr})$.

□

Corolario 3.13. *Si K es un cuerpo completo para una valoración discreta y $L|K$ es una extensión finita, $G_{-1}/G_0 = G/G_0 \simeq Gal(\lambda|\kappa)$, donde $\lambda|\kappa$ es la extensión inducida en los cuerpos residuales.*

Demostración. En efecto, $\mathrm{Gal}(\lambda|\kappa) \simeq \mathrm{Gal}(K^{nr}|K) = \mathrm{Gal}(L|K)/\mathrm{Gal}(L|K^{nr}) = G/G_0$. □

Corolario 3.14. *Si $i \geq 0$, los $i-$ésimos grupos de ramificación de una extensión $L|K$ coinciden con los $i-$ésimos grupos de ramificación de la extensión $L|K^{nr}$.*

Observación 3.15. Esto implica que se puede suponer, para el estudio de dichos grupos de ramificación, que la extensión de cuerpos $L|K$ asociada es totalmente ramificada. En particular, se puede suponer, si B y A son los anillos de valoración de L y K respectivamente, que Π es un generador de B como $A-$álgebra (tal y como se vio en la observación 2.46). Esto permite simplificar las condiciones de la proposición 3.8 para estudiar si un elemento de G_0 pertenece a G_i, pues basta con comprobar que $\sigma(\Pi)/\Pi \equiv 1 \mod \mathfrak{q}^i$. Efectivamente, como $w(\sigma(\Pi) - \Pi) \geq i + 1$ se deduce que $w(\sigma(\Pi)/\Pi - 1) \geq i$.

Definición 3.16. Sea $L|K$ una extensión finita, se define el *$i-$ésimo grupo de unidades* de L como $U^{(i)} = B^*$, si $i = 0$ y $U^{(i)} = 1 + \mathfrak{q}^i$ si $i \geq 1$.

Observación 3.17. Los $i-$ésimos grupos de unidades son efectivamente subgrupos de B^*. Para ello sea $i \geq 0$ fijado y $x, y \in U^{(i)}$, de modo que $x = 1 + x'$ e $y = 1 + y'$, con $x', y' \in \mathfrak{q}^i$. Entonces $xy^{-1} - 1 = (1 + x')(1 + y')^{-1} - 1 = (x' - y')(1 + y')^{-1}$, y por tanto $w(x/y - 1) = w(x' - y') \geq \text{ínf}\{w(x'), w(y')\} \geq i$. Además es claro que $U^{(i)} \subset U^{(j)}$ si $j \leq i$.

Proposición 3.18. *El cociente $U^{(i)}/U^{(i+1)}$ es isomorfo al grupo multiplicativo de λ si $i = 0$ y al subgrupo aditivo de λ, si $i \geq 1$.*

Demostración. Si $i = 0$, entonces la aplicación $U^{(0)} \to \lambda^*$ definida como $x \mapsto x \mod \mathfrak{q}$ está bien definida y define un homomorfismo sobreyectivo de grupos, cuyo núcleo es $\{x \in U^{(0)} \mid x \equiv 1 \mod \mathfrak{q}\} = \{x \in U^{(0)} \mid x = 1 + z, z \in \mathfrak{q}\} = U^{(1)}$, de modo que el primer teorema de isomorfía nos permite concluir. Para la segunda parte se define la aplicación $U^{(i)} \mapsto \mathfrak{q}^i/\mathfrak{q}^{i+1}$ como $x \mapsto x - 1$

mód $\mathfrak{q}^{i+1}$, que es un homomorfismo de grupos sobreyectivo cuyo núcleo coincide con $U^{(i+1)}$. En efecto, si $x, y \in \mathfrak{q}^i$, $(1+x)(1+y) = 1+x+y+xy \equiv 1+x+y \mod \mathfrak{q}^{i+1}$. Finalmente, $\mathfrak{q}^i/\mathfrak{q}^{i+1}$ es un $\lambda-$espacio vectorial de dimensión 1 generado por la clase de Π^i, y entonces isomorfo a λ. □

Observación 3.19. Si $i, j \geq 0$, $x \in \mathfrak{q}^i$ y $y \in \mathfrak{q}^j$, la operación $(x \mod \mathfrak{q}^{i+1})(y \mod \mathfrak{q}^{j+1}) = xy$ mód $\mathfrak{q}^{i+j+1}$ define una multiplicación en $G(A) = \bigoplus_{i\geq 0} \mathfrak{q}^i/\mathfrak{q}^{i+1}$ que la convierte en una $\lambda-$álgebra graduada (en el sentido de [AM, págs. 124-125]). En efecto es claro que $xy \in \mathfrak{q}^{i+j}$, de modo que para comprobar que está bien definida, basta con ver que no depende de los representantes escogidos, sean pues $z \in \mathfrak{q}^{i+1}$, $z' \in \mathfrak{q}^{j+1}$, entonces $(x+z)(y+z') = xy + xz' + yz + zz' \equiv xy$ mód $\mathfrak{q}^{i+j+1}$.

Proposición 3.20. *Si $i \geq 0$, la aplicación $\theta_i : G_i \to U^{(i)}/U^{(i+1)}$ definida como $\sigma \mapsto \sigma(\Pi)/\Pi$ mód $U^{(i+1)}$ induce un homomorfismo inyectivo de G_i/G_{i+1} a $U^{(i)}/U^{(i+1)}$ que es independiente de la elección de uniformizante.*

Demostración. Veamos que dicha aplicación está bien definida, dado que $\sigma \in G_i$, $\sigma(\Pi) = \Pi + \Pi^{i+1}x$, con $x \in B$, de modo que $\sigma(\Pi)/\Pi = 1 + \Pi^i x \in U^{(i)}$. Para comprobar que no depende de la elección de uniformizante, sea Π' otro uniformizante de B, de modo que $\Pi' = u\Pi$, con $u \in B^*$, y por tanto $\sigma(\Pi')/\Pi' = (\sigma(\Pi)/\Pi)\ (\sigma(u)/u)$. Pero, como $\sigma \in G_i$, $\sigma(u) \equiv u \mod \mathfrak{q}^{i+1}$, con lo que existe un elemento $x \in B$ tal que $\sigma(u) = u + x\Pi^{i+1}$, o equivalentemente, $\sigma(u)/u = 1 + u^{-1}x\Pi^{i+1} \equiv 1 \mod U^{(i+1)}$. Para comprobar que es un homomorfismo, sean $\sigma, \tau \in G_i$, esto implica que $u = \tau(\Pi)/\Pi \in U^{(i+1)}$, y por tanto $u \equiv 1 \mod \mathfrak{q}^{i+1}$. En consecuencia:

$$\frac{\sigma\tau(\Pi)}{\Pi} = \frac{\sigma\tau(\Pi)}{\sigma(\Pi)}\frac{\Pi}{\tau(\Pi)}\frac{\sigma(\Pi)}{\Pi}\frac{\tau(\Pi)}{\Pi} = \frac{\sigma(u)}{u}\frac{\sigma(\Pi)}{\Pi}\frac{\tau(\Pi)}{\Pi} = \frac{\sigma(\Pi)}{\Pi}\frac{\tau(\Pi)}{\Pi} \in U^{(i)}/U^{(i+1)}$$

Además, $\ker(\theta_i) = \{\sigma \in G_i \,|\, \sigma(\Pi)/\Pi \in U^{(i+1)}\} = \{\sigma \in G_i \,|\, \sigma(\Pi)/\Pi \equiv 1 \mod \mathfrak{q}^{i+1}\} = G_{i+1}$. Con lo que el primer teorema de isomorfía nos asegura que existe un isomorfismo entre G_i/G_{i+1} y $\mathrm{Im}(\theta_i) \subset U^{(i)}/U^{(i+1)}$. □

Observación 3.21. Dado que $U^{(i)}/U^{(i+1)} \simeq \mathfrak{q}^i/\mathfrak{q}^{i+1}$ si $i > 0$, se denotará indistintamente a la imagen de un elemento $\overline{\sigma} \in G_i/G_{i+1}$ por la aplicación θ_i como $\sigma(\Pi)/\Pi \equiv 1+x \mod U^{(i+1)} \equiv x$ mód $\mathfrak{q}^{i+1}$, siendo $x \in \mathfrak{q}^i$ el (único) elemento tal que $\sigma(\Pi)/\Pi = 1 + x$, siendo σ un representante de $\overline{\sigma}$ en G_i.

Corolario 3.22. *El cociente G_0/G_1 es cíclico, y su orden es coprimo con la característica de λ.*

Demostración. Dado que el subgrupo de G_0/G_1 es finito y $U^{(0)}/U^{(1)} \simeq \lambda^*$, la imagen de θ_i, al corresponderse con un subgrupo finito del grupo multiplicativo de λ (que es finito al ser L local, y por tanto cíclico) es finito. Dado que $|G_0/G_1|$ divide a $|\lambda^*| = p-1$, por el teorema de Lagrange, es claro que es coprimo con $p =$car(K).

□

Corolario 3.23. *El grupo G_1 es un $p-$grupo, donde p es la característica de λ.*

Demostración. Para cada $i \geq 1$, el cociente $U^{(i)}/U^{(i+1)}$ es isomorfo a λ, de modo que como λ es finito de característica p, su orden es una potencia de p. Así, para G_i/G_{i+1}, al ser isomorfo a un subgrupo de $U^{(i)}/U^{(i+1)}$, su orden será también una potencia de p. Si i denota el menor índice tal que $G_i = \{1\}$, dado que $|G_1| = |G_1/G_2||G_2/G_3|\dots|G_{i-1}/G_i||G_i|$, es claro que G_1 es un $p-$grupo. □

Proposición 3.24. *Si $\sigma \in G_0$ y $\tau \in G_i$, con $i \geq 1$, y $\overline{\sigma}$, $\overline{\tau}$ denotan sus representantes en G_0/G_1 y G_i/G_{i+1} respectivamente, entonces $\theta_i(\overline{\sigma\tau\sigma^{-1}}) = \theta_0(\overline{\sigma})^i\theta_i(\overline{\tau})$, donde $\theta_0(\overline{\sigma})$ y $\theta_i(\overline{\tau})$ son considerados como elementos del $\lambda-$álgebra $G(A)$ definida en la observación 3.19.*

Demostración. Dado que G_i es un subgrupo normal de $G = \mathrm{Gal}(L|K)$, si tomamos $\sigma \in G_0$ y $\tau \in G_i$, es claro que $\sigma\tau\sigma^{-1} \in G_i$, de modo que la igualdad del enunciado de la proposición tiene sentido. Sea Π un uniformizante de B y sea $\Pi' = \sigma^{-1}(\Pi)$, es claro que Π' es un uniformizante de B, de modo que si $\tau \in G_i$, se cumple que $\tau(\Pi') = \Pi'(1+x)$, siendo $x \in \mathfrak{q}^i$, y por tanto $\theta_i(\overline{\tau}) = x \mod \mathfrak{q}^{i+1}$. Esto implica que $\sigma\tau\sigma^{-1}(\Pi) = \sigma\tau(\Pi') = \sigma(\Pi'(1+x)) = \Pi(1+\sigma(x))$, con lo que $\theta_i(\overline{\sigma\tau\sigma^{-1}}) = \sigma(x) \mod \mathfrak{q}^{i+1}$. Dado que $x \in \mathfrak{q}^i$, $x = y\Pi^i$ para $y \in B$, y como $\sigma(\Pi)$ es un uniformizante de B existe una unidad $u \in B^*$ tal que $\sigma(\Pi) = u\Pi$, cuya clase $\overline{u} \in \lambda$ cumplirá que $\theta_0(\overline{\sigma}) = \overline{u}$. De este modo podemos expresar $\sigma(x) = \sigma(y\Pi^i) = \sigma(y)u^i\Pi^i$. Como $\sigma \in G_0$, $\sigma(y) \equiv y \mod \mathfrak{q}$, entonces $\theta_i(\overline{\sigma\tau\sigma^{-1}}) = \sigma(x) \mod \mathfrak{q}^{i+1} = \sigma(y)u^i\Pi^i \mod \mathfrak{q}^{i+1} = (\sigma(y)u^i \mod \mathfrak{q})(\Pi^i \mod \mathfrak{q}^{i+1}) = (yu^i \mod \mathfrak{q})(\Pi^i \mod \mathfrak{q}^{i+1}) = (u \mod U^{(1)})^i(y\Pi^i \mod \mathfrak{q}^{i+1}) = \theta_0(\overline{\sigma})^i\theta_i(\overline{\tau})$, como queríamos probar. □

Corolario 3.25. *Sea $\sigma \in G_0$ y $\tau \in G_i$, para $i \geq 1$. Entonces el conmutador $\sigma\tau\sigma^{-1}\tau^{-1}$ pertenece a G_{i+1} si y solo si $\sigma^i \in G_1$ o $\tau \in G_{i+1}$.*

Demostración. Si $\tau \in G_{i+1}$, entonces $(\sigma\tau\sigma^{-1})\tau^{-1} \in G_{i+1}$, ya que G_{i+1} es normal en G. Si $\tau \notin G_{i+1}$, la condición dada por el enunciado es equivalente a que la clase de $\sigma\tau\sigma^{-1}$ en G_i/G_{i+1} coincida con la de τ, que a su vez es equivalente a que $\theta_i(\overline{\sigma\tau\sigma^{-1}}) = \theta_i(\overline{\tau})$, dada la inyectividad de la aplicación θ_i. Ahora bien, por la proposición anterior $\theta_i(\overline{\sigma\tau\sigma^{-1}}) = \theta_0(\overline{\sigma})^i\theta_i(\overline{\tau}) = \theta_i(\overline{\tau})$ si y solo si $\theta_0(\overline{\sigma})^i = \theta_0(\overline{\sigma^i}) = 1$, lo cual es equivalente a que $\sigma^i \in G_1$, como queríamos probar. □

Corolario 3.26. *Sea K un cuerpo local y $L|K$ una extensión finita y abeliana. Si r es el orden de G_0/G_1 entonces $G_i = G_{i+1}$ para todo número no divisible por r.*

Demostración. Dado que la inclusión $G_{i+1} \subset G_i$ es general, sea $\tau \in G_i$ y $\sigma \in G_0$ tal que su clase en G_0/G_1 sea un generador de dicho grupo, que es cíclico por la proposición 3.22. Dado que G es abeliano, el conmutador $\sigma\tau\sigma^{-1}\tau^{-1} = 1 \in G_{i+1}$. Así, dado que $\sigma^i \notin G_1$ (ya que i no es divisible por r), el corolario anterior implica que $\tau \in G_{i+1}$. □

Lema 3.27. *Sean $i, j \geq 1$ y $\sigma \in G_i$ y $\tau \in G_j$, entonces $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j}$ y $\theta_{i+j}(\sigma\tau\sigma^{-1}\tau^{-1}) = (j-i)\theta_i(\overline{\sigma})\theta_j(\overline{\tau})$, donde $\theta_i(\overline{\sigma})$ y $\theta_j(\overline{\tau})$ son considerados como elementos de $G(A)$.*

Demostración. Sea $\sigma(\Pi) = \Pi(1+x)$ y $\tau(\Pi) = \Pi(1+y)$, siendo $x \in \mathfrak{q}^i$ e $y \in \mathfrak{q}^j$, con lo que $\theta_i(\overline{\sigma}) = x \mod \mathfrak{q}^{i+1}$ y $\theta_j(\overline{\tau}) = y \mod \mathfrak{q}^{j+1}$. De este modo se tiene que $\sigma\tau(\Pi) = \sigma(\Pi)(1+\sigma(y)) =$

$\Pi(1+x)(1+\sigma(y)) = \Pi(1+z)$, donde $z = x+\sigma(y)+x\sigma(y)$ y que $\tau\sigma(\Pi) = \Pi(1+y)(1+\tau(x)) = \Pi(1+t)$, con $t = y+\tau(x)+y\tau(x)$. Sean $a, b \in B$ tales que $x = a\Pi^i$, $y = b\Pi^j$, entonces $\sigma(y) = \sigma(b)\sigma(\Pi^i) = \sigma(b)\sigma(\Pi)^i = \sigma(b)\Pi^i(1+x)^i$. Como $\sigma \in G_i$ se cumple que $\sigma(b) \equiv b \mod \mathfrak{q}^{i+1}$ y además $(1+x)^j \equiv 1+jx$, donde se ha usado el binomio de Newton, junto con el hecho de que $x \in \mathfrak{q}^i$. Esto implica, usando la expresión de la multiplicación en $G(A)$, que $\sigma(y) \equiv b\Pi^j(1+jx) = y+jxy$, y consecuentemente $z \equiv x+y+(j+1)xy \mod \mathfrak{q}^{i+j+1}$ y $t \equiv x+y+(i+1)xy$ mód $\mathfrak{q}^{i+j+1}$. Ahora necesitamos una expresión de $\theta_{i+j}(\overline{\sigma\tau\sigma^{-1}\tau^{-1}})$, sea para ello el uniformizante $\Pi' = \tau\sigma(\Pi) = \Pi(1+t)$, luego $\sigma\tau\sigma^{-1}\tau^{-1}(\Pi') = \sigma\tau(\Pi) = \Pi(1+z) = \Pi'(1+z)(1+t)^{-1} = \Pi'(1+s)$, con $s = (z-t)(1+t)^{-1} \equiv ((1+t)^{-1} \mod U^{(1)})(z-t \mod \mathfrak{q}^{i+j+1}) \equiv (j-i)xy \mod \mathfrak{q}^{i+j+1}$, donde se usaron las expresiones de z, t módulo $\mathfrak{q}^{i+j+1}$ y el hecho de que $1+t \in U^{(1)}$. Con esto podemos concluir pues, como $xy \in \mathfrak{q}^{i+j}$, lo anterior nos permite asegurar que $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j}$, y además $\theta_{i+j}(\overline{\sigma\tau\sigma^{-1}\tau^{-1}}) = s \mod \mathfrak{q}^{i+j+1} = (j-i)xy \mod \mathfrak{q}^{i+j+1} = (j-i)(x \mod \mathfrak{q}^{i+1})(y \mod \mathfrak{q}^{j+1}) = (j-i)\theta_i(\overline{\sigma})\theta_j(\overline{\tau})$, como queríamos probar. □

Corolario 3.28. *Los enteros $i \geq 1$ tales que $G_i \neq G_{i+1}$ pertenecen a la misma clase módulo p, siendo p la característica de λ.*

Demostración. Si $G_1 = 1$ el resultado es trivialmente cierto, así que sea j el mayor entero positivo que cumple que $G_j \neq 1$. Sea i un número entero donde se produce un cambio en los grupos de ramificación, $G_i \neq G_{i+1}$, y sean $\sigma \in G_i - G_{i+1}$, $\tau \in G_j - \{1\}$. Por el lema anterior, $\sigma\tau\sigma^{-1}\tau^{-1} = 1$, y por tanto $\theta_{i+j}(\overline{\sigma\tau\sigma^{-1}\tau^{-1}}) = 0$ ya que el conmutador pertenece a $G_{i+j} \subset G_{j+1} = \{1\}$. Pero como $\theta_i(\sigma)$ y $\theta_j(\tau)$ no son cero (vistos como elementos de $\mathfrak{q}^i/\mathfrak{q}^{i+1}$), solo queda la posibilidad de que $j-i = 0 \mod \mathfrak{q}^{i+j}$, que solo puede suceder si $j-i \equiv 0 \mod p$, siendo p la característica de λ. □

Corolario 3.29. *Si i, j son enteros mayores que 1, y $\sigma \in G_i$, $\tau \in G_j$, entonces el conmutador $\sigma\tau\sigma^{-1}\tau^{-1}$ pertenece a G_{i+j+1}.*

Demostración. Si $\sigma \in G_{i+1}$ o si $\tau \in G_{j+1}$ el corolario está probado. Si no, por el corolario anterior $i \equiv j \mod p$ (ya que en ambos casos se producirían saltos en los grupos de ramificación), y por el lema 3.27, $\theta_{i+j}(\sigma\tau\sigma^{-1}\tau^{-1}) = 0$, con lo que $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j+1}$. □

3.2. Módulo de diferenciales de Kähler. Diferente de una extensión

Definición 3.30. Sea A un anillo, B una $A-$álgebra y M un $B-$módulo. Una $A-$derivación D de B en M es una aplicación aditiva $D : B \to M$ que cumple:

1. $D(a) = 0$, para todo $a \in A \subset B$
2. (Regla de Leibniz) $D(bb') = bD(b') + b'D(b)$, para todo $b, b' \in B$

Observación 3.31. El conjunto de todas las derivaciones de B en M, $\mathrm{Der}_A(B,M)$, tiene una estructura de $B-$módulo dada por las operaciones $(D+D')(b) = D(b)+D'(b)$, $(bD)b' = bD(b')$ para $D, D' \in \mathrm{Der}_A(B,M)$ y $b, b' \in B$. Las dos condiciones de la definición anterior implican que toda $A-$derivación entre una $A-$álgebra B y un $B-$módulo es un homomorfismo de $A-$módulos. Además, si $f : A \to A'$ es un homomorfismo de anillos y B es un $A'-$álgebra, entonces toda $A-$derivación D entre B y un $B-$módulo M es una $A'-$derivación si y solo si $D(a') = 0$ para todo $a' \in A'$ (por definición, pues la regla de Leibniz sigue cumpliéndose en ambos casos).

Proposición 3.32. *Sean A, B, C anillos*

1. *Sean $A \to B$, $A \to C$ dos homomorfismos de anillos y M un $B-$módulo, entonces $Der_B(B \otimes_A C, M) \simeq Der_A(C, M)$*

2. *Sea $A \to B$ un homomorfismo de anillos, T un subconjunto multiplicativo de B y M un $T^{-1}B-$módulo, entonces $Der_A(T^{-1}B, M) \simeq Der_A(B, M)$*

Demostración. Para el primer apartado basta con comprobar si el homomorfismo definido por restricción $\varphi : \mathrm{Der}_B(B \otimes_A C, M) \to \mathrm{Der}_A(C, M)$; $\varphi(D)(c) = D(1 \otimes c)$, para $c \in C$, es un isomorfismo, pero esto es inmediato, pues dada $D \in \mathrm{Der}_A(C, M)$ se puede extender por linealidad (y de modo único) a $\mathrm{Der}_B(B \otimes_A C, M)$ mediante $D'(b \otimes c) = bD(c)$, para $b \in B$, $c \in C$.

Para el segundo apartado comprobaremos también si el homomorfismo dado por restricción $\varphi : \mathrm{Der}_A(T^{-1}B, M) \to \mathrm{Der}_A(B, M)$, $\varphi(D)(b) = D(b/1)$, para $b \in B$ es un isomorfismo. Sea $D \in \mathrm{Der}_A(B, M)$, veamos que se extiende de modo único a una $A-$derivación $D' \in \mathrm{Der}_A(T^{-1}B, M)$. Se define $D' : T^{-1}B \to M$ como:

$$D'\left(\frac{b}{t}\right) = \frac{D'(b)t - bD'(t)}{t^2}$$

Es claro que D' satisface la regla de Leibniz, y $D'|_B = D$, por lo que define una $A-$derivación de $T^{-1}B$ a M. Para demostrar su unicidad basta con ver que, si existiese otra extensión $D'' \in \mathrm{Der}_A(T^{-1}B, M)$, para $b \in B$, $t \in T$:

$$D(t)\frac{b}{t} + tD'\left(\frac{b}{t}\right) = D'\left(\frac{b}{t}t\right) = D'(b) = D''(b) = D''\left(\frac{b}{t}t\right) = D(t)\frac{b}{t} + tD''\left(\frac{b}{t}\right),$$

con lo que $D'(b/t) = D''(b/t)$, como queríamos probar. □

Sea A un anillo, B una $A-$álgebra y $C = B \otimes_A B$, entonces, por la propiedad universal del producto tensorial, la aplicación $\varepsilon : C \to B$ definida como $x \otimes y \mapsto xy$ está bien definida y es un homomorfismo de $A-$módulos. Además, el homomorfismo $B \to C$ definido como $x \mapsto x \otimes 1$ hace de C un $B-$módulo de modo natural.

Definición 3.33. Sea A un anillo, B una $A-$álgebra y $C = B \otimes_A B$, se define el *módulo de diferenciales (de Kähler)* de B sobre A como el $B-$módulo $\Omega_{B|A} = I/I^2$, donde $I = \ker \varepsilon$, siendo $\varepsilon : B \to C$ el homomorfismo anterior a C, visto como $B-$módulo.

Proposición 3.34. *Sea A un anillo y B un $A-$módulo. Entonces la aplicación $d : B \to \Omega_{B|A}$ definida como $b \mapsto b \otimes 1 - 1 \otimes b + I^2$ es una $A-$derivación de B sobre $\Omega_{B|A}$. Además $\Omega_{B|A}$ está generado por $\{db \,|\, b \in B\}$ como $B-$módulo.*

Demostración. Dicha aplicación está bien definida, pues $\varepsilon(1\otimes b - b\otimes 1) = b - b = 0$, y es inmediato comprobar que se trata un homomorfismo de $A-$módulos. Para comprobar que verifica la regla de Leibniz basta ver que:

$$\begin{aligned} &d(bb') = 1 \otimes bb' - bb' \otimes 1 + I^2 = (1 \otimes b - b \otimes 1)(b' \otimes 1) + (b \otimes 1)(1 \otimes b' - b' \otimes 1) + \\ &+ (1 \otimes b - b \otimes 1)(1 \otimes b' - b' \otimes 1) + I^2 = (1 \otimes b - b \otimes 1)(b' \otimes 1) + (b \otimes 1)(1 \otimes b' - b' \otimes 1) + I^2 \\ &= b'd(b) + bd(b'), \end{aligned}$$

donde para la última igualdad se usó explicitamente la estructura de $B-$módulo de C. Para comprobar la segunda parte sea $\sum_i x_i \otimes y_i \in I$, entonces $\varepsilon(\sum_i x_i \otimes y_i) = \sum_i x_i y_i = 0$, de modo que:

$$\sum_i x_i \otimes y_i = \sum_i x_i \otimes y_i - \left(\sum_i x_i y_i \right) \otimes 1 = \sum_i x_i \otimes y_i - \sum_i x_i y_i \otimes 1 = \sum_i (x_i \otimes 1)(1 \otimes y_i + y_i \otimes 1),$$

y por tanto $\sum_i x_i \otimes y_i + I^2 = \sum_i x_i dy_i$. En consecuencia $\{1 \otimes x - x \otimes 1 \,|\, x \in B\}$ es un conjunto de generadores de I como $B-$módulo y así $\{dx \,|\, x \in B\}$ es un conjunto de generadores de $\Omega_{B|A}$ como $B-$módulo, como queríamos probar. □

Observación 3.35. En lo posterior, la aplicación d se denotará como $d_{B|A} \in \mathrm{Der}_A(B, \Omega_{B|A})$ cuando se quiera hacer explícito a dónde pertenezca.

Proposición 3.36. *Sea A un anillo, B una $A-$álgebra, entonces el par (Ω_B, d) satisface que, para todo $B-$módulo M y para toda $A-$derivación $D : B \to M$ existe un único homomorfismo de $B-$módulos $f : \Omega_{B|A} \to M$ tal que $D = f \circ d$. De este modo se tiene el isomorfismo de $B-$módulos $Hom_B(\Omega_{B|A}, M) \simeq Der_A(B, M)$.*

Demostración. Sea M un $B-$módulo y $D : B \to M$ una $A-$derivación de B en M. Se define el homomorfismo de $B-$módulos $\theta : B \otimes_A B \to M$ como $\theta(b \otimes b') = bD(b')$. Dado que para $x, y \in B$:

$$\theta((1\otimes x - x\otimes 1)(1\otimes y - y\otimes 1)) = \theta(1\otimes xy - x\otimes y - y\otimes x + xy\otimes 1) = D(xy) - xD(y) - yD(x) + xyD(1) = 0,$$

donde para la última igualdad se usó la regla de Leibniz y el hecho de que D es una $A-$derivación. De este modo $\theta(I^2) = 0$, y por tanto $\theta|_I$ induce un homomorfismo de $B-$módulos $f : \Omega_{B|A} \to M$ dado por $f(dy) = \theta(1\otimes y - y\otimes 1) = D(y) - yD(1) = D(y)$, como queríamos probar. La unicidad de f se deduce de que es un homomorfismo de $B-$módulos definido en un conjunto de generadores. Por otro lado, es claro que si $f : M \to N$ es un homomorfismo de $B-$módulos y $D : B \to M$ es una $A-$derivación, la aplicación $f \circ D : B \to N$ es una $A-$derivación de B en N, de modo que la aplicación $\mathrm{Hom}_B(\Omega_{B|A}, M) \to \mathrm{Der}_A(B, M)$ dada por $f \to f \circ d$ está bien definida y es un isomorfismo de $B-$módulos, por el razonamiento anterior.

□

Proposición 3.37. *[Mat, th. 57] Sean $A \xrightarrow{h} B \xrightarrow{g} C$ homomorfismos de anillos. Entonces existe una sucesión exacta de $C-$módulos:*

$$\Omega_{B|A} \otimes_B C \to \Omega_{C|A} \to \Omega_{C|B} \to 0$$

Demostración. Definimos los homomorfismos de $C-$módulos $\Omega_{B|A} \otimes_B C \xrightarrow{u} \Omega_{C|A} \xrightarrow{v} \Omega_{C|B}$ como $u(d_{B|A}(b) \otimes c) = cd_{C|A}(g(b))$ y $v(d_{C|A}(c)) = d_{C|B}(c)$. Es claro que la aplicación v es sobreyectiva (pues lleva un conjunto de generadores en un conjunto de generadores), de modo que para comprobar su exactitud, por [AM, prop. 2.9], basta comprobar la exactitud de:

$$0 \to \mathrm{Hom}_C(\Omega_{C|B}, M) \xrightarrow{\overline{v}} \mathrm{Hom}_C(\Omega_{C|A}, M) \xrightarrow{\overline{u}} \mathrm{Hom}_C(\Omega_{B|A} \otimes_B C, M) \simeq \mathrm{Hom}_B(\Omega_{B|A}, M),$$

siendo M un $C-$módulo y $\overline{u}, \overline{v}$ homomorfismos de $C-$módulos definidos como $\overline{u}(f) = f \circ u$, $\overline{v}(f) = f \circ v$. Comprobar la exactitud de la sucesión anterior, por el isomorfismo natural dado en la proposición 3.36, es equivalente a comprobar la exactitud de la exactitud inducida en derivaciones:

$$0 \to \mathrm{Der}_B(C, M) \xrightarrow{\widehat{v}} \mathrm{Der}_A(C, M) \xrightarrow{\widehat{u}} \mathrm{Der}_A(B, M)$$

donde $\widehat{u}(D) = \widehat{u}(f \circ d_{C|A}) = \overline{u}(f) \circ d_{C|A} = (f \circ u) \circ d_{C|A} = f \circ d_{C|A} \circ g = D \circ g$, siendo $D \in \mathrm{Der}_A(C, M)$ y $f \in \mathrm{Hom}_C(\Omega_{C|A}, M)$ es el homomorfismo inducido por D. La expresión de la aplicación $\widehat{v}$ es análoga, y se comprueba que para $D = f \circ d_{C|B} \in \mathrm{Der}_B(C, M)$ se cumple que $\widehat{v}(D) = \overline{v}(f) \circ d_{C|A} = (f \circ v) \circ d_{C|A}$, que por la expresión del homomorfismo v es la aplicación de restricción de escalares, que envía cada derivación $D \in \mathrm{Der}_B(C, M)$ a la misma derivación, vista como elemento de $\mathrm{Der}_A(C, M)$. Dicha sucesión es exacta pues, como se vio en la observación 3.31, una $A-$derivación es una $B-$derivación si y solo si la aplicación D restringida a B es trivial. De modo que la sucesión $\Omega_{B|A} \otimes_B C \to \Omega_{C|A} \to \Omega_{C|B} \to 0$ definida anteriormente es exacta, como queríamos probar.

□

Proposición 3.38. *[Mat, th. 58] Sean $A \xrightarrow{f} B \xrightarrow{g} C$ homomorfismos de anillos, siendo g sobreyectivo. Entonces, si $I = \ker g$, existe una sucesión exacta de $C-$módulos:*

$$I/I^2 \xrightarrow{u} \Omega_{B|A} \otimes_B C \xrightarrow{v} \Omega_{C|A} \to 0$$

dada por $u : x + I^2 \mapsto d_{B|A}x \otimes 1$ y $v : d_{B|A}x \otimes c \mapsto cd_{C|A}(g(x))$

Demostración. La segunda flecha está bien definida y es un homomorfismo de $C-$módulos por la proposición 3.37 que además es sobreyectivo (dado que g lo es). Veamos que la primera flecha está bien definida, consideremos la composición:

$$I \hookrightarrow B \xrightarrow{d} \Omega_{B|A} \to \Omega_{B|A} \otimes_B C \simeq \Omega_{B|A}/I\Omega_{B|A}$$

donde se utilizó para la última igualdad que $C \simeq B/I$, por el primer teorema de isomorfía y [AM, ej. 2.2]. La composición anterior está bien definida y es un homomorfismo de $B-$módulos.

Efectivamente, la aditividad es inmediata y se deduce de la aditividad de d, así que sea $b \in B$. Entonces se cumple que $d(bx)+I\Omega_{B|A} = bdx+xdb+I\Omega_{B|A} = bdx+I\Omega_{B|A}$. Además es inmediato comprobar que dicho homomorfismo se anula en I^2, de modo que induce el homomorfismo de $C-$módulos $I/I^2 \to \Omega_{B|A} \otimes_B C$, $x + I^2 \mapsto dx \otimes 1$, que coincide con el del enunciado de la proposición.

Para comprobar que la sucesión anterior es exacta, basta comprobar la exactitud de:

$$0 \to \mathrm{Hom}_C(\Omega_{C|A}, M) \xrightarrow{\overline{v}} \mathrm{Hom}_C(\Omega_{B|A} \otimes_B C, M) = \mathrm{Hom}_B(\Omega_{B|A}, M) \xrightarrow{\overline{u}} \mathrm{Hom}_C(I/I^2, M).$$

donde M es un $C-$módulo. Ahora bien, $\mathrm{Hom}_C(I/I^2, M) = \mathrm{Hom}_C(I \otimes_B C, M) = \mathrm{Hom}_B(I, M)$. Por la proposición 3.36, la sucesión anterior es exacta si y solo si lo es la sucesión inducida en derivaciones:

$$0 \to \mathrm{Der}_A(C, M) \xrightarrow{\widehat{v}} \mathrm{Der}_A(B, M) \xrightarrow{\widehat{u}} \mathrm{Hom}_B(I, M),$$

donde $\widehat{v} : D \mapsto D \circ g$, como se vio en la demostración de la proposición 3.37. La aplicación $\widehat{u}$ coincide con la restricción $D \mapsto D|_I$, de donde se sigue la exactitud buscada. Este hecho se deduce de que, una vez hecha la identificación $\mathrm{Hom}_C(I/I^2, M) = \mathrm{Hom}_B(I, M)$, la expresión del homomorfismo de $B-$módulos $\overline{u}$ es $f \mapsto f \circ d_{B|A} \circ j$, donde $j : I \hookrightarrow B$, de donde se deriva que el homomorfismo inducido en derivaciones tiene la forma $D = f \circ d_{B|A} \mapsto D \circ j = D|_I$, como queríamos probar.

□

Proposición 3.39 (Cambio de base)**.** *Sean $A \to B$ y $A \to C$ homomorfismos de anillos. Entonces existe un isomorfismo de $B \otimes_A C-$módulos $\Omega_{B|A} \otimes_A C \simeq \Omega_{B\otimes_A C|C}$.*

Demostración. Definimos la aplicación $u : \Omega_{B|A} \otimes_A C \to \Omega_{B\otimes_A C|C}$ como $b'd_{B|A}(b) \otimes c \mapsto (b' \otimes 1)d_{B\otimes_A C|C}(b\otimes c)$. Dicha aplicación está bien definida y es un homomorfismo de $B\otimes_A C-$módulos: en efecto, la aditividad es evidente, y además $u((b'\otimes c')(d_{A|B}(b)\otimes c)) = (b'\otimes 1)d_{B\otimes_A C|C}(b\otimes cc') = (b' \otimes 1)d_{B\otimes_A C|C}((b \otimes c)(1 \otimes c')) = (b' \otimes c')d_{B\otimes_A C|C}(b \otimes c) + (b'b \otimes c)d_{B\otimes_A C|C}(1 \otimes c') = (b' \otimes c')d_{B\otimes_A C|C}(b \otimes c)$. Para comprobar que es un isomorfismo basta con demostrar que la aplicación inducida $\mathrm{Hom}_{B\otimes_A C}(\Omega_{B\otimes_A C|C}, M) \to \mathrm{Hom}_{B\otimes_A C}(\Omega_{B|A} \otimes_B (B \otimes_A C), M) = \mathrm{Hom}_B(\Omega_{B|A}, M)$ (donde M es un $B \otimes_A C-$módulo) es un isomorfismo. Esto es equivalente a que la aplicación inducida en las derivaciones es un isomorfismo. No obstante, es inmediato comprobar que esta aplicación coincide con el isomorfismo φ definido en la demostración de la proposición 3.32 (1), lo cual nos permite concluir. □

Proposición 3.40 (Localización)**.** *Sea $\varphi : A \to B$ un homomorfismo de anillos y $S \subset A$, $T \subset B$ subconjuntos multiplicativos tales que $\varphi(S) \subset T$. Entonces $\Omega_{T^{-1}B|S^{-1}A} = T^{-1}\Omega_{B|A}$*

Demostración. Definimos la aplicación $v : \Omega_{T^{-1}B|A} \to T^{-1}\Omega_{B|A}$ como $d(b/t) \mapsto t^{-2}(bdt - td(b))$. Es claro que dicha aplicación es un homomorfismo de $T^{-1}B-$módulos. Para comprobar que es un isomorfismo basta ver que la aplicación inducida $\mathrm{Hom}_{T^{-1}B}(T^{-1}\Omega_{B|A}, M) \to$

$\mathrm{Hom}_{T^{-1}B}(\Omega_{T^{-1}B|A}, M)$ (donde M es un $T^{-1}B-$módulo) es un isomorfismo o equivalentemente, que la aplicación inducida en derivaciones es un isomorfismo, lo cual se cumple por la proposición 3.32. Dado que $\Omega_{T^{-1}B|A} \simeq T^{-1}\Omega_{B|A}$, si probamos que $\Omega_{T^{-1}B|A} = \Omega_{T^{-1}B|S^{-1}A}$, [1] la proposición estará demostrada. Para ello basta ver que, como $\Omega_{S^{-1}A|A} = 0$ (basta aplicar lo anterior tomando $B = A$, y teniendo en cuenta que como $\mathrm{Der}_A(A, M) = 0$ para todo $A-$módulo M, $\Omega_{S^{-1}A|A} = 0$), la sucesión exacta de la proposición 3.37, aplicada a $A \to S^{-1}A \to T^{-1}B$, sería $0 = \Omega_{S^{-1}A|A} \otimes_{S^{-1}A} B \to \Omega_{B|A} \to \Omega_{B|S^{-1}A} \to 0$, y por ello se deduce $\Omega_{B|A} = \Omega_{B|S^{-1}A}$, como queríamos probar. □

Proposición 3.41. *Sea A un anillo, entonces si B es el anillo de polinomios $A[X_1, \cdots, X_n]$, el $B-$módulo $\Omega_{B|A}$ es un $B-$módulo libre finitamente generado.*

Demostración. La aplicación $B \to B^{(n)}$, $f \mapsto (\partial_i f)_{i=1}^n$, donde ∂_i denota la derivada usual con respecto a la variable $i-$ésima, es una $A-$derivación, de modo que induce, por la proposición 3.36, un homomorfismo de $B-$módulos $\varphi : \Omega_{B|A} \to B^{(n)}$ dado por $df \mapsto (\partial_i f)_{i=1}^n$, veamos que dicha aplicación es un isomorfismo. Es inmediato comprobar que es sobreyectiva, pues $\{\varphi(dX_i)\}$ es una base de $B^{(n)}$ (es de hecho la canónica). Por otro lado sea $\psi : B^{(n)} \to \Omega_{B|A}$ definida como $(f_i)_i \mapsto \sum_i f_i dX_i$, es claro que dicha aplicación es un homomorfismo de $B-$módulos y que $\varphi \circ \psi = \mathrm{Id}_{B^{(n)}}$, veamos que $\psi \circ \varphi = \mathrm{Id}_{\Omega_{B|A}}$. Basta probar que $df = \sum_i (\partial_i f) dX_i$, para ello basta comprobar que la aplicación $d' : B \mapsto \Omega_{B|A}$ $f \mapsto \sum_i (\partial_i f) dX_i$ coincide con la derivación natural $d : B \to \Omega_{B|A}$. Es inmediato comprobar que d' es una $A-$derivación, usando el hecho de que ∂_i es una A derivación de B en B para todo $i = 1, \ldots, n$, que $d(X_j^i) = iX^{i-1} dX_j$ y que $d(X_i) = d'(X_i)$, de modo que $d = d'$, al coincidir en la base $\{X_i^t\}_{\substack{i=1,\ldots,n \\ t\in\mathbb{N}}}$ de B. De este modo se concluye que φ es un isomorfismo de $B-$módulos, y que $\Omega_{B|A}$ es un $B-$módulo libre de base $\{dX_1, \ldots, dX_n\}$. □

Corolario 3.42. *Sea A un anillo. Si B es una $A-$álgebra de tipo finito, entonces $\Omega_{B|A}$ es un $B-$módulo finitamente generado.*

Demostración. Como B es una $A-$álgebra de tipo finito, se tiene que $B \simeq A[X_1 \ldots X_n]/I$ con $I \subset A[X_1, \ldots, X_n]$ un ideal. Dado que $\Omega_{A[X_1,\ldots,X_n]|A} \otimes B = B^{(n)}$ (por la distributividad del producto tensorial respecto de la suma directa), se tiene, por la proposición 3.38 aplicada a $A \to A[X_1, \ldots, X_n] \to B$, la sucesión $I/I^2 \xrightarrow{d} \Omega_{A[X_1,\ldots,X_n]|A} \otimes B \simeq B^{(n)} \to \Omega_{B|A} \to 0$, donde se deduce que $\Omega_{B|A} \simeq B^{(n)}/d(I/I^2)$. En consecuencia $\Omega_{B|A}$ es un $B-$módulo finitamente generado. □

Observación 3.43. En el caso en el que $B = A[X_1, \ldots, X_n]/I$, siendo $I = (f_1, \ldots, f_m)$ entonces, usando la definición de la primera flecha de la sucesión exacta dada por la proposición 3.38 y la expresión explícita del homomorfismo $\Omega_{A[X_1,\ldots,X_n]|A} \simeq B^{(n)}$, se tiene que $d(I/I^2)$ es el $B-$módulo generado por $\{(\partial_i f_j + I^2)_{i=1}^n\}_{j=1}^m$, lo cual da una expresión explícita del módulo de relaciones de $\Omega_{B|A}$.

[1] Este último tiene sentido pues, dado que $\varphi(S) \subset T$, el homomorfismo de anillos φ puede extenderse de modo único a un homomorfismo de anillos $S^{-1}A \to T^{-1}B$

Lema 3.44. *Sea K un cuerpo y α un elemento algebraico sobre K. Entonces $K[\alpha] \mid K$ es separable si y solo si $\Omega_{K[\alpha] \mid K} = 0$.*

Demostración. Sea f el polinomio irreducible de α sobre K. Entonces $K[\alpha] \simeq K[X]/(f)$ (explicitamente por $\alpha \mapsto X + (f)$), y por lo visto en la proposición 3.41, en el lema 3.42 y en la observación 3.43, se tiene la sucesión exacta de homomorfismos de $K[\alpha]-$ módulos (y por tanto de $K[\alpha]-$espacios vectoriales) $(f)/(f^2) \xrightarrow{d} K[\alpha] \to \Omega_{K[\alpha]|K} \to 0$, donde la primera flecha viene dada por $f + (f^2) \mapsto f'(\alpha)$. Por la exactitud del diagrama, $\Omega_{K[\alpha]|K} = 0$ es equivalente a que d sea sobreyectiva, que es a su vez equivalente a que exista un elemento $g + (f^2) \in (f)/(f^2)$ con imagen no nula (pues $\dim_{K[\alpha]} K[\alpha] = 1$). De este modo la equivalencia $K[\alpha]|K$ separable $\Leftrightarrow$ $f'(\alpha) \neq 0$ nos permite concluir. □

Lema 3.45. *[Spr, lem. 4.2.7] Sea $L|E|K$ una torre de extensiones finitas de cuerpos. Si la subextensión $L|E$ es separable entonces la sucesión de la proposición 3.37 es exacta corta.*

Demostración. Por la proposición 3.37, basta con demostrar que el homomorfismo $u : \Omega_{E|K} \otimes_E L \to \Omega_{L|K}$ es inyectivo. Dado que $L|K$ y $L|E$ son extensiones finitas, por la proposición 3.42, $\Omega_{L|K}$ y $\Omega_{L|E}$ son $L-$espacios vectoriales de dimensión finita. Además, puesto que $E|K$ es una extensión finita, $\Omega_{E|K}$ es un $E-$espacio vectorial de dimensión finita, y por tanto $\Omega_{E|K} \otimes_E L$ es un $L-$espacio vectorial de dimensión finita (ya que $\dim_L(\Omega_{E|K} \otimes_E L) = \dim_E(\Omega_{E|K})$). Dado que en espacios vectoriales de dimensión finita dualizar mantiene y refleja las sucesiones exactas, probar que el homomorfismo u es inyectivo equivale a probar que $\overline{u} : \mathrm{Hom}_L(\Omega_{L|K}, L) \to \mathrm{Hom}_L(\Omega_{E|K} \otimes L, L) = \mathrm{Hom}_E(\Omega_{E|K}, L)$, equivalentemente $\widehat{u} : \mathrm{Der}_K(L, L) \to \mathrm{Der}_K(E, L)$ (por el isomorfismo natural), es sobreyectivo. Para comprobar esto último basta con probar que toda derivación $D \in \mathrm{Der}_K(E, L)$ se puede extender a una derivación $D' \in \mathrm{Der}_K(L, L)$. Ya que la extensión $L|E$ es finita separable existe un elemento $\alpha \in L$ tal que $L = E(\alpha)$. Sea $f(X) = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m$ el polinomio irreducible de α sobre E. Dado que $f(\alpha) = 0$, toda $K-$derivación $D' : L \to L$ que extienda $D \in \mathrm{Der}_K(E, L)$ por la regla de Leibniz debe satisfacer $0 = D'(f(\alpha)) = f'(\alpha)D'(\alpha) + D^*f(\alpha)$, donde se ha introducido la aplicación $D^* : E[X] \to L[X]$ $b_0 + b_1X + \cdots + b_mX^m \mapsto D(b_0) + D(b_1)X + \cdots + D(b_m)X^m$, que define una $K[X]-$derivación de $E[X]$ en $L[X]$ que extiende D de modo natural. Para probar esto último basta con demostrar que satisface la regla de Leibniz, pues la $K[X]-$linealidad es evidente. Sean $g = b_0 + b_1X + \cdots + b_tX^t$ y $h = c_0 + c_1X + \cdots + c_mX^m$ polinomios de $E[X]$, entonces:

$$D^*(gh) = D^*\left(\sum_{k=0}^{m+t}\left(\sum_{i+j=k} b_ic_j\right)X^k\right) = \sum_{k=0}^{m+t}\left(\sum_{i+j=k} b_iD(c_j) + c_jD(b_i)\right)X^k = gD^*(h) + hD^*(g)$$

Puesto que $L|E$ es separable, $f'(\alpha) \neq 0$, y por tanto existe un único valor de $D'(\alpha) = -D^*f(\alpha)/f'(\alpha)$. Lo anterior implica que si una $K-$derivación $D : E \to L$ admite una extensión a $D' \in \mathrm{Der}_K(L, L)$, dicha extensión es única. Dado que todo elemento de L puede expresarse como $g(\alpha)$, con $g \in E[X]$, definimos la extensión de $D \in \mathrm{Der}_K(E, L)$ a $\mathrm{Der}_K(L, L)$

como $D'(g(\alpha)) = D^*g(\alpha) - g'(\alpha)D^*f(\alpha)/f'(\alpha) = D^*g(\alpha) + g'(\alpha)D'(\alpha)$. La aplicación D' está bien definida por el razonamiento anterior y define una $K-$derivación de L en L. En efecto, como la $K-$linealidad es clara, basta comprobar que satisface la regla de Leibniz, pero si $g, h \in E[X]$, entonces $D'(g(\alpha)h(\alpha)) = D^*(gh)(\alpha) + (gh)'(\alpha)D'(\alpha) = g(\alpha)(D^*h(\alpha) + h'(\alpha)D'(\alpha)) + h(\alpha)(D^*g(\alpha) + g'(\alpha)D'(\alpha)) = g(\alpha)D'(h(\alpha)) + h(\alpha)D'(g(\alpha))$, como queríamos probar. De este modo la aplicación $\widehat{u}$ es sobreyectiva (y además es un isomorfismo, ya que de la unicidad de la extensión probada anteriormente se deduce su inyectividad), y por tanto u es inyectiva.

□

Proposición 3.46. *Sea K un cuerpo y $L|K$ una extensión finita de cuerpos, entonces $L|K$ es separable si y solo si $\Omega_{L|K} = 0$*

Demostración. Para el *solo si*, si $L|K$ es separable, al ser finita, el teorema del elemento primitivo asegura la existencia de un elemento $\alpha \in L$ tal que $L = K[\alpha]$, de modo que el resultado se sigue del lema 3.44.

Para el *si*, como la extensión $L|K$ es finita, admite un número finito de generadores. Para demostrar esta implicación utilizaremos inducción en m, el número de generadores de la extensión. El caso $m = 1$ ha sido probado en 3.44, de modo que supongamos que la propiedad se cumple para el caso $m - 1$, y comprobemos que se cumple para el caso m. Sea entonces $L = K(\alpha_1, \ldots, \alpha_m)$ y $E = K(\alpha_1)$. Aplicando el lema 3.45 a $K \to E \to L$ obtenemos la sucesión exacta corta $0 \to \Omega_{E|K} \otimes_E L \to \Omega_{L|K} \to \Omega_{L|E} \to 0$, con la que podemos deducir que $\Omega_{L|E} = 0$ y $\Omega_{E|K} \otimes_E L = 0$ ya que por hipótesis $\Omega_{L|K} = 0$. Dado que $\Omega_{L|E} = 0$, por hipótesis de inducción se cumple que la extensión $L|E$ es separable, y dado que $\dim_L(\Omega_{E|K} \otimes_E L) = \dim_E(\Omega_{E|K}) = 0$, $\Omega_{E|K} = 0$, por lo que la extensión $E|K$ es separable por 3.44. De este modo, por un argumento de transitividad se cumple que la extensión $L|K$ es separable, como queríamos probar. □

Proposición 3.47. *Sea A un anillo de valoración discreta, K su cuerpo de fracciones y $L|K$ una extensión finita separable de cuerpos. Si la clausura íntegra B de A en L es un anillo de valoración discreta, $\Omega_{B|A} = 0$ si y solo si la extensión $L|K$ es no ramificada.*

Demostración. Supongamos que $\mathfrak{m}$, κ y $\mathfrak{n}$, λ son los ideales maximales y cuerpos residuales de A y B, respectivamente. Para el *si* basta con tener en cuenta que, al ser $L|K$ no ramificada, $\mathfrak{m}B = \mathfrak{n}$ y la extensión $\lambda|\kappa$ es finita separable, y por tanto simple, por el lema del elemento primitivo, de modo que $\Omega_{B|A} \otimes_A \kappa = \Omega_{B \otimes_A \kappa|\kappa} = \Omega_{\lambda|\kappa} = 0$, donde para la primera igualdad se utilizó la proposición 3.39, para la segunda la igualdad $B \otimes_A A/\mathfrak{m} = B/\mathfrak{m}B = B/\mathfrak{n} = \lambda$ [AM, ej. 2.2] y para la tercera que $\lambda|\kappa$ es simple y separable y la proposición 3.44. De lo anterior se deduce que $\Omega_{B|A} \otimes_B \lambda = \Omega_{B|A} \otimes_B (B \otimes_A \kappa) = \Omega_{B|A} \otimes_A \kappa = 0$, y dado que B es una $A-$álgebra de tipo finito, $\Omega_{B|A}$ es un $B-$módulo finitamente generado por la proposición 3.42, de modo que $\Omega_{B|A} = 0$ por el lema de Nakayama [AM, ej. 2.3].

Para el *solo si*, supongamos que en las hipótesis de la proposición $\Omega_{B|A} = 0$, y veamos que $L|K$ es no ramificada. En primer lugar, aplicando la proposición 3.38 a $A \to B \to \lambda$ se obtiene la sucesión exacta:

$$\mathfrak{n}/\mathfrak{n}^2 \to \Omega_{B|A} \otimes_B \lambda \to \Omega_{\lambda|A} \to 0,$$

de lo que se deduce que $\Omega_{\lambda|A} = 0$ (al cumplirse $\Omega_{B|A} = 0$). Por otro lado, aplicando de nuevo la proposición 3.37 a $A \to \kappa \to \lambda$ se obtiene la sucesión exacta:

$$\Omega_{\kappa|A} \otimes_\kappa \lambda \to \Omega_{\lambda|A} \to \Omega_{\lambda|\kappa} \to 0,$$

por lo que $\Omega_{\lambda|\kappa} = 0$, y en consecuencia, la extensión $\lambda|\kappa$ es separable, por la proposición 3.46.

Sean ahora π, Π uniformizantes de A y B respectivamente, y $\mathfrak{n}$ el ideal maximal de B. Dado que la extensión $L|K$ es separable, por la proposición 2.45 y la observación 2.46 existe un elemento $x \in B$ tal que el conjunto $\{x^i\Pi^j\}_{\substack{i=0,\dots,f-1\\ j=0,\dots,e-1}}$ es una base de B como $A-$módulo libre, siendo $e \geq 1$ el índice de ramificación de la extensión $L|K$ y $f = [\lambda : \kappa]$ (dado que la extensión $\lambda|\kappa$ es finita separable existe un elemento $\overline{x}$ tal que $\lambda = \kappa[\overline{x}]$, de modo que podemos tomar $\alpha_j = x^j$ en la demostración de la proposición 2.45, donde $x \in B$ es un representante de $\overline{x}$). Por la proposición 1.46 se cumple que $\mathfrak{m}B = \mathfrak{n}^e = (\Pi^e)$, veamos que $e = 1$. Supongamos que $e > 1$, definimos entonces la aplicación $D : B \to \lambda$ como $x^i\Pi^j \mapsto \overline{x}^i\delta_{j1}$ (donde δ_{ij} es la delta de Kronecker), extendida por $A-$linealidad a todo B. Veamos que D es una $A-$derivación de B sobre λ. En efecto, D es no nula (pues $D(\Pi) = \overline{1} \neq 0$) y $D|_A = 0$, ya que $D(a) = aD(1) = 0$ para todo $a \in A$. Puesto que D es un homomorfismo de $A-$módulos, solo queda comprobar que satisface la regla de Leibniz. Sean entonces $i, i' \in \{0, \dots, f-1\}$ y $j, j' \in \{0, \dots, e\}$. Supongamos que $j, j' > 0$. Una puntualización importante es que x^f puede expresarse como combinación $A-$lineal de las x^i por la proposición 1.35, de modo que como D es $A-$lineal, en lo que sigue podemos suponer sin pérdida de generalidad que $x^{i+i'}$ está en la base. Si $j + j' \geq e$, entonces, dado que $\Pi^e = u\pi$ para $u \in A^*$, $D(x^i\Pi^j x^{i'}\Pi^{j'}) = D(x^{i+i'}\Pi^{j+j'}) = D(x^{i+i'}u\pi\Pi^{j+j'-e}) = \pi D(ux^{i+i'}\Pi^{j+j'-e}) = 0 = x^i\Pi^j D(x^{i'}\Pi^{j'}) + x^{i'}\Pi^{j'}D(x^i\Pi^j)$. Si $2 \leq j + j' \leq e - 1$, entonces $D(x^{i+i'}\Pi^{j+j'}) = 0 = x^i\Pi^j D(x^{i'}\Pi^{j'}) + x^{i'}\Pi^{j'}D(x^i\Pi^j)$. Supongamos ahora que $j = 0$ y $j' = 1$ (o su caso simétrico), entonces $D(x^{i+i'}\Pi) = \overline{x}^{i+i'} = x^i D(x^{i'}\Pi) + \Pi x^{i'}D(x^i)$. Finalmente el caso $j = j' = 0$ es trivial por la definición de D. De este modo hemos probado que D es una $A-$derivación de B en λ, de modo que $\mathrm{Der}_A(B, \lambda) \neq 0$, y en consecuencia $\mathrm{Hom}_B(\Omega_{B|A}, \lambda) \neq 0$. Por lo tanto $\Omega_{B|A} \neq 0$, como queríamos demostrar.

□

Proposición 3.48. *[Ser, cap. III, th.1] Sea A un dominio de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita separable de cuerpos y B la clausura íntegra de A en L. Sea $\mathfrak{q}$ un ideal primo de B y $\mathfrak{p} = \mathfrak{q} \cap A$. Son equivalentes:*

1. $(\Omega_{B|A})_\mathfrak{q} = 0$.
2. *La extensión $L|K$ es no ramificada en $\mathfrak{q}$.*

Demostración. Basta tener en cuenta que, por la proposición 3.40, $(\Omega_{B|A})_{\mathfrak{q}} = \Omega_{B_{\mathfrak{q}}|A_{\mathfrak{p}}}$, y aplicar la proposición anterior. □

Definición 3.49. Sea A un anillo de valoración discreta, K su cuerpo de fracciones y $L|K$ una extensión finita separable. Si B es la clausura íntegra de A en L, se define el *diferente* de la extensión $L|K$, como el $B-$módulo $\mathfrak{D}_{L|K} = (0 : \Omega_{B|A})$.

Observación 3.50. Por el teorema anterior, el diferente de una extensión finita de dominios de Dedekind contiene bastante información sobre la ramificación de la misma. En el caso en el que K sea un cuerpo completo para una valoración y la extensión $L|K$ separable, siendo B la clausura íntegra de A en K, entonces se demostró que existe un elemento $x \in B$ tal que $B = A[x]$. De este modo, por lo visto en la observación 3.43, $\mathfrak{D}_{L|K} = (f'(x))$, siendo f el polinomio irreducible de x sobre K (que pertenecerá a $A[X]$) y f' su derivada. Además el diferente se relaciona con los grupos de ramificación definidos en la sección anterior:

Proposición 3.51. *Si $\mathfrak{D}_{L|K}$ denota el diferente asociado a la extensión de Galois finita $L|K$ de cuerpos locales, entonces:*

$$v_L(\mathfrak{D}_{L|K}) = \sum_{\sigma \neq 1} i_G(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1),$$

donde la suma tiene sentido, al cumplirse que $G_i = 1$ para todo i a partir de un índice $i_0 \geq 0$.

Demostración. Sean A, B los anillos de valoración de K y L, respectivamente. Como $L|K$ es separable existe un elemento $x \in B$ tal que $B = A[x]$, sea f su polinomio irreducible sobre K (que en particular pertenece a $A[X]$). El diferente $\mathfrak{D}_{L|K}$, por lo visto en la observación anterior, está generado por $f'(x)$, pero dado que $f = \prod_{\sigma \in G}(X - \sigma(x))$, se cumple que:

$$f'(X) = \sum_{\tau \in G} \prod_{\sigma \in G - \{\tau\}} (X - \sigma(x)) \quad ; \quad f'(x) = \prod_{\sigma \in G - \{1\}} (x - \sigma(x)),$$

con lo que $w(f'(x)) = \sum_{\sigma \in G-\{1\}} w(x - \sigma(x)) = \sum_{\sigma \in G-\{1\}} i_G(\sigma)$, lo que prueba la primera igualdad. Para la segunda igualdad basta con ver que $i_G(\sigma) = i + 1$ es constante para $\sigma \in G_i - G_{i+1} = (G_i - \{1\}) - (G_{i+1} - \{1\})$ y que $G - 1 = \cup_{i=-1}^{\infty}[(G_i - \{1\}) - (G_{i+1} - \{1\})]$, con lo que, al ser la unión anterior disjunta, $|G - 1| = \sum_{i=-1}^{\infty}(r_i - r_{i+1})$, siendo $r_i = |G_i|$. Consecuentemente:

$$\sum_{\sigma \in G-\{1\}} i_G(\sigma) = \sum_{i=-1}^{\infty} (i+1)(r_i - r_{i+1}) = \sum_{i=0}^{\infty} (i+1)(r_i - r_{i+1}) = r_0 - r_1 + 2(r_1 - r_2) +$$

$$+ 3(r_2 - r_3) + \cdots = r_0 + r_1 + r_2 + r_3 + \cdots = \sum_{i=0}^{\infty} r_i,$$

lo cual prueba la segunda igualdad. □

Bibliografía

[AM] I.G. Atiyah M.F.; Macdonald. *Introducción al Álgebra Conmutativa*. Editorial Reverté, 1969.

[Iwa] K. Iwasawa. *Local Class Field Theory*. Oxford Mathematical Monographs. Oxford University Press, 1989.

[Mat] H. Matsumura. *Commutative Algebra*. Mathematics Lecture Note Series. The Benjamin/Cummings Publishing Company, 1980.

[Mil] James S. Milne. *Algebraic Number Theory (v3.08)*. Disponible en `www.jmilne.org/math/`. 2020.

[Neu] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1999.

[Ser] J.P. Serre. *Local Fields*. Graduate texts in mathematics; 67. Springer-Verlag, 1979.

[Spr] T.A Springer. *Linear Algebraic Groups*. Modern Birckhäuser Clasics. Springer Verlag, 1998.

[Sut] A. Sutherland. *Number Theory I. Massachusetts Institute of Technology: MIT OpenCourseWare*. Disponible en `https://ocw.mit.edu`. 2019.

Índice alfabético