Universidad Autónoma de Zacatecas
"Francisco García Salinas"

Unidad Académica de Matemáticas

Un problema tipo Northcott

Tesis

Para obtener el título de

Maestro en Matemáticas

Presenta

Samuel Carrillo Piñon

Asesor

Dr. Santos Hernández Hernández

Zacatecas, Zacatecas, Octubre 2019

Agradecimientos

Prefacio

El objetivo de esta tesis es estudiar un resultado obtenido por Enrico Bombieri y Umberto Zannier en su artículo "A note on heights in certain infinite extensions of $\mathbb{Q}$"([1]) publicado en 2001. Con este propósito, la tesis se divide en cinco capítulos:

El primer capítulo se centra en introducir las nociones básicas que se utilizan en la teoría de números algebraicos, a saber, la norma y la traza, dominios de Dedekind, índice de ramificación y grado residual y el discriminante. Esta teoría se puede consultar a detalle en los textos [5], [6], [8] y [4].

El segundo capítulo trata sobre valores absolutos definidos en un campo arbitrario K y la manera en que éstos se pueden extender a valores absolutos sobre una extensión de K. Asimismo, se definen el índice de ramificación y grado residual que se estudian en el primer capítulo ahora desde el punto de vista de los valores absolutos y sus extensiones. La teoría de este capítulo se puede encontrar en [4].

En el tercer capítulo se definen los campos $\mathfrak{p}$-ádicos, herramienta fundamental para el desarrollo de la tesis. Conoceremos sus características básicas y aplicaciones de estos al estudio de campos de números algebraicos. Esta teoría se puede consultar con mayor detalle en [8].

En el cuarto capítulo se presentan la fórmula del producto y la altura logarítmica de números algebraicos, otra herramienta fundamental.

Por último, el quinto capítulo presentan la propiedad de Northcott, definida para subconjuntos de una cerradura algebraica de $\mathbb{Q}$, se definen los campos $K^{(d)}$ y $K_{ab}^{(d)}$, y el resultado principal de la tesis, el cual establece que $K_{ab}^{(d)}$ tiene tal propiedad. Este capítulo está basado en el ya mencionado artículo artículo de [1].

Introducción

Sea $\mathbb{Q}^a$ la cerradura algebraica de $\mathbb{Q}$ y consideremos $h\colon \mathbb{Q}^a \to \mathbb{R}_{\geq 0}$ la altura logarítmica absoluta, función que se define en la Sección 4.2. En 2001, Enrico Bombieri y Umberto Zannier definen que: un subconjunto $\mathcal{A} \subseteq \mathbb{Q}^a$ tiene la propiedad de Northcott si para toda $T \in \mathbb{R}_{>0}$ el conjunto

$$\mathcal{A}(T) = \{\alpha \in \mathcal{A} : h(a) \leq T\}$$

es finito.

En la Sección 5.1 se demuestra que si K es una extensión finita de $\mathbb{Q}$ entonces para cada $T \in \mathbb{R}_{>0}$ la cantidad de elementos $\alpha \in K$ con $h(\alpha) \leq T$ es finita. Esto se conoce como el Lema de Northcott.

Por lo anterior es natural el problema de saber si existen extensiones infinitas sobre $\mathbb{Q}$ que tengan la propiedad de Northcott. En su artículo [1], Bombieri y Zannier construyen extensiones infinitas con tal propiedad. El propósito de esta tesis en estudiar estos resultados.

Índice general

Capítulo 1

Lenguaje preliminar

Este primer capítulo está destinado a introducir resultados básicos necesarios para el desarrollo de la tesis. La teoría de la Sección 1.1 se encuentra principalmente en [5]; la de 1.2 en [6]; la de 1.3 en [8]; y la de 1.4 en [4] y [8].

1.1. La norma y la traza

Consideremos una extensión de campos L/K finita. Para un elemento $x \in L$ consideremos la aplicación $r_x : y \mapsto xy$ definida de L en sí mismo. Ésta es una aplicación K lineal y como tal, dada una base fija para L como K-espacio vectorial, le corresponde una única matriz A_x de tamaño $[L : K] \times [L : K]$. Se define *la traza de x respecto a la extensión L/K* como $T_{L/K}(x) = \mathrm{tr}(A_x)$. De manera similar se define *la norma de x respecto a la extensión L/K* como $N_{L/K}(x) = \det(A_x)$. Estas definiciones no dependen de la elección de la base.

La norma y la traza tienen las siguientes propiedades básicas: Sean L/E y E/K extensiones finitas de campos, $x, y \in L, a \in K$, y $[L : K] = n$, entonces

i) $T_{L/K}(x + y) = T_{L/K}(x) + T_{L/K}(y)$.

ii) $T_{L/K}(ax) = aT_{L/K}(x)$.

iii) $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.

iv) $N_{L/K}(ax) = a^n N_{L/K}(x)$.

v) $T_{L/K}(x) = T_{E/K}(T_{L/E}(x))$.

La demostración de éstas se puede consultar en la Proposición 5.1, Capítulo 1 de [5].

Cuando la extensión L/K es separable la norma y la traza se pueden calcular también de la siguiente manera: supongamos que $G = Aut(L/K)$, entonces se tiene

$$T_{L/K}(x) = \sum_{\sigma \in G} \sigma x, \qquad \text{y} \qquad N_{L/K}(x) = \prod_{\sigma \in G} \sigma x.$$

La equivalencia de estas fórmulas con la definición anterior se puede consultar en [3, pág 16].

1.2. Dominios de Dedekind

Sea R un dominio contenido en un campo K. Un elemento $\alpha \in K$ se dice *entero sobre* R si existen $a_1, a_2, \ldots, a_r \in R$ tales que

$$\alpha^r + a_1\alpha^{r-1} + \cdots + a_r = 0.$$

Definimos la *cerradura entera de* R *en* K como $\overline{R_K} = \{\alpha \in K : \alpha \text{ es entero sobre } R\}$. Se puede demostrar que $\overline{R_K}$ es un subanillo de K. Si K es el campo de cocientes de R, decimos que R es *enteramente cerrado* cuando $\overline{R_K} = R$.

Se dice que un dominio R con campo de cocientes K es *dominio de Dedekind*[1] si cumple las siguientes tres propiedades:

1. Todos sus ideales son finitamente generados (un anillo R se dice *noetheriano*[2] si tiene esta propiedad).

2. Es enteramente cerrado.

3. Todos sus ideales primos (no cero) son maximales.

Sean R dominio de Dedekind y K su campo de cocientes. Un *ideal fraccionario de* R *en* K es un R-módulo $\mathfrak{a} \subseteq K$ tal que existe $c \in R \setminus \{0\}$ que satisface $c\mathfrak{a} = \{ca : a \in \mathfrak{a}\} \subseteq R$. Los ideales del dominio son ideales fraccionarios tomando $c = 1$. Así, la definición de ideal fraccionario es una generalización de la definición de ideal. A los ideales les llamaremos *ideales enteros* o simplemente ideales (si no hay peligro de confusión).

Para dos ideales fraccionarios $\mathfrak{a}_1, \mathfrak{a}_2$ se define el producto como

$$\mathfrak{a}_1\mathfrak{a}_2 = \left\{ \sum_{i=1}^{r} a_{1i}a_{2i} : r < \infty,\ a_{1i} \in \mathfrak{a}_1,\ a_{2i} \in \mathfrak{a}_2 \right\}.$$

Se puede demostrar que el producto es un ideal fraccionario. Además el producto es conmutativo y asociativo.

[1] Por Richard Dedekind.
[2] Por Emmy Noether.

Teorema 1.2.1 *Sean R dominio de Dedekind y K su campo de cocientes. Entonces cada ideal entero de R se puede factorizar de manera única (salvo el orden) en producto de ideales primos, y el conjunto de los ideales fraccionarios (no cero) forma un grupo respecto al producto definido anteriormente.*

La demostración de este resultado se puede encontrar en [6], Capítulo 1, Teorema 2.

Aunque la demostración se omite, señalamos que en el grupo de los ideales fraccionarios quien juega el papel de neutro es R y que dado un ideal fraccionario $\mathfrak{a}$ su inverso es $\mathfrak{a}^{-1} := \{x \in K : x\mathfrak{a} \subseteq R\}$.

Sean $\mathfrak{a}$ un ideal fraccionario y $c \in R$ tal que $c\mathfrak{a} \subseteq R$. Notemos que $c\mathfrak{a}$ es un ideal entero. Entonces escribiendo $c\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ y $\langle c \rangle = \mathfrak{q}_1 \dots \mathfrak{q}_l$, se tiene que $\mathfrak{p}_1 \dots \mathfrak{p}_r = c\mathfrak{a} = \langle c \rangle \mathfrak{a} = \mathfrak{q}_1 \dots \mathfrak{q}_l \mathfrak{a}$. Por tanto

$$\mathfrak{a} = \frac{\mathfrak{p}_1 \dots \mathfrak{p}_r}{\mathfrak{q}_1 \dots \mathfrak{q}_l}.$$

En particular, si cancelamos los factores repetidos en el numerador y el denominador obtenemos la factorización única para $\mathfrak{a}$.

En R podemos hablar de divisibilidad respecto a sus ideales. Diremos que un ideal $\mathfrak{a}$ divide al ideal $\mathfrak{b}$, denotado como $\mathfrak{a}|\mathfrak{b}$, si y sólo si existe un tercer ideal $\mathfrak{c}$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

Proposición 1.2.1 $\mathfrak{a}|\mathfrak{b}$ *si y sólo si* $\mathfrak{a} \supseteq \mathfrak{b}$.

Demostración: Si $\mathfrak{a}|\mathfrak{b}$, digamos $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$, entonces cada $x \in \mathfrak{b} = \mathfrak{a}\mathfrak{c}$ se puede escribir como suma finita $\sum a_i c_i$, y esta suma pertenece a $\mathfrak{a}$ puesto que éste es un ideal. Recíprocamente, si $\mathfrak{a} \supseteq \mathfrak{b}$, entonces se tiene que $\mathfrak{c} = \mathfrak{b}\mathfrak{a}^{-1} \subseteq R$. El resultado se sigue. ■

Ejemplos:

• $\mathbb{Z}$ es un dominio de Dedekind: Demostraremos que es enteramente cerrado (el campo de cocientes de $\mathbb{Z}$ es $\mathbb{Q}$). Sea $\frac{\alpha}{\beta} \in \mathbb{Q}$ entero sobre $\mathbb{Z}$. Supongamos $(\alpha, \beta) = 1$. Si $(\frac{\alpha}{\beta})^n + a_{n-1}(\frac{\alpha}{\beta})^{n-1} + \dots + a_1\frac{\alpha}{\beta} + a_0 = 0$ con $a_i \in \mathbb{Z}$, entonces, multiplicando por β^n se obtiene

$$\alpha^n + a_{n-1}\beta\alpha^{n-1} + \dots + a_1\beta^{n-1}\alpha + \beta^n a_0 = 0$$
$$\alpha^n + \beta\left(a_{n-1}\alpha^{n-1} + \dots + a_1\beta^{n-2}\alpha + \beta^{n-1}a_0\right) = 0$$

La última ecuación implica que $\beta|\alpha$, lo cual es imposible a menos que $\beta = \pm 1$. Así, $\frac{\alpha}{\beta} = \pm\alpha \in \mathbb{Z}$. Por tanto $\overline{\mathbb{Z}_{\mathbb{Q}}} = \mathbb{Z}$. Las propiedades *1* y 3 claras. De hecho todo dominio de ideales principales es de Dedekind y la prueba es análoga a

la de $\mathbb{Z}$.

• Un campo K se llama *campo de números* o *campo de números algebraicos* cuando es extensión finita de $\mathbb{Q}$, y a sus elementos se les llama *números algebraicos*. En este caso sea $\mathcal{O}_K$ la cerradura entera de $\mathbb{Z}$ en K. A $\mathcal{O}_K$ se le llama *anillo de enteros de* K o *anillo de enteros algebraicos de* K. A los elementos de este anillo se les conoce como *enteros algebraicos* o simplemente *enteros* si no hay ambigüedad. Se puede demostrar el siguiente resultado:

Teorema 1.2.2 *Si R es un dominio de Dedekind con campo de cocientes K y L es una extensión finita separable sobre K, entonces $\overline{R_L}$ es dominio de Dedekind.*

Como caso particular se tiene que $\mathcal{O}_K$ es dominio de Dedekind, pues $\mathbb{Z}$ lo es.

Para terminar esta sección daremos un criterio de irreducibilidad para polinomios sobre el campo de cocientes de un dominio de Dedekind. Sean D de Dedekind, K su campo de cocientes y $\mathfrak{p} \leq D$ un ideal primo. Decimos que un polinomio $X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in D[X]$ es un *polinomio de Eisenstein respecto a* $\mathfrak{p}$ si $a_1, \ldots, a_{n-1}, a_n \in \mathfrak{p}$ y $a_n \notin \mathfrak{p}^2$.

Teorema 1.2.3 *(Criterio de Eisenstein) Si $f(X) \in D[X]$ es de Eisenstein respecto a $\mathfrak{p}$ entonces es irreducible en K.*

Demostración: Sea $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ de Eisenstein, y supongamos que tenemos una factorización $f(X) = g(X)h(X)$ con $g, h \in K[X]$. Sin pérdida de generalidad podemos suponer que g y h son mónicos, digamos

$$g(X) = X^m + b_1X^{m-1} + \cdots + b_n$$

y

$$h(X) = X^l + c_1X^{l-1} + \cdots + a_l$$

con $m, l \geq 1$. Notemos que las raíces de g y h son también raíces de f y por tanto enteras sobre D. Como los coeficientes de g y h están dados en términos de sumas y productos de sus raíces se sigue que son enteros sobre D y por tanto pertenecen a éste por ser enteramente cerrado. Así tenemos que $h(X), g(X) \in D[X]$.

Por lo anterior, podemos considerar $\overline{f}, \overline{g}, \overline{h} \in (D/\mathfrak{p})[X]$ los polinomios que se obtienen de f, g y h respectivamente al reducir sus coeficientes módulo $\mathfrak{p}$ que claramente es un homomorfismo de anillos. Por tanto tenemos $\overline{f} = \overline{g}\overline{h}$. Por otro lado, como $a_1, \ldots, a_n \in \mathfrak{p}$ se tiene $\overline{f} = X^n$. En particular todas las raíces de $\overline{f}$ son iguales al cero de $D/\mathfrak{p}$. Como $\mathfrak{p}$ es maximal se tiene que $D/\mathfrak{p}$ es campo y por tanto $(D/\mathfrak{p})[X]$ es un dominio de factorización única. Entonces

$\overline{g} = X^m$ y $\overline{h}(X) = X^l$. Se sigue que $b_m, c_l \in \mathfrak{p}$ y por tanto $a_n = b_m c_l \in \mathfrak{p}^2$, que contradice el hecho de que f es de Eisenstein. ■

1.3. Índice de ramificación y grado residual

Sea L/K una extensión de campos de números. Se puede demostrar que $\mathcal{O}_L$ es la cerradura entera de $\mathcal{O}_K$ en L. Si $\mathfrak{q} \leq \mathcal{O}_L$ es un ideal primo, notamos que $\mathfrak{q} \cap \mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$. Si $K = \mathbb{Q}$, entonces $\mathfrak{q} \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ y por tanto un ideal principal, digamos $\langle p \rangle$ con $p \in \mathbb{Z}$ un número primo. Notemos que p es el único número primo en $\mathfrak{q} \cap \mathbb{Z}$ y nos referimos a él como *el entero primo de* $\mathfrak{q}$.

Un ideal primo $\mathfrak{p} \leq \mathcal{O}_K$ se puede extender a un ideal en $\mathcal{O}_L$ como

$$\mathfrak{p}\mathcal{O}_L = \left\{ \sum_{i=1}^{r} p_i x_i : r < \infty, p_i \in \mathfrak{p}, x_i \in \mathcal{O}_L \right\}.$$

El ideal obtenido es propio mas no necesariamente primo. Para un ideal primo $\mathfrak{q} \leq \mathcal{O}_L$ consideramos el ideal $(\mathfrak{q} \cap \mathcal{O}_K)\mathcal{O}_L$, se puede demostrar que $\mathfrak{q}$ divide a este ideal y la potencia exacta a la que lo hace (mediante la factorización única de ideales) se conoce como *índice de ramificación de* $\mathfrak{q}$ *en* L/K y se denota como $e_{L/K}(\mathfrak{q})$.

Decimos que un primo $\mathfrak{q} \leq \mathcal{O}_L$ *no se ramifica en* L/K si su índice de ramificación es igual a 1, en otro caso decimos que *se ramifica*. Si $\mathfrak{q}$ se ramifica, decimos que *se ramifica salvajemente* cuando el entero primo de $\mathfrak{q}$ divide al índice de ramificación, en otro caso decimos que *se ramifica mansamente*.

Por otro lado, para un ideal primo $\mathfrak{p} \leq \mathcal{O}_K$ consideramos la factorización única

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g}.$$

Decimos que un primo $\mathfrak{p} \leq \mathcal{O}_K$ *se ramifica en* L/K si al menos uno de sus divisores se ramifica en L/K, de lo contrario decimos que *no se ramifica*. Similarmente, decimos que *se ramifica mansamente* si todos sus divisores lo hacen. Por último, decimos que $\mathfrak{p}$ es completamente ramificado si $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^{[L:K]}$. En el caso particular de $K = \mathbb{Q}$ decimos que un primo $p \in \mathbb{Z}$ *se ramifica en* L si $\langle p \rangle \leq \mathbb{Z}$ se ramifica en $L/\mathbb{Q}$. Similarmente el resto de las definiciones anteriores.

Ahora supongamos que $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_K$, entonces tenemos un encaje natural de $\mathcal{O}_K/\mathfrak{p}$ en $\mathcal{O}_L/\mathfrak{q}$, definido mediante $x + \mathfrak{p} \mapsto x + \mathfrak{q}$, pues $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Así, podemos identificar a $\mathcal{O}_K/\mathfrak{p}$ como un subcampo de $\mathcal{O}_L/\mathfrak{q}$. Se define $f_{L/K}(\mathfrak{q}) := [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$. A este número se le conoce como *grado residual de* $\mathfrak{q}$ *en* L/K. Se puede demostrar que $\mathcal{O}_L/\mathfrak{q}$ es una extensión finita de $\mathbb{Z}/(\mathfrak{q} \cap \mathbb{Z})$,

el cual es un campo finito, de donde se sigue que $\mathcal{O}_L/\mathfrak{q}$ y $\mathcal{O}_K/\mathfrak{p}$ son también campos finitos. En particular se tiene que $f_{L/K}(\mathfrak{q})$ es finito.

1.4. El discriminante

Consideremos una extensión L/K de campos de números, $\mathcal{O}_L$ y $\mathcal{O}_K$ sus anillos de enteros respectivamente. Dada una base $\{v_1, \ldots, v_n\}$ para L como K espacio vectorial, definimos el *el discriminante de esta base* como

$$d(v_1, \ldots, v_n) = \det(T_{L/K}(v_i v_j)).$$

Es un resultado conocido que si una extensión finita L/K es separable, el cual es nuestro caso, entonces $d(v_1, \ldots, v_n) \neq 0$ para cualquier base de L/K (ver por ejemplo (1.25.b) de [3]).

El ideal discriminante de $\mathcal{O}_L/\mathcal{O}_K$ se define como

$$d_{\mathcal{O}_L/\mathcal{O}_K} = \langle d(v_1, \ldots, v_n) : \{v_1, \ldots, v_n\} \subseteq \mathcal{O}_L \text{ es base para } L/K \rangle.$$

Este ideal nos permite conocer cuáles ideales de $\mathcal{O}_K$ se ramifican en L/K. Se tiene el siguiente resultado:

Teorema 1.4.1 *(del discriminante) Sea L/K extensión finita de campos de números. Entonces un ideal primo $\mathfrak{p} \leq \mathcal{O}_K$ no cero se ramifica en L/K si y sólo si $\mathfrak{p} | d_{\mathcal{O}_L/\mathcal{O}_K}$.*

La demostración de este resultado se puede consultar en [4], Teorema 10.13.

Corolario 1.4.1 *Existe sólo una cantidad finita de ideales primos de $\mathcal{O}_K$ que se ramifican en L/K.*

En el caso particular de $K = \mathbb{Q}$ definimos una base entera de $L/\mathbb{Q}$ como un conjunto $\{v_1, \ldots, v_n\} \subseteq \mathcal{O}_L$ linealmente independiente sobre $\mathbb{Q}$ que genera a $\mathcal{O}_L$ como $\mathbb{Z}$-módulo. Notemos que una base entera es una base para la extensión $L/\mathbb{Q}$. Además se puede probar que todo campo de números tiene una base entera (ver por ejemplo Teorema 1 cap. I de [6]).

Ahora definimos el *discriminante de L (sobre $\mathbb{Q}$)* como el discriminante $d(L) := d(v_1, \ldots, v_n)$ con $\{v_1, \ldots, v_n\}$ una base entera de $L/\mathbb{Q}$. Notemos en este caso que $d(L) \in \mathbb{Z}$. La definición no depende de la elección de la base, pues si $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_n\}$ son dos bases enteras, podemos escribir $w_i = \sum c_{ij} v_j$ con $c_{ij} \in \mathbb{Z}$. En particular notemos que (c_{ij}) es la matriz de cambio de base y por tanto $\det(c_{ij}) = \pm 1$. Se verifica que

$$(T_{L/\mathbb{Q}}(w_i w_j)) = (c_{ij})(T_{L/\mathbb{Q}}(v_i v_j))(c_{ij})^t.$$

Si tomamos el determinante en la igualdad anterior obtenemos

$$d(w_1, \ldots, w_n) = \det(c_{ij})^2 d(v_1, \ldots, v_n) = d(v_1, \ldots, v_n).$$

Más aún, lo anterior es válido incluso si $\{w_1, \ldots, w_n\} \subseteq \mathcal{O}_L$ no es una base entera sino sólo una base para $L/\mathbb{Q}$, salvo que en tal caso $\det(c_{ij})$ no necesariamente es ± 1, pero sigue siendo un número entero. En particular obtenemos que $d_{\mathcal{O}_L/\mathbb{Z}} \subseteq \langle d(L) \rangle$. La contención opuesta se sigue del hecho de que $d(L)$ es uno de los generadores de $d_{\mathcal{O}_L/\mathbb{Z}}$. Es decir que tenemos $d_{\mathcal{O}_L/\mathbb{Z}} = \langle d(L) \rangle$.

Corolario 1.4.2 *(del Teorema del discriminante) Sea L un campo de números. Un primo $p \in \mathbb{Z}$ se ramifica en $L/\mathbb{Q}$, si y sólo si $p \mid d(L)$.*

Demostración: Por el Teorema del discriminante p se ramifica si y sólo si $\langle p \rangle \mid d_{\mathcal{O}_L/\mathbb{Z}} = \langle d(L) \rangle$, es decir $\langle p \rangle \supseteq \langle d(L) \rangle$, por tanto se ramifica si y sólo si $p \mid d(L)$. ■

Con respecto al discriminante se tiene el siguiente resultado:

Teorema 1.4.2 *(de Hermite) Sólo una cantidad finita de campos de números pueden tener el mismo discriminante.*

La demostración de este toerema se puede consultar en [8], Teorema 2.24.

Finalmente, otro resultado que necesitaremos es el siguiente:

Teorema 1.4.3 *Sea $p \in \mathbb{Z}$ primo y $n = \sum_j b_j p^j$ con $0 \leq b_j < p$, $A = \#\{b_j \neq 0\}$. Si $[K : \mathbb{Q}] = n$, entonces la máxima potencia de p que divide a $d(K)$ es menor o igual a $N(n, p) = \sum_j (j+1) b_j p^j - A$.*

Ver [8], Nota 9, Capítulo 2.

Capítulo 2

Teoría de valuaciones

Éste capítulo está basado principalmente en [4], Capítulo 9. En éste estableceremos el lenguaje básico acerca de valores absolutos y algunos conceptos fundamentales.

2.1. Valores absolutos y extensiones

Un *valor absoluto* sobre un campo K es una aplicación $|\ |: K \to \mathbb{R}_{\geq 0}$ que satisface:

1. $|x| = 0$ si y sólo si $x = 0$;

2. Para todo $x, y \in K,\ |xy| = |x||y|$;

3. Para todo $x, y \in K, |x + y| \leq |x| + |y|$.

Decimos que un valor absoluto es *no arquimediano* si podemos cambiar *3* por

3'. Para todo $x, y \in K, |x + y| \leq \text{máx}\{|x|, |y|\}$.[1]

En otro caso decimos que es un valor absoluto *arquimediano*.

Supongamos que $|\ |$ es un valor absoluto sobre el campo K y E una extensión finita de K. En esta sección responderemos las preguntas ¿se puede extender $|\ |$ a un valor absoluto sobre E? y ¿de cuantas maneras distintas puede hacerse?

Para resolver este problema estudiaremos algunos casos por separado, los cuales especificaremos un poco más adelante cuando tengamos los conceptos necesarios.

[1] Notemos que *3'* implica *3*.

Algunas propiedades: Si $|\ |$ es un valor absoluto definido en K y $a, b \in K$, entonces se cumplen

- $|1| = 1$.
- Si para algún $n \in \mathbb{N}$ $a^n = 1$, entonces $|a| = 1$.
- $|-a| = |a|$.
- Si $a \neq 0$, $|a^{-1}| = |a|^{-1}$.
- Si denotamos $|\ |_\infty$ al valor absoluto usual de $\mathbb{R}$, entonces $||a| - |b||_\infty \leq |a - b|$.

Ejemplos:

- El valor absoluto usual de $\mathbb{R}$ es arquimediano, pues por ejemplo $|1 + 1|_\infty = 2 > 1 = \text{máx}\{|1|_\infty, |1|_\infty\}$.
- En un campo arbitrario podemos definir un valor absoluto trivial, es decir, para cada $x \neq 0$ en K, $|x| = 1$ y $|0| = 0$. Éste es un valor absoluto no arquimediano.
- Un ejemplo particularmente interesante de un valor absoluto no arquimediano es el siguiente:

Con $K = \mathbb{Q}$, fijamos $p \in \mathbb{Z}$ un número primo. Dado cualquier número racional $x \in \mathbb{Q} \setminus \{0\}$, la factorización única de $\mathbb{Z}$ garantiza que existen únicos $v_p(x), a, b \in \mathbb{Z}$ tales que $(p, a) = (p, b) = (a, b) = 1$ y $x = p^{v_p(x)}\frac{a}{b}$, por tanto tenemos la aplicación

$$v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

$$x \mapsto \begin{cases} v_p(x), & x \neq 0 \\ \infty, & x = 0 \end{cases}$$

Ésta aplicación tiene las siguientes propiedades:

i) $v_p(x) = \infty$ si y sólo si $x = 0$;

ii) Para $x, y \in \mathbb{Q}$, $v_p(xy) = v_p(x) + v_p(y)$;

iii) Para $x, y \in \mathbb{Q}$, $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

A v_p se le llama *valuación p-ádica* de $\mathbb{Q}$, en general, una aplicación definida sobre un campo que satisface $i), ii)$ y $iii)$ se llama *valuación (exponencial)*, diremos más acerca de este tipo de funciones más adelante.

Ahora podemos definir $|\ |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ mediante $x \mapsto \left(\frac{1}{p}\right)^{v_p(x)}$, donde definimos $\left(\frac{1}{p}\right)^{\infty} = 0$. A partir de $i), ii)$ y $iii)$ se tiene *1,2* y *3'* respectivamente. Así, $|\ |_p$ es un valor absoluto no arquimediano y se le conoce como *valor absoluto p-ádico.*

La siguiente proposición da una caracterización para los valores absolutos no arquimedianos.

Proposición 2.1.1 *Un valor absoluto $|\ |$ definido en un campo K es no arquimediano si y sólo si $|n1| \leq 1$ para todo $n \in \mathbb{Z}$.*

La demostración se puede consultar en [4], Teorema 9.2.

Corolario 2.1.1 *Cualquier valor absoluto en un campo de característica $p > 0$ es no arquimediano.*

Demostración: Se puede identificar $\mathbb{F}_p = \mathbb{Z}/\langle p\rangle$ como un subcampo de K. Si 1 denota a la identidad de $\mathbb{F}_p \subseteq K$ entonces para todo $n \in \mathbb{N}$ tenemos $n1 \in \mathbb{F}_p$. Si $n1 \neq 0$ entonces $(n1)^{p-1} = 1$, por tanto $|n1| = 1$. Si $n1 = 0$ entonces $|n1| = 0$. Por la proposición se sigue que $|\ |$ es no arquimediano. ■

Diremos que dos valores absolutos $|\ |_1$ y $|\ |_2$ definidos en un campo K son *equivalentes* si existe $s \in \mathbb{R}_{>0}$ tal que $|\ |_2 = |\ |_1^s$. Tenemos el siguiente teorema acerca de los valores absolutos que se pueden definir en $\mathbb{Q}$.

Teorema 2.1.1 *Un valor absoluto $|\ |$ no trivial definido en $\mathbb{Q}$ tiene únicamente dos opciones (salvo equivalencia): es el valor absoluto usual, o es un valor absoluto p-ádico para algún $p \in \mathbb{Z}$ primo.*

La demostración del teorema se sigue de los Teoremas 9.4 y 9.5 de [4].

Cuando tenemos un valor absoluto $|\ |$ sobre K podemos definir, de manera natural, una función distancia entre los elementos del campo, a saber, $d(x, y) = |x - y|$. Con esta función se tiene el espacio métrico (K, d). Nos referimos a él como el espacio métrico K. Podemos tomar la completación de (K, d), denotémosla como (K_v, d_v). A K_v se le puede dar estructura de campo mediante las siguientes operaciones: Sean $a, b \in K_v$ y supongamos que $a = \lim a_n$, $b = \lim b_n$ con $(a_n), (b_n)$ sucesiones en K. Entonces se define $a + b = \lim(a_n + b_n)$ y $ab = \lim(a_n b_n)$. Estas operaciones no dependen

de la elección de (a_n) y (b_n). Además restringidas a K coinciden con las operaciones de K de modo que K_v/K es una extensión de campos.

Además en K_v se define un valor absoluto mediante $|a|_v = d_v(a, 0)$, o de manera equivalente, si $a = \lim a_n$ con (a_n) sucesión en K se define $|a|_v = \lim |a_n|$. Si $a \in K$ entonces $|a|_v = d_v(a, 0) = d(a, 0) = |a|$ de modo que $|\ |_v$ es extensión de $|\ |$.

Esto se puede enunciar formalmente como:

Teorema 2.1.2 *Todo campo K con un valor absoluto $|\ |$ tiene una completación K_v. Ésta tiene la siguiente propiedad: Si L es un campo completo respecto a un valor absoluto $|\ |_w$ tal que existe un encaje $\sigma : K \to L$ que satisface $|\sigma\alpha|_w = |\alpha|$, entonces existe un único $\overline{\sigma} : K_v \to L$ encaje de campos extensión de σ que satisface $|\overline{\sigma}\alpha|_w = |\alpha|$ y $\overline{\sigma}K_v = \overline{\sigma K}$, donde $\overline{\sigma K}$ denota la cerradura topológica de σK en L. El encaje $\overline{\sigma}$ está dado por $\overline{\sigma}(\alpha) = \lim \sigma(\alpha_n)$, donde (α_n) es una sucesión de K que converge a α.*

El resultado se deduce del Teorema 9.7 de [4].

En particular, el teorema implica que la completación de un campo es única salvo isomorfismo.

Ahora podemos regresar al problema de extender un valor absoluto. De manera general tenemos los siguientes resultados:

Teorema 2.1.3 *Supongamos que K es completo respecto al valor absoluto $|\ |_K$, y sea E una extensión finita sobre K. Supongamos que $|\ |_K$ se puede extender a un valor absoluto sobre E. Entonces esta extensión es única y está dada por*

$$|a|_E = |N_{E/K}(a)|_K^{1/[E:K]},$$

donde del lado izquierdo tomamos el valor absoluto de E, del lado derecho el valor absoluto de K, y $N_{E/K}(a) \in K$ es la norma de a en E/K. Además, E es completo.

La demostración se puede ver en [4], Teorema 9.8.

Este teorema no garantiza la existencia de una extensión, sin embargo, si logramos demostrar que existe una, entonces el teorema nos da tres características importantes: unicidad, completitud, y una fórmula explícita. El siguiente lema es un caso particular en el que si se garantiza la existencia de la extensión.

Lema 2.1.1 *Sean K un campo de característica $\neq 2$, completo respecto a un valor absoluto $|\ |_K$ y sea E una extensión cuadrática de K. Entonces*

$$|\alpha|_E := |N_{E/K}(\alpha)|_K^{1/2}$$

define un valor absoluto sobre E que es extensión de $|\ |_K$.

La demostración se puede ver en [4, pág 570].

Para responder las preguntas de antes: ¿se puede extender un valor absoluto? y ¿de cuantas maneras distintas puede hacerse? consideraremos los siguientes casos: primero supondremos K completo y $|\ |$ arquimediano; después supondremos K completo y $|\ |$ no arquimediano; y por último, K y $|\ |$ arbitrarios.

2.1.1. Caso I: K completo y $|\ |$ arquimediano

Teorema 2.1.4 *(de Ostrowski): Los únicos campos completos respecto a un valor absoluto arquimediano son $\mathbb{R}$ y $\mathbb{C}$.*

Demostración: Sea K completo respecto a $|\ |$ y éste no arquimediano. Notemos primero que el corolario 2.1.1 implica que K es de característica cero. Por tanto se puede identificar $\mathbb{Q} \subseteq K$. Como $|\ |$ restringido a $\mathbb{Q}$ sigue siendo arquimediano, por el Teorema 2.1.1, es (sin pérdida de generalidad) el valor absoluto usual $|\ |_\infty$. Por el Teorema 2.1.2 podemos identificar $\mathbb{R} = \mathbb{Q}_v$ en K. Además $|\ |$ restringido a $\mathbb{R}$ sigue coincidiendo con el usual.

Supongamos primero que en F existe un elemento i que satisface $i^2 = -1$, en este caso $\mathbb{C} = \mathbb{R}(i) \subseteq K$. Como $\mathbb{C}/\mathbb{R}$ es una extensión finita y en $\mathbb{C}$ conocemos un valor absoluto que extiende al usual de $\mathbb{R}$, el Teorema 2.1.3 garantiza que la restricción de $|\ |$ a $\mathbb{C}$ coincide con el usual. Demostraremos que $K = \mathbb{C}$.

Supongamos que existe $a \in K \setminus \mathbb{C}$. Definamos

$$\begin{aligned} \psi\colon \mathbb{C} &\to \mathbb{R} \\ x &\mapsto |a - x| \end{aligned}$$

si $x_n \to x \in \mathbb{C}$, tenemos $||x_n - a| - |x - a||_\infty \leq |x_n - a - x + a| = |x_n - x|$, se sigue que $\psi(x_n) \to \psi(x)$ y por tanto ψ es continua.

Sea $r = \text{ínf}\{|\gamma - a| : \gamma \in \mathbb{C}\}$. Afirmamos que existe un $\gamma_0 \in \mathbb{C}$ con $|\gamma_0 - a| = r$. Notemos que $r = \text{ínf}\{|\gamma - a| : \gamma \in \mathbb{C}, |\gamma - a| \leq r + 1\}$ y sea $A = \{\gamma \in \mathbb{C} : |\gamma - a| \leq r + 1\}$. Éste es cerrado: $\psi^{-1}([0, r+1]) = \{\gamma \in \mathbb{C} : 0 \leq |\gamma - a| \leq r + 1\} = A$. Y es acotado pues para $\gamma \in A$, $|\gamma| - |a| \leq |\gamma - a| \leq r + 1$, entonces $|\gamma| \leq r + 1 + |a|$. Por tanto A es compacto. Como ψ es continua, alcanza un mínimo en A. Notemos que éste es el γ_0 que queremos pues es tal que $|\gamma_0 - a| = r$. En particular $r > 0$ y para todo $\gamma \in \mathbb{C}$ tenemos $|\gamma - a| \geq |\gamma_0 - a|$.

Sea $D = \{\gamma \in \mathbb{C} : |\gamma - a| = r\} \neq \emptyset$, es decir que $D = \psi^{-1}(\{r\})$. En particular D es cerrado.

A continuación demostraremos que D también es abierto. Basta demostrar que si $\gamma \in D$, entonces para cada γ' tal que $|\gamma - \gamma'| < r$ se tiene $\gamma' \in D$, pues esto significa que $B_r(\gamma) \subseteq D$. Supongamos que $\gamma \in D$ y $|\gamma - \gamma'| < r$. Notemos que para cada $n \in \mathbb{N}$, $(\gamma-a)^n-(\gamma-\gamma')^n = \prod_{i=1}^{n}((\gamma-a)-\omega^i(\gamma-\gamma'))$ con ω una raíz n-ésima primitiva de 1, por tanto

$$\frac{|(\gamma-a)^n-(\gamma-\gamma')^n|}{|(\gamma-a)-(\gamma-\gamma')|} = \frac{|(\gamma-a)^n-(\gamma-\gamma')^n|}{|\gamma'-a|} = \prod_{i=1}^{n-1}|(\gamma-a)-\omega^i(\gamma-\gamma')|$$
$$= \prod_{i=1}^{n-1}|(\gamma-\omega^i(\gamma-\gamma'))-a)| \geq r^{n-1}$$

entonces

$$|\gamma'-a| \leq \frac{|(\gamma-a)^n-(\gamma-\gamma')^n|}{r^{n-1}} \leq r\left(\frac{|\gamma-a|^n}{r^n}+\frac{|\gamma-\gamma'|^n}{r^n}\right)$$
$$= r\left(1+\left(\frac{|\gamma-\gamma'|}{r}\right)^n\right) \longrightarrow r.$$

Por tanto $|\gamma' - a| \leq r \leq |\gamma' - a|$, es decir, $|\gamma' - a| = r$. Se sigue que D es abierto. Ahora, D es abierto y cerrado no vacío en $\mathbb{C}$, se sigue que $D = \mathbb{C}$ por la conexidad de $\mathbb{C}$.

Por otro lado, para cada $\gamma \in D$ tenemos $|\gamma| - |a| \leq |\gamma - a| = r$. Entonces $|\gamma| \leq r + |a|$, es decir $D = \mathbb{C}$ es acotado, que es falso. Por tanto $K = \mathbb{C}$.

Por último, supongamos que en K no existe el elemento i. Consideremos entonces $E = K(i)$, extensión cuadrática de K. Por el Lema 2.1.1, $|\ |$ se extiende a E de modo que éste es un campo completo donde podemos identificar a $\mathbb{C}$ con el valor absoluto usual. Ahora aplicamos la primer parte de la demostración a E y obtenemos que $\mathbb{R} \subseteq K \subseteq E = \mathbb{C}$, como $[\mathbb{C} : \mathbb{R}] = 2 = [\mathbb{C} : K]$, entonces $K = \mathbb{R}$. ■

Ahora podemos enunciar el teorema mas general en el caso arquimediano.

Teorema 2.1.5 *Sea K completo respecto a un valor absoluto arquimediano $|\ |$, y sea E una extensión finita sobre K. Entonces $|\ |$ se puede extender a E de una única manera, a saber,*

$$|a| = |N_{E/K}(a)|^{1/[E:K]},$$

además, con este valor absoluto E es completo.

Demostración: Por el Teorema de Ostrowski, $K = \mathbb{C}$ o $K = \mathbb{R}$. Si $K = \mathbb{C}$, no hay extensiones algebraicas que contengan propiamente a $\mathbb{C}$, y no hay nada que demostrar. Si $K = \mathbb{R}$, su única extensión finita algebraica es $\mathbb{C}$ y podemos aplicar el Lema 2.1.1. ■

2.1.2. Caso II: K completo y $|\ |$ no arquimediano

De la definición de valor absoluto no arquimediano notemos que la operación suma de $\mathbb{R}$ no juega un papel importante, para dar tal definición es suficiente considerar la operación producto y el orden. Teniendo esto en mente, este caso se estudiara como sigue.

Un *grupo abeliano ordenado* es un par (G, H) donde G es un grupo abeliano y H un subconjunto de G que satisfacen

1) $G = H \sqcup \{1\} \sqcup H^{-1}$.

2) H es cerrado respecto al producto de G.

El nombre de grupo abeliano ordenado se debe a que en este caso se tiene un orden en G. En efecto , sean $g_1, g_2 \in G$, decimos que $g_1 > g_2$ si $g_1^{-1}g_2 \in H$. Este orden tiene las siguientes propiedades:

1. Es transitivo: si $g_1 > g_2$ y $g_2 > g_3$, entonces $g_1 > g_3$.

2. Es total: para cada pareja $g_1, g_2 \in G$ se tiene una y sólo una de las siguientes $g_1 > g_2$, $g_2 > g_1$, o $g_1 = g_2$.

3. Es compatible con el producto de G: si $g_1 > g_2$ y $g \in G$, entonces $gg_1 > gg_2$.

Escribiremos indistintamente $g_1 > g_2$ o $g_2 < g_1$.

Recíprocamente, si G es un grupo abeliano con una relación de orden que satisface 1, 2, y 3, con $H = \{h \in G : h < 1\}$ se tiene que la pareja (G, H) es un grupo abeliano ordenado.

Notemos que en un grupo abeliano ordenado G a partir de 1, 2 y 3, se tienen las siguientes propiedades:

4. Si $g_1 > g_2$ y $g_3 > g_4$, entonces $g_1g_3 > g_2g_4$.

5. Si $g_1 > g_2$, entonces $g_2^{-1} > g_1^{-1}$.

Ejemplo: Consideramos $\mathbb{R}_{>0}$ con el orden usual. Sabemos que es transitivo, total y compatible con el producto. Además $\mathbb{R}_{>0}$ es un grupo abeliano respecto al producto. Por tanto, si $H = \{x \in \mathbb{R} : x < 1\}$, entonces $(\mathbb{R}_{>0}, H)$ es un grupo abeliano ordenado.

Sean (G, H) y (G', H') grupos abelianos ordenados. Un *homomorfismo (ordenado)* de (G, H) en (G', H') es un homomorfismo de grupos $\varphi : G \to G'$ tal que $\varphi(H) \subseteq H'$. Notemos que esta condición es equivalente con decir que para cualesquiera $g_1, g_2 \in G$ si $g_1 < g_2$, entonces $\varphi(g_1) < \varphi(g_2)$.

Sean (G, H) un grupo abeliano ordenado y $N \leq G$ un subgrupo. Se puede verificar que $N \cap H$ tiene las propiedades 1) y 2), es decir que $(N, N \cap H)$ es un grupo abeliano ordenado. De este modo tenemos en N un orden heredado del orden de G.

Un *grupo abeliano ordenado con cero adjunto* es $G \cup \{0\}$, donde G es un grupo abeliano ordenado[2] y se define $00 = 0$, $g > 0$ y $0g = g0 = 0$ para todo $g \in G$.

Ejemplo: $\mathbb{R}_{>0} \cup \{0\} = \mathbb{R}_{\geq 0}$, donde $\mathbb{R}_{>0}$ tiene la estructura del ejemplo anterior.

Sea K un campo y $G \cup \{0\}$ un grupo abeliano ordenado con cero adjunto, definimos una *valuación* sobre K como una aplicación $\varphi : K \to G \cup \{0\}$ tal que para cualesquiera $a, b \in K$

i) $\varphi(a) = 0$ si y sólo si $a = 0$.

ii) $\varphi(ab) = \varphi(a)\varphi(b)$.

iii) $\varphi(a + b) \leq \text{máx}\{\varphi(a), \varphi(b)\}$.

Ejemplo: Si $|\ |$ es un valor absoluto no arquimediano sobre K. Entonces es una valuación. Recíprocamente, si φ es una valuación sobre K con imagen en el grupo ordenado abeliano con cero adjunto $\mathbb{R}_{\geq 0}$, entonces es un valor absoluto.

Nota: Se pueden dar definiciones análogas para el caso en que el grupo abeliano G se escribe de forma aditiva. En este caso el orden inducido por un subconjunto H es: $g_1 > g_2$ si y sólo si $g_1 - g_2 \in H$, y en lugar de adjuntar un cero adjuntamos ∞ definiendo $\infty + \infty = \infty$, $\infty > g$, $\infty + g = g + \infty = \infty$ para todo $g \in G$.

Ejemplo: Consideramos $\mathbb{Z}$ con el orden usual. Definimos $H = \{n \in \mathbb{Z} : n > 0\}$, entonces $(\mathbb{Z}, H)$ es un grupo abeliano ordenado con notación aditiva.

En este caso, si K es un campo y $G \cup \{\infty\}$ es un grupo abeliano ordenado aditivo con ∞ adjunto, definimos una *valuación exponencial* sobre K como una aplicación $v : K \to G \cup \{\infty\}$ que para cualesquiera $a, b \in K$ satisface

i) $v(a) = \infty$ si y sólo si $a = 0$.

[2]Como abuso de lenguaje omitimos mencionar al subconjunto H que induce el orden de G.

ii) $v(ab) = v(a) + v(b)$.

iii) $v(a+b) \geq \text{mín}\{v(a), v(b)\}$.

Consideremos K un campo, $\varphi : K \to G \cup \{0\}$ una valuación y K^* el grupo multiplicativo de K, entonces $\varphi(K^*)$ es un subgrupo de G. Llamamos a éste el *grupo de valuación* de K. Siempre podemos remplazar, sin pérdida de generalidad, el grupo G por $\varphi(K^*)$.

Teorema 2.1.6 *Sean φ_0 una valuación de K y E una extensión finita de K. Entonces existen un grupo ordenado G que es extensión del grupo de valuación de K y una valuación de E con valores en $G \cup \{0\}$ que es extensión de φ_0.*

Se puede ver la demostración en [4], Teorema 9.11.

Lema 2.1.2 *Sean E/K una extensión de campos de grado $[E:K] = n < \infty$ y φ una valuación sobre E. Consideremos $G = \varphi(E)$ y $G_0 = \varphi(K)$ los grupos de valuación de E y K respectivamente.*[3] *Entonces $[G : G_0] \leq n$.*

Demostración: Supongamos que $[G : G_0] > n$, en particular el cociente G/G_0 tiene al menos $n+1$ elementos distintos. Por tanto podemos tomar $y_1, \ldots, y_n, y_{n+1} \in K \setminus \{0\}$ tales que para $i \neq j$ se tiene $\varphi(y_i)G_0 \neq \varphi(y_j)G_0$.

Ahora supongamos que

$$0 = a_1 y_1 + \cdots + a_n y_n + a_{n+1} y_{n+1} \tag{2.1}$$

con $a_i \in K$ no todos cero. Se verifica que existen i, j distintos con $\varphi(a_i y_i) = \varphi(a_j y_j)$. Se sigue que $\varphi(y_i)\varphi(y_j)^{-1} = \varphi(a_j a_i^{-1}) \in \varphi(K) = G_0$, es decir que $\varphi(y_i)G_0 = \varphi(y_j)G_0$. Esto contradice la elección de los $y_1, \ldots, y_n, y_{n+1}$ por tanto en 2.1 todos los coeficientes deben ser ceros. Se sigue que $y_1, \ldots, y_n, y_{n+1}$ son linealmente independientes y entonces $[E : K] \geq n+1$. ■

Lema 2.1.3 *Sean E una extensión finita de K, $\varphi_0 \colon K \to G_0 \cup \{0\}$ valuación de K, y $\varphi : E \to G \cup \{0\}$ valuación de E que extiende a φ_0. Entonces G es isomorfo (ordenado) a un subgrupo de G_0.*

Demostración: Sea $l = [G : G_0] \leq [E : K] < \infty$. Definimos la aplicación $s : G \to G_0$ mediante $g \mapsto g^l$; como $\#G/G_0 = l$, para todo $g \in G$ tenemos $g^l G_0 = (gG_0)^l = G_0$ de modo que $g^l \in G_0$. Por tanto la aplicación está bien definida.

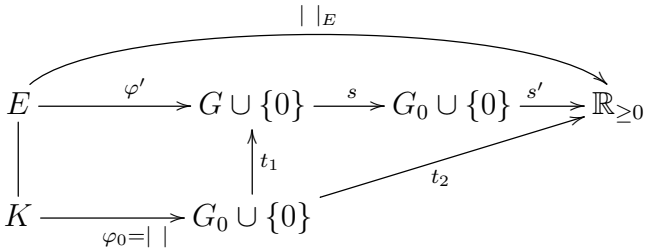
Además, $s(gh) = (gh)^l = g^l h^l = s(g)s(h)$, por tanto s es homomorfismo de grupos. También es fácil ver que un grupo abeliano ordenado no tiene

[3] Hay que notar que $\varphi|_K$ es una valuación sobre K y por tanto G_0 tiene sentido.

elementos de torsión, de donde se sigue que $g^l = s(g) = 1$ implica $g = 1$. De este modo s es inyectivo y tenemos el isomorfismo de G con $s(G) \leq G_0$.

Teorema 2.1.7 *Sea K un campo con un valor absoluto no arquimediano $|\ |$ y E una extensión finita de K. Entonces $|\ |$ se puede extender a un valor absoluto sobre E. Éste es necesariamente no arquimediano.*

Demostración: El grupo de valuación G_0 de $\varphi_0 = |\ |$ es un subgrupo de $\mathbb{R}_{>0}$. Por el Teorema 2.1.6 φ_0 se extiende a una valuación φ' sobre E con grupo de valuación G que contiene (de manera isomorfa) a G_0.
Consideramos $s : G \to G_0$ como en el lema anterior y definimos $s' : G_0 \to \mathbb{R}_{>0}$ mediante $x \mapsto x^{1/l}$, con l como en el lema. Notemos que s' es un isomorfismo ordenado, y tenemos el diagrama siguiente:



donde t_1 y t_2 son los encajes naturales inducidos por las contenciones $G_0 \subseteq G$ y $G_0 \subseteq \mathbb{R}_{>0}$ respectivamente. Ahora sólo hay que notar que $|\ |_E = s's\varphi'$ es un valor absoluto de F que extiende a $|\ | = \varphi_0$. ■

Se tiene el siguiente enunciado análogo al Teorema 2.1.5 para el caso no arquimediano.

Teorema 2.1.8 *Sea K completo respecto a un valor absoluto no arquimediano y no trivial $|\ |$, y sea E una extensión finita sobre K. Entonces $|\ |$ se puede extender a E de una única manera, a saber,*

$$|a| = |N_{E/K}(a)|^{1/[E:K]}.$$

Además, con este valor absoluto E es completo.

Demostración: Por el Teorema anterior existe una extensión de $|\ |$, y por el Teorema 2.1.3, dicha extensión tiene las características deseadas. ■

2.1.3. Caso III: K y $|\ |$ arbitrarios

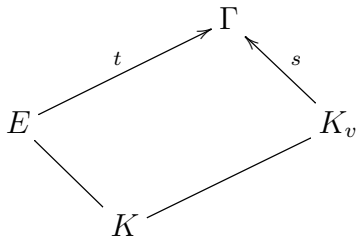
Sean K un campo, E y F dos extensiones de K. Definimos una *composición de E y F* como una terna (Γ, t, s), con Γ es una extensión de K, y donde

$t\colon E \to \Gamma$, $s\colon F \to \Gamma$ son encajes de campos que dejan fijos a los elementos de K, y además $\Gamma = K(t(E), s(F))$ (es decir, Γ está generado sobre K por las imágenes de t y s).

Diremos que dos composiciones (Γ, t, s) y (Γ', t', s') son *equivalentes* si existe un isomorfismo $u\colon \Gamma \to \Gamma'$ tal que los siguientes diagramas conmutan:

Esta noción de equivalencia define en efecto una relación de equivalencia.

Para nuestro estudio de valores absolutos consideremos K un campo con un valor absoluto $|\ |$ y E una extensión finita sobre K. Sea K_v la completación de K con valor absoluto $|\ |$. Y sea (Γ, t, s) una composición de E y K_v, es decir, tenemos el diagrama



De este diagrama, como E es finito sobre K se sigue que Γ es finito sobre $s(K_v)$. Denotaremos el valor absoluto de K_v (con el cual es completación de K) como $|\ |$. En $s(K_v)$ definimos la función $|\ |_s\colon s(K_v) \to \mathbb{R}_{\geq 0}$ mediante $|s(a)|_s = |a|$. Ésto define un valor absoluto sobre $s(K_v)$, con el cual es un campo completo. Los dos casos anteriores garantizan que $|\ |_s$ se puede extender a un valor absoluto sobre Γ de manera única. A tal extensión la denotamos como $|\ |_\Gamma$. Si $\alpha \in K \subseteq K_v$, entonces $\alpha = s(\alpha) \in s(K_v)$ y por tanto $|\alpha|_\Gamma = |s(\alpha)|_s = |\alpha|$, es decir, $|\ |_\Gamma$ es extensión del valor absoluto $|\ |$ original. Por último, definimos la función $|\ |_E\colon E \to \mathbb{R}_{\geq 0}$ mediante $|\alpha|_E = |t(\alpha)|_\Gamma$. Ésta resulta ser un valor absoluto sobre E. Además, si $\alpha \in K$, entonces $\alpha = t(\alpha)$, y por tanto $|\alpha|_E = |\alpha|_\Gamma = |\alpha|$, es decir, $|\ |_E$ es una extensión del valor absoluto original.

Supongamos que (Γ_1, t_1, s_1) y (Γ_2, t_2, s_2) son dos composiciones equivalentes, y sea $u : \Gamma_1 \to \Gamma_2$ isomorfismo tal que $ut_1 = t_2$ y $us_1 = s_2$. Con la construcción anterior obtenemos los valores absolutos $|\ |_{s_i}, |\ |_{\Gamma_i}, |\ |_{E_i}$ correspondientes a la composición (Γ_i, t_i, s_i) $(i = 1, 2)$. Definimos en Γ_1 la aplicación $|\ |_u$ mediante $|a|_u = |u(a)|_{\Gamma_2}$. Éste es un valor absoluto sobre Γ_1. Ahora, si

$a \in K_v$, es decir, $s_1(a) \in s_1(K_v)$, tenemos

$$|s_1(a)|_u = |us_1(a)|_{\Gamma_2} = |s_2(a)|_{\Gamma_2} = |s_2(a)|_{s_2} = |a| = |s_1(a)|_{s_1}.$$

Así, $|\ |_u$ es extensión de $|\ |_{s_1}$, por la unicidad de la extensión tenemos $|\ |_u = |\ |_{\Gamma_1}$. Se sigue que para todo $b \in E$

$$|b|_{E_1} = |t_1(b)|_{\Gamma_1} = |t_1(b)|_u = |ut_1(b)|_{\Gamma_2} = |t_2(b)|_{\Gamma_2} = |b|_{E_2}.$$

Por tanto, composiciones equivalentes inducen el mismo valor absoluto sobre E.

Por otro lado, supongamos que las composiciones (Γ_1, t_1, s_1) y (Γ_2, t_2, s_2) inducen el mismo valor absoluto, es decir $|\ |_{E_1} = |\ |_{E_2}$. Notemos que $s_i(K_v) \subseteq \overline{t_i(E)}$, donde la cerradura se toma respecto a la topología inducida por $|\ |_{\Gamma_i}$: Sea $s_i(a) \in s_i(K_v)$, es decir $a \in K_v$. Tomemos una sucesión (a_n) en $K \subseteq E$ tal que $a_n \to a$, entonces $(s_i(a_n))$ es una sucesión en $s_i(K_v)$ tal que $s_i(a_n) \to s_i(a)$, además, para cada n, $s_i(a_n) = a_n = t_i(a_n)$. Por tanto $(s_i(a_n)) = (t_i(a_n))$ es una sucesión en $t_i(E)$. Se sigue que $s_i(a) \in \overline{t_i(E)}$. También tenemos que $t_i(E) \subseteq \overline{t_i(E)}$ y notemos que $\overline{t_i(E)}$ es un subcampo de Γ_i. Se sigue que $\Gamma_i = K(t_i(E), s_i(K_v)) \subseteq \overline{t_i(E)}$ y por tanto $t_i(E)$ es denso en Γ_i.

Definamos $u_0 \colon t_1(E) \to \Gamma_2$ mediante $u_0(t_1(b)) = t_2(b)$. Notamos que Γ_1 es la completación de $t_1(E)$, pues es una extensión de $t_1(E)$, es completo y $t_1(E)$ es denso en él. Como para todo $b \in E$, $|\ |_{E_1} = |\ |_{E_2}$, entonces $|t_1(b)|_{\Gamma_1} = |t_2(b)|_{\Gamma_2}$, luego

$$|u_0(t_1(b))|_{\Gamma_2} = |t_2(b)|_{\Gamma_2} = |t_1(b)|_{\Gamma_1}.$$

El Teorema 2.1.2 implica que u_0 se puede extender a un encaje $u : \Gamma_1 \to \Gamma_2$. Ahora, como Γ_2 es la completación de $t_2(E)$, se tiene $a \in \Gamma_2$ y una sucesión $(t_2(b_n)) \in t_2(E)$ tal que $t_2(b_n) \to a$. Entonces $c = \lim t_1(b_n) \in \Gamma_1$ satisface $u(c) = \lim u_0(t_1(b_n)) = \lim t_2(b_n) = a$. Por tanto u es un isomorfismo. Además, para $a \in K_v$ podemos tomar una sucesión (a_n) en K tal que $a_n \to a$, notamos que entonces $t_i(a_n) = a_n = s_i(a_n) \to s_i(a)$ por tanto

$$us_1(a) = \lim(u_0(t_1(a_n))) = \lim(t_2(a_n)) = \lim(s_2(a_n)) = s_2(a)$$

así $us_1 = us_2$. Por otro lado, para $b \in E$ se tiene $t_1(b) \in t_1(E)$, por tanto $ut_1(b) = u_0(t_1(b)) = t_2(b)$, es decir, $ut_2 = t_1$. Así, las composiciones (Γ_1, t_1, s_1) y (Γ_2, t_2, s_2) son equivalentes.

En particular, se demostró que si (Γ, t, s) es una composición de E y K_v, entonces $t(E)$ es denso en Γ, esto implica que Γ es (isomorfo a) la completación de E respecto al valor absoluto obtenido con nuestra construcción.

Ahora consideremos $|\ |'$ un valor absoluto sobre E que extiende a $|\ |$ y sea $E_{v'}$ la completación de E respecto a $|\ |'$. Notemos que $E, K_v \subseteq E_{v'}$, por tanto podemos considerar EK_v el menor subcampo de $E_{v'}$ que contiene a E y K_v, es decir que (EK_v, inc_E, inc_{K_v}) es una composición de E y K_v. Además el valor absoluto de $E_{v'}$ restringido a EK_v es extensión del valor absoluto de K_v. Por los Teoremas 2.1.5 y 2.1.8, EK_v es completo. Por tanto se sigue que $E_{v'} = EK_v$, y el valor absoluto inducido por (EK_v, inc_E, inc_{K_v}) es $|\ |'$.

Por lo anterior, existe una biyección entre el conjunto de extensiones del valor absoluto de K a un valor absoluto de E y el conjunto de clases de equivalencia de las composiciones de E y K_v. Así las preguntas sobre extensión de valores absolutos se transforman en ¿existen siempre composiciones de la extensión E y la completación K_v? y ¿cuántas existen?

Sean K, E, F como al principio de la subsección. En particular podemos considerar a E y F como K-álgebras, y por tanto podemos considerar $E \otimes_K F$ también con estructura de K-álgebra.

Sea $\mathfrak{p} \leq E \otimes_K F$ un ideal primo, entonces el cociente $(E \otimes_K F)/\mathfrak{p}$ es un dominio. Denotemos con $\Gamma_\mathfrak{p}$ a su campo de cocientes. Definimos las funciones

$$t_\mathfrak{p} \colon E \to (E \otimes_K F)/\mathfrak{p} \subseteq \Gamma_\mathfrak{p} \qquad s_\mathfrak{p} \colon F \to (E \otimes_K F)/\mathfrak{p} \subseteq \Gamma_\mathfrak{p}$$

$$\alpha \mapsto \alpha \otimes 1 + \mathfrak{p} \qquad \alpha \mapsto 1 \otimes \alpha + \mathfrak{p}$$

Estas son encajes de campos. Si además identificamos $K \subseteq (E \otimes_K F)/\mathfrak{p}$ mediante el encaje

$$K \hookrightarrow (E \otimes_K F)/\mathfrak{p}$$
$$\alpha \mapsto \alpha \otimes 1 + \mathfrak{p} = 1 \otimes \alpha + \mathfrak{p}$$

entonces $t_\mathfrak{p}(\alpha) = \alpha \otimes 1 + \mathfrak{p} = \alpha$, y $s_p(\alpha) = 1 \otimes \alpha + \mathfrak{p} = \alpha$, es decir, $t_\mathfrak{p}$ y $s_\mathfrak{p}$ dejan fijos a los elementos de K. Por otro lado, notemos que $\Gamma_\mathfrak{p}$ consiste de los elementos de la forma $\frac{\sum a_i \otimes b_i + \mathfrak{p}}{\sum a'_j \otimes b'_j + \mathfrak{p}}$. Por tanto si $\alpha \in K$ tenemos $\alpha = \alpha \otimes 1 + \mathfrak{p} = \frac{a \otimes 1 + \mathfrak{p}}{1 \otimes 1 + \mathfrak{p}} \in \Gamma_\mathfrak{p}$; si $\alpha \in E$ entonces $t_\mathfrak{p}(\alpha) = a \otimes 1 + \mathfrak{p} = \frac{\alpha \otimes 1 + \mathfrak{p}}{1 \otimes 1 + \mathfrak{p}} \in \Gamma_\mathfrak{p}$; y si $\alpha \in F$, entonces $s_\mathfrak{p}(\alpha) = 1 \otimes \alpha + \mathfrak{p} = \frac{1 \otimes \alpha + \mathfrak{p}}{1 \otimes 1 + \mathfrak{p}} \in \Gamma_\mathfrak{p}$. Tenemos entonces que $K, t_\mathfrak{p}(E), s_\mathfrak{p}(F) \subseteq \Gamma_\mathfrak{p}$ y por tanto $K(t_\mathfrak{p}(E), s_\mathfrak{p}(F)) \subseteq \Gamma_\mathfrak{p}$. También notemos que para cualesquiera $\alpha \in E$ y $\beta \in F$ se tiene $\alpha \otimes 1 + \mathfrak{p}, 1 \otimes \beta + \mathfrak{p} \in K(t_\mathfrak{p}(E), s_\mathfrak{p}(F))$, por tanto $(\alpha \otimes 1 + \mathfrak{p})(1 \otimes \beta + \mathfrak{p}) = \alpha \otimes \beta + \mathfrak{p} \in K(t_\mathfrak{p}(E), s_\mathfrak{p}(F))$, así, los cocientes de sumas finitas de elementos como este pertenecen también a $K(t_\mathfrak{p}(E), s_\mathfrak{p}(F))$, es decir $\Gamma_p \subseteq K(t_\mathfrak{p}(E), s_\mathfrak{p}(F))$. Se sigue que son iguales.

Hemos demostrado que dado un ideal primo $\mathfrak{p} \leq E \otimes_K F$, $(\Gamma_\mathfrak{p}, t_\mathfrak{p}, s_\mathfrak{p})$ es una composición de E y F. Esto respondiendo la primera pregunta: siempre existe al menos una composición de dos extensiones de K, pues todo anillo distinto de cero contiene un ideal primo.

Ahora consideremos $\mathfrak{p}, \mathfrak{p}' \leq E \otimes_K F$ dos ideales primos tales que sus correspondientes composiciones $(\Gamma_\mathfrak{p}, t_\mathfrak{p}, s_\mathfrak{p})$ y $(\Gamma_{\mathfrak{p}'}, t_{\mathfrak{p}'}, s_{\mathfrak{p}'})$ son equivalentes, es decir, que existe $u\colon \Gamma_\mathfrak{p} \to \Gamma_{\mathfrak{p}'}$ isomorfismo tal que $ut_\mathfrak{p} = t_{\mathfrak{p}'}$ y $us_\mathfrak{p} = s_{\mathfrak{p}'}$. Notemos que para todos $\alpha \in E, \beta \in F$ se tiene

$$u(\alpha \otimes 1 + \mathfrak{p}) = u(t_\mathfrak{p}(\alpha)) = t_{\mathfrak{p}'}(\alpha) = \alpha \otimes 1 + \mathfrak{p}'$$

y

$$u(1 \otimes \beta + \mathfrak{p}) = u(s_\mathfrak{p}(\beta)) = s_{\mathfrak{p}'}(\beta) = 1 \otimes \beta + \mathfrak{p}',$$

por tanto

$$u\left(\sum \alpha_i \otimes \beta_i + \mathfrak{p}\right) = \sum u(\alpha \otimes 1 + \mathfrak{p})u(1 \otimes \beta_i + \mathfrak{p}) = \sum \alpha \otimes \beta_i + \mathfrak{p}'.$$

En particular, si $\sum a_i \otimes b_i \in \mathfrak{p}$, entonces $\sum a_i \otimes b_i + \mathfrak{p} = \mathfrak{p}$ y como u es homomorfismo,

$$\sum a_i \otimes b_i + \mathfrak{p}' = u\left(\sum a_i \otimes b_i + \mathfrak{p}\right) = \mathfrak{p}'.$$

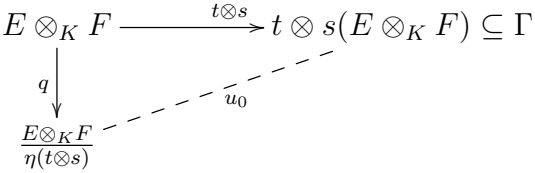
Se sigue que $\sum a_i \otimes b_i \in \mathfrak{p}'$ y por tanto $\mathfrak{p} \subseteq \mathfrak{p}'$. Análogamente (usando u^{-1}) se tiene que $\mathfrak{p}' \subseteq \mathfrak{p}$, por tanto $\mathfrak{p} = \mathfrak{p}'$. Así, hemos demostrado que ideales distintos inducen composiciones no equivalentes.

Por último consideraremos una composición (Γ, t, s). Definimos

$$f\colon E \times F \to \Gamma$$

$$(\alpha, \beta) \mapsto t(\alpha)s(\beta)$$

Notemos que f es una aplicación bilineal. Por la propiedad universal del producto tensorial existe una única $t \otimes s\colon E \otimes_K F \to \Gamma$ tal que $t \otimes s(\alpha \otimes \beta) = t(\alpha)s(\beta)$. Tenemos el siguiente diagrama:



donde q es la aplicación cociente y u_0 es el isomorfismo único inducido por $t \otimes s$. Como Γ es campo, entonces la imagen $t \otimes s(E \otimes_K F)$ es un dominio y por tanto $\mathfrak{p} = \eta(t \otimes s)$ es un ideal primo. Consideremos la composición $(\Gamma_\mathfrak{p}, t_\mathfrak{p}, s_\mathfrak{p})$ construida con el procedimiento anterior. Notemos que u_0 se puede extender a un encaje $u : \Gamma_p \to \Gamma$. Además, un elemento de $\Gamma = K(t(E), s(F))$ es

de la forma $\frac{\sum t(a_i)s(b_i)}{\sum t(a'_j)s(b'_j)}$, por tanto $\frac{\sum a_i\otimes b_i+\mathfrak{p}}{\sum a'_j\otimes b'_j+\mathfrak{p}} \in \Gamma_p$ satisface $u\left(\frac{\sum a_i\otimes b_i+\mathfrak{p}}{\sum a'_j\otimes b'_j+\mathfrak{p}}\right) = \frac{\sum t(a_i)s(b_i)}{\sum t(a'_j)s(b'_j)}$, es decir, u es sobreyectiva y por tanto un isomorfismo. Por último notemos que para todo $a \in E$ se tiene $u(t_\mathfrak{p}(a)) = u(a \otimes 1 + \mathfrak{p}) = t(a)s(1) = t(a)$, es decir $ut_\mathfrak{p} = t$. Análogamente $us_\mathfrak{p} = s$, por tanto (Γ, t, s) y (Γ_p, t_p, s_p) son equivalentes.

Con lo anterior hemos definido una aplicación biyectiva

$$\{\mathfrak{p} \leq E \otimes_K F : \text{ideal primo}\} \to \{(\Gamma, t, s) : \text{composición de } E \text{ y } F\}/\sim$$

$$\mathfrak{p} \mapsto [(\Gamma_\mathfrak{p}, t_\mathfrak{p}, s_\mathfrak{p})]$$

donde del lado derecho hacemos cociente sobre la relación de equivalencia de las composiciones.

Ahora la segunda pregunta que queremos responder se ha transformado a ¿cuántos ideales primos tiene el producto tensorial $E \otimes_K F$? Para responder ésto nos restringiremos al caso en que E es separable sobre K.[4] Tenemos el siguiente resultado técnico:

Lema 2.1.4 *Sean E, F y K como antes. Si $E = K[X]/\langle f\rangle$ para algún $f \in K[X]$ con $\partial f \geq 1$, entonces $E \otimes_K F \cong F[X]/\langle f\rangle_F$, donde $\langle f\rangle_F$ denota al ideal de $F[X]$ generado por f.*

Para la demostración se puede consultar [3, pág 25].

Teorema 2.1.9 *Sean E, F y K como antes, y además E separable sobre K. Entonces $E \otimes_K F$ es producto de extensiones finitas y separables sobre F.*

Demostración: Como E es separable y finito sobre K, entonces existe $\alpha \in E$ tal que $E = K(\alpha)$. Sea $f(X) \in K[X]$ el polinomio irreducible de α. Entonces $E = K(\alpha) = K[X]/\langle f\rangle$, y por el lema anterior $E \otimes_K F \cong F[X]/\langle f\rangle_F$. Supongamos que en $F[X]$ se tiene la factorización $f(X) = f_1(X)\dots f_l(X)$ con los $f_i(X)$ irreducibles.

Tenemos que $\cap_i\langle f_i\rangle = \langle f\rangle_F$. En efecto: Si $h \in \cap_i\langle f_i\rangle$, entonces, $f_1|h$, digamos $h(X) = f_1(X)h_1(X)$ con $h_1 \in F[X]$. También $f_2|h$, y como los f_i son irreducibles se sigue que $f_2|h_1$, digamos $h_1(X) = f_2(X)h_2(X)$ con $h_2 \in F[X]$, entonces $h(X) = f_1(X)f_2(X)h_2(X)$. Inductivamente $h(X) = f_1(X)f_2(X)\dots f_l(X)h_l(X) = f(X)h_l(X)$ con $h_l \in F[X]$. Así $h \in \langle f\rangle$. Recíprocamente, como cada $f_i|f$, entonces $\langle f\rangle \subseteq \langle f_i\rangle$. La afirmación se sigue. Además, para $i \neq j$, $(f_i, f_j) = 1$, entonces existen $q_1, q_2 \in F[X]$ tales que $1 = f_i(X)q_1(X) + f_j(X)q_2(X)$, por tanto $\langle f_i\rangle + \langle f_j\rangle = \langle 1\rangle = F[X]$.

[4] Este problema tiene solución en el caso general, pero para nuestros fines basta estudiar el caso separable.

Por el Teorema chino del residuo tenemos

$$F[X]/\langle f\rangle_F = F[X]/\cap_i \langle f_i\rangle \cong F[X]/\langle f_1\rangle \times \cdots \times F[X]/\langle f_l\rangle.$$

Resta notar que, como cada f_i es irreducible separable en $F[X]$, entonces cada factor $F[X]/\langle f_i\rangle$ es una extensión separable de F. ■

De hecho la descomposición de la que habla el teorema es única. Se puede consultar por ejemplo en [3, pág 19].

Sea K un campo con valor absoluto $|\ |$ y E es una extensión finita separable sobre K. Por el teorema anterior con $F = K_v$ se tiene que $E \otimes_K K_v$ se descompone como producto de extensiones finitas separables sobre K_v, digamos $E \otimes_K K_v = L_1 \times \cdots \times L_r$. Notemos que $E \otimes_K K_v$ tiene exactamente r ideales primos, a saber, $L_1 \times \cdots \times 0 \times \cdots \times L_r$ donde el cero aparece en el i-ésimo factor ($i = 1, \ldots, r$, y r es el número de factores irreducibles de $Irr(\alpha, K)(X)$ en $K_v[X]$). De hecho, estos ideales son maximales.

Concluimos que el valor absoluto de K se puede extender a E de r formas distintas. Además, si nos fijamos en el i-ésimo ideal primo de $E \otimes_K K_v$ y su composición correspondiente mediante el estudio anterior, el campo de ésta es

$$\frac{E \otimes_K K_v}{L_1 \times \cdots \times 0 \times \cdots \times L_r} = \frac{L_1 \times \cdots \times L_r}{L_1 \times \cdots \times 0 \times \cdots \times L_r} \cong L_i,$$

se sigue que el i-ésimo factor de $E \otimes_K K_v$ es (isomorfo a) la completación de E respecto a la i-ésima extensión del valor absoluto a la cual denotaremos como E_{v_i}.

Definimos el *grado local* de E sobre K respecto a la i-ésima extensión como $n_i = [E_{v_i} : K_v]$. Si $[E : K] = n$ y $\{u_1, \ldots, u_n\}$ es una base para E sobre K, se puede demostrar que $\{1 \otimes u_1, \ldots, 1 \otimes u_n\}$ es base para $E \otimes_K K_v$ sobre K_v. Por tanto

$$\begin{aligned} n &= \dim_{K_v}(E \otimes_K K_v) = \dim_{K_v}(E_{v_1} \times \cdots \times E_{v_r}) = \sum \dim_{K_{v_i}}(E_{v_i}) \\ &= \sum [E_{v_i} : K_v] = \sum n_i \end{aligned}$$

Escribimos estos resultados en el siguiente teorema:

Teorema 2.1.10 *Sea K un campo con valor absoluto $|\ |$ y K_v su completación. Sea $E = K(a)$ una extensión separable sobre K de grado n con $f(X) \in K[X]$ el polinomio irreducible de a. Si en $K_v[X]$ se tiene la factorización $f(X) = f_1(X) \ldots f_r(X)$ con los f_i irreducibles, entonces existen exactamente r extensiones de $|\ |$ a un valor absoluto de E. Las correspondiente completaciones de E son isomorfas a $K_v[X]/\langle f_i(X)\rangle$, y el grado local es $n_i = \partial f_i$, además $\sum n_i = n$.*

2.2. Índice de ramificación y grado residual

En la Sección 1.3 definimos el índice de ramificación y el grado residual de los ideales primos de un campo de números respecto a una extensión finita de éste. En esta sección veremos de qué forma se relacionan estos valores con las extensiones de valores absolutos.

Sea K un campo con un valor absoluto no arquimediano $|\ |$. Definamos

$$R = \{x \in K : |x| \leq 1\} \quad \text{y} \quad \mathfrak{p} = \{x \in K : |x| < 1\}.$$

R resulta ser un subanillo de K y se le conoce como *el anillo de valuación de* $|\ |$ *o de* K, y $\mathfrak{p}$ es un ideal de R, de hecho es su único ideal maximal y se le llama *ideal de valuación de* $|\ |$ *o de* K. Podemos notar que para cada elemento $x \in K$ se tiene $x \in R$ o $x^{-1} \in R$, de manera general, decimos que un subanillo de un campo es *un anillo de valuación* si tiene esta propiedad. En un anillo de valuación se puede probar que las no unidades forman un ideal, de hecho es el único ideal maximal del anillo. En nuestro caso, las unidades de R son $U(R) = \{x \in K : |x| = 1\} = R \setminus \mathfrak{p}$, por tanto $\mathfrak{p}$ es el único ideal maximal de R. En particular el cociente $R/\mathfrak{p}$ es un campo y se le conoce como *el campo residual de* $|\ |$ *o de* K.

Si E es una extensión (finita o infinita) de K y $|\ |$ se extiende a E, sean S y $\mathfrak{B}$ el anillo e ideal de valuación de $|\ |$ en E, R y $\mathfrak{p}$ como antes. Entonces se tiene un encaje natural de campos:

$$\begin{aligned} R/\mathfrak{p} &\to S/\mathfrak{B} \\ a + \mathfrak{p} &\mapsto a + \mathfrak{B} \end{aligned}$$

mediante el cual podemos identificar a $R/\mathfrak{p}$ como un subcampo de $S/\mathfrak{B}$ y podemos considerar $f = [S/\mathfrak{B} : R/\mathfrak{p}]$, a este número le llamamos *grado residual de E sobre K respecto al valor absoluto* $|\ |$.

Por otro lado, consideremos los grupos de valuación $|K^*|$ y $|E^*|$, éstos son subgrupos de $\mathbb{R}_{>0}$ y es claro que $|K^*| \leq |E^*|$, por tanto podemos considerar $e = [|E^*| : |K^*|]$, a éste número se le llama *índice de ramificación de E sobre K* respecto a $|\ |$.

Cuando E es una extensión finita de K, e y f también son finitos. De hecho se tiene $ef \leq [E : K]$. Pero se puede dar información mas precisa acerca de estos valores cuando $|\ |$ cumple una propiedad extra: decimos que un valor absoluto no arquimediano $|\ |$ es *discreto* si su grupo de valuación es cíclico. Se tienen los siguientes resultados:

Proposición 2.2.1 *Sea K un campo completo respecto a un valor absoluto $|\ |$ discreto y E una extensión finita de K. Entonces $ef = [E : K]$.*

La demostración se puede consultar en [4], Proposición 9.3.

Teorema 2.2.1 *Sean K un campo con un valor absoluto $|\ |$ discreto, E una extensión separable finita sobre K de grado n y $|\ |_1, \ldots, |\ |_r$ las distintas extensiones de $|\ |$ a un valor absoluto sobre E con e_i y f_i el índice de ramificación y grado residual respecto a $|\ |_i$ $(i = 1 \ldots, r)$. Entonces $\sum_i e_i f_i = n$.*

Demostración: Si E_{v_i} denota la completación de E respecto a $|\ |_i$, la proposición anterior dice que $e_i f_i = [E_{v_i} : K_v] = n_i$, y por el Teorema 2.1.10 tenemos $[E : K] = n = \sum n_i = \sum e_i f_i$. ■

Ahora consideremos K campo de números, $\mathcal{O}_K$ su anillo de enteros y $\mathfrak{p} \leq \mathcal{O}_K$ un ideal primo. Para cada $a \in K \setminus \{0\}$, $\langle a \rangle = \{ax : x \in \mathcal{O}_K\}$ es un ideal fraccionario y podemos escribir $\langle a \rangle = \mathfrak{p}^{v_\mathfrak{p}(a)} \frac{\mathfrak{a}}{\mathfrak{b}}$ con $v_\mathfrak{p}(a) \in \mathbb{Z}$, $\mathfrak{p} \nmid \mathfrak{a}, \mathfrak{b}$, y con $\mathfrak{a}$ y $\mathfrak{b}$ sin factores primos en común. Por el Teorema 1.2.1 y la observación subsecuente a éste se tiene que la expresión para $\langle a \rangle$ es única y por tanto podemos definir la aplicación

$$\begin{aligned} v_\mathfrak{p} \colon K &\to \mathbb{Z} \cup \{\infty\} \\ a &\mapsto \begin{cases} v_\mathfrak{p}(a), & a \neq 0 \\ \infty, & a = 0 \end{cases} \end{aligned}$$

Esta aplicación define una valuación sobre K.

Sea p el entero primo de $\mathfrak{p}$, en particular se tiene que $\mathfrak{p}$ divide a $p\mathcal{O}_K$, digamos $p\mathcal{O}_K = \mathfrak{p}^e \mathfrak{a}$ con $\mathfrak{p} \nmid \mathfrak{a}$, es decir que $e = e_{K/\mathbb{Q}}(\mathfrak{p})$ es el índice de ramificación de $\mathfrak{p}$ en $K/\mathbb{Q}$ definido en la Sección 1.3. Si $a \in \mathbb{Q} \setminus \{0\}$, supongamos que $a = p^{v_p(a)} \frac{\alpha}{\beta}$ con $(\alpha, \beta) = (\alpha, p) = (\beta, p) = 1$ y calculemos

$$\langle a \rangle_K = \langle a \rangle_\mathbb{Q} \mathcal{O}_K = (p\mathcal{O}_K)^{v_p(a)} \mathfrak{b} = \mathfrak{p}^{e v_p(a)} \mathfrak{a}^{v_p(a)} \mathfrak{b},$$

donde $\mathfrak{b} = \frac{\alpha}{\beta} \mathcal{O}_K$ y por tanto $v_\mathfrak{p}(a) = e v_p(a)$.

Definamos

$$\begin{aligned} |\ |_\mathfrak{p} \colon K &\to \mathbb{R}_{\geq 0} \\ a &\mapsto (1/p)^{\frac{v_\mathfrak{p}(a)}{e}} \end{aligned}$$

Éste es un valor absoluto sobre K, además es extensión de $|\ |_p$ el valor absoluto p-ádico definido al principio del capítulo, pues para cada $a \in \mathbb{Q} \setminus \{0\}$ tenemos

$$|a|_\mathfrak{p} = (1/p)^{\frac{v_\mathfrak{p}(a)}{e}} = (1/p)^{\frac{e v_p(a)}{e}} = (1/p)^{v_p(a)} = |a|_p.$$

Éste valor absoluto es conocido como *el valor absoluto $\mathfrak{p}$-ádico* sobre K.

Tenemos el siguiente resultado:

Proposición 2.2.2 *Sea $\mathcal{O}_K$ el anillo de enteros de un campo de números K, entonces:*

1) *Cualquier anillo de valuación de K que contiene a $\mathcal{O}_K$ es una localización $\mathcal{O}_{K,\mathfrak{p}}$ de éste.*

2) *Cualquier valor absoluto no arquimediano en K que tiene anillo de valuación igual a una localización $\mathcal{O}_{K,\mathfrak{p}}$ es (equivalente a) el valor absoluto $\mathfrak{p}$-ádico.*

3) *Existe un isomorfismo de $\mathcal{O}_K/\mathfrak{p}$ en $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ definido mediante $a+\mathfrak{p} \mapsto a+\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$.*

El resultado se puede consultar en [4], Proposición 10.10.

Teorema 2.2.2 *Sean K un campo de números y E extensión finita sobre K, $\mathfrak{p} \leq \mathcal{O}_K$ un ideal primo, $|\ |_{\mathfrak{p}}$ valor absoluto $\mathfrak{p}$-ádico en K, y $\mathfrak{p}\mathcal{O}_E = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_r^{e_r}$ la factorización de $\mathfrak{p}\mathcal{O}_E$ en ideales primos de $\mathcal{O}_E$. Entonces, para cada $\mathfrak{q}_i$ existe una única extensión de $|\ |_{\mathfrak{p}}$ a un valor absoluto $\mathfrak{q}_i$-ádico $|\ |_{\mathfrak{q}_i}$ en E, a saber, $|\ |_{\mathfrak{q}_i} = \gamma^{v_{\mathfrak{p}}(-)/e_i}$ con $\gamma = \left(\frac{1}{p}\right)^{\frac{1}{e_{K/\mathbb{Q}}(\mathfrak{p})}}$. Además $|\ |_{\mathfrak{q}_i}$ y $|\ |_{\mathfrak{q}_j}$ son no equivalentes cuando $i \neq j$, y éstas son las únicas extensiones de $|\ |_{\mathfrak{p}}$ a E.*

Para la demostración se puede consultar el Teorema 10.9 de [4].

El siguiente resultado nos da la relación que queremos:

Teorema 2.2.3 *Con la notación anterior, e_i es el índice de ramificación de E sobre K respecto a $|\ |_{\mathfrak{q}_i}$ y $[\mathcal{O}_E/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$ es el grado residual.*

Demostración: Notemos que $|K^*|_{\mathfrak{p}} = \langle\gamma\rangle$ y $|E^*|_{\mathfrak{q}_i} = \langle\gamma^{1/e_i}\rangle$ con $\gamma = \frac{1}{p}$, por tanto el índice de ramificación es

$$[|E^*|_{\mathfrak{q}_i} : |K^*|_{\mathfrak{p}}] = [\langle\gamma^{1/e_i}\rangle : \langle\gamma\rangle] = e_i.$$

Para la segunda afirmación se demuestra que dada una base $\{v_j + \mathfrak{q}_i : j \in J\}$ para $\mathcal{O}_E/\mathfrak{q}_i$ como $\mathcal{O}_K/\mathfrak{p}$ - espacio vectorial, entonces $\{\frac{v_j}{1} + \mathfrak{q}_i\mathcal{O}_{E,\mathfrak{q}_i} : j \in J\}$ es base para $\mathcal{O}_{E,\mathfrak{q}_i}/\mathfrak{q}_i\mathcal{O}_{E,\mathfrak{q}_i}$ como $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ - espacio vectorial. Por tanto el grado residual es

$$[\mathcal{O}_{E,\mathfrak{q}_i}/\mathfrak{q}_i\mathcal{O}_{E,\mathfrak{q}_i} : \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}] = [\mathcal{O}_E/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]. \qquad \blacksquare$$

Teorema 2.2.4 *Si E/K es una extensión normal de campos de números, $\mathfrak{p} \leq \mathcal{O}_L$ es un ideal primo y $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_r^{e_r}$, entonces $e_1 = \cdots = e_r = e$ y $f_1 = \cdots = f_r = f$ y por tanto $[E : K] = ref$.*

Demostración: Para cada $\mathfrak{B}_i$ y $\sigma \in Gal(E/K)$ se tiene que $\sigma\mathfrak{B}_i$ es un divisor de $\mathfrak{p}\mathcal{O}_E$. Además, para $\mathfrak{B}_i$ y $\mathfrak{B}_j$ en la factorización de $\mathfrak{p}\mathcal{O}_E$ siempre podemos encontrar $\sigma \in Gal(E/K)$ tal que $\mathfrak{B}_i = \sigma\mathfrak{B}_j$ (Proposición 11, Capítulo 1 de [6]). De este modo $\sigma \in Gal(E/K)$ permuta a los divisores de $\mathfrak{p}\mathcal{O}_E$, entonces tenemos

$$\mathfrak{p}\mathcal{O}_E = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_j^{e_j} \cdots \mathfrak{B}_r^{e_r} = \sigma\mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_i^{e_j} \cdots \sigma\mathfrak{B}_r^{e_r}$$

y por la factorización única de ideales se tiene $e_i = e_j$. Para la igualdad de los grados residuales notemos que la aplicación

$$\begin{aligned} \mathcal{O}_L/\mathfrak{B}_j &\to \mathcal{O}_L/\mathfrak{B}_i \\ x + \mathfrak{B}_j &\mapsto \sigma x + \mathfrak{B}_i \end{aligned}$$

es un isomorfismo de campos, por tanto

$$f_i = [\mathcal{O}_L/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\mathfrak{B}_j : \mathcal{O}_K/\mathfrak{p}] = f_j.$$

La última afirmación se sigue de lo anterior y el Teorema 2.2.1. ■

Capítulo 3

Campos $\mathfrak{p}$-ádicos

3.1. Definición y características inmediatas

Consideremos un campo de números K, su anillo de enteros algebraicos $\mathcal{O}_K$ y un ideal primo $\mathfrak{p} \leq \mathcal{O}_K$. Sabemos que $\mathfrak{p}$ induce un valor absoluto no arquimediano y discreto $|\ |_\mathfrak{p}$ sobre K. Notemos que $\mathcal{O}_K$ está contenido en el anillo de valuación de $|\ |_\mathfrak{p}$ y por *1)* de la Proposición 2.2.2 el anillo de valuación es una localización de $\mathcal{O}_K$, de hecho es $\mathcal{O}_{K,\mathfrak{p}}$ y por tanto su ideal de valuación es el único ideal maximal de $\mathcal{O}_{K,\mathfrak{p}}$, es decir $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$.

Recordemos que el campo residual se define como el cociente del anillo de valuación sobre el ideal de valuación. En este caso particular el campo residual es $k_K = \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ y *3)* de la Proposición 2.2.2 implica que $k_K \cong \mathcal{O}_K/\mathfrak{p}$. Además, por el Teorema 2.2.3, $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$ es el grado residual de K sobre $\mathbb{Q}$ respecto a $|\ |_p$, que es finito por el Teorema 2.2.1. En particular se deduce que k_K es un campo finito.

Ahora consideremos a $K_\mathfrak{p}$, la completación de K respecto a $|\ |_\mathfrak{p}$. Un campo como este, es decir, la completación de un campo de números respecto a un valor absoluto discreto, se conoce como *campo* $\mathfrak{p}$*-ádico*. Sean R el anillo de valuación de $K_\mathfrak{p}$ respecto a $|\ |_\mathfrak{p}$ y denotemos al ideal de valuación como $\overline{\mathfrak{p}}$.

Tenemos un encaje natural de k_K en el campo residual de $K_\mathfrak{p}$ definido como

$$\begin{gathered} k_K = \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \to R/\overline{\mathfrak{p}} = k_{K_\mathfrak{p}}. \\ x + \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \mapsto x + \overline{\mathfrak{p}} \end{gathered}$$

De hecho esta aplicación es un isomorfismo. En efecto, si $a \in R \subseteq K_\mathfrak{p}$, por la densidad de de K en $K_\mathfrak{p}$ podemos tomar $b \in K$ tal que $|a - b|_\mathfrak{p} < 1$. En particular $a - b \in \overline{\mathfrak{p}}$. Notemos $|b|_\mathfrak{p} = |a - (a - b)|_\mathfrak{p} \leq \text{máx}\{|a|_\mathfrak{p}, |a - b|_\mathfrak{p}\} \leq 1$,

de modo que $b \in \mathcal{O}_{K,\mathfrak{p}}$. Así

$$k_K \ni b + \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \mapsto b + \overline{\mathfrak{p}} = a + \overline{\mathfrak{p}}.$$

Por tanto $k_K \cong k_{K_\mathfrak{p}}$. En particular, el campo residual de un campo $\mathfrak{p}$-ádico es finito.

También podemos notar que los grupos de valuación de K y $K_\mathfrak{p}$ coinciden. En efecto, es claro que $|K^*|_\mathfrak{p} \subseteq |K_\mathfrak{p}^*|_\mathfrak{p}$. Por otro lado, si $|a|_\mathfrak{p} \in |K_\mathfrak{p}^*|_\mathfrak{p}$, por la densidad de K en $K_\mathfrak{p}$ podemos tomar $b \in K$ tal que $|a-b|_\mathfrak{p} < |a|_\mathfrak{p}$, entonces se tiene $|b|_\mathfrak{p} = |a|_\mathfrak{p}$. De este modo $|a|_\mathfrak{p} = |b|_\mathfrak{p} \in |K^*|_\mathfrak{p}$. En particular, $|\ |_\mathfrak{p}$ en $K_\mathfrak{p}$ es discreto.

Teorema 3.1.1 *Sean $K_\mathfrak{p}$ un campo $\mathfrak{p}$-ádico y $|\ |_\mathfrak{p}$ su valor absoluto, R y $\overline{\mathfrak{p}}$ el anillo e ideal de valuación respectivamente. Entonces R es un dominio de ideales principales (y por tanto de Dedekind). Los elementos de K se pueden expresar de manera única como $a\pi^m$ con π un generador fijo $\overline{\mathfrak{p}}$, $m \in \mathbb{Z}$, y $a \in R$ tal que $\pi \nmid a$.*

Demostración: Sea $|\pi|_\mathfrak{p}$ un generador del grupo $|K_\mathfrak{p}^*|_\mathfrak{p}$. Podemos suponer sin pérdida de generalidad que $|\pi|_\mathfrak{p} < 1$, es decir que $\pi \in \mathfrak{p}$. Demostraremos que $\overline{\mathfrak{p}} = \langle \pi \rangle$. Sea $x \in \overline{\mathfrak{p}}$ y escribamos $|x|_\mathfrak{p} = |\pi|_\mathfrak{p}^m$ con $m \in \mathbb{Z}$. Como $|x|_\mathfrak{p} < 1$ entonces se sigue que $m > 0$. Por otro lado $|x\pi^{-m}| = 1$ y así $x\pi^{-m} = u \in U(R)$, es decir que $x = \pi^m u \in \langle \pi \rangle$ y por tanto $\overline{\mathfrak{p}} \subseteq \langle \pi \rangle$. La otra contención se sigue de que $\pi \in \overline{\mathfrak{p}}$.

Si $a \in R \setminus \overline{\mathfrak{p}}$, entonces $\pi \nmid a$: si no, $a = \pi b$ con $b \in R$, como $|a|_\mathfrak{p} = 1$ y $|\pi|_\mathfrak{p} < 1$, se sigue que $|b|_\mathfrak{p} > 1$, que contradice el hecho de que $b \in R$. Por tanto para $x \in \mathfrak{p} = \langle \pi \rangle$ tenemos que la escritura $a\pi^m$ con $a \in U(R)$ es única.

Si $|x|_\mathfrak{p} > 1$, se tiene $x^{-1} \in \overline{\mathfrak{p}}$ y por tanto podemos escribir de manera única $x^{-1} = a\pi^m$ con $a \in U(R)$ y $m > 0$, entonces $x = a^{-1}\pi^{-m}$. Basta notar que $a^{-1} \in R$. Por último, si $|x|_\mathfrak{p} = 1$, escribimos $x = x\pi^0$.

Por último demostraremos que todos los ideales de R son de la forma $\langle \pi^m \rangle$ con $m \in \mathbb{N}$. Sea $\mathfrak{a} \leq R$ un ideal, del Teorema 1.2.1 tenemos una factorización de $\mathfrak{a}$ como producto de primos, pero en este caso $\overline{\mathfrak{p}}$ es el único ideal primo (porque es el único maximal) entonces la factorización es de la forma $\mathfrak{a} = \overline{\mathfrak{p}}^{\,m} = \langle \pi \rangle^m = \langle \pi^m \rangle$. ■

Corolario 3.1.1 *Todos los ideales fraccionarios de R son de la forma $\langle \pi^m \rangle$ con $m \in \mathbb{Z}$.*

Demostración: Si $\mathfrak{a}$ es un ideal fraccionario se puede escribir como el cociente de dos ideales enteros, digamos $\langle \pi^{m_1} \rangle / \langle \pi^{m_2} \rangle = \langle \pi^{m_1 - m_2} \rangle$. ■

Proposición 3.1.1 *Sean K campo de números, $\mathfrak{p} \leq \mathcal{O}_K$ ideal primo, $K_\mathfrak{p}$ la completación de K respecto a $|\ |_\mathfrak{p}$, $\overline{\mathfrak{p}}$ y R el ideal y anillo de valuación. Entonces para todo $t \in \mathbb{N}$ tenemos $\mathfrak{p}^t R = (\overline{\mathfrak{p}})^t$ y $\overline{\mathfrak{p}}^t \cap \mathcal{O}_K = \mathfrak{p}^t$.*

En particular notemos que $\overline{\mathfrak{p}} \cap \mathbb{Z} = (\overline{\mathfrak{p}} \cap \mathcal{O}_K) \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ para algún primo $p \in \mathbb{Z}$. Al igual que en el caso de campos de números, nos podemos referir a p como el entero primo de $\overline{\mathfrak{p}}$.

Sea K un campo $\mathfrak{p}$-ádico, R su anillo de valuación y $\mathfrak{p}$ el único ideal maximal, a continuación se dan algunos resultados topológicos.

Lema 3.1.1 *R es compacto.*

Demostración: Sea $X = \{x_j : j \in J,\ \#J = \infty\}$ un subconjunto infinito de R. Demostraremos que X tiene un punto de acumulación. Como el campo residual es finito y podemos tomar A un sistema de representantes finito de R módulo $\mathfrak{p}$. Sea π un generador de $\mathfrak{p}$.

Para cada $j \in J$ tenemos: $x_j = a_{j0} + u_0\pi$ con $a_{j0} \in A$, y $u_0 \in R$. Análogamente, $u_0 = a_{j1} + u_1\pi$, entonces $x_j = a_{j0} + (a_{j1} + u_1\pi)\pi = a_{j0} + a_{j1}\pi + u_1\pi^2$. Repitiendo el procedimiento iteradas veces obtenemos una expresión para x_j como serie de potencias $\sum_{n=0}^{\infty} a_{jn}\pi^n$ con coeficientes en A.

Como A es finito, existe $a_0^* \in A$ tal que $a_0^* = a_{j0}$ para una cantidad infinita de $j's$. Sea $J_0 = \{j \in J : a_{j0} = a_0^*\} \subseteq J$, por la observación anterior J_0 es un conjunto infinito. Asimismo, podemos encontrar a_1^* tal que $a_1^* = a_{j1}$ para una cantidad infinita de $j's$ en J_0, y definimos $J_1 = \{j \in J_0 : a_1^* = a_{j1}\}$. Inductivamente encontramos una sucesión (a_n^*) en A y una sucesión de subconjuntos de J.

Entonces $a^* = \sum_{n=0}^{\infty} a_n^*\pi^n$ es un punto de acumulación de X: Para $\varepsilon > 0$ fijo, sean $l \in \mathbb{N}$ tal que $|\pi|_\mathfrak{p}^l < \varepsilon$ y $j \in J_{l-1} \setminus J_l$. Si $s_m = \sum_{n=l}^{m}(a_{jn} - a_n^*)\pi^n$ $(m \geq l)$, entonces

$$\begin{aligned} |x_j - a^*|_\mathfrak{p} &= \left| \sum_{n=0}^{\infty} a_{jn}\pi^n - \sum_{n=0}^{\infty} a_n^*\pi^n \right|_\mathfrak{p} = \left| \sum_{n=0}^{\infty} (a_{jn} - a_n^*)\pi^n \right|_\mathfrak{p} \\ &= \left| \lim_{m\to\infty} s_m \right|_\mathfrak{p} = \lim_{m\to\infty} |s_m|. \end{aligned}$$

Ahora, tenemos que

$$|s_m| \leq \max_{n=l}^{m}\{|a_{jn} - a_n^*||\pi|^n\} \leq \max_{n=l}^{m}\{|\pi|^n\} = |\pi|^l;$$

por tanto

$$|x_j - a^*|_\mathfrak{p} = \lim_{m\to\infty} |s_m| \leq \lim_{m\to\infty} |\pi|^l = |\pi^l| < \varepsilon. \qquad \blacksquare$$

Del lema en particular se sigue que R es cerrado en K, pues es un subconjunto compacto en un espacio Hausdorff.

Lema 3.1.2 $\mathfrak{p}$ *es abierto en* K

Demostración: Para $x \in \mathfrak{p}$ sea $\varepsilon = 1 - |x| > 0$. Cada $y \in B_\varepsilon(x)$ satisface

$$|y| = |y - x + x| \leq |y - x| + |x| < \varepsilon + |x| = 1 - |x| + |x| = 1$$

por tanto $y \in \mathfrak{p}$ y así $B_\varepsilon(x) \subseteq \mathfrak{p}$. ■

Proposición 3.1.2 *Sea $x \in R$. La aplicación $izq_x : R \to R$ definida mediante $a \mapsto x + a$ es un homeomorfismo.*

Demostración: Notemos primero que R es un grupo topológico, es decir que las aplicaciones

$$\begin{array}{lll} s\colon R \times R \to R & & i\colon R \to R \\ \quad (a,b) \mapsto a+b & \text{y} & \quad a \mapsto -a \end{array}$$

son continuas. Ahora consideramos el subespacio $\{x\} \times R \subseteq R \times R$ y la aplicación $\alpha = s\,|_{\{x\}\times R}$. Tenemos que $izq_x = \alpha \circ inc$ donde inc es la inclusión de R en $\{x\} \times R$ mediante $a \mapsto (x, a)$. Como α e inc son continuas se sigue que izq_x lo es también.

El mismo argumento demuestra que izq_{-x} es continua. Y además se tiene que $izq_x^{-1} = izq_{-x}$ por lo que izq_x es biyectiva continua y con inversa continua, es decir, un homeomorfismo. ■

Lema 3.1.3 $\mathfrak{p}$ *es compacto en* K.

Demostración: Basta ver que es compacto en R. Notemos que $\mathfrak{p}$ es un subgrupo (aditivo) abierto del grupo topológico compacto R. Podemos escribir a R como la unión disjunta de las clases laterales de $\mathfrak{p}$, es decir

$$R = \bigsqcup_{i\in I}(x_i + \mathfrak{p}) = \bigsqcup_{i\in I} izq_{x_i}(\mathfrak{p}).$$

Como $\mathfrak{p}$ es abierto y cada izq_{x_i} homeomorfismo se sigue que cada $izq_{x_i}(\mathfrak{p})$ es abierto. De este modo $\{izq_{x_i}(\mathfrak{p}) : i \in I\}$ es una cubierta abierta para R que por compacidad debe ser finita, digamos $\{izq_{x_1}(\mathfrak{p}), \ldots, izq_{x_r}(\mathfrak{p})\}$. Sin pérdida de generalidad podemos suponer $x_1 = 0$, es decir, $izq_{x_1}(\mathfrak{p}) = \mathfrak{p}$ y entonces

$$\mathfrak{p} = R \setminus \left(\bigsqcup_{i=2}^{r} izq_{x_i}(\mathfrak{p}) \right).$$

Así, $\mathfrak{p}$ es el complemento de un abierto en R y por tanto cerrado. De topología general se sabe que un cerrado dentro de un compacto es también compacto.■

Lema 3.1.4 $\mathfrak{p}^t$ *es compacto.*

Demostración: Si $* : K \times K \to K$ es la aplicación producto, ésta es continua y $*(\mathfrak{p} \times \mathfrak{p}) = \mathfrak{p}^2$, es decir que $\mathfrak{p}^2$ es la imagen continua de un compacto, por tanto es compacto. Lo anterior se generaliza por inducción. ■

Lema 3.1.5 $\mathfrak{p}^t$ *es abierto.*

Demostración: Definamos la aplicación $Izq_\pi : K \to K$ mediante $a \mapsto \pi a$, de manera similar a la Proposición 3.1.2 se demuestra que Izq_π es un homeomorfismo. Notemos que $\mathfrak{p}^2 = \pi\mathfrak{p} = Izq_\pi(\mathfrak{p})$ y como $\mathfrak{p}$ es abierto en K también lo es $\mathfrak{p}^2$. Lo anterior se generaliza por inducción. ■

Para terminar esta sección tenemos el siguiente teorema que caracteriza los campos $\mathfrak{p}$-ádicos:

Teorema 3.1.2 *Sea K un campo con un valor absoluto $|\ |_v$. Son equivalentes*

1. *K es un campo $\mathfrak{p}$-ádico.*
2. *K satisface*
   a) *$Char(K) = 0$,*
   b) *K es completo respecto a $|\ |_v$ y éste es discreto,*
   c) *El campo residual de K es finito.*
3. *K es extensión finita de $\mathbb{Q}_p$ para algún $p \in \mathbb{Z}$ primo.*

La demostración se puede consultar en [8], Teorema 5.10 de [8].

3.2. Teoremas de ramificación

En adelante K será un campo $\mathfrak{p}$-ádico, R su anillo de valuación y denotaremos su ideal de valuación también como $\mathfrak{p}$. Sea L una extensión de K de grado n. Denotaremos como S al anillo de valuación de L respecto a la única extensión del valor absoluto de K (única en virtud del Teorema 2.1.8), y $\mathfrak{B}$ a su único ideal primo. Del teorema anterior se tiene que L es también un campo $\mathfrak{p}$-ádico y de la Proposición 2.2.1 tenemos $n = ef$ con e el índice de ramificación y f el grado residual de L sobre K respecto a sus valores absolutos.

Al igual que en la Sección 1.3 se pueden definir el índice de ramificación y el grado residual mediante la factorización del ideal primo de un campo

$\mathfrak{p}$-ádico (puesto que su anillo de valuación es un dominio de Dedekind). Se demuestra que tal definición coincide con la dada en la Sección 2.2. De este modo tenemos la expresión $\mathfrak{p}S = \mathfrak{B}^e$, donde e es el índice de ramificación de $\mathfrak{B}$ en L/K. Como $\mathfrak{p}$ y $\mathfrak{B}$ son los únicos ideales primos en sus respectivos anillos, podemos referirnos a e como *el índice de ramificación de* L/K, y lo denotaremos en este caso como $e(L/K)$. Asimismo, denotaremos al grado residual de la extensión como $f = f(L/K)$.

De manera similar a las definiciones de la Sección 1.3 diremos que la extensión L/K es no ramificada cuando $e = 1$; completamente ramificada cuando $e = n$; mansamente ramificada cuando p, el entero primo de $\mathfrak{p}$, no divide a e; y salvajemente ramificada cuando es ramificada y $p|e$.

Denotemos con v_K y v_L a las valuaciones correspondientes a los valores absolutos de K y L, respectivamente. Notemos que si $x = a\pi^m \in K$ con $\pi \in \mathfrak{p}$ un generador y $\pi \nmid a$, entonces $v_K(x) = m$. Una fórmula análoga se obtiene para v_L.

Lema 3.2.1 *(de Hensel) Sean $F \in R[X]$ un polinomio y $\overline{F} \in k_K$ el polinomio que se obtiene al reducir los coeficientes de F módulo $\mathfrak{p}$. Si $\overline{F}$ se puede escribir como producto de dos polinomios primos relativos no constantes $g, h \in k_K[X]$, entonces existen dos polinomios primos relativos $G, H \in R[X]$ que satisfacen $\partial G = \partial g$, $\overline{G} = g$, $\overline{H} = h$, $F = GH$. Si además g es mónico podemos elegir G mónico.*

Para la demostración se puede consultar en [8], Teorema 5.6.

Corolario 3.2.1 *Sean F y $\overline{F}$ como en el lema. Si $\overline{F}$ tiene una raíz simple $\alpha \in k_K$, entonces existe $a \in R$ tal que $F(a) = 0$ y $\overline{a} = \alpha$.*

Demostración: Por hipótesis podemos escribir $\overline{F}(X) = (X - \alpha)h(X)$ con h primo relativo de $X - \alpha$. Del lema se sigue en particular que existe $G \in R[X]$ que satisface $\partial G = 1$ y $\overline{G} = X - \alpha$. Como $(X - \alpha)$ es mónico, G debe ser de la forma $G(X) = X - a$ y $X - \alpha = \overline{G} = X - \overline{a}$. Así, $F(a) = 0$ y $\overline{a} = \alpha$. ■

Corolario 3.2.2 *Si $F \in R[X]$ es irreducible sobre K entonces $\overline{F}$ es potencia de un irreducible sobre $k_K[X]$.*

Demostración: Si no, entonces podemos encontrar $g, h \in k_K[X]$ primos relativos tales que $\overline{F} = gh$ y del lema se sigue que F se puede factorizar en R y por tanto en K. ■

Lema 3.2.2 *Sea L/K extensión de campos $\mathfrak{p}$-ádicos. L es no ramificada si y sólo si existe $a \in S$ con $L = K(a)$ que satisface la siguiente propiedad:*

Si $F(X) \in R[X]$ es el polinomio irreducible de a y $\varphi(X) \in k_K[X]$ es el polinomio que se obtiene al reducir los coeficientes de F módulo $\mathfrak{p}$, entonces $a + \mathfrak{B} \in k_L$ es raíz simple de φ.

Demostración: Si L es no ramificada sobre K, entonces $n = f = [k_L : k_K]$. Notemos que la extensión de campos residuales es separable (extensión de campos finitos). Sean $a+\mathfrak{B} \in k_L$ generador de la extensión y $\varphi(X) \in k_K[X] \subseteq k_L[X]$ el polinomio irreducible de $a + \mathfrak{B}$, además tomemos $F[X] \in R[X] \subseteq S[X]$ mónico tal que al reducir sus coeficientes módulo $\mathfrak{p}$ obtenemos a φ, notemos que al reducir los coeficientes módulo $\mathfrak{B}$ obtenemos también a φ. Por el Corolario 3.2.1 se tiene $a' \in S$ raíz de F tal que $a' + \mathfrak{B} = a + \mathfrak{B}$, sin pérdida de generalidad $a = a'$. Se sigue que a tiene la propiedad indicada.

Recíprocamente, como F es irreducible sobre K, el Corolario 3.2.2 implica que φ es la potencia de un polinomio irreducible en $k_K[X]$. Como φ tiene una raíz simple, se tiene de hecho que es un polinomio irreducible. Por tanto

$$n = \partial F = \partial \varphi \leq [k_L : k_K] = f \leq n,$$

es decir que $f = n$ y entonces $e = 1$. ■

Corolario 3.2.3 *Si L/K es una extensión de campos $\mathfrak{p}$-ádicos y M es la composición de todos las extensiones no ramificadas de K contenidas en L, entonces M/K es no ramificada y L/M es completamente ramificada. Por tanto cada extensión de campos $\mathfrak{p}$-ádicos se puede descomponer en dos subextensiones, la primera no ramificada y la segunda completamente ramificada.*

Demostración: Si la extensión es no ramificada es inmediato que $L = M$, y si es completamente ramificada no existen extensiones no ramificadas intermedias por tanto en tal caso tenemos $M = K$. Supongamos que no es ninguno de estos casos. Puesto que la extensión L/K es separable, existe sólo una cantidad finita de campos intermedios. En particular, una cantidad finita de campos no ramificados sobre K. Por tanto M es una composición finita de campos y para que sea no ramificada sobre K basta demostrar que la composición de dos campos no ramificados sobre K es no ramificada sobre K. El resto, se sigue por inducción.

Sean L y E dos campos intermedios no ramificados sobre K. Supongamos que $L = K(a)$ con a, F y φ como en el lema. Denotemos como $R_E, \mathfrak{p}_E$ y k_E al anillo de valuación, el ideal de valuación y el campo residual de E, y similarmente $S_{LE}, \mathfrak{B}_{LE}$ y k_{LE} los respectivos objetos de LE. Tenemos $a \in S \subseteq S_{LE}$ tal que $LE = K(a)E = E(a)$. Si $G(X) \in R_E[X]$ es el polinomio irreducible de a en E, como $F \in R[X] \subseteq R_E[X]$ y a es raíz de F, entonces $G(X)|F(X)$. Si $\psi \in k_E[X]$ es el polinomio que se obtiene al reducir G módulo

$\mathfrak{p}_E$, entonces $\psi|\varphi$. Como $K_{LE} \ni a+\mathfrak{B}_{LE} = a+\mathfrak{B}$ es raíz simple de φ, entonces es raíz simple de ψ. Del lema se sigue que LE es no ramificada sobre L, entonces tenemos $e(LE/K) = e(LE/L)e(L/E) = 1$, es decir que LE es no ramificada sobre K.

Sea $f_1 = [k_L : k_M]$ es el grado residual de L/M, queremos ver que $f_1 = 1$. Podemos escribir $k_L = \mathbb{F}_p(\zeta_r)$ para algún r no divisible por p y ζ_r una raíz r-ésima primitiva de 1, de modo que el polinomio $(1+\mathfrak{B})X^r - (1+\mathfrak{B}) \in k_L[X]$ tiene r raíces distintas en k_L, del Corolario citecoro 1 de hensel se sigue que $X^r - 1$ tiene r raíces distintas en $S \subseteq L$.

Así, si N es el campo de descomposición de $X^r - 1$, notamos que $N \subseteq L$. Ahora, si $w_1, \ldots, w_r$ son todas las raíces del polinomio anterior entonces del lema precedente $K(w_i)$ es no ramificada sobre K y por tanto $w_i \in K(w_i) \subseteq M$. Así, todas las raíces de $X^r - 1$ están en M. Se sigue que todas las raíces de $(1 + \mathfrak{B})X^r - (1 + \mathfrak{B})$ están en el campo residual k_M. Así, $k_L = \mathbb{F}_p(\zeta_r) \subseteq k_M \subseteq k_L$, de donde $f_1 = 1$. Por tanto L/M es completamente ramificada. La última afirmación se sigue de lo ya demostrado. ■

Teorema 3.2.1 *Sea K campo $\mathfrak{p}$-ádico. Entonces, a cada extensión finita k de k_K le corresponde una única extensión L/K no ramificada con $k_L = k$. Esta extensión es normal y $Gal(L/K) \cong Gal(k/k_K)$.*

Demostración: Sean $a \in k$ un generador sobre k_K, es decir $k = k_K(a)$, $\varphi \in k_K[X]$ el polinomio irreducible de a y $F \in R[X]$ mónico tal que al reducirlo módulo $\mathfrak{p}$ se obtiene φ. Si b es una raíz de F en $\mathbb{Q}_p^a$, consideremos $L = K(b)$. Denotemos como S al anillo de valuación de L y $\mathfrak{B}$ al ideal de valuación. Notemos que al reducir a F módulo $\mathfrak{B}$ obtenemos el mismo polinomio φ de cual $b+\mathfrak{B}$ es una raíz, es decir que a y $b+\mathfrak{B}$ son conjugados. Podemos suponer que $a = b + \mathfrak{B}$. Se sigue que $k \subseteq k_L$ y entonces

$$[L : K] \leq \partial F = \partial\varphi = [k : k_K] \leq [k_L : k_K] = f(L/K) \leq [L : K].$$

Por lo anterior tenemos que F es irreducible, $k = k_L$ y $f(L/K) = [L : K]$ por tanto $e(L/K) = 1$ y la extensión es no ramificada.

Ahora supongamos que L_1 es otra extensión no ramificada sobre K con $k_{L_1} = k$. Por el Corolario 3.2.1 podemos tomar $b_1 \in L_1$ raíz de F, entonces $K(b_1) \cong K(b) = L$, además

$$[K(b_1) : K] = \partial F = [k : k_K] = [k_{L_1} : k_K] = [L_1 : K]$$

de donde $L \cong L_1$. Para ver que de hecho son iguales demostraremos que L/K es normal, así el isomorfismo $L \to L_1 \subseteq \mathbb{Q}_p^a$ que deja fijos a los elementos de K será un automorfismo (Teorema 3.3, Capítulo V de [7]).

Como k/k_K es normal, k es el campo de descomposición de φ. Sea a_1 raíz de φ. Por el corolario 1 del Teorema 5.6 de [8] tenemos $b_1 \in S$ raíz de F y tal que $b_1 + \mathfrak{B} = a_1$. Si $\varphi(X) = (X - a_1)\varphi_1(X)$ y $F(X) = (X - b_1)F_1(X)$ se sigue que al reducir los coeficientes de F_1 módulo $\mathfrak{p}$ obtenemos a φ_1. Si repetimos el proceso inductivamente obtenemos que $F(X)$ se descompone en factores lineales en $S \subseteq L$ además L está generado por una de sus raíces (para algún i tenemos $b = b_i$), entonces L es el campo de descomposición de F y se sigue que L/K es normal.

Para la última afirmación definamos la aplicación

$$\begin{aligned} \Psi \colon Gal(L/K) &\to Gal(k/k_K) \\ \sigma &\mapsto \overline{\sigma} \colon x + \mathfrak{B} \mapsto \sigma(x) + \mathfrak{B} \end{aligned}$$

En efecto $\overline{\sigma} \in Gal(k_L/k_K)$. Además Ψ es isomorfismo de grupos: Si $\sigma, \tau \in Gal(L/K)$, entonces para todo $x + \mathfrak{B} \in k_L$ se tiene

$$\begin{aligned} \overline{\sigma \circ \tau}(x + \mathfrak{B}) &= \sigma \circ \tau(x) + \mathfrak{B} = \sigma(\tau(x)) + B = \overline{\sigma}(\tau(x) + \mathfrak{B}) \\ &= \overline{\sigma}(\overline{\tau}(x + \mathfrak{B})) = \overline{\sigma} \circ \overline{\tau}(x + \mathfrak{B}) \end{aligned}$$

Por tanto $\Psi(\sigma \circ \tau) = \Psi(\sigma) \circ \Psi(\tau)$. Es decir que Ψ es homomorfismo de grupos.

Para la sobreyectividad, sean a, F, b como antes. Si $\tau \in Gal(k/k_K)$, $\tau a = a_1$ es raíz de φ, entonces existe $b_1 \in S$ tal que $F(b_1) = 0$ y $b_1 + \mathfrak{B} = a_1$, tal b_1 es único. Sea $\sigma \in Gal(L/K)$ tal que $\sigma b = b_1$, entonces

$$\overline{\sigma} a = \overline{\sigma}(b + \mathfrak{B}) = \sigma b + \mathfrak{B} = b_1 + \mathfrak{B} = a_1 = \tau a_1$$

de este modo $\Psi(\sigma) = \overline{\sigma} = \tau$.

Por último, notemos que $\#Gal(L/K) = [L : K] = [k : k_K] = \#Gal(k/k_L)$, por tanto se tiene el isomorfismo. ■

Corolario 3.2.4 *Un Campo $\mathfrak{p}$-ádico tiene exactamente una extensión no ramificada de grado dado.*

Demostración: De la teoría de campos finitos se sabe que dado $n \in \mathbb{N}$ existe una única extensión sobre un campo finito de grado n. En particular, para K $\mathfrak{p}$-ádico y $n \in \mathbb{N}$ fijo existe una una única extensión k de grado n sobre k_K. La afirmación se sigue del teorema. ■

Teorema 3.2.2 *Si K es un campo $\mathfrak{p}$-ádico, entonces la extensión L/K es no ramificada si y sólo si $L = K(\zeta_m)$ con ζ_m una raíz m-ésima primitiva de 1 y el entero primo de $\mathfrak{p}$ no divide a m.*

Para la demostración ver [8], Teorema 5.26.

Teorema 3.2.3 *Sea K un campo $\mathfrak{p}$-ádico y L una extensión completamente ramificada sobre K. Entonces, existe un polinomio de Eisenstein en $K[X]$ y una raíz a de éste tal que $L = K(a)$. Recíprocamente, cada extensión generada por la raíz de un polinomio de Eisenstein es completamente ramificada.*

Demostración: Supongamos primero que $L = K(a)$ con a raíz del polinomio de Eisenstein $X^n + \sum_{i=0}^{n-1} c_i X^i$. Como $c_0 \in \mathfrak{p} \setminus \mathfrak{p}^2 = \langle \pi \rangle \setminus \langle \pi^2 \rangle$, se sigue que $v_K(c_0) = 1$. Además, notemos que para todo $l \in \mathbb{N}$ se tiene $\mathfrak{p}^l S = (\mathfrak{p}S)^l$, se sigue que $c_0 \in \mathfrak{B}^e \setminus \mathfrak{B}^{e+1}$ entonces $v_L(c_0) = e$ con $e = e(L/K)$. Por otro lado tenemos que $a^n = -\sum_{i=0}^{n-1} c_i a^i$, entonces

$$\begin{aligned} n v_L(a) &\geq \text{mín}\left\{v_L(c_i a^i) : i = 0, \ldots, n-1\right\} \\ &= v_L(c_{i_0}) + i_0 v_L(a) \qquad \text{para algún } i_0 \text{ entre 0 y } n-1 \\ &> i_0 v_L(a), \end{aligned}$$

luego $(n - i_0)v_L(a) > 0$ y por tanto $v_L(a) \geq 1$. Por otro lado tenemos que

$$n v_L(a) = v_L(a^n) = v_L(c_0) = e, \tag{3.1}$$

y si fuera $n > e$ entonces $n v_L(a) > e$ que contradice lo anterior, por tanto $n = e$. Así la extensión es completamente ramificada.

Ahora supongamos que L/K es completamente ramificada, fijemos $\pi \in \mathfrak{p}$ y $\Pi \in \mathfrak{B}$ generadores de los ideales, entonces tenemos

$$\langle \pi \rangle = \mathfrak{p} = \mathfrak{B}^e = \langle \Pi^e \rangle.$$

Podemos suponer sin pérdida de generalidad que $\Pi^e = \pi$, es decir que Π es raíz del polinomio de Eisenstein $X^e - \pi \in K[X]$, además se sigue que

$$[K(\Pi) : K] = e = n = [L : K],$$

por tanto $L = K(\Pi)$. ■

Corolario 3.2.5 *Sea $L = K(a)$ generado sobre K por la raíz de un polinomio de Eisenstein. Entonces $v_L(a) = 1$*

Demostración: Se sigue de la Ecuación (3.1) y que $n = e$. ■

Corolario 3.2.6 *Un campo $\mathfrak{p}$-ádico tiene una cantidad finita de extensiones de grado dado.*

Demostración: Sean K un campo $\mathfrak{p}$-ádico y $n \in \mathbb{N}$ fijo. Por el corolario 3.2.3, si L es una extensión de K de grado n siempre tenemos una torre $L \supseteq M \supseteq K$ con M la extensión no ramificada sobre K más grande contenida en L. Por

el corolario 3.2.4 tenemos opciones finitas para M, a saber, exactamente una opción para M por cada divisor de n. Basta entonces demostrar que si se ha fijado M, éste tiene una cantidad finita de extensiones completamente ramificadas de grado m (m divisor de n).

Denotaremos R al anillo de valuación de M y $\mathfrak{p}$ a su ideal maximal, y definimos $\Omega = \mathfrak{p} \times \cdots \times \mathfrak{p} \times (\mathfrak{p} \setminus \mathfrak{p}^2)$ con $m-1$ factores $\mathfrak{p}$ y con la topología producto. Como $\mathfrak{p}$ es compacto (Lema 3.1.3) y $\mathfrak{p}^2$ abierto (Lema 3.1.5), tenemos que $\mathfrak{p} \setminus \mathfrak{p}^2$ es compacto. Se sigue que Ω es compacto. Ahora definamos

$$\Psi \colon \{f \in R[X] : f \text{ de Eisenstein }, \partial f = m\} \to \Omega$$
$$X^m + \sum_{j=0}^{m-1} a_j X^j \mapsto (a_{m-1}, \ldots, a_0)$$

Notemos que Ψ es una biyección. Por otro lado, si N es una extensión completamente ramificada sobre M y de grado m, sea V_N el conjunto de todos los polinomios de Eisenstein cuyas raíces incluyen un generador de N. Del Teorema 3.2.3 tenemos que V_N es no vacío. Demostraremos que es un conjunto abierto: Sean $(a_{m-1}, \ldots, a_0) \in V_N$ y $F = \Psi^{-1}(a_{m-1}, \ldots, a_0)$. Por la Proposición 5.9 de [8] existe ε suficientemente chico tal que si G es un polinomio con coeficientes ε-cerca de los coeficientes de F (es decir que $\Psi(G) \in B_\varepsilon(a_{m-1}, \ldots, a_0)$), entonces es un polinomio irreducible y tiene una raíz que genera a N. Se sigue que $B_\varepsilon(a_{m-1}, \ldots, a_0) \subseteq V_N$.

Notemos entonces que

$$\{\Psi(V_N) : N \text{ es completamente ramificada de grado } m\}$$

es una cubierta abierta para Ω, pues cada conjunto es abierto y para cada elemento $(a_{m-1}, \ldots, a_0) \in \Omega$, sean $F = \Psi^{-1}(a_{m-1}, \ldots, a_0)$ y α raíz de F, entonces $(a_{m-1}, \ldots, a_0) = \Psi(F) \in \Psi(V_{M(\alpha)})$. Por la compacidad de Ω podemos obtener una subcubierta finita, digamos $\{\Psi(V_{N_1}), \ldots \Psi(V_{N_l})\}$.

Si N es una extensión de de M completamente ramificada y de grado m, entonces $\Psi(V_N) \subseteq \cup_{i=1}^{l} \Psi(V_{N_i})$, luego $V_N \subseteq \cup_{i=1}^{l} N_{N_i}$. Si $f \in V_N$, entonces $f \in V_{N_{i_0}}$, por tanto una raíz de f genera a N y otra a N_{i_0} de modo que $N \cong N_{i_0}$. Así, todas las extensiones completamente ramificadas de M son o bien algún N_i o bien algún campo isomorfo a éste, en total, una cantidad finita. ■

Teorema 3.2.4 *Si K es un campo $\mathfrak{p}$-ádico entonces una extensión L/K es completa y mansamente ramificada si y sólo si $K(a)$ con a en S raíz de un polinomio $X^n - \pi$, π un generador de $\mathfrak{p}$ y $p \nmid n$.*

Demostración: Si $L = K(a)$ como en el enunciado, notemos que $X^n - \pi$ es un polinomio de Eisenstein, por el Teorema 3.2.3 la extensión es completamente ramificada. Además $e(L/K) = [L : K] = n$ por tanto $p \nmid e(L/K)$ y la extensión es mansamente ramificada.

Supongamos ahora que L/K es completa y mansamente ramificada, y sea π un generador de $\mathfrak{p}$. Sin pérdida de generalidad podemos suponer que $\pi = \Pi^n$ pues $n = e(L/K)$. En particular, Π es una raíz del polinomio $X^n - \pi$. Como tal polinomio es de Eisenstein es también irreducible, por tanto $[K(\Pi) : K] = n$ y como $K(\Pi) \subseteq L$ se sigue que $L = K(\Pi)$. ■

Corolario 3.2.7 *Si L/K es extensión finita de campos $\mathfrak{p}$-ádicos y M es la composición de todas las extensiones mansamente ramificadas de K contenidas en L, entonces M/K es mansamente ramificada, y si $M \neq L$, entonces L/M es salvaje y completamente ramificada de grado una potencia p, el entero primo de $\mathfrak{p}$. Tenemos $e(L/K) = e_1 p^k$ con $p \nmid e_1 = e(M/K)$ y $p^k = [L : M]$.*

Para la demostración ver [8], Corolario 3 del Teorema 5.29.

Corolario 3.2.8 *(Lema de Abhyankar) Sea L una extensión mansamente ramificada sobre K y M una extensión finita. Si $e(L/K) = e(M/K)$ entonces LM es no ramificada sobre K.*

Demostración: Sea L_0 el campo intermedio de L/K no ramificado sobre K maximal como en el Corolario 3.2.3 y escribamos $L_0 = K(a)$ con a como en el Lema 3.2.2. Entonces $L_0 M = M(a)$. Por el mismo lema, la extensión $L_0 M/M$ es no ramificada y por tanto

$$e(L_0 M/K) = e(L_0 M/M)e(M/K) = e(M/K),$$

de donde

$$e(M/K) = e(L_0 M/K) = e(L_0 M/L_0)e(L_0/K) = e(L_0 M/L_0).$$

Por otro lado, como L_0/K es la extensión no ramificada maximal se tiene que L/L_0 es completamente ramificada, y como L/K es mansa entonces lo es también L/L_0. Por el teorema anterior podemos escribir $L = L_0(\Pi)$ con Π raíz del polinomio $X^e - \pi_0$ y generador de $\mathfrak{B}$, y π_0 es generador del ideal de valuación de L_0. Si $b \in L_0 M$ es un generador de su ideal de valuación, entonces tenemos $\pi_0 = u b^{e(M/K)}$ con u una unidad del anillo de valuación de $L_0 M$. Como $e = e(L/L_0) = e(L/K)|e(M/K)$, podemos escribir $\Pi^e = \pi_0 = u b^{ee'}$ con $e' = e(M/K)/e$, entonces $(\Pi b^{-e'}) = u^{1/e}$, donde $u^{1/e}$ denota a una raíz e-ésima fija de u, y por tanto $LM = L_0 M(\Pi) = L_0 M(u^{1/e})$.

La Proposición 5.16 de [8] implica que $u = \zeta u_1$ con ζ raíz de 1 de orden no divisible por p y u_1 una unidad del anillo de valuación de $L_0 M$. Como

$p \nmid e$, entonces $1/e \in \mathbb{Z}_p$. El Teorema 5.18 de [8] implica que $u_1^{1/e} \in L_0M$. Se sigue que

$$LM = L_0M\left(u^{1/e}\right) = L_0M\left(\zeta^{1/e}u_1^{1/e}\right) = L_0M(\xi)$$

con $\xi = \zeta^{1/e}$ raíz de 1 de orden no divisible por p y por el Teorema 3.2.2 la extensión LM/L_0M es no ramificada, luego

$$e(LM/M) = e(LM/L_0M)e(L_0M/M) = 1$$

es decir que LM/M es no ramificada. ■

3.3. El grupo de inercia

En esta sección consideraremos una extensión normal L/K de campos $\mathfrak{p}$-ádicos; la notación para los anillos, ideales de valuación y campos residuales de L y K será como en la sección anterior. Consideremos la aplicación

$$\begin{aligned}\Phi\colon Gal(L/K) &\to Gal(k_L/k_K)\\ \sigma &\mapsto \overline{\sigma}\colon a+\mathfrak{B} \mapsto \sigma a+\mathfrak{B}\end{aligned}$$

Proposición 3.3.1 *Φ es homomorfismo de grupos sobreyectivo y su núcleo es $G_0 = \{\sigma \in Gal(L/K) : \forall y \in S,\ \sigma y \equiv y \mod \mathfrak{B}\}$.*

Demostración: La demostración de que es homomorfismo sobreyectivo es análoga a la de la aplicación ψ en la demostración del Teorema 3.2.1. Para la afirmación sobre el núcleo tenemos

$$\begin{aligned}\sigma \in \eta(\Phi) &\Leftrightarrow \overline{\sigma} = id_{k_L}\\ &\Leftrightarrow \forall y \in S,\ \overline{\sigma}(y+\mathfrak{B}) = \sigma y+\mathfrak{B} = y+\mathfrak{B}\\ &\Leftrightarrow \sigma y \equiv y \mod \mathfrak{B}\\ &\Leftrightarrow \sigma \in G_0.\end{aligned}$$

■

A G_0 es le llama *el grupo de inercia de la extensión L/K*. Para $i = 1, 2, \ldots$ definimos el i-ésimo grupo de ramificación como

$$G_i = \{\sigma \in G_0 : \forall y \in S,\ \sigma y \equiv y \mod \mathfrak{B}^{i+1}\}.$$

Éstos son en efecto grupos: Si $\sigma \in G_i$ e $y \in S$, entonces $\sigma y - y \in \mathfrak{B}^{i+1}$, y por tanto $y - \sigma^{-1}y = \sigma^{-1}(\sigma y - y) \in \sigma^{-1}\mathfrak{B}^{i+1} \subseteq \mathfrak{B}^{i+1}$. Y si $\tau \in G_i$ entonces $\sigma\tau y - y = (\sigma(\tau y) - \tau y) + (\tau y - y) \in \mathfrak{B}^{i+1}$, pues $\tau y \in S$.

Teorema 3.3.1 *Sea L/K una extensión normal de campos $\mathfrak{p}$-ádicos y sea $G = Gal(L/K)$. Entonces*

1. *Sea L_0 el campo intermedio de L/K no ramificado maximal, entonces mediante la correspondencia de Galois tenemos $L_0 = L^{G_0}$ y $G_0 = Gal(L/L_0)$. El grupo de inercia es normal en G de orden $e(L/K)$ y G/G_0 es cíclico de orden $f(L/K)$.*

2. *Sea L_1 el campo intermedio de L/K mansamente ramificado maximal, entonces mediante la correspondencia de Galois tenemos $L_1 = L^{G_1}$ y $Gal(L/L_1) = G_1$. G_1 es normal en G, es un p grupo (p el entero primo de $\mathfrak{p}$) y G_0/G_1 es cíclico de orden no divisible por p. Además existe un encaje de G_0/G_1 en k_L^*.*

Demostración: 1. Denotaremos a los anillos e ideales de valuación de L y K como antes, y sean S_0 y $\mathfrak{B}_0$ el anillo e ideal de valuación de L_0.

Sean $\sigma \in Gal(L/L_0)$ e $y \in S$. Como la extensión L/L_0 es completamente ramificada se tiene $1 = f(L/L_0) = [k_L : k_{L_0}]$, es decir que $k_L = k_{L_0}$. En particular podemos tomar $y' \in S_0 \subseteq L_0$ tal que $y + \mathfrak{B} = y' + \mathfrak{B}_0 = y' + \mathfrak{B}$ y entonces tenemos

$$y + \mathfrak{B} = y' + \mathfrak{B} = \sigma y' + \mathfrak{B} = \overline{\sigma}(y' + \mathfrak{B}) = \overline{\sigma}(y + \mathfrak{B}) = \sigma y + \mathfrak{B}$$

de este modo $\sigma y - y \in \mathfrak{B}$, por tanto $\sigma \in G_0$ y $Gal(L/L_0) \subseteq G_0$. Para demostrar que los grupos son iguales demostraremos que tienen la misma cardinalidad.

Como k_L/k_K es extensión finita, a k_L le corresponde un única extensión no ramificada sobre K con campo residual k_L (por el Teorema 3.2.1), como $k_L = k_{L_0}$, por la únicidad éste debe ser precisamente L_0. Por el mismo teorema se tiene que L_0/K es normal y $Gal(L_0/K) \cong Gal(k_{L_0}/K)$. En particular se sigue el isomorfismo $Gal(L_0/K) \cong G/Gal(L/L_0)$ y por tanto

$$\#Gal(L/L_0)\#Gal(L_0/K) = \#G. \tag{3.2}$$

Por otro lado, del homomorfismo Φ se deduce que

$$G/G_0 \cong Gal(k_L/k_K) = Gal(k_{L_0}/k_K) \cong Gal(L_0/K),$$

luego $\#G = \#G_0\#Gal(L_0/K)$. Por la igualdad anterior y la (3.2) se tiene $\#G_0 = \#Gal(L/L_0)$, por tanto $G_0 = Gal(L/L_0)$.

Además, como $G/G_0 \cong Gal(k_L/k_K)$ se sigue que es cíclico de orden

$$\#(G/G_0) = \#Gal(k_L/k_K) = [k_L : k_K] = f(L/K)$$

y también tenemos que

$$\#G_0 = \#G/\#Gal(k_L/k_K) = [L/K]/f(L/K) = e(L/K).$$

2. Definimos la aplicación $\Psi : G_0 \to k_L^*$ mediante $\sigma \mapsto \sigma(\Pi)\Pi^{-1} + \mathfrak{B}$ con $\Pi \in \mathfrak{B}$ un generador. Como $|\sigma\Pi|_{\mathfrak{p}} = |\Pi|_p$, tenemos que $|\sigma(\Pi)\Pi^{-1}|_{\mathfrak{p}} = 1$ y en efecto $\sigma(\Pi)\Pi \in S$. Además para cada ε unidad de S, como $\sigma \in G_0$, tenemos que $\sigma\varepsilon - \varepsilon \in \mathfrak{B}$, entonces $\sigma(\varepsilon)\varepsilon^{-1} - 1 \in \mathfrak{B}$. Por tanto, si consideramos otro generador de $\mathfrak{B}$, éste es de la forma $\varepsilon\Pi$ y tenemos

$$\sigma(\varepsilon\Pi)(\varepsilon\Pi)^{-1} = \sigma(\varepsilon)\varepsilon^{-1}\sigma(\Pi)\Pi^{-1} \equiv \sigma(\Pi)\Pi^{-1} \quad \text{mód } \mathfrak{B},$$

de modo que Ψ no depende del generador de $\mathfrak{B}$ que se tome.

La aplicación es de hecho un homomorfismo de grupos: Sean $\sigma, \tau \in G_0$, notemos primero que $\tau\Pi = \varepsilon\Pi$ para algún ε unidad de S, entonces

$$\begin{aligned}\Psi(\sigma\tau) &= \sigma(\tau(\Pi))\Pi^{-1} + \mathfrak{B} = \sigma(\tau(\Pi))(\tau\Pi^{-1}\tau\Pi)\Pi^{-1} + \mathfrak{B} \\ &= \sigma(\varepsilon\Pi)(\varepsilon\Pi)^{-1}\tau(\Pi)\Pi^{-1} + \mathfrak{B} = (\sigma(\varepsilon\Pi)(\varepsilon\Pi)^{-1} + \mathfrak{B})(\tau(\Pi)\Pi^{-1} + \mathfrak{B}) \\ &= \Psi(\sigma)\Psi(\tau)\end{aligned}$$

Se puede calcular que su núcleo es G_1; de modo que Ψ induce un encaje de G_0/G_1 en k_L^*. Si $e_2 = \#\Psi(G_0)$, entonces $e_2 \mid \#k_L^* \equiv 1 \mod p$, por tanto $p \nmid e_2$.

Sea $M = L^{G_1}$, demostraremos que $M = L_1$. Para la contención $M \subseteq L_1$ basta ver que M/K es mansamente ramificada: Como $G_0 \supseteq G_1$ se tiene $L_0 \subseteq M$, además

$$[L : M] = \#G_1 = \#G_0/\#\Psi(G_0) = e(L/K)/e_2,$$

y

$$[L : M][M : L_0] = [L : L_0] = e(L/L_0) = e(L/M)e(M/L_0).$$

Se sigue que las extensiones M/L_0 y L/M son ambas completamente ramificadas y entonces también lo son L/L_1 y L_1/M. También tenemos

$$e_2 = \#\Psi(G_0) = \#G_0/\#G_1 = e(L/K)/[L : M] = e(L/K)/e(L/M) = e(M/K),$$

en particular, vemos que M/K es mansamente ramificada.

Para la otra contención consideremos la torre

$$K \subseteq L_0 \subseteq M \subseteq L_1 \subseteq L.$$

Por el corolario 3.2.7 tenemos $e(L/K) = e(L/L_0) = e_1p^k$, con $p \nmid e_1 = e(L_1/K) = e(L_1/L_0)$ y $p^k = e(L/L_1) = [L : L_1]$, además

$$e_2 = e(M/K) = e(M/L_0) = [M : L_0]$$

y $[L_1 : M] = [L_1 : L_0]/[M : L_0] = e_1/e_2$, denotaremos éste valor como e_3. Y por último, $[L_0 : K] = f(L_0/K) = f$.

Como $p \nmid e_1$, entonces $p \nmid e_3$ y por tanto L_1/M es una extensión mansa y completamente ramificada. Por el Teorema 3.2.4 podemos escribir $L_1 = M(\Pi_1)$ con Π_1 un generador del ideal de valuación en L_1, y éste satisface un polinomio $X^{e_3} - \pi_M$ con π_M generador del ideal de valuación de M.

Si $\sigma \in G_1$, podemos escribir $\sigma\Pi_1 - \Pi_1 = b\Pi^2$ con $b \in S$, entonces

$$\Pi_1^{e_3} = \pi_M = \sigma\pi_M = \sigma(\Pi_1^{e_3}) = (\sigma\Pi_1)^{e_3} = (\Pi_1 + b\Pi^2)^{e_3},$$

si definimos $u = 1 + \frac{b\Pi^2}{\Pi_1}$ tenemos $1 = u^{e_3}$, el Teorema 5.18 de [8] implica que u tiene una única raíz e_3-ésima, por tanto $u = 1$, entonces $b = 0$ y $\sigma\Pi_1 = \Pi_1$. Así, σ deja fijos a los elementos de L_1, de modo que $L_1 \subseteq L^{G_1} = M$. Se sigue la igualdad $L_1 = M$.

Para ver la normalidad de G_1 en G, tomemos $\sigma \in G, \tau \in G_1$, y $x \in S$, tenemos

$$\begin{aligned}
\sigma\tau\sigma^{-1}(x) - x &= \sigma\left(\tau\left(\sigma^{-1}(x)\right)\right) - x \\
&= \sigma\left(\tau\left(\sigma^{-1}(x)\right) - \sigma^{-1}(x) + \sigma^{-1}(x)\right) - x \\
&= \sigma\left(\tau\left(\sigma^{-1}(x)\right) - \sigma^{-1}(x)\right) + \sigma\sigma^{-1}x - x \\
&= \sigma\left(\tau\left(\sigma^{-1}(x)\right) - \sigma^{-1}(x)\right)
\end{aligned}$$

como $\sigma^{-1}(x) \in S$, entonces $\tau\left(\sigma^{-1}(x)\right) - \sigma^{-1}(x) \in \mathfrak{B}^2$, y

$$\sigma\left(\tau\left(\sigma^{-1}(x)\right) - \sigma^{-1}(x)\right) \in \sigma\mathfrak{B}^2 \subseteq \mathfrak{B}^2.$$

Por tanto $\sigma G_1 \sigma^{-1} \subseteq G_1$ y $G_1 \trianglelefteq G$. Además G_1 es un p-grupo puesto que su orden coincide con $[L : L_1] = p^k$.

El encaje de la última afirmación es el ya mencionado Ψ, y de éste modo G_0/G_1 se identifica con un subgrupo del grupo cíclico k_L^*, y su orden es $\#\left(G_0/G_1\right) = \#\Psi(G_0) = e_2$, que como dijimos antes, no es divisible por p. ■

3.4. Aplicaciones en campos de números

Cuando tenemos una extensión de campos de números, digamos L/K, sabemos que dado un ideal primo $\mathfrak{B} \leq \mathcal{O}_L$ la intersección $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$, y que se puede identificar la completación $K_\mathfrak{p}$ como un subcampo de la completación $L_\mathfrak{B}$. De este modo, una vez fijos los ideales $\mathfrak{p}$ y $\mathfrak{B}$, a la extensión L/K de campos de números le corresponde una extensión de campos $\mathfrak{p}$-ádicos.

En esta sección veremos que clase de información podemos obtener para la extensión de campos de números a partir de los teoremas que conocemos de la sección anterior.

Proposición 3.4.1 *Un ideal primo $\mathfrak{B} \leq \mathcal{O}_L$ es no ramificado (respectivamente manso o salvaje) si y sólo si la correspondiente extensión $L_{\mathfrak{B}}/K_{\mathfrak{p}}$ lo es.*

Demostración: Sean $\overline{\mathfrak{p}} \leq R$ y $\overline{\mathfrak{B}} \leq S$ los ideales y anillos de valuación de $K_{\mathfrak{p}}$ y $L_{\mathfrak{B}}$. De la Proposición 3.1.1 tenemos $\mathfrak{p}R = \overline{\mathfrak{p}}$ y $\mathfrak{B}S = \overline{\mathfrak{B}}$. Así

$$\begin{aligned}\overline{\mathfrak{p}}S = (\mathfrak{p}R)S = \mathfrak{p}S = (\mathfrak{p}\mathcal{O}_L)S = \left(\mathfrak{B}^e\mathfrak{B}_1^{e_1}\cdots\mathfrak{B}_g^{e_g}\right)S \\ = (\mathfrak{B}S)^e(\mathfrak{B}_1S)^{e_1}\cdots(\mathfrak{B}_gS)^{e_g} = (\mathfrak{B}S)^e = \overline{\mathfrak{B}}^e.\end{aligned}$$

Por tanto $e_{L/K}(\mathfrak{B}) = e_{L_{\mathfrak{B}}/K_{\mathfrak{p}}}(\overline{\mathfrak{B}}) = e(L_{\mathfrak{B}}/K_{\mathfrak{p}})$ y el resultado se sigue de las definiciones. ■

Ahora supondremos adicionalmente que la extensión L/K es normal.

Teorema 3.4.1 *Si $\mathfrak{p} \leq \mathcal{O}_K$ es un ideal primo y $\mathfrak{B} \leq \mathcal{O}_L$ es un divisor primo de $\mathfrak{p}\mathcal{O}_L$, entonces la extensión $L_{\mathfrak{B}}/K_{\mathfrak{p}}$ es normal, existe un encaje natural de $Gal(L_{\mathfrak{B}}/K_{\mathfrak{p}})$ en $Gal(L/K)$, y el índice de la imagen de $Gal(L_{\mathfrak{B}}/K_{\mathfrak{p}})$ en $Gal(L/K)$ es igual al número de divisores primos de $\mathfrak{p}\mathcal{O}_L$.*

Demostración: Por la normalidad de L/K podemos tomar un polinomio $F(X) \in K[X]$ tal que L es su campo de descomposición, digamos $L = K(\alpha_1, \ldots, \alpha_r)$ con $\alpha_1, \ldots, \alpha_r$ las raíces de F. Entonces

$$L_{\mathfrak{B}} = K_{\mathfrak{p}}L = K_{\mathfrak{p}}K(\alpha_1, \ldots, \alpha_r) = K_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_r),$$

y como $F(X)$ en particular es un polinomio de $K_{\mathfrak{p}}$, entonces $L_{\mathfrak{B}}$ es el campo de descomposición de un polinomio en $K_{\mathfrak{p}}$ y por tanto se tiene la normalidad de la extensión.

Ahora consideremos la aplicación

$$\begin{aligned}Gal(L_{\mathfrak{B}}/K_{\mathfrak{p}}) &\to Gal(L/K). \\ \sigma &\mapsto \sigma|_L\end{aligned}$$

Éste es el encaje que queremos: primero notemos que en efecto $\sigma|_L$ pertenece a $Gal(L/K)$, pues a los elementos de $K \subseteq K_{\mathfrak{p}}$ los deja fijos y permuta a las raíces de F de modo que

$$\sigma_L(L) = \sigma(K(\alpha_1, \ldots, \alpha_r)) = \sigma(K)(\sigma\alpha_1, \ldots, \sigma\alpha_r) \subseteq K(\alpha_1, \ldots, \alpha_r) = L.$$

Se sabe que si L/K es una extensión algebraica y σ es un encaje de L en sí mismo que el Lema 2.1, Capítulo V de [7].

En nuestro caso, el cálculo anterior implica que $\sigma|_L$ es un automorfismo de L. Además la aplicación es un homomorfismo de grupos, y es inyectiva: En efecto, supongamos que $\sigma|_L = id_L$, en particular para las raíces de F tenemos $\sigma|_L(\alpha_i) = \sigma\alpha_i = \alpha_i$, y como en $K_\mathfrak{p}$ es también la identidad se sigue que lo es en $K_\mathfrak{p}(\alpha_1, \ldots, \alpha_r) = L_\mathfrak{B}$, por tanto $\sigma = id_{L_\mathfrak{B}}$.

Por último, recordemos que por el Teorema 2.2.4 tenemos $[L : K] = ref$ con r el número de divisores primos de $\mathfrak{p}\mathcal{O}_L$, entonces

$$\begin{aligned}[Gal(L/K) : Gal(L_\mathfrak{B}/K_\mathfrak{p})] &= \#Gal(L/K)/\#Gal(L_\mathfrak{B}/K_\mathfrak{p}) \\ &= [L : K]/[L_\mathfrak{B} : K_\mathfrak{p}] \\ &= ref/ef \\ &= r. \end{aligned}$$ ■

La identificación de $Gal(L_\mathfrak{B}/K_\mathfrak{p})$ es llamada *grupo de descomposición del ideal* $\mathfrak{B}$. Con ésta identificación, el grupo de inercia y los de ramificación se pueden considerar como subgrupos de $Gal(L/K)$, y en éste contexto los llamaremos *el grupo de inercia* y *los grupos de ramificación de* $\mathfrak{B}$.

Se tiene el siguiente resultado en términos de subgrupos de $Gal(L/K)$.

Proposición 3.4.2 *Sea L/K una extensión normal de campos de números. Sea $\mathfrak{B} \leq \mathcal{O}_L$ un ideal primo, y definamos*

$$G_{-1}(\mathfrak{B}) = \{\sigma \in Gal(L/K) : \sigma\mathfrak{B} = \mathfrak{B}\},$$

y para $i = 1, 2, \ldots$

$$G_i(\mathfrak{B}) = \{\sigma \in Gal(L/K) : \sigma x - x \in \mathfrak{B}^{i+1} \forall x \in \mathcal{O}_L\}.$$

Entonces $G_{-1}(\mathfrak{B})$ es el grupo de descomposición de $\mathfrak{B}$, G_0 es el grupo de inercia de $\mathfrak{B}$, y $G_i(\mathfrak{B})$ el i-ésimo grupo de ramificación de $\mathfrak{B}$.

La demostración se puede consultar en [8] Proposición 6.6.

Teorema 3.4.2 *Sea L/K una extensión normal de campos de números, $\mathfrak{p} \leq \mathcal{O}_K$ un ideal primo y $\mathfrak{B}_1, \mathfrak{B}_2$ dos divisores primos de $\mathfrak{p}\mathcal{O}_L$, entonces existe $\sigma \in Gal(L/K)$ tal que $G_0(\mathfrak{B}_2) = \sigma G_0(\mathfrak{B}_1)\sigma^{-1}$.*

Demostración: Sabemos que existe $\sigma \in Gal(L/K)$ tal que $\mathfrak{B}_2 = \sigma\mathfrak{B}_1$ (ver por ejemplo la Proposición 11, Capítulo I de [6]). Este es el automorfismo que queremos: Si $\tau \in G_0(\mathfrak{B}_1)$ y $x \in \mathcal{O}_L$, entonces

$$\begin{aligned}\sigma\tau\sigma^{-1}x - x &= \sigma\left(\tau(\sigma^{-1}x) - \sigma^{-1}x + \sigma^{-1}x\right) - x \\ &= \sigma\left(\tau(\sigma^{-1}x) - \sigma^{-1}x\right) + x - x \\ &= \sigma\left(\tau(\sigma^{-1}x) - \sigma^{-1}x\right),\end{aligned}$$

y este último valor pertenece a $\sigma\mathfrak{B}_1 = \mathfrak{B}_2$ puesto que $\sigma^{-1}x \in \mathcal{O}_L$. Por tanto $\sigma\tau\sigma^{-1} \in G_0(\mathfrak{B}_2)$ y se sigue la contención $\sigma G_0(\mathfrak{B}_1)\sigma^{-1} \subseteq G_0(\mathfrak{B}_2)$.

Para la otra contención, si $\tau \in G_0(\mathfrak{B}_2)$, basta demostrar que $\tau' = \sigma^{-1}\tau\sigma \in G_0(\mathfrak{B}_1)$, lo cual se hace de manera análoga a lo anterior. ■

El campo intermedio de L/K correspondiente a $G_{-1}(\mathfrak{B})$ mediante la teoría de Galois se denota como K_{-1} y es llamado *campo de descomposición de* $\mathfrak{B}$. Similarmente definimos K_0 *el campo de inercia de* $\mathfrak{B}$, y K_i *el* i*-ésimo campo de ramificación de* $\mathfrak{B}$.

Teorema 3.4.3 *Sea L/K una extensión normal de campos de números. Fijamos $\mathfrak{B} \leq \mathcal{O}_L$ un ideal primo y $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$, denotaremos $\mathfrak{B}_i = \mathfrak{B} \cap \mathcal{O}_{K_i}$ con $i = -1, 0, 1, \ldots$, p el entero primo de $\mathfrak{p}$, y escribimos $e_{L/K}(\mathfrak{B}) = e = e_0 p^m$ con $p \nmid e_0$ y $f = f_{L/K}(\mathfrak{B})$. Entonces*

1. *En K_{-1} tenemos $e_{K_{-1}/K}(\mathfrak{B}_{-1}) = 1 = f_{K_{-1}/K}(\mathfrak{B}_{-1})$. Además K_{-1} es el mayor subcampo con estas propiedades.*

2. *En K_0 tenemos $e_{K_0/K}(\mathfrak{B}_0) = 1$.*

<u>*Demostración*</u>*: 1.* Demostraremos que $K_\mathfrak{p}$ coincide con $(K_{-1})_{\mathfrak{B}_{-1}}$. La contención $K_\mathfrak{p} \subseteq (K_{-1})_{\mathfrak{B}_{-1}}$ ya se tiene. Sea $x \in (K_{-1})_{\mathfrak{B}_{-1}}$, podemos asumir que es de la forma $x = \lim x_n$ con (x_n) una sucesión en $K_{-1} = L^{G_{-1}}$. Con $\sigma \in Gal(L_\mathfrak{B}/K_\mathfrak{p}) = G_{-1}$ tenemos

$$\sigma x = \sigma(\lim x_n) = \lim \sigma x_n = \lim x_n = x,$$

por tanto $x \in L_\mathfrak{B}^{Gal(L_\mathfrak{B}/K_\mathfrak{p})} = K_\mathfrak{p}$. Así, tenemos también $(K_{-1})_{\mathfrak{B}_{-1}} \subseteq K_\mathfrak{p}$.

De este modo tenemos $e_{K_{-1}/K}(\mathfrak{B}_{-1}) f_{K_{-1}/K}(\mathfrak{B}_{-1}) = [(K_{-1})_{\mathfrak{B}_{-1}} : K_\mathfrak{p}] = 1$, de donde se sigue la primera parte del enunciado.

Si M es otro campo intermedio con estas propiedades, y $\mathfrak{B}_M \leq \mathcal{O}_M$ es su ideal de valuación, entonces también se tiene $M_{\mathfrak{B}_M} = K_\mathfrak{p}$. Si $x \in M \subseteq M_{\mathfrak{B}_M}$ y $\sigma \in G_{-1} = Gal(L_\mathfrak{B}/K_\mathfrak{p}) = Gal(L_\mathfrak{B}/M_{\mathfrak{B}_M})$ entonces $\sigma x = x$, por tanto $x \in L^{G_{-1}} = K_1$, de modo que $M \subseteq K_{-1}$.

2. Demostraremos que $(K_0)_{\mathfrak{B}_0} \subseteq L_\mathfrak{B}^{G_0}$. Si $x \in (K_0)_{\mathfrak{B}_0}$, digamos $x = \lim x_n$ con (x_n) sucesión en $K_0 = L^{G_0}$ y $\sigma \in G_0$, entonces

$$x = \lim x_n = \lim \sigma x_n = \sigma \lim x_n = \sigma x,$$

de este modo $x \in L_\mathfrak{B}^{G_0}$ y se sigue la contención deseada. Por *1.* del Teorema 3.3.1 sabemos que $L_\mathfrak{B}^{G_0}$ es el campo intermedio de $L_\mathfrak{B}/K_\mathfrak{p}$ no ramificado maximal, y además

$$1 = e(L_\mathfrak{B}^{G_0}/K_\mathfrak{p}) = e(L_\mathfrak{B}^{G_0}/(K_0)_{\mathfrak{B}_0}) e((K_0)_{\mathfrak{B}_0}/K_\mathfrak{p}).$$

Se sigue que $1 = e((K_0)_{\mathfrak{B}_0}/K_\mathfrak{p}) = e(K_0/K)(\mathfrak{B}_0)$. ■

Capítulo 4

Altura de números algebraicos

4.1. La fórmula del producto

Sea K un campo de números. La *fórmula del producto* establece que para cada elemento no cero de K, el producto de todos sus valores absolutos posibles en K (salvo equivalencia) es igual a 1. Para poder llegar a este resultado es necesario fijar de alguna forma los valores absolutos que consideraremos, es decir, de cada clase de equivalencia de valores absolutos sobre K fijaremos un representante.

En $\mathbb{Q}$ fijamos los siguientes valores absolutos: $|\ |_\infty$ el usual, y para cada $p \in \mathbb{Z}$ primo fijamos $|\ |_p$ el valor absoluto p-ádico. Por el Teorema 2.1.1, cualquier otro valor absoluto sobre $\mathbb{Q}$ es equivalente a alguno de éstos. De este modo podemos considerar el conjunto de representantes $M_\mathbb{Q} = \{\infty, 2, 3, 5, \dots\}$, donde $p \in M_\mathbb{Q}$ representa al valor absoluto $|\ |_p$.

La fórmula del producto en $\mathbb{Q}$ dice lo siguiente:

Teorema 4.1.1 *(Fórmula del producto para $\mathbb{Q}$) Para cada $x \in \mathbb{Q}^*$ se tiene*

$$\prod_{p \in M_\mathbb{Q}} |x|_p = 1.$$

Demostración: Sea $x \in \mathbb{Q}^*$, digamos $x = \pm \frac{p_1^{\alpha_1} \dots p_m^{\alpha_m}}{q_1^{\beta_1} \dots q_l^{\beta_l}}$ con los $p_i's$ y $q_j's$ primos distintos, entonces tenemos: $|x|_{p_i} = (1/p_i)^{\alpha_i} = 1/p_i^{\alpha_i}$; $|x|_{q_j} = (1/q_j)^{-\beta_i} = q_j^{\beta_j}$; $|x|_\infty = \frac{p_1^{\alpha_1} \dots p_m^{\alpha_m}}{q_1^{\beta_1} \dots q_l^{\beta_l}}$; y $|x|_p = 1$ para todo $p \neq p_i, q_j, \infty$. De este modo se tiene

$$\prod_{v \in M_\mathbb{Q}} |x|_v = \frac{1}{p_1^{\alpha_1}} \dots \frac{1}{p_m^{\alpha_m}} q_1^{\beta_1} \dots q_l^{\beta_l} \frac{p_1^{\alpha_1} \dots p_m^{\alpha_m}}{q_1^{\beta_1} \dots q_l^{\beta_l}} = 1. \qquad \blacksquare$$

Proposición 4.1.1 *Sean L/K una extensión de campos de números y $|\ |_v$ un valor absoluto sobre K. Si $|\ |_{w_1}, \ldots, |\ |_{w_m}$ son las distintas extensiones a L y $x \in L$, entonces*

$$N_{L/K}(x) = \prod_{i=1}^{m} N_{L_{w_i}/K_v}(x) \qquad y \qquad T_{L/K}(x) = \sum_{i=1}^{m} T_{L_{w_i}/K_v}(x)$$

La demostración se puede consultar en [8], corolario de la Proposición 6.1.

Ahora, sea K campo de números, en la Sección 2.1 aprendimos que un valor absoluto $|\ |_p$ en $\mathbb{Q}$ tiene una cantidad finita de extensiones a un valor absoluto sobre K. De este modo, si en $\mathbb{Q}$ consideramos el valor absoluto usual $|\ |_\infty$, éste tiene una cantidad finita de extensiones a un valor absoluto sobre K, a los cuales les llamaremos *valores absolutos infinitos*. Si $|\ |_p$ es un valor absoluto p-ádico, el Teorema 2.2.2 nos dice que sus extensiones son $\mathfrak{p}$-ádicos correspondientes a los divisores primos de $p\mathcal{O}_K$. Cualquier otro valor absoluto sobre K es equivalente con alguno de los ya mencionados. Así pues, en K podemos fijar el conjunto de representantes $M_K = \{\text{infinitos}\} \cup \{\mathfrak{p}\text{-ádicos}\}$.

Teorema 4.1.2 *(Fórmula del producto) Para cada $x \in K^*$ se tiene*

$$\prod_{v \in M_K} |x|_v^{d_v} = 1,$$

donde d_v es el grado local de K sobre $\mathbb{Q}$ respecto a v, es decir, $d_v = [K_v : \mathbb{Q}_p]$ con v extensión de p.

Demostración: Primero notemos que en particular x es un elemento de K_v, y por los Teoremas 2.1.5 y 2.1.8 se tiene $|x|_v^{d_v} = |N_{K_v/\mathbb{Q}_p}(x)|_p$, luego

$$\begin{aligned}\prod_{v \in M_K} |x|_v^{d_v} &= \prod_{p \in M_\mathbb{Q}} \left(\prod_{v \in M_K, v|p} |x|_v^{d_v} \right) = \prod_{p \in M_\mathbb{Q}} \left| \prod_{v \in M_K, v|p} N_{K_v/\mathbb{Q}_p}(x) \right| \\ &= \prod_{p \in M_\mathbb{Q}} |N_{K/\mathbb{Q}}(x)|_p = 1\end{aligned}$$

donde la notación $v|p$ significa que $|\ |_v$ es extensión de $|\ |_p$. ∎

4.2. La función altura

Sean K un campo de números y $\alpha \in K$ un elemento. Se define *la altura de α sobre K* como

$$H_K(\alpha) = \prod_{v \in M_K} \text{máx}\{1, |\alpha|_v\}^{d_v},$$

similarmente definimos *la altura logarítmica de α sobre K* como

$$h_K(\alpha) = \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha|_v\}.$$

Ejemplo: Sean $K = \mathbb{Q}$, $\alpha = \frac{a}{b} \in \mathbb{Q}$ con $(a, b) = 1$ y en este caso notamos que $d_p = 1$ para cada $p \in M_{\mathbb{Q}}$. Entonces calculamos

$$H_{\mathbb{Q}}\left(\frac{a}{b}\right) = \prod_{p \in M_{\mathbb{Q}}} \text{máx}\left\{1, \left|\frac{a}{b}\right|_p\right\}^{d_p} = \prod_{p \in M_{\mathbb{Q}}} \text{máx}\left\{1, \left|\frac{a}{b}\right|_p\right\} \prod_{p \in M_{\mathbb{Q}}} |b|_p,$$

donde la segunda igualdad se sigue de la fórmula del producto aplicada a b. Ahora,

$$\prod_{p \in M_{\mathbb{Q}}} \text{máx}\left\{1, \left|\frac{a}{b}\right|_p\right\} \prod_{p \in M_{\mathbb{Q}}} |b|_p = \prod_{p \in M_{\mathbb{Q}}} \text{máx}\{|b|_p, |a|_p\}.$$

Si $p \in M_{\mathbb{Q}}$ es un número primo que divide a a, entonces $v_p(a) \geq 1$ y $|a|_p = \left(\frac{1}{p}\right)^{v_p(a)} < 1$. En este caso $p \nmid b$ y por tanto $|b|_p = \left(\frac{1}{p}\right)^{v_p(b)} = \left(\frac{1}{p}\right)^0 = 1$. De este modo tenemos $\text{máx}\{|b|_p, |a|_p\} = 1$. Similarmente, si $p|b$ o $p \nmid a, b$ se obtiene el mismo resultado. Por tanto

$$H_{\mathbb{Q}}\left(\frac{a}{b}\right) = \prod_{p \in M_{\mathbb{Q}}} \text{máx}\{|b|_p, |a|_p\} = \text{máx}\{|b|_\infty, |a|_\infty\}.$$

También tenemos que $h_{\mathbb{Q}}(\frac{a}{b}) = \log\left(\text{máx}\{|b|_\infty, |a|_\infty\}\right)$.

Proposición 4.2.1 *Existe sólo una cantidad finita de racionales con altura acotada.*

Demostración: Sea $T \in \mathbb{R}_{\geq 0}$. Por el ejemplo anterior, $h(\frac{a}{b}) \leq T$ sólo si $\text{máx}\{|a|_\infty, |b|_\infty\} \leq T$. Como a y b son números enteros, sólo hay una cantidad finita de posibilidades para a y para b. ■

Sea L/K una extensión de campos de números. El siguiente lema nos dice de qué forma se relacionan h_K y h_L:

Lema 4.2.1 *Sean L/K extensión de campos de números y $\alpha \in K$. Entonces $h_L(\alpha) = [L : K]h_K(\alpha)$. En Particular $H_L(\alpha) = H_K(\alpha)^{[L:K]}$.*

Demostración: Para $p \in M_{\mathbb{Q}}$, $v \in M_K$ y $w \in M_L$ tal que $w|v$ y $v|p$ podemos identificar $\mathbb{Q}_p \subseteq K_v \subseteq L_w$, por tanto $d_w = [L_w : \mathbb{Q}_p] = [L_w : K_v][K_v : \mathbb{Q}_p] =$

$[L_w : K_v]d_v$. Para $\alpha \in K$ tenemos

$$\begin{aligned} h_L(\alpha) &= \sum_{w\in M_L} d_w \log \text{máx}\{1, |\alpha|_w\} = \sum_{v\in M_K} \left(\sum_{w|v} d_w \log \text{máx}\{1, |\alpha|_v\} \right) \\ &= \sum_{v\in M_K} \left(\sum_{w|v} [L_w : K_v] d_v \log \text{máx}\{1, |\alpha|_v\} \right) \\ &= \sum_{v\in M_K} \left[\left(\sum_{w|v} [L_w : K_v] \right) d_v \log \text{máx}\{1, |\alpha|_v\} \right], \end{aligned}$$

que por la afirmación final del Teorema 2.1.10,

$$\begin{aligned} &= \sum_{v\in M_K} [L : K] d_v \log \text{máx}\{1, |\alpha|_v\} = [L : K] \sum_{v\in M_K} d_v \log \text{máx}\{1, |\alpha|_v\} \\ &= [L : K] h_K(\alpha). \end{aligned}$$ ■

A continuación definiremos la función altura sobre una cerradura algebraica de $\mathbb{Q}$ fija, la cual denotaremos mediante $\mathbb{Q}^a$. Sea $\alpha \in \mathbb{Q}^a$, es decir algebraico sobre $\mathbb{Q}$. Se define *la altura (absoluta)* como la función

$$\begin{aligned} H : \mathbb{Q}^a &\to \mathbb{R}_{\geq 0} \\ \alpha &\mapsto H_K(\alpha)^{\frac{1}{[K:\mathbb{Q}]}} \end{aligned}$$

donde K es cualquier campo de números que contiene a α. Similarmente, se define *la altura logarítmica (absoluta)* como la función

$$\begin{aligned} h : \mathbb{Q}^a &\to \mathbb{R}_{\geq 0} \\ \alpha &\mapsto \frac{1}{[K : \mathbb{Q}]} h_K(\alpha) \end{aligned}$$

definimos la *altura (absoluta)* de α como $H(\alpha) = H_K(\alpha)^{\frac{1}{[K:\mathbb{Q}]}}$ con K campo de números que contiene a α. Similarmente definimos la *altura logarítmica (absoluta)* como $h(\alpha) = \frac{1}{[K:\mathbb{Q}]} h_K(\alpha)$.

H y h están bien definidas, es decir que no dependen de la elección del campo de números. En efecto, supongamos que K_1 y K_2 son dos campos de números que contienen a α. Podemos considerar un campo de números L que contenga a K_1 y K_2 (por ejemplo la composición K_1K_2). Por el lema anterior se tiene que

$$\frac{h_{K_1}(\alpha)}{[K_1 : \mathbb{Q}]} = \frac{h_L(\alpha)}{[L : K_1][K_1 : \mathbb{Q}]} = \frac{h_L(\alpha)}{[L : \mathbb{Q}]} = \frac{h_L(\alpha)}{[L : K_2][K_2 : \mathbb{Q}]} = \frac{h_{K_2}(\alpha)}{[K_2 : \mathbb{Q}]}.$$

Teorema 4.2.1 *La función altura h tiene las siguientes propiedades:*

1) $h(\alpha) \geq 0$*;*

2) $h(\alpha_1 \dots \alpha_l) \leq h(\alpha_1) + \cdots + h(\alpha_l)$*;*

3) $h(\alpha_1 + \cdots + \alpha_l) \leq h(\alpha_1) + \cdots + h(\alpha_l) + \log(l)$*;*

4) $h(\alpha^n) = |n|h(\alpha)$*, con* $n \in \mathbb{Z}$ *y* $|\ |$ *el usual;*

5) Para cada $\sigma \in Gal(\mathbb{Q}^a/\mathbb{Q})$*,* $h(\alpha) = h(\sigma\alpha)$*.*

Demostración: Durante la demostración supondremos que K es un campo de números que contiene a $\alpha_1, \dots, \alpha_l, \alpha$.

1) Se sigue de la definición.

2) Por definición tenemos

$$h(\alpha_1 \dots \alpha_l) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha_1 \dots \alpha_l|_v\}.$$

Notemos que para cada $v \in M_K$ se tiene

$$|\alpha_1 \dots \alpha_l|_v = |\alpha_1|_v \dots |\alpha_l|_v \leq \text{máx}\{1, |\alpha_1|_v\} \dots \text{máx}\{1, |\alpha_l|_v\}.$$

De donde se sigue que

$$\text{máx}\{1, |\alpha_1 \dots \alpha_l|_v\} \leq \text{máx}\{1, |\alpha_1|_v\} \dots \text{máx}\{1, |\alpha_l|_v\}.$$

Por tanto

$$\begin{aligned} h(\alpha_1 \dots \alpha_l) &\leq \sum_{v \in M_K} d_v \log \left(\text{máx}\{1, |\alpha_1|_v\} \dots \text{máx}\{1, |\alpha_l|_v\}\right) \\ &= \sum_{i=1}^{l} \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha_i|_v\} \\ &= \sum_{i=1}^{l} h(\alpha_i). \end{aligned}$$

3) Sea $v \in M_K$. Si $|\ |_v$ es no arquimediano, tenemos

$$|\alpha_1 + \cdots + \alpha_l|_v \leq \text{máx}\{|\alpha_1|_v, \dots, |\alpha_l|_v\} \leq l\, \text{máx}\{|\alpha_1|_v, \dots, |\alpha_l|_v\},$$

y si $|\ |_v$ es arquimediano

$$|\alpha_1 + \cdots + \alpha_l|_v \leq |\alpha_1|_v + \cdots + |\alpha_l|_v \leq l\, \text{máx}\{|\alpha_1|_v, \dots, |\alpha_l|_v\}.$$

En ambos casos se sigue que

$$|\alpha_1 + \cdots + \alpha_l|_v \leq l \,\text{máx}\{|\alpha_1|_v, \ldots, |\alpha_l|_v\} \leq l \prod_{i=1}^{l} \text{máx}\{1, |\alpha_i|_v\}.$$

En particular

$$\text{máx}\{1, |\alpha_1 + \cdots + \alpha_l|_v \leq l \prod_{i=1}^{l} \text{máx}\{1, |\alpha_i|_v\}.$$

Ahora calculamos,

$$\begin{aligned} h(\alpha_1 + \cdots + \alpha_l) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha_1 + \ldots \alpha_l|_v\} \\ &\leq \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \left(l \prod_{i=1}^{l} \text{máx}\{1, |\alpha_i|_v\} \right) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \left(\log l + \sum_{i=1}^{l} \log \text{máx}\{1, |\alpha_i|_v\} \right) \\ &= \frac{1}{[K:\mathbb{Q}]} \log l \sum_{v \in M_K} d_v + \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \sum_{i=1}^{l} \log \text{máx}\{1, |\alpha_i|_v\}, \end{aligned}$$

que por el Teorema 2.1.10, se obtiene

$$\begin{aligned} &= \log l + \sum_{i=1}^{l} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha_i|_v\} \\ &= \log l + \sum_{i=1}^{l} h(\alpha_i). \end{aligned}$$

4) Supongamos primero que $n > 0$. Tenemos $\text{máx}\{1, |\alpha^n|_v\} = \text{máx}\{1, |\alpha|_v^n\} = \text{máx}\{1, |\alpha|_v\}^n$, por tanto

$$\begin{aligned} h(\alpha^n) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha|_v\}^n \\ &= n \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha|_v\} \\ &= n h(\alpha). \end{aligned}$$

Si $n \leq -1$, en particular $-n > 0$, tenemos $h(\alpha^n) = h((\alpha^{-1})^{-n}) = -nh(\alpha^{-1})$. Por tanto en este caso basta ver que $h(\alpha) = h(\alpha^{-1})$. Para este fin, notemos que $\log \text{máx}\{1, |\alpha|_v^{-1}\} = -\log \text{mín}\{1, |\alpha|_v\}$, entonces calculamos

$$\begin{aligned} h(\alpha) - h(\alpha^{-1}) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \left(\log \text{máx}\{1, |\alpha|_v\} - \log \text{máx}\{1, |\alpha|_v^{-1}\} \right) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \left(\log \text{máx}\{1, |\alpha|_v\} + \log \text{mín}\{1, |\alpha|_v\} \right) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log |\alpha|_v \\ &= \frac{1}{[K:\mathbb{Q}]} \log \left(\prod_{v \in M_K} |\alpha|_v^{d_v} \right) \\ &= 0. \end{aligned}$$

Por último, en el caso $n = 0$ tenemos $h(\alpha^0) = h(1) = h_{\mathbb{Q}}(1) = \log(1) = 0 = 0h(\alpha)$.

5) Sea $\sigma \in Gal(\mathbb{Q}^a/\mathbb{Q})$ un automorfismo fijo. Denotaremos $\sigma = \sigma|_K$. en particular se tiene que $\sigma \in Gal(K/\mathbb{Q})$. Definimos una aplicación

$$\begin{aligned} M_K &\to M_K \\ v &\mapsto v^\sigma \end{aligned}$$

con $|x|_{v^\sigma} = |\sigma x|_v$. Esta aplicación es una biyección (su inversa es $v \mapsto v^{\sigma^{-1}}$). Así,

$$\begin{aligned} h(\sigma\alpha) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log \text{máx}\{1, |\sigma\alpha|_v\} = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha|_{v^\sigma}\} \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \text{máx}\{1, |\alpha|_v\} = h(\alpha). \end{aligned}$$

■

Capítulo 5

La propiedad de Northcott

Sea $\mathcal{A} \subseteq \mathbb{Q}^a$ un conjunto de números algebraicos. Decimos que $\mathcal{A}$ tiene *la propiedad de Northcott* si para cada $T \in \mathbb{R}_{>0}$ el conjunto

$$\mathcal{A}(T) = \{\alpha \in \mathcal{A} : h(\alpha) \leq T\}$$

es finito.

Probaremos que si K es un campo de números entonces tiene la propiedad de Northcott, éste será el Corolario 5.1.2. Por tanto se plantea el problema de si existen extensiones algebraicas infinitas sobre $\mathbb{Q}$ que tienen la propiedad de Northcott. Bombieri y Zannier en [1] construyen una extensión infinita que tiene esta propiedad. El propósito de este capítulo es exponer este resultado.

5.1. El lema de Northcott

Un primer resultado acerca de la propiedad de Northcott es el siguiente:

Lema 5.1.1 *(de Northcott): Para $d \in \mathbb{Z}_{\geq 1}$ fijo, el conjunto $\mathcal{A} = \{\alpha \in \mathbb{Q}^a : [\mathbb{Q}(\alpha) : \mathbb{Q}] = d\}$ tiene la propiedad de Northcott.*

Demostración: Sean $T \in \mathbb{R}_{>0}$ fijo y $\alpha \in \mathcal{A}$ con $h(\alpha) \leq T$. Consideremos $f(X) = Irr(\alpha, \mathbb{Q})(X) \in \mathbb{Q}[X]$, digamos $f(x) = X^d + a_1 X^{d-1} + \cdots + a_d$. Si $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ son todas las raíces de f, las relaciones de Vieta nos dicen que

$$-\sum_{i=1}^{d} \alpha_i = a_1; \quad \sum_{1 \leq i < j} \alpha_i \alpha_j = a_2; \quad \text{etc.}$$

Tomemos, por ejemplo, la primera igualdad y calculemos la altura de a_1: Por *3)* del Teorema 4.2.1 tenemos

$$h(a_1) = h\left(-\sum_{i=1}^{d} \alpha_i\right) \leq \sum_{i=1}^{d} h(\alpha_i) + \log(d),$$

y notando que cada α_i es la imagen de α respecto a algún automorfismo de $Gal(\mathbb{Q}^a/\mathbb{Q})$, por *5)* del mismo teorema tenemos

$$\sum_{i=1}^{d} h(\alpha_i) + \log(d) = \sum_{i=1}^{d} h(\alpha) + \log(d) = dh(\alpha) + \log(d) \leq dT + \log(d).$$

De este modo, la altura de a_i está acotada por $dT + \log(d)$, que está fijo. Por la Proposición 4.2.1 tenemos opciones finitas para a_i. Similarmente, con el resto de las relaciones de Vieta, se deduce que hay opciones finitas para cada coeficiente de f y por tanto para f mismo. Se sigue que hay sólo una cantidad finita de elementos $\alpha \in \mathcal{A}$ con $h(\alpha) \leq T$, es decir, $\mathcal{A}$ tiene la propiedad de Northcott. ■

Corolario 5.1.1 $\mathcal{A} = \{\alpha \in \mathbb{Q}^a : [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d\}$ *tiene la propiedad de Northcott.*

Demostración: Para $T \in \mathbb{R}_{>0}$ fijo notemos que $\mathcal{A}(T) = \bigcup_{i=1}^{d} \mathcal{A}_i(T)$ con $\mathcal{A}_i = \{\alpha \in \mathbb{Q}^a : [\mathbb{Q}(\alpha) : \mathbb{Q}] = i\}$. Por el lema cada $\mathcal{A}_i(T)$ es finito, por tanto lo es también $\mathcal{A}(T)$. ■

Corolario 5.1.2 *Todo campo de números K tiene la propiedad de Northcott*

Demostración: Supongamos que $[K : \mathbb{Q}] = d$, entonces $K \subseteq \mathcal{A}$ con $\mathcal{A}$ definido como en el corolario anterior, entonces $K(T) \subseteq \mathcal{A}(T)$, y este último es finito por el corolario, por tanto también lo es $K(T)$. ■

Por último, se tiene la siguiente aplicación del Lema de Northcott.

Lema 5.1.2 *(de Kronecker):* $h(\alpha) = 0$ *si y sólo si* $\alpha = 0$ *o* α *una raíz de* 1.

Demostración: Si $\alpha = 0$ se sigue que $h(\alpha) = 0$. Supongamos que α es raíz de 1, digamos $\alpha^n = 1$ con $n \in \mathbb{N}$, entonces $0 = h(1) = h(\alpha^n) = |n|_\infty h(\alpha)$, esto último por *4)* del Teorema 4.2.1. Se sigue que $h(\alpha) = 0$. Recíprocamente, supongamos que $h(\alpha) = 0$ y $\alpha \neq 0$. Notemos que para todo $n \in \mathbb{N}$ $h(\alpha^n) = |n|_\infty h(\alpha) = 0$ y que $\alpha^n \in \mathbb{Q}(\alpha)$, de este modo, para todo $T \in \mathbb{R}_{>0}$ tenemos

$$\{1, \alpha, \alpha^2, \dots\} \subseteq \mathbb{Q}(\alpha)(T)$$

y como en particular $\mathbb{Q}(\alpha)$ es un campo de números, el corolario anterior dice que $\mathbb{Q}(\alpha)(T)$ es finito. Se sigue que $\{1, \alpha, \alpha^2, \dots\}$ es finito, es decir que existen $l, m \in \mathbb{N}$ tales que $\alpha^l = \alpha^m$. Supongamos que $l < m$, entonces para $n = m - l$ se tiene $\alpha^n = 1$. ■

5.2. Los campos $K^{(d)}$ y $K_{ab}^{(d)}$

Dada una familia de campos $\mathcal{K}$ tal que cada $K \in \mathcal{K}$ está contenida en un campo más grande L, definimos su composición como

$$\mathrm{Comp}(\mathcal{K}) = \left\{ \sum_{i=1}^{n} a_{i_1} a_{i_2} \cdots a_{i_n} : n < \infty,\ a_{i_j} \in K_i,\ K_i \in \mathcal{K} \right\}.$$

Este es el menor subcampo de L que contiene a cada $K \in \mathcal{K}$.

Sea K un campo de números. Para $d \in \mathbb{Z}_{\geq 2}$ consideramos las siguientes familias de campos:

$$\mathcal{L}^{(d)} = \{L \text{ extensión de } K : [L : K] \leq d\},$$

y

$$\mathcal{L}_{ab}^{(d)} = \{L \text{ extensión abeliana de } K : [L : K] \leq d\}.$$

Definimos $K^{(d)}$ como la composición de la familia $\mathcal{L}^{(d)}$. Similarmente, definimos $K_{ab}^{(d)}$ como la composición de $\mathcal{L}_{ab}^{(d)}$. El resto del capítulo se centra en estudiar algunas propiedades de estos campos. El teorema principal nos dice que $K_{ab}^{(d)}$ tiene la propiedad de Northcott. Fijemos K^a una cerradura algebraica K, en adelante trabajaremos dentro de este campo fijo.

Proposición 5.2.1 *$K^{(d)}$ es una extensión normal sobre K.*

Demostración: Se sabe que si todo encaje σ de $K^{(d)}$ en K^a que restringido a K es la identidad resulta ser un automorfismo de $K^{(d)}$, entonces la extensión $K^{(d)}/K$ es normal (ver por ejemplo el Teorema 3.3, Capítulo V de [7]). Consideremos entonces σ un encaje con las hipótesis anteriores. Demostraremos que es un automorfismo de $K^{(d)}$.

Notemos que si $L \in \mathcal{L}^{(d)}$ entonces $\sigma L \in \mathcal{L}^{(d)}$, pues $[\sigma L : K] = [L : K] \leq d$. De manera que si $\alpha \in K^{(d)}$, digamos $\alpha = \sum_i a_{i1} a_{i2} \dots a_{im}$ con $a_{ij} \in L_j \in \mathcal{L}^{(d)}$, entonces se tiene

$$\sigma\alpha = \sum_i (\sigma a_{i1})(\sigma a_{i2}) \dots (\sigma a_{im})$$

con $\sigma\alpha_{ij} \in \sigma L_j \in \mathcal{L}^{(d)}$, por tanto $\sigma\alpha \in K^{(d)}$. Se sigue que $\sigma K^{(d)} \subseteq K^{(d)}$. De este modo tenemos una extensión algebraica $K^{(d)}/K$ y un encaje σ de $K^{(d)}$

en sí mismo que restringido a K es la identidad. Con dichas hipótesis el Lema 2.1, Capítulo V de [7] afirma que σ es un automorfismo. ■

Proposición 5.2.2 *$K_{ab}^{(d)}$ es una extensión abeliana sobre K.*

Demostración: Demostraremos primero que es normal. Sea σ un encaje de $K_{ab}^{(d)}$ en K^a tal que $\sigma|_K = id_K$. Notemos que si $L \in \mathcal{L}_{ab}^{(d)}$ entonces $\sigma L \in \mathcal{L}_{ab}^{(d)}$, pues los grupos $Gal(L/K)$ y $Gal(\sigma L/K)$ son isomorfos mediante la aplicación $\tau \mapsto \tau\sigma^{-1}$. Por tanto σL es extensión abeliana de K y $[\sigma L : K] = [L : K] \leq d$. Con un procedimiento idéntico al de la proposición anterior obtenemos que $K_{ab}^{(d)}$ es normal sobre K.

Ahora consideremos $\sigma, \tau \in Gal\left(K_{ab}^{(d)}/K\right)$. Notemos que si $L \in \mathcal{L}_{ab}^{(d)}$ entonces $\sigma|_L, \tau|_L \in Gal(L/K)$. Si $\alpha \in K_{ab}^{(d)}$, digamos $\alpha = \sum_i a_{i1} \dots a_{im}$ con $a_{ij} \in L_j \in \mathcal{L}_{ab}^{(d)}$, como cada L_j es abeliano sobre K tenemos

$$\tau\sigma\alpha = \sum_i (\tau|_L \sigma|_L a_{i1}) \dots (\tau|_L \sigma|_L a_{im}) = \sum_i (\sigma|_L \tau|_L a_{i1}) \dots (\sigma|_L \tau|_L a_{im}) = \sigma\tau\alpha,$$

por tanto $Gal\left(K_{ab}^{(d)}/K\right)$ es abeliano, es decir, la extensión es abeliana. ■

Proposición 5.2.3 *Los campos $K^{(d)}$ y $K_{ab}^{(d)}$ son extensiones infinitas sobre K.*

Demostración: Como $K_{ab}^{(d)} \subseteq K^{(d)}$, basta demostrar que $K_{ab}^{(d)}$ es infinita sobre K. Sea $p_1 \in \mathbb{Z}$ un primo que no se ramifica en K, y fijemos $\mathfrak{p}_1 \leq \mathcal{O}_K$ un divisor primo de $p_1\mathcal{O}_K$. Notemos que el polinomio $X^2 - p_1$ es de Eisenstein respecto a $\mathfrak{p}_1$, pues $p_1 \in \mathfrak{p}_1$, y si fuera el caso que $p_1 \in \mathfrak{p}_1^2$, entonces $\mathfrak{p}^2 | p\mathcal{O}_K$ que contradice la no ramificación de p_1. Por el criterio de Eisenstein (Teorema 1.2.3) el polinomio es irreducible y por tanto $[K(\sqrt{p_1}) : K] = 2$.

Como $K(\sqrt{p_1})$ es también un campo de números podemos tomar $p_2 \in \mathbb{Z}$ primo que no se ramifica en éste. Si fijamos $\mathfrak{p}_2 \leq \mathcal{O}_{K(\sqrt{2})}$ divisor primo de $p_2\mathcal{O}_{K(\sqrt{2})}$, entonces el polinomio $X^2 - p_2$ es de Eisenstein respecto a $\mathfrak{p}_2$. El argumento es idéntico al anterior. Se sigue que $[K(\sqrt{p_1}, \sqrt{p_2}) : K(\sqrt{p_1})] = 2$ y por tanto $[K(\sqrt{p_1}, \sqrt{p_2}) : K] = 4$.

Inductivamente, si $n \in \mathbb{N}$ está fijo, podemos encontrar $p_1, \dots, p_n \in \mathbb{Z}$ primos tales que $[K(\sqrt{p_1}, \dots, \sqrt{p_n}) : K] = 2^n > n$.

Además, notemos que $K(\sqrt{p_i}) \in \mathcal{L}_{ab}^{(d)}$, de modo que

$$\begin{aligned} K_{ab}^{(d)} &= \text{Comp}(\mathcal{L}_{ab}^{(d)}) \\ &\supseteq \text{Comp}(K(\sqrt{p_i}) : i = 1, \dots n) \\ &= K(\sqrt{p_1}, \dots, \sqrt{p_n}). \end{aligned}$$

Como el grado de $K(\sqrt{p_1}, \ldots, \sqrt{p_n})$ sobre K es mayor a n, entonces también lo es el de $K_{ab}^{(d)}$, se sigue que tal grado no se puede acotar y por tanto es infinito. ■

Proposición 5.2.4 *Sea $|\ |_v$ un valor absoluto sobre K y supongamos que $|\ |_v$ se puede extender a un valor absoluto $|\ |_w$ sobre $K^{(d)}$, entonces el grado local $[(K^{(d)})_w : K_v]$ es finito.*

Demostración: Si $|\ |_v$ es arquimediano, por el Teorema de Ostrowski (2.1.4) se tiene $K_v = \mathbb{R}$ o $\mathbb{C}$, lo mismo sucede para $(K^{(d)})_w$ y por tanto $[(K^{(d)})_w : K_v] = 1$ o 2. No hay nada que demostrar en este caso.
Supongamos entonces que $|\ |_v$ es no arquimediano. Si $L \in \mathcal{L}^{(d)}$, y denotamos por $|\ |_v$ a la restricción de $|\ |_w$ a L, notemos que $[L_v : K_v] \leq [L : K] \leq d$, por tanto tenemos

$$K^{(d)} = \mathrm{Comp}(\mathcal{L}^{(d)}) \subseteq \mathrm{Comp}\{L_v : L \in \mathcal{L}^{(d)}\} \subseteq \mathrm{Comp}\{F : [F : K_v] \leq d\} = F'.$$

Por otro lado, del corolario 3.2.6 K_v tiene sólo una cantidad finita de extensiones de grado menor o igual a d, es decir que $r = \#\{F : [F : K_v] \leq d\}$ es finito, así $[F' : K_v] \leq dr$. En particular F' es un campo $\mathfrak{p}$-ádico (por *3.* del Teorema 3.1.2) y por tanto completo, como $K^{(d)} \subseteq F'$, el Teorema 2.1.2 implica $(K^{(d)})_w \subseteq F'$ y así

$$[(K^{(d)})_w : K_v] \leq [F' : K_v] \leq dr,$$

es decir, el grado local $[(K^{(d)})_w : K_v]$ es finito. ■

Ahora enunciamos el resultado principal de esta tesis:

Teorema 5.2.1 *Para $d \geq 2$ fijo, $K_{ab}^{(d)}$ tiene la propiedad de Northcott.*

La demostración de este teorema se presentará en la sección final de este capítulo.

5.3. Algunos cálculos preliminares

En esta sección se demostraran algunos lemas que se utilizarán en la demostración del Teorema principal (5.2.1). Será útil la siguiente definición:

Si G es un grupo y 1 su elemento identidad, definimos *el exponente de G* como el menor entero positivo e tal que para todo $g \in G$ se tiene $g^e = 1$. Lo denotaremos como $\exp(G)$.

Lema 5.3.1 *1. Si $H \leq G$, entonces* $\exp(H) | \exp(G)$.

2. *Si* $H \trianglelefteq G$, *entonces* $\exp(G/H) | \exp(G)$.

3. *Si* $G = G_1 \times G_2$ *y* $\exp(G_1), \exp(G_2) | n$, *entonces* $\exp(G) | n$.

En los siguientes tres resultados consideraremos K un campo arbitrario.

Teorema 5.3.1 *Sea* K *un campo, si* $f(X) \in K[X]$ *tiene* n *raíces distintas en su campo de descomposición* L, *entonces* $Gal(L/K)$ *es isomorfo a un subgrupo del grupo simétrico* S_n *y su orden es un divisor de* $n!$.

Demostración: Sea $A = \{\alpha_1, \dots \alpha_n\}$ el conjunto de raices de f. Si $\sigma \in Gal(L/K)$, entonces éste permuta las raices de f, es decir que $\sigma(A) = A$. Podemos definir la aplicación

$$\begin{aligned} Gal(L/K) &\to S_A \\ \sigma &\mapsto \sigma|_{S_A} \end{aligned}$$

ésta es un homomorfismo de grupos, y es inyectivo pues si $\sigma|_{S_A} = id_A$ significa que deja fijas a las raíces de f las cuales generan a L sobre K entonces σ es la identidad en L. Por último sólo hay que notar que $S_A \cong S_n$. ■

Lema 5.3.2 *Sean* E, L *extensiones abelianas sobre un campo* K, *si* E *y* L *son subcampos de un campo común, entonces la composición* EL *es abeliana sobre* K.

Demostración: La composición EL es de Galois sobre K (Teorema 1.4, Capítulo VI de [7]), y notemos que para cada $\sigma \in Gal(EL/K)$ tenemos $\sigma|_E \in Gal(E/K)$ y $\sigma|_L \in Gal(L/K)$. Así que si $\sigma, \tau \in Gal(EL/K)$ y $x = \sum_i e_i l_i$ tenemos

$$\sigma\tau x = \sum_i (\sigma|_E \tau|_E e_i)(\sigma|_L \tau|_L l_i) = \sum_i (\tau|_E \sigma|_E e_i)(\tau|_L \sigma|_L l_i) = \tau\sigma x. \qquad ■$$

Teorema 5.3.2 *Sea* L/K *una extensión finita de Galois,* $Gal(L/K) = H_1 \times \cdots \times H_m$ *producto de grupos, y sea* $L_i = L^{H_1 \times \cdots \times \{id\} \times \cdots \times H_m}$ *el campo fijo del grupo producto con* $\{id\}$ *en el* i*-ésimo factor. Entonces* L_i/K *es de Galois,* $L_{i+1} \cap (L_1 \cdots L_i) = K$, *y* $L = L_1 \cdots L_m$.

Para la demostración se puede consultar el Corolario 1.16, Capítulo VI de [7].

Corolario 5.3.1 *Con la notación del teorema, si cada* H_i *es cíclico y además* $\exp(Gal(L/K)) | D$, *entonces* L *es la composición de extensiones cíclicas de* K *de grado a lo más* D.

Demostración: Definamos $E_i = L^{H_i}$. Tenemos las siguientes contenciones:

$$\begin{aligned}
H_1 &\subseteq H_1 \times \{id\} \times \cdots \times H_m,\ H_1 \times H_2 \times \{id\} \times \cdots \times H_m, \ldots \\
H_2 &\subseteq \{id\} \times H_2 \times \cdots \times H_m,\ H_1 \times H_2 \times \{id\} \times \cdots \times H_m, \ldots \\
&\vdots \\
H_m &\subseteq \{id\} \times H_2 \times \cdots \times H_m,\ H_1 \times \{id\} \times H_3 \times \cdots \times H_m, \ldots
\end{aligned}$$

que por la teoría de Galois implican las contenciones

$$\begin{aligned}
E_1 &\supseteq L_2, L_3, \ldots, L_m \\
E_2 &\supseteq L_1, L_3, \ldots, L_m \\
&\vdots \\
E_m &\supseteq L_1, L_2, \ldots, L_{m-1}.
\end{aligned}$$

De este modo tenemos

$$E_1 \cdots E_m \supseteq L_1 \cdots L_m = L \supseteq E_1 \cdots E_m,$$

por tanto L es la composición de las extensiones cíclicas E_i de K de grado $\#H_i$. Y además se tiene

$$\#H_i = \exp(H_i) | \exp(Gal(L/K)) | D.$$

De donde $\#H_i \leq D$ para cada i. ■

En los siguientes cuatro resultados consideraremos K un campo de números.

Lema 5.3.3 *Sea K un campo de números y α algebraico sobre K. Si $K(\alpha)_{ab}^{(d)}$ tiene la propiedad de Northcott, entonces también la tiene $K_{ab}^{(d)}$.*

Demostración: Demostraremos que $K_{ab}^{(d)} \subseteq K(\alpha)_{ab}^{(d)}$: Sea $L \in \mathcal{L}_{ab}^{(d)}$, notemos que $L(\alpha)/K(\alpha)$ es una extensión abeliana y $[L(\alpha) : K(\alpha)] \leq [L : K] \leq d$. De este modo

$$L(\alpha) \in \{F \text{ extensión abeliana de } K(\alpha) : [F : K(\alpha)] \leq d\}.$$

Sea $x \in K_{ab}^{(d)}$, entonces x pertenece a una composición finita $L_1 \cdots L_r$ con $L_i \in \mathcal{L}_{ab}^{(d)}$, y así

$$\begin{aligned}
x &\in L_1 \cdots L_r \\
&\subseteq L_1(\alpha) \cdots L_r(\alpha) \\
&\subseteq \text{Comp}\left(\{F \text{ extensión abeliana de } K(\alpha) : [F : K(\alpha)] \leq d\}\right) \\
&= K(\alpha)_{ab}^{(d)}.
\end{aligned}$$

Por tanto se tiene la contención deseada, ahora sólo notemos que para todo $T \in \mathbb{R}_{>}0$ se tiene

$$\{\beta \in K_{ab}^{(d)} : h(\beta) \leq T\} \subseteq \{\beta \in K(\alpha)_{ab}^{(d)} : h(\beta) \leq T\},$$

si el conjunto de la derecha es finito, entonces también lo es el de la izquierda.■

Lema 5.3.4 *Sean $\alpha \in K_{ab}^{(d)}$ y $L = K(\alpha)$, entonces L/K es una extensión finita, normal y el exponente de $Gal(L/K)$ divide a $D = d!$.*

Demostración: Para la finitud no hay nada que demostrar. Como $K \subseteq L \subseteq K_{ab}^{(d)}$ y $K_{ab}^{(d)}/K$ es abeliana, entonces también lo es L/K puesto que $Gal(L/K) \cong Gal(K_{ab}^{(d)}/K)/Gal(K_{ab}^{(d)}/L)$.

Ahora, podemos suponer que $\alpha \in L_1 \cdots L_s$ con $L_i \in \mathcal{L}_{ab}^{(d)}$. Tenemos la torre $K \subseteq L \subseteq L_1 \cdots L_s$ y con un argumento idéntico al de L tenemos que $L_1 \cdots L_s$ es abeliano sobre K. En particular tenemos

$$Gal(L/K) \cong \frac{Gal(L_1 \cdots L_s/K)}{Gal(L_1 \cdots L_s/L)}.$$

Por *2.* del Lema 5.3.1, para ver que el exponente de $Gal(L/K)$ divide a D basta ver que el exponente de $Gal(L_1 \cdots L_s/K)$ lo divide.

Se sabe que $Gal(L_1 \cdots L_s/K) \lesssim Gal(L_1/K) \times \cdots \times Gal(L_s/K)$ (ver Teorema 1.4, Capítulo VI de [7]). Por *1.* y *3.* del Lema 5.3.1 basta demostrar que el exponente de cada $Gal(L_i/K)$ divide a D.

Como L_i/K es normal, existe $f \in K[X]$ tal que L_i es su campo de descomposición, y éste tiene $n = \partial f \leq d$ raíces distintas en L_i. El Teorema 5.3.1 implica que

$$\exp(Gal(L_i/K))|\#Gal(L_i/K)|n!|d! = D. \qquad \blacksquare$$

Lema 5.3.5 *Sean L/K una extensión de Galois abeliana de campos de números tal que $\exp(Gal(L/K))|D = d!$, $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y p su entero primo. Si $p > d$, entonces $\mathfrak{p}$ es mansamente ramificado en L/K.*

Demostración: Por el Teorema 2.2.4 podemos suponer una factorización $\mathfrak{p}\mathcal{O}_L = (\mathfrak{B}_1 \cdots \mathfrak{B}_g)^e$ con los $\mathfrak{B}_j$ distintos. Hay que demostrar que $p \nmid e$. Supongamos que si lo divide. Si escribimos $Gal(L/K)$ como producto de grupos cíclicos, digamos $H_1 \times \cdots \times H_m$ tenemos

$$p|e|[L : K] = \#Gal(L/K) = \#H_1 \cdots \#H_m,$$

entonces para algún i entre 1 y m

$$p|\#H_i = \exp(H_i)|\exp(Gal(L/K))|D = d!,$$

por tanto $p \leq d$. ■

Lema 5.3.6 *Sea $\mathfrak{p} \leq \mathcal{O}_K$ un ideal primo y $K_\mathfrak{p}$ la completación de K respecto al valor absoluto $\mathfrak{p}$-ádico $|\ |_\mathfrak{p}$. Si L/K es una extensión finita y $\mathfrak{B}$ es un divisor primo de $\mathfrak{p}\mathcal{O}_L$, entonces la completación de $L_\mathfrak{B}$ de L respecto al valor absoluto $\mathfrak{B}$-ádico $|\ |_\mathfrak{B}$ es la composición de L y $K_\mathfrak{p}$.*

Demostración: Sea $\{a_1, \ldots, a_n\}$ una base para L como K-espacio vectorial. Definimos $L_1 = a_1K_\mathfrak{p} + \cdots + a_nK_\mathfrak{p}$. Se tiene que $L \subseteq L_1 \subseteq L_\mathfrak{B}$, y se puede demostrar que L_1 es cerrado en $L_\mathfrak{B}$. Como L es denso en $L_\mathfrak{B}$ se sigue que de hecho $L_1 = L_\mathfrak{B}$.

Por otro lado, es claro que $L, K_\mathfrak{p} \subseteq L_\mathfrak{B}$, y si L_2 es un campo que contiene a L y $K_\mathfrak{p}$ entonces éste contiene a $L_1 = L_\mathfrak{B}$. De este modo $L_\mathfrak{B}$ es el menor campo que contiene a L y $K_\mathfrak{p}$, es decir que $L_\mathfrak{B} = LK_\mathfrak{p}$ ■

Por último, en el siguiente resultado consideraremos K un campo $\mathfrak{p}$-ádico.

Lema 5.3.7 *Si L/K es una extensión no ramificada de campos $\mathfrak{p}$-ádicos y $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ es un polinomio de Eisenstein sobre K, entonces es también de Eisenstein en L.*

Demostración: Denotemos $\mathfrak{p} \leq R$ y $\mathfrak{B} \leq S$ a los ideales y anillos de valuación de K y L respectivamente. Notemos que $\mathfrak{p} \subseteq \mathfrak{B}$ y $\mathfrak{B}^2 \cap R = \mathfrak{p}^2$, por tanto $a_1, \ldots, a_n \in \mathfrak{p} \subseteq \mathfrak{B}$ y $a_n \notin \mathfrak{B}^2$, pues de lo contrario $a \in \mathfrak{B}^2 \cap R = \mathfrak{p}^2$. ■

5.4. Demostración del teorema

Por el Lema 5.3.3 podemos suponer que $\sqrt[p]{1} \in K$ con $D = d!$. Sean $T \in \mathbb{R}_{>0}$ fijo y $\alpha \in K_{ab}^{(d)}$ con $h(\alpha) \leq T$. Denotemos $K(\alpha) = L$, por el Lema 5.3.4 L sobre K es finita, abeliana y de exponente que divide a D.

Sea $p \in \mathbb{Z}$ un primo que no se ramifica en K, cuya existencia se garantiza por el Corolario 1.4.2. Sea $\mathfrak{p} \leq \mathcal{O}_K$ uno de los divisores primos de $p\mathcal{O}_K$. Como L/K es de Galois se tiene la factorización $\mathfrak{p}\mathcal{O}_L = (\mathfrak{B}_1 \cdots \mathfrak{B}_g)^e$ con los $\mathfrak{B}_j$ ideales primos de $\mathcal{O}_L$ distintos (Teorema 2.2.4).

Si $p > d$ entonces $\mathfrak{p}$ es manso en L/K (Lema 5.3.5). Por tanto, $\mathfrak{B}_j$ divisor de $\mathfrak{p}\mathcal{O}_L$ es mansamente ramificado en L/K y por la Proposición 3.4.1 $L_{\mathfrak{B}_j}/K_\mathfrak{p}$ es mansamente ramificada, en particular el campo intermedio de $L_{\mathfrak{B}_j}/K_\mathfrak{p}$ mansamente ramificado maximal es precisamente $L_{\mathfrak{B}_j}$. Mediante la

identificación del grupo de inercia y los grupos de ramificación de $L_{\mathfrak{B}_j}/K_{\mathfrak{p}}$ en $Gal(L/K)$ vista en la Sección 3.4 y por *2.* del Teorema 3.3.1 tenemos que $G_1(\mathfrak{B}_j) = Gal(L_{\mathfrak{B}_j}/L_{\mathfrak{B}_j}) = \langle id \rangle$ y $G_0(\mathfrak{B}_j) = G_0(\mathfrak{B}_j)/G_1(\mathfrak{B}_j)$ es cíclico de orden e. En particular tenemos

$$e = \#G_0(\mathfrak{B}_j) = \exp(G_0(\mathfrak{B}_j))|\exp(Gal(L/K))|D.$$

Ahora consideremos el polinomio $X^e - p \in K[X]$ y fijamos una raíz θ de éste. Tenemos la torre $L(\theta) \supseteq K(\theta) \supseteq K$. Sea $\mathfrak{q} \leq \mathcal{O}_{K(\theta)}$ un divisor primo de $\mathfrak{p}\mathcal{O}_{K(\theta)}$ y $\mathfrak{D} \leq \mathcal{O}_{L(\theta)}$ un divisor primo de $\mathfrak{q}\mathcal{O}_{L(\theta)}$. Del Lema 5.3.6 podemos notar que $L(\theta)_{\mathfrak{D}} = L_{\mathfrak{B}}(\theta)$ con $\mathfrak{B} = \mathfrak{D} \cap \mathcal{O}_L$ y $K(\theta)_{\mathfrak{q}} = K_{\mathfrak{p}}(\theta)$.

Como $X^e - p$ es un polinomio de Eisenstein en $K_{\mathfrak{p}}$, por el Teorema 3.2.3 $K_{\mathfrak{p}}(\theta)/K_{\mathfrak{p}}$ es completamente ramificada, así

$$e_{K(\theta)/K}(\mathfrak{q}) = e(K_{\mathfrak{p}}(\theta)/K_{\mathfrak{p}}) = [K_{\mathfrak{p}}(\theta) : K_{\mathfrak{p}}] = e.$$

Por otro lado, $L_{\mathfrak{B}}$ es mansamente ramificado sobre $K_{\mathfrak{p}}$, pues $\mathfrak{B}$ es uno de los divisores de $\mathfrak{p}\mathcal{O}_L$, $K_{\mathfrak{p}}(\theta)/K_{\mathfrak{p}}$ es finita, y $e(L_{\mathfrak{B}}/K_{\mathfrak{p}})|e(K_{\mathfrak{p}}(\theta)/K_{\mathfrak{p}})$. Por el Lema de Abhyankar (Corolario 3.2.8), $L_{\mathfrak{B}}K_{\mathfrak{p}}(\theta) = L_{\mathfrak{B}}(\theta)$ es no ramificada sobre $K_{\mathfrak{p}}(\theta)$, y por tanto $e_{L(\theta)/K(\theta)}(\mathfrak{D}) = e(L_{\mathfrak{B}}(\theta)/K_{\mathfrak{p}}(\theta)) = 1$. Se sigue que para cualquier divisor primo $\mathfrak{D}$ de $\mathfrak{p}\mathcal{O}_{L(\theta)}$

$$e_{L(\theta)/K}(\mathfrak{D}) = e_{L(\theta)/K(\theta)}(\mathfrak{D})e_{K(\theta)/K}(\mathfrak{q}) = e_{K(\theta)/K}(\mathfrak{q}) = e.$$

A continuación se demostrará que $K(\theta)/K$ es de Galois. Como $e_{K(\theta)/K}(\mathfrak{q}) = e = [K(\theta) : K]$, en particular se sigue del Teorema 2.2.4 que $\mathfrak{p}\mathcal{O}_{K(\theta)} = \mathfrak{q}^e$, es decir que $\mathfrak{q}$ es el único divisor primo de $\mathfrak{p}\mathcal{O}_{K(\theta)}$.

Notemos que si ζ es una raíz e-ésima primitiva de 1, como $\sqrt[D]{1} \in K$ y $e|D$, entonces $K(\theta)$ es el campo de descomposición de $X^e - p$, pues todas sus raíces son de la forma $\zeta^r\theta$ con $r = 0, \ldots, e-1$ y éstas pertenecen a $K(\theta)$. En particular $K(\theta)/K$ es de Galois y su grupo de Galois es $Gal(K(\theta)/K) = \{\sigma_0, \ldots, \sigma_{e-1}\}$, donde $\sigma_r : \theta \mapsto \zeta^r\theta$, que podemos notar, es abeliano. Por el Lema 5.3.2 se tiene que $K(\theta)L = L(\theta)$ es abeliano sobre K y por el Teorema 3.4.2 los grupos de inercia de los diferentes divisores de $\mathfrak{p}\mathcal{O}_{L(\theta)}$ son conjugados unos de otros. Se sigue que todos los grupos de inercia coinciden. Denotemos a este grupo común como I, y sea $U = L(\theta)^I$ el campo fijo de I mediante la correspondencia de Galois de $L(\theta)/K$. Con un argumento análogo al de L/K se observa que U/K es abeliano.

De *2.* del Teorema 3.4.3 $\mathfrak{p}$ es no ramificado en U y por *1.* del Teorema 3.3.1 $[L(\theta) : U] = \#Gal(L(\theta)/U) = \#I = e$.

Como $\mathfrak{p}\mathcal{O}_{K(\theta)} = \mathfrak{q}^e$, se deduce que $\mathfrak{p}\mathcal{O}_{U\cap K(\theta)} = \mathfrak{q}_0^{e_{U\cap K(\theta)/K}(\mathfrak{q}_0)}$ con $\mathfrak{q}_0$ el único divisor primo de $\mathfrak{p}\mathcal{O}_{U\cap K(\theta)}$ y por el Teorema 2.2.1 se deduce $[U \cap K(\theta) : K] =$

$e_{U\cap K(\theta)/K}(\mathfrak{q}_0)$. Por otra parte, $\mathfrak{p}$ es no ramificado en U, así que si $\mathfrak{D}_0$ es un divisor de $\mathfrak{p}\mathcal{O}_U$, en particular es divisor de $\mathfrak{q}_0\mathcal{O}_U$ y se tiene

$$e_{U\cap K(\theta)/K}(\mathfrak{q}_0) = e_{U/K}(\mathfrak{D})/e_{U/U\cap K(\theta)}(\mathfrak{D}) = 1,$$

se sigue que $K = U \cap K(\theta)$. Notemos que $X^e - p \in U[X]$ es irreducible (si tuviera una raíz en U, ésta estaría en $U \cap K(\theta) = K$, lo cual es imposible), entonces $[U(\theta) : U] = e$, y como $U(\theta) \subseteq L(\theta)$ y ambos son de grado e sobre U se deduce que $U(\theta) = L(\theta)$. Como además $\alpha \in L \subseteq L(\theta) = U(\theta)$, entonces escribimos a α como elemento de $U(\theta)$ mediante

$$\alpha = \beta_0 + \beta_1\theta + \cdots + \beta_{e-1}\theta^{e-1}$$

con $\beta_i \in U$.

Estimemos la altura de los sumandos $\beta_j\theta^j$. Notemos primero que

$$T_{U(\theta)/U}(\theta^j) = \sum_{r=0}^{e-1} \zeta^{rj}\theta^j = \theta^j \sum_{r=0}^{e-1} \zeta^{rj},$$

pues los conjugados de θ son $\zeta^r\theta$ y por tanto los de θ^j son $\zeta^{rj}\theta^j$. Si $j = 0$ tenemos $T_{U(\theta)/U}(\theta^j) = e$; y si j no es múltiplo de e, entonces $T_{U(\theta)/U}(\theta^j) = 0$. En efecto, con $j = 0$ tenemos $T_{U(\theta)/U}(\theta^0) = T_{U(\theta)/U}(1) = e$; y para $e \nmid j$, digamos $j = em + l$ con $0 < l < e$ tenemos

$$\begin{aligned} T_{U(\theta)/U}(\theta^j) &= \theta^j \sum_{r=0}^{e-1} \zeta^{rj} = \theta^j \sum_{r=0}^{e-1} \zeta^{rem+rl} = \theta^j \sum_{r=0}^{e-1} \zeta^{rl} \\ &= \theta^j \left(1 + \zeta^l + \cdots + \zeta^{(e-1)l}\right) = \theta^j \frac{1-\zeta^{el}}{1-\zeta^l} = \theta^j 0 = 0. \end{aligned}$$

Para $0 \le j \le e-1$, consideramos $\alpha\theta^{-j} = \beta_0\theta^{-j} + \cdots + \beta_j + \cdots + \beta_{e-1}\theta^{e-1-j}$ y calculamos su traza sobre U, entonces

$$\begin{aligned} T_{U(\theta)/U}(\alpha\theta^{-j}) &= \beta_0 T_{U(\theta)/U}(\theta^{-j}) + \cdots + \beta_j T_{U(\theta)/U}(1) + \ldots \\ &\qquad \cdots + \beta_{e-1} T_{U(\theta)/U}(\theta^{e-1-j}) \\ &= e\beta_j, \end{aligned}$$

luego

$$\beta_j = \frac{1}{e} T_{U(\theta)/U}(\alpha\theta^{-j}) = \frac{1}{e} \sum_{r=0}^{e-1} \alpha_r \zeta^{-rj}\theta^{-j} = \frac{1}{e\theta^j} \sum_{r=0}^{e-1} \alpha_r \zeta^{-rj},$$

con α_r los conjugados de α en $U(\theta)$. Notamos que en particular α y α_r son conjugados en $\mathbb{Q}^a$, por tanto, *5.* del Teorema 4.2.1 implica que $h(\alpha) = h(\alpha_r)$.

Ahora, con las propiedades de la altura (Teorema 4.2.1) se tiene

$$\begin{aligned} h(\beta_j\theta^j) = h\left(\frac{1}{e}\sum_{r=0}^{e-1}\alpha_r\zeta^{-rj}\right) &\leq h\left(\frac{1}{e}\right) + h\left(\sum \alpha_r\zeta^{-rj}\right) \\ &\leq \log(e) + \sum h(\alpha_r\zeta^{-rj}) + \log(e) \\ &\leq 2\log(e) + \sum \left(h(\alpha_r) + h(\zeta^{-rj})\right); \end{aligned}$$

Por el Lema de Kronecker (Lema 5.1.2) $h(\zeta^{-rj}) = 0$ por tanto

$$h(\beta_j\theta^j) \leq 2\log(e) + \sum h(\alpha_r) = 2\log(e) + eh(\alpha) \leq 2\log(D) + DT. \quad (5.1)$$

Por otro lado, para $\mathfrak{D} \leq U(\theta)$ un divisor de $\mathfrak{p}\mathcal{O}_{U(\theta)}$ y $\mathfrak{D}_0 = \mathfrak{D} \cap \mathcal{O}_U$ consideramos la torre de las completaciones $K_\mathfrak{p} \subseteq U_{\mathfrak{D}_0} \subseteq U(\theta)_\mathfrak{D}$. Como $\mathfrak{p}$ es no ramificado en U/K la extensión $U_{\mathfrak{D}_0}/K_\mathfrak{p}$ es no ramificada. Además $X^e - p$ es de Eisenstein en $K_\mathfrak{p}[X]$, por el Lema 5.3.7, es de Eisenstein en $U_{\mathfrak{D}_0}$. Se sigue del Corolario 3.2.5 que $v_\mathfrak{D}(\theta) = v_{U(\theta)}(\theta) = 1$. Para $1 \leq j \leq e-1$ supongamos que $\beta_j \neq 0$, entonces con $\gamma = \beta_j\theta^j$ tenemos $v_\mathfrak{D}(\gamma) = v_\mathfrak{D}(\beta) + j$. Como $\beta \in U$, del Teorema 2.2.2 se deduce que $v_\mathfrak{D}(\beta_j) = ev_{\mathfrak{D}_0}$. Se sigue que $v_\mathfrak{D}(\gamma) \neq 0$ y por tanto $|v_\mathfrak{D}(\gamma)| \geq 1$.

Además,

$$|\gamma|_\mathfrak{D} = \left(\frac{1}{p}\right)^{\frac{v_\mathfrak{D}(\gamma)}{e_{U(\theta)/\mathbb{Q}^{(\mathfrak{D})}}}} = \left(\frac{1}{p}\right)^{\frac{v_\mathfrak{D}(\gamma)}{e_{U(\theta)/K^{(\mathfrak{D})}}}} = \left(\frac{1}{p}\right)^{\frac{v_\mathfrak{D}(\gamma)}{e_{L(\theta)/K^{(\mathfrak{D})}}}} = \left(\frac{1}{p}\right)^{\frac{v_\mathfrak{D}(\gamma)}{e}}$$

por tanto $|\log|\gamma|_\mathfrak{D}| = \left|\frac{v_\mathfrak{D}(\gamma)}{e}\right| |\log(1/p)| \geq \frac{\log(p)}{e}$. Calculamos ahora

$$\begin{aligned} h_{U(\theta)}(\gamma) + h_{U(\theta)}(\gamma^{-1}) &= \sum_{w\in M_{U(\theta)}} d_w \left(\log \text{máx}\{1, |\gamma|_w\} + \log \text{máx}\{1, |\gamma^{-1}|_w\}\right) \\ &= \sum_{w\in M_{U(\theta)}} d_w \log\left(\text{máx}\{1, |\gamma|_w\}\,\text{máx}\{1, |\gamma^{-1}|_w\}\right) \\ &= \sum_{w\in M_{U(\theta)}} d_w |\log|\gamma|_w| \geq \sum_{w|v_p} d_w |\log|\gamma|_w|; \end{aligned}$$

Si $w|v_p$, entonces es el valor absoluto $|\ |_w$ corresponde a un ideal en $\mathcal{O}_{U(\theta)}$ divisor de $\mathfrak{p}\mathcal{O}_{U(\theta)}$, es decir, $|\ |_w = |\ |_\mathfrak{D}$ para algún $\mathfrak{D}$ que satisface los cálculos

anteriores, de modo que

$$h_{U(\theta)}(\gamma) + h_{U(\theta)}(\gamma^{-1}) \geq \sum_{w|v_{\mathfrak{p}}} d_w |\log|\gamma|_w| \geq \sum_{w|v_{\mathfrak{p}}} d_w \frac{\log(p)}{e}$$
$$= \frac{\log(p)}{e} \sum_{w|v_{\mathfrak{p}}} d_w = \frac{\log(p)}{e}[U(\theta) : K]$$

donde la última igualdad se debe a que la suma de los grados locales es el grado de la extensión (Teorema 2.1.10). Y entonces tenemos

$$2h(\gamma) = h(\gamma) + h(\gamma^{-1}) = \frac{1}{[U(\theta) : \mathbb{Q}]} \left(h_{U(\theta)}(\gamma) + h_{U(\theta)}(\gamma^{-1})\right) \geq \frac{\log(p)}{e[K : \mathbb{Q}]}.$$

Es decir que $h(\gamma) \geq \frac{\log(p)}{2e[K:\mathbb{Q}]}$ que junto con la desigualdad (5.1) implica

$$\log(p) \leq 2e[K : \mathbb{Q}](\log(D) + DT) =: C.$$

Sea $S = \{p \in \mathbb{Q} \text{ primo } : p > \exp(C),\ p \text{ no ramificado en } K\}$, donde $\exp(C)$ la función exponencial aplicada a C. Demostramos que si algún $\beta_j \neq 0$, entonces $p \notin S$. Equivalentemente, si tomamos $p \in S$ entonces garantizamos que $\alpha = \beta_0 \in U$, y por tanto $K(\alpha) \subseteq U$. Como $\mathfrak{p}$ es no ramificado en U entonces lo es también en $K(\alpha)$. Se sigue que cada $p \in S$ es no ramificado en $K(\alpha)$.

Ahora, como podemos descomponer $Gal(K(\alpha)/K)$ en producto de grupos cíclicos, el corolario 5.3.1 dice que $K(\alpha)$ es la composición de extensiones cíclicas de K de grado a lo más D. Además también se tiene que cada primo en S es no ramificado en éstas.

Si intentamos estimar el discriminante de E_i, por el Teorema del discriminante (corolario 1.4.2) sabemos que ningún $p \in S$ divide a éste, y para cada primo que divide a $d(E_i)$ el Teorema 1.4.3 nos da una cota para su potencia máxima. Se sigue que el discriminante de E_i está acotado. Por el Teorema 1.4.2 las opciones para cada E_i son acotadas, por tanto las opciones para $K(\alpha)$ son finitas.

Cada $\alpha \in K_{ab}^{(d)}$ con altura a lo más T genera uno de los campos $K(\alpha)$ que son en particular campos de números. Del corolario 5.1.2 se deduce en particular que $K(\alpha)$ tiene a lo más una cantidad finita de generadores con altura acotada por T. Se sigue que $\{\alpha \in K_{ab}^{d} : h(\alpha) \leq T\}$ es un conjunto finito. ■

Corolario 5.4.1 *El campo $K^{(2)}$ tiene la propiedad de Northcott.*

Demostración: Si L es una extensión de grado ≤ 2 de K, ésta es automáticamente abeliana, de modo que $\mathcal{L}^{(2)} = \mathcal{L}_{ab}^{(2)}$ y por tanto $K^{(2)} = K_{ab}^{(2)}$. El resultado se sigue del teorema. ■

Corolario 5.4.2 *Para cualquier $m \geq 2$ el campo $\mathbb{Q}\left(\sqrt[m]{1},\ \sqrt[m]{2},\ \sqrt[m]{3}, \dots\right)$ tiene la propiedad de Northcott.*

Sea $K = \left(\sqrt[m]{1}\right)$. Notemos que para $a \geq 2$, $K\left(\sqrt[m]{a}\right)$ es una extensión abeliana de grado a lo más m, de modo que

$$\left\{K\left(\sqrt[m]{a}\right) : a = 2, 3, \dots\right\} \subseteq \mathcal{L}_{ab}^{(m)}$$

y por tanto

$$\mathbb{Q}\left(\sqrt[m]{1},\ \sqrt[m]{2},\ \sqrt[m]{3}, \dots\right) = \mathrm{Comp}\left(\left\{K\left(\sqrt[m]{a}\right) : a = 2, 3, \dots\right\}\right) \subseteq K_{ab}^{(m)}.$$

Como $K_{ab}^{(m)}$ tiene la propiedad de Northcott, entonces con mayor razón la tiene $\mathbb{Q}\left(\sqrt[m]{1},\ \sqrt[m]{2},\ \sqrt[m]{3}, \dots\right)$. ■

Bibliografía

[1] E. Bombieri - U. Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. Rend. Mat. Acc. Lincei. s. 9 v. 12. p. 5-14. (2001).

[2] J.W.S. Cassels. (1993). Local fields. Cambridge university press.

[3] A. Fröhlich, M. J. Taylor. (1991). Algebraic number theory. University press of Cambridge.

[4] N. Jacobson. (2009). Basic algebra II. Second edition. Dover.

[5] G. J. Janusz. (1996). Algebraic number fields. Second edition.

[6] S. Lang. (1994). Algebraic number theory. Second edition. Springer-Verlag.

[7] S. Lang. (2002). Algebra. Third edition. Springer-Verlag.

[8] W. Narkiewicz. (2004). Elementary and analytic theory of algebraic numbers. Third edition. Springer-Verlag.

[9] J. Rotman. (1990). Galois theory. Second edition. Springer.