Dominios de Dedekind

Lorenzo José Escané Amat

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director del trabajo: Fernando Montaner Frutos
25/06/2021

Abstract

The main goal of this project will be the definition of Dedekind domains as a means of finding a set over an extension of $\mathbb{Q}$ where we can define the best possible division relation (in the sense of being similar to the fundamental theorem of arithmetic) . For this purpose, we shall define the concepts of absolute value and the related concept of valuation (valuations are functions over fields that take values on Abelian ordered groups). Although there is a more general theory (see [5] for example).

The first chapter will deal about absolute values:

We will give a few properties of them to quickly classify them as archimedean or non archimedean (for the later ones will be equivalent to valuations). Then, by the topology defined by the associated metrics, we will define an equivalence relation among the absolute values.

In fact, we will prove a theorem of approximation for non equivalent absolute values that, in a way, generalizes the Chinese remainder theorem and shows that finite family of non equivalent absolute values are unrelated (as having the values in every absolute value except one gives us no information about the value that it takes).

The second chapter draws a more insightful picture of our goal thanks to the p-adics valuations over $\mathbb{Q}$. This valuations shall give an insight in how we must attack the classification problem by giving us a relation between $\mathbb{Z}$ and the non negative elements of our valuations.

By defining the concept of valuation and relating it to the non archimedean absolute values, we obtain an equivalence relation over the valuations. Doing so, and proving that the possible images of valuations in $\mathbb{R}$ are either isomorphic to $\mathbb{Z}$, dense in $\mathbb{R}$ or trivial, we shall define the concept of a principal (or discrete) valuation .

Discrete valuations determine rings inside the fields where they are defined, called valuation rings. Valuation rings can also be intrinsically defined by a property inside the fields, every element or its inverse will lay in the ring. This will be of great interest in the last chapter when dealing with families of valuations.

We will need to define the concept of place and relate it to the concept of valuation ring. Places will be functions over fields with images in fields plus a simbol ∞ such that: the application restricted to preimage of the field is an homomorphism, the elements that takes the value ∞ are not zero and the inverse of the elements that takes the value ∞ take the zero value.

In order to achieve our goal, we need to work with a family of non equivalent valuations, but, as the examples shall show, we must choose carefully our family (for a one too big or a one too small will be of no use). The property of the strong approximation will prove to be enough to avoid overdetermining or undetemining our set.

Finally, We need two concepts related to valorations. Namely, fractional ideals and the divisor group. This concepts arise from two points of view on valuations:

1. Given a ring R in a field, the fractional ideals of that ring will be R-submodules that are in contained in aR where a is an element of the field. We will use the ring of integers (which is the result of intersecting all the valuations ring from a family of valuations).

2. The divisor group is the free Abelian group generated by the places.

And so, proving that there exist an isomorphism between this two concepts (fractional ideals and the divisor groupr), we obtain that the fractional ideals can be factorized as products of prime integral

ideals (integral ideals are the ideals in our ring of integers). We shall define a Dedekind domain as a ring whose fractional ideals in its field of fractions can be factorized as a product of integral ideals.

We will prove that we can also define Dedekind domain as a ring which is a Noetherian ring such that every proper prime ideal of the ring is maximal and all the roots of every monic polynomial with coefficients in the ring are in the ring (the ring is integrally closed).

Proving that the integral closure of a separable extension of a Dedekind domain is again another Dedekind domain we will obtain that any number field will contain a Dedekind domain, namely the integral closure of $\mathbb{Z}$ in the extension. This is the ring that we were seeking from the beginning, the ring with the best arithmetic inside a number field for it is a Dedekind domain, hence it has a unique factorization at the level of ideals rather than at the level of numbers.

One possible extension of this work would be the study of ramification theory and the study of how many valuations appears when we consider an extension field.

Índice general

Capítulo 1

Valores absolutos

1.1. Definición y primeras propiedades.

Definición. Sea A un anillo. Se llamará valor absoluto en A $|\ |$ a una aplicación con valores en $\mathbf{R}^+ \cup \{0\}$ cumpliendo:

1. $|x| > 0$ para $x \in A$, $x \neq 0$ y $|0| = 0$.
2. $|x+y| \leq |x| + |y|$ (desigualdad triangular).
3. $|xy| = |x||y|$.

Para $x, y \in A$.

Proposición 1.1. *Sea A un anillo y $|\ |$ un valor absoluto sobre él. Se sigue que:*

1. $|1| = 1$.
2. $a^n = 1$ *implica que* $|a| = 1$.
3. $|-x| = |x|$.
4. *A es un dominio de integridad (DI).*
5. *Si x tiene inverso (x^{-1}), entonces* $|x^{-1}| = |x|^{-1}$.

Demostración. 1. $|1| = |1|^2$ y $|1| > 0$ da el resultado.

2. $|a^n| = |a|^n = 1$ luego a es raíz n-ésima de la unidad, y por 1. de la definición es real y positivo.
3. $1 = (-1)^2$ y 2. lleva a que $|-1| = 1$. Aplicando que $|-x| = |-1||x|$ se tiene el resultado.
4. Sean x e $y \in A^*$ tales que $xy = 0$, entonces:

$$0 = |0| = |x||y| > 0$$

   Que es una contradicción, luego tales x, y no pueden existir.

5. $1 = |1| = |x||x^{-1}|$.

□

Ejemplos:

1. Valor absoluto trivial:

   Dado A un anillo cualquiera (que sea DI), definimos el valor absoluto trivial dado por:

$$|x| = \begin{cases} 1 & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

2. Los valores absolutos usuales en $\mathbf{C}$ y $\mathbf{R}$.

3. P-ádicos sobre $\mathbf{Q}$:

   Dado $p \in \mathbf{N}$ un número primo, todo $q \in \mathbf{Q}^*$ admite una única expresión de la forma:

   $$q = p^v \frac{n}{m}, \text{ donde: } v,n \in \mathbf{Z},\ m \in \mathbf{N} \text{ y } p \nmid nm$$

   Entonces podemos definir el valor absoluto p-ádico de q como:

   $$|q| = \begin{cases} 2^{-v} & \text{si } q \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

   Que se cumplan la primera y tercera parte de la definición se sigue de manera inmediata, veamos la desigualdad triangular:

   Sean $q_1, q_2 \in \mathbf{Q}^*$ (si alguno fuese nulo sería inmediato) con sus respectivas representaciones:

   $$q_i = p^{v_i} \frac{n_i}{m_i}, \text{ con } i = 1,2.$$

   Entonces:

   $$q_1 + q_2 = \frac{p^{v_1} n_1 m_2 + p^{v_2} n_2 m_1}{m_1 m_2}$$

   Por un lado se tiene que:

   $$p \nmid n_1 m_1, n_2 m_2 \text{ lleva a que } p \nmid m_1 m_2, n_1 m_2, n_2 m_1$$

   Luego si $v_1 \neq v_2$, pongamos que v_1 es el mínimo entre ambos, tenemos:

   $$|q_1 + q_2| = |p^{v_1} \frac{n_1 m_2 + p^{v_2 - v_1} n_2 m_1}{m_1 m_2}| = 2^{-v_1} \leq |q_1| + |q_2|$$

   Si $v_1 = v_2$ notamos que $p \nmid m_1 m_2$ implica que:

   $$|q_1 + q_2| = |p^{v_1} \frac{n_1 m_2 + n_2 m_1}{m_1 m_2}| = |p^{v_1}(n_1 m_2 + n_2 m_1)| \leq |p^{v_1}| = |q_1| \leq |q_1| + |q_2|$$

   Donde la primera desigualdad se logra gracias al carácter decreciente del valor p-ádico respecto a v, notamos entonces que podemos definir los valores absolutos p-ádicos de la forma:

   $$|q| = c^{-v}$$

   Siempre y cuando c sea mayor que 1.

4. p-ádicos sobre cuerpos de polinomios:

   Dado K un cuerpo, $K[X]$ su anillo de polinomios y $K(X)$ su cuerpo de polinomios podemos definir los valores p-ádicos de manera análoga al caso de $\mathbf{Q}$:

   Sea p un polinomio irreducible en $K[X]$, cualquier otra función racional $q(x)$ en $k(X)$ no nula admite una única expresión del tipo:

   $$q(x) = p(x)^v \frac{n(x)}{m(x)}, \text{ donde: } v \in \mathbb{Z},\ n,m \in K[X] \text{ y } p(x) \nmid n(x)m(x)$$

   De esta forma podemos definir $|q(x)| = \begin{cases} 2^{-v} & \text{si } q(x) \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$. Donde la prueba de que cumple la desigualdad triangular es análoga al del caso anterior.

Nota. Se observa que, salvo los valores absolutos usuales en $\mathbb{C}$ y $\mathbb{R}$, los valores absolutos citados cumplen una versión más fuerte de la desigualdad triangular:

$$\text{Dados } x,y \in A \ (A \text{ un DI}): \ |x+y| \leq \text{máx}\{|x|,|y|\}$$

Definición. A la desigualdad anterior se le llama ultramétrica y a los valores absolutos que la cumplen para todo par de elementos se les llama no arquimedianos. A los que no la cumplan para todo par de elementos se les llamará arquimedianos.

1.2. Equivalencia de valores absolutos.

Lema 1.1. *Dado K un cuerpo y $|\cdot|$ un valor absoluto sobre él se tiene que la aplicación d de $K\times K$ en $\mathbb{R}^+$ dada por:*

$$d(x,y)=|x-y|$$

es una medida.

Demostración. La aplicación d así definida es simétrica, positiva y además $d(x,y)=0$ si y solo si $x=y$. Por otra parte cumple la desigualdad triangular:

$$d(x,y)=|x-y|=|x-z+z-y|\leq|x-z|+|z-y|=d(x,z)+d(z,y)$$

y se tiene que $d(ax,ay)=|a|d(x,y)$, $d(x+a,y+a)=d(x,y)$ □

Lema 1.2. *Con la notación del teorema anterior, el espacio métrico (K,d) es tal que las operaciones de suma, producto e inversión (para elementos no nulos) son continuas.*

Demostración. Suma:

$$|(x-y)-(a-b)|\leq|x-a|+|y-b|$$

Producto:

$$|xy-ab|=|(x-a)(y-b)+(x-a)b+a(y-b)|\leq|x-a||y-b|+|x-a||b|+|a||y-b|,$$

Inversión para elementos no nulos: Dado $a\neq 0$ se tiene:

$$|x^{-1}-a^{-1}|=|x^{-1}||a^{-1}||x-a|,\text{ para todo } x\neq 0.$$

Y dado $\varepsilon>0$ tomamos $\delta=\frac{1}{2}min\{|a|,\varepsilon|a|^2\}$ con lo que:

$$|x-a|<\delta \text{ implica que}\frac{1}{2}|a|\leq|x|,$$

Con lo cual:

$$|x^{-1}-a^{-1}|\leq 2|a|^2|x-a|<\varepsilon.$$

□

Nota. De manera natural, sobre todo espacio métrico tenemos una topología inducida por la métrica, luego podemos referirnos a la topología inducida por los valores absolutos.

Definición. Dos valores absolutos sobre el mismo cuerpo K se dirán equivalentes si definen la misma topología sobre K.

Nota. Que sea una relación de equivalencia quedará claro a través de los dos siguientes resultados.

Proposición 1.2. *Dado K cuerpo, un valor absoluto es el trivial si y solo si la topología que define es la discreta.*

Demostración. Veamos que en la topología inducida por el valor absoluto trivial los puntos son abiertos: Dado $x\in K$ consideramos $d(x,.)$ de K en $\{0,1\}\subset\mathbb{R}$ y $\{x\}=d^{-1}(\frac{-1}{2},\frac{1}{2})$ luego los puntos son abiertos y la topología del trivial es discreta.

Supongamos ahora que un valor absoluto no es trivial:

Existe entonces $a\in k^*$ tal que $|a|\neq 1$ y podemos tomarlo tal que $0<|a|<1$ (si $|a|>1$ basta invertir). Entonces:

$$\lim_{n\to\infty}|a^n|=\lim_{n\to\infty}|a|^n=0$$

Y la topología no puede ser discreta. □

Nota. Por lo tanto el único valor absoluto que es equivalente al trivial es él mismo.

Teorema 1.1. *Dado K cuerpo y dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ no triviales sobre K. Se tienen las siguientes equivalencias:*

1. $|\cdot|_1$ *es equivalente a* $|\cdot|_2$.
2. $|x|_1 < 1$ *implica* $|x|_2 < 1$.
3. $|x|_1 > 1$ *implica* $|x|_2 > 1$.
4. $|x|_1 = |x|_2^u$ *para* $x \in K$, $u \in \mathbb{R}^+$, $u \neq 0$ *fijo.*

Demostración. 1.⇒2.

$|x|_1 < 1$ implica que $|x^n|_1 \xrightarrow{n} 0$ en la métrica del primero, luego tambien en la del segundo ($|x^n|_2 \xrightarrow{n} 0$) y necesariamente $|x|_2 < 1$.

2.⇒3.

Directo invirtiendo si $x \neq 0$.

3.⇒4.

Sea $x \in K$ tal que $|x|_1 > 1$ (existe por no ser equivalente al trivial), entonces $|x|_2 > 1$. Sea ahora $y \in K$ tal que $|y|_1 > 1$ y definimos $q = \frac{log|y|_1}{log|x|_1}$ de manera que:

$$|y|_1 = |x|_1^q$$

Entonces $|y|_2 = |x|_2^q$ ya que:

1. Si $|y|_2 < |x|_2^q$ se tendría que habría $M < q$ cumpliendo $|y|_2 = |x|_2^M$ y tomando un número racional entre q y M, $M < \frac{n}{m} < q$, se tendría:
$$\frac{|y^m|_1}{|x^n|_1} > 1$$
Que lleva a que:
$$|y|_2 > |x^{\frac{n}{m}}|_2 > |x|_2^M = |y|_2.$$
2. Si $|y|_2 > |x|_2^q$ repetimos el proceso con $M > \frac{n}{m} > q$ y llegamos a:
$$|y|_1 < |x^{\frac{n}{m}}|_1$$
Luego:
$$|x^{\frac{n}{m}}|_2 > |y|_2 = |x^M|$$

Se tiene entonces que la relación:

$$\frac{log|x|_2}{log|x|_1} = \frac{log|x|_2}{log|x|_1} = u$$

Se cumple para cualquier $y \in K$ con valor absoluto mayor que 1. Si tiene valor menor que 1 basta con invertir para ver que se sigue cumpliendo y si es 1 basta tomar xy ya que:

$$|xy|_1 > 1 \text{ lleva a que } |x|_2|y|_2 = (|x|_1|y|_1)^u = |x|_1^u = |x|_2.$$

□

Corolario 1.1. *La relación entre valores absolutos dada por: $|.|_1$ esta relacionado con $|.|_2$ si definen la misma topología es de equivalencia.*

Demostración. Basta usar la última equivalencia del teorema 1.1. □

Finalizamos esta sección con el teorema de aproximación:

Teorema 1.2. *Dados r valores absolutos que no son equivalentes 2 a 2 ni triviales en un cuerpo K cumple que toda r-tupla sobre K puede ser aproximada simultaneamente sobre las valoraciones, es decir, para cualquieras $a_1,\dots,a_n \in K$ y $\varepsilon > 0$ existe $\alpha \in K$ tal que:*

$$|\alpha - a_i|_i < \varepsilon, \text{ para } i = 1,\dots r.$$

Demostración. Si $r = 2$ por no ser equivalentes existen $a,b \in K$ tales que

$$|a|_1 > 1 \geq |a|_2 \text{ y } |b|_2 > 1 \geq |b|_1,$$

Luego $c = ab^{-1}$ cumple $|c|_1 > 1 > |c|_2$. Sea ahora $r > 2$, por inducción existe un $a \in K$ tal que $|a|_1 > 1 > |a|_i$ para $i = 2,\dots,r-1$ y $b \in K$ tal que $|b|_1 > 1 > |b|_r$ (este b surge con el mismo proceso que antes). Entonces, o bien $|a|_r \leq 1$, en cuyo caso $c_n = a^n b$ cumple $|c_n|_1 > 1 > |c_n|_r$ y para n suficientemente grande $|c_n|_1 > 1 > |c_n|_i$ para $i = 1,\dots,r-1$. O bien, $|a|_r > 1$ y $c_n = ba^n(1+a^n)^{-1}$ es tal que:

$$|c_n|_1 \to |b|_1 > 1,\ |c_n|_r \to |b|_r < 1 \text{ y } |c_n|_i \to 0 \text{ para } i = 2,\dots,r-1.$$

Ya que $|a^n(1+a^n)^{-1}|_1 \to 1$, puesto que $|a|_1 > 1$ implica que no puede ser una unidad, en particular no puede ser una raiz de la unidad y $a^n \neq -1$ para cualquier n y la norma del producto anterior tiende a 1.

Tenemos entonces que existe un elemento $c \in K$ tal que:

$$|c|_1 > 1,\ |c|_i < 1 \text{ para } i = 1,\dots,r.$$

Por lo tanto, tal c cumple que $c^n(1+c^n)$ tiende a 1 en el valor absoluto $|\cdot|_1$ y a cero en el resto.

Podemos repetir este proceso con cada valor absoluto de manera que existen elementos $x_i \in K$ tales que, dado $\delta > 0$, $|x_i - 1|_i < \delta$, $|x_i|_j < \delta$ para $j \neq i$. Por lo tanto, tomando $\delta < \frac{\varepsilon}{máx_i\{\sum_j |a_j|_i\}}$, y $\alpha = \sum a_i x_i$ se tiene que:

$$|\alpha - a_i|_i = |a_i(1-x_i) + \sum_{i\neq j} a_j x - j|_i \leq |a_i(x_i-1)|_i + \sum_{j\neq i} |a_j x_j|_i \leq \delta máx_i\{\sum_j |a_j|_i\} < \varepsilon.$$

□

Capítulo 2

Valoraciones

2.1. Definición y primeras propiedades.

Definición. Sea A un anillo, se llamará valoración sobre A a una aplicación v de A en $\mathbb{R} \cup \{\infty\}$ cumpliendo:

1. $v(x)$ es real para todo x no nulo y $v(0) = \infty$
2. $v(x+y) \geq min\{v(x), v(y)\}$
3. $v(xy) = v(x) + v(y)$

Nota. En general, se pueden definir valoraciones con imágenes grupos abelianos totalmente ordenados generales a los que se les añade un símbolo ∞ cumpliendo las relaciones: $\infty > x, x + \infty = \infty$ para cualquier x en el grupo.

Proposición 2.1. *Sea A un anillo sobre el que esta definida una valoración v, se tiene:*

1. $v(1) = 0$.
2. *Si* $a \in A$ *es tal que* $a^n = 1$ *para* $n \in \mathbb{N}$, *se tiene que* $v(a) = 0$.
3. $v(-a) = v(a)$.
4. *Si* $a \in A$ *tiene inverso respecto al producto en A se tiene que* $v(a^{-1}) = -v(a)$.
5. *A es un DI.*
6. *Si* $a_1 + \ldots + a_n = 0$ *se tiene que el valor de la valoración coincide en al menos dos elementos, para* $a_i \in A$ $i = 1, \ldots, n$. *En particular si* $a_1 \neq a_2$ *se sigue que* $v(a_1 + a_2) = min\{v(a_1), v(a_2)\}$.

Demostración.

1. $v(1) = v(1) + v(1)$.
2. $0 = v(a^n) = nv(a)$.
3. $(-1)^2 = 1$ nos lleva a que $v(-1) = 0$ por el apartado anterior luego $v(-a) = v(-1) + v(a) = v(a)$.
4. Aplicando el primer apartado y la tercera propiedad de la defínción se tiene el resultado.
5. Si existiesen $x, y \in A^*$ tales que $xy = 0$ se tendría que $\infty > v(x) + v(y) = v(xy) = v(0) = \infty$.
6. Suponer que no es cierto y que existe una cadena de desigualdades estrictas:

   $$v(a_1) < \ldots < v(a_n).$$

   Se sigue que $v(-a_1) = v(a_2 + \ldots + a_n) \geq min\{v(a_2), \ldots, v_(a_n)\} > v(a_1)$ que es una contradicción.

   La segunda parte es inmediata teniendo en cuenta que $-(a_1 + a_2) + a_1 + a_2 = 0$.

□

Ejemplos:

1. La valoración trivial:

   Dado A un DI, definimos la valoración trivial como aquella dada por:

$$v(x) = \begin{cases} 0 & \text{si } x \neq 0 \\ \infty & \text{si } x = 0 \end{cases}$$

2. Las valoraciones p-ádicas:

   Dado $p \in \mathbb{N}$ primo podemos expresar cualquier elemento de $\mathbb{Q}^*$ como $q = p^v \frac{n}{m}$ con $p \nmid nm$ y $v \in \mathbb{Z}$. Entonces, $v_p(q) = v$ para $q \neq 0$ e ∞ para 0 es una valoración.

La aparente relación que existe entre valoraciones y valores absolutos queda confirmada a través de la siguiente proposición:

Proposición 2.2. *Sea A un DI, entonces:*

1. *Dado $|\cdot|$ valor absoluto no arquimediano, obtenemos una valoración sobre A a través de la fórmula:*

$$v(x) = \begin{cases} -log(|x|) & si\ x \neq 0 \\ \infty & si\ x = 0 \end{cases}$$

2. *Dada una valoración v sobre A, obtenemos un valor absoluto no arquimediano a través de la fórmula:*

$$|x| = \begin{cases} e^{-v(x)} & si\ x \neq 0 \\ 0 & si\ x = 0 \end{cases}$$

Ambas fórmulas son una inversa de la otra.

Demostración. 1. v así definida cumple la primera y tercera propiedad de la definición de manera directa, veamos la segunda:

Sean $x, y \in A^*$ (si alguno fuese nulo sería inmediato) se tiene que $|x+y| \leq máx\{|x|,|y|\}$ lleva a que

$$log(|x+y|) \leq log(máx\{|x|,|y|\}) = máx\{log(|x|), log(|y|)\} = -mín\{-log(|x|), -log(|y|)\}$$

Luego $v(x+y) = -log(|x+y|) \geq mín\{-log(|x|), -log(|y|)\} = mín\{v(x), v(y)\}$.

2. Nuevamente, la primera y tercera propiedad de la defínción de valor absolutos se obtiene de manera directa y sin usar ni siquiera la segunda propiedad de las valoraciones. Veamos que cumple la desigualdad ultramétrica:

   Sean $x, y \in A^*$ (si alguno fuese nulo es inmediato), teniendo en cuenta que:

$$v(x+y) \geq mín\{v(x), v(y)\} = -máx\{-v(x), -v(y)\},$$

   Se tiene que:

$$|x+y| = e^{-v(x+y)} \leq e^{máx\{-v(x),-v(y)\}} = máx\{|x|,|y|\}.$$

La última afirmación es inmediata. □

Nota. Observamos entonces que es lo mismo hablar de valoraciones sobre un DI que de valores absolutos no arquimedianos sobre él. Con lo que podemos hablar de la valoración o de su valor absoluto asociado.

Definición. Dado A un DI, diremos que dos valoraciones sobre A son equivalentes si lo son sus valores absolutos asociados.

Lema 2.1. *Dado A un DI y dos valoraciones no triviales v_1, v_2 sobre él, serán equivalentes si y solo si existe un $u \in \mathbb{R}^+$, $u \neq 0$, tal que $v_1(x) = uv_2(x)$ para todo x en A. La única valoración equivalente a la trivial es ella misma.*

Demostración. Usando el teorema 1.1 del capítulo anterior, tenemos que los valores absolutos asociados estarán relacionados si y solo si existe $u \in \mathbb{R}^+$ no nula tal que $|\cdot|_1 = |\cdot|_2^u$, luego: $v_1(\cdot) = uv_2(\cdot)$ a través de 2.2.

Por otra parte, la única valoración equivalente a la trivial es ella misma, por ser el valor absoluto trivial el único asociado a él mismo por 1.2 del capítulo anterior. □

A partir de ahora, cuando hablemos de valoraciones podremos tomarlas como representantes de su clase de equivalencia.

Proposición 2.3. *Dado K cuerpo y v una valoración sobre él los valores que adquiere la valoración en $\mathbb{R}$ o son de la forma $\lambda\mathbb{Z}$ con $\lambda \in \mathbb{R}$ o son densos en $\mathbb{R}$.*

Demostración. Si v es trivial bastará tomar λ nulo. Supongamos que no es trivial, con lo que la valoración toma valores positivos y pueden surgir dos situaciones:

Supongamos en primer lugar que existe un elemento mínimo en el conjunto de valores positivos que toma v, llamemoslo λ. Por la tercera propiedad de la definición se tiene que $\lambda\mathbb{Z}$ pertenece al conjunto de valores que toma v. Sea ahora $b \notin \lambda\mathbb{Z}$ que pertenezca a la imagen de v, pongamos que $b = v(c)$ para cierto c de K, se tiene que existe $n_0 \in \mathbb{N}$ tal que:

$$(n_0 - 1)\lambda \leq b < n_0\lambda$$

Lo que nos lleva a:

$$0 \leq v(ca^{1-n_0}) = b - (n_0 - 1)\lambda < \lambda$$

Y por hipótesis λ es el mínimo, luego $b = n_0\lambda$.

Si no existe ese λ y la valoración no es trivial, necesariamente para cualquier abierto del tipo $(0, a)$ existe un elemento de K cuya imagen esta contenida en ese intervalo. Sean ahora dos números cualequiera ($b < a$), vamos a ver que siempre existe entre ellos otro que es imagen de la valoración:

Si $b \leq 0 < a$ basta considerar el intervalo del tipo $(0, a)$ anterior, y si son ambos negativos podemos considerar sus opuestos, encontrar el elemento cuya imagen vive entre los opuestos e invertirlo. Sean pues $0 < b < a$, entonces existe $c \in K$ tal que:

$$0 < v(c) < a - b$$

Y existe a su vez $n_0 \in \mathbb{N}$ tal que:

$$(n_0 - 1)v(c) < b < n_0v(c) < a$$

Luego c^{n_0} es el elemento buscado y la imagen es densa en $\mathbb{R}$. □

Definición. Diremos que una valoración es discreta si su imagen es isomorfa a $\mathbb{Z}$.

Nota. Obtenemos entonces que, si dos valoraciones son equivalentes, necesariamente sus imagenes grupos abelianos ordenados isomorfos y en el caso de que sean discretas y no triviales podremos coger el representante cuya imagen sea precisamente $\mathbb{Z}$.

Definición. Al representante de la valoraciones discretas cuya imagen sea precisamente $\mathbb{Z}$ se le llamará valoración normalizada.

Nota. Por el momento la segunda propiedad de la definición de valoración puede parecer forzada para asociar los valores absolutos no arquimedianos con las valoraciones. Cabría pensar que dando una definición más general de valoración podriamos cubrir más casos. Sin embargo su utilidad se hará evidente en la prueba del siguiente resultado.

Proposición 2.4. *Las únicas valoraciones discretas sobre $\mathbb{Q}$ son la trivial y las equivalentes a las p-ádicas.*

Demostración. Sea v una valoración discreta sobre $\mathbb{Q}$, se tiene por la segunda propiedad de la definición que, $v(1) = 0$ implica que $v(n) = v(1+\ldots+1) \geq 0$ por inducción sobre n, y por el tercer apartado de la proposición 2.1 podemos extender el resultado a todo $\mathbb{Z}$.

Consideramos ahora $P = \{n \in \mathbb{Z}/v(n) \geq 0\}$, veamos que es un ideal primo de $\mathbb{Z}$: Que sea un ideal se deriva nuevamente de la segunda propiedad de la definición:

Dados $x, y \in P$ y $n \in \mathbb{Z}$, $v(x+y) \geq mín\{v(x), v(y)\} \geq 0$, luego $x+y \in P$ y $v(nx) = v(n)+v(x) \geq 0$, por lo que $nx \in P$ también.

Que sea primo:

Dados $x, y \in \mathbb{Z}$, $xy \in P$ si y solo si $v(xy) \geq 0$, y $v(x)+v(y) = v(xy) \geq 0$ lleva a que al menos uno de los dos está en P.

Por ser $\mathbb{Z}$ un dominio de ideales principales llegamos a que $P = (p)$ para cierta p prima. Y para cada $k \in \mathbb{Z}$ tal que $p \nmid k$ se tendrá que $v(k) = 0$.

Podemos extender esto a $\mathbb{Q}$ usando que, si $q = p^j \frac{n}{m}$ con $p \nmid nm$ y $j \in \mathbb{Z}$:

$$v(q) = jv(pn) - v(m) = jv(p).$$

□

Nota. Observamos que nuestra herramienta fundamental en la demostración ha sido el ideal P, de cara a generalizarlo a otros cuerpos definiremos el conceptos de anillo de valoración.

2.2. Anillos de valoración, lugares y equivalencia con valoraciones.

Lema 2.2. *Dado K cuerpo y v una valoración sobre K se tiene que el conjunto* $A_v = \{x \in K / v(x) \geq 0\}$ *es un anillo.*

Demostración. Por un lado, sabemos que $v(1) = 0$ y $v(0) = \infty$, por lo tanto pertenecen al conjunto.

Dados dos elementos de A_v se tiene que $v(x+y) \geq mín\{v(x), v(y)\} \geq 0$, por lo que la suma volverá a pertenecer, y el producto también puesto que $v(xy) = v(x) + v(y) \geq 0$. □

Definición. Sea K cuerpo y v una valoración discreta sobre K. Llamaremos anillo de valoración de v al anillo:

$$A_v = \{x \in K / v(x) \geq 0\}$$

.

Notas.

1. Observamos que, si $x \notin A_v$ necesariamente $v(x) < 0$ y nos lleva a que $v(x^{-1}) > 0$. Luego los anillos de valoración nos dividen K de manera que, si un elemento no esta en el anillo, su inverso si.

2. Usando que dos valoraciones equivalentes son iguales salvo constante multiplicativa positiva, es claro que un anillo de valoración es característico de cada clase de equivalencia.

Lema 2.3. *Dado un cuerpo K con valoración v, y llamando* $\hat{A}_v = \{x \in K / v(x) \leq 0\}$*, se tiene que* $K = \hat{A}_v \cup A_v$ *y que* $\hat{A}_v \cap A_v$ *son las unidades de* A_v*.*

Demostración. La primera parte es inmediata teniendo en cuenta que $v(x)$ será o negativo o no negativo.

Para la segunda basta tener en cuenta que un elemento tendra inverso en A_v si y solo si $v(x) = 0$ ya que en otro caso el inverso no podría estar en A_v. □

De hecho, podemos extender el resultado anterior a la siguiente equivalencia con la definición de anillo de valoración.

Lema 2.4. *Sea K un cuerpo y A un subanillo de K cumpliendo que, para todo elemento* $x \in K^*$*, si* $x \notin A$ *implique que* $x^{-1} \in A$*. Entonces existe v valoración sobre K de manera que A es su anillo de valoración.*

Demostración. Definimos $A^{-1} = \{x \in K / x \notin A\}$, se tiene entonces que las unidades de A será el conjunto $U = A \cap A^{-1}$.

Por otra parte, podemos definir una relación de divisibilidad relativa a A de manera que: $a \mid b$ si y solo si $ba * -1 \in A$. Así, tenemos que es una relación reflexiva, transitiva y multiplicativa, es por tanto un preordenamiento de K.

De esta manera, podemos definir el homomorfismo v que surge de manera natural entre K^* y K^*/U. Notamos que sobre este segundo conjunto existe un orden heredado del preordenamiento anterior: $v(b) \geq v(a)$ si y solo si $a \mid b$. De esta manera, si a v le asignamos el valor ∞ en el 0 tendremos que v es una valoración que toma imágen en el grupo abeliano K^*/U:

La primera y tercera propiedad son inmediatas, para la segunda: sean $x, y \in K^*$, si alguno fuese nulo sería trivial. Supongamos que $v(x) > v(y)$, entonces $xy^{-1} \in A$, luego $xy^{-1} + 1 \in A$ y se sigue que $v(x+y) > v(y)$.

Por último, para ver que el anillo inicial es precisamente el de valoración asociado a v basta tener en cuenta que los x de K tales que $v(x) \geq 0$ son precisamente los que pertenecen a A.

□

Proposición 2.5. *Sea K cuerpo y v valoración discreta sobre K. El anillo de valoración* A_v *tiene un ideal maximal. Es más, todo ideal de* A_v *es de la forma* $\{x \in \mathbb{Z} / v(x) > n\}$ *para* $n \in \mathbb{N} \cup 0$*.*

Demostración. Probaremos primero la segunda afirmación:

Sea I un ideal de A_v, sea $m = min\{v(x)/x \in I\}$ entonces para cualquier otro elemento y de I se tiene que $v(y) \geq m$, luego $I = \{x \in \mathbb{Z}/v(x) > m-1$. Notar que m no puede ser 0, ya que eso implicaría que I posee una unidad, y sería por tanto A_v.

La primera afirmación es ahora directa teniendo en cuenta que, si llamamos $I_m = \{x \in \mathbb{Z}/v(x) \geq m$ para $m \geq 1$, tendremos la cadena de ideales:

$$I_1 \supset I_2 \supset \dots$$

E I_1 será el ideal maximal. □

Lema 2.5. *Todo anillo de valoración posee un único ideal maximal.*

Demostración. Basta ver que las no unidades del anillo conforman un ideal:

Sean a, b no nulas ni unidades en el anillo, entonces o bien $\frac{a}{b}$ o bien $\frac{b}{a}$ están el anillo de valoración por el lema 2.4. Si $a+b$ fuese una unidad del anillo y $\frac{a}{b}$ estuviese en él se tendría que:

$$b(1+\frac{a}{b}) = u, \text{ donde u es una unidad y } b[(1+\frac{a}{b})u^{-1}] = 1$$

Lo que llevaría a que b es una unidad. De manera análoga se ve que requeriría que a fuese una unidad, lo que lleva a que es un ideal. □

Hemos observado en la proposición 2.3 que los valores que adquiere una valoración están determinados (salvo factor multiplicativo), pero el argumento inverso es también cierto, según los valores que toma se puede determinar toda la valoración. Para verlo vamos a definir el concepto de lugar y mostrar su equivalencia al de anillo de valoración.

Definición. Dados dos cuerpos K y F llamaremos lugar de K en F a una aplicacion p de K en $F \cup \{\infty\}$ de manera que p restringida a la preimagen de F sea un homomorfismo y que $s(x) = \infty$ implique que: $x \neq 0, s(x^{-1}) = 0$. Si $C \subset K$ es un subcuerpo sobre el que s es un isomorfismo diremos que s es un lugar sobre C.

Ejemplo: Dado el cuerpo de funciones racionales de cierto cuerpo K, para cada $a \in K$ podemos escribir cualquier $u(x) = \frac{f(x)}{g(x)}$.Si $f(a)$ y $g(a)$ no se anulan a la vez podemos definir el valor de u como:

$$s(u) = \begin{cases} u(a) & \text{si } g(a) \neq 0 \\ \infty & \text{si } g(a) = 0, f(a) \neq 0 \end{cases}$$

Tenemos así un lugar sobre K.

Proposición 2.6. *Existe una biyección entre las clases de isomorfía de lugares y los anillos de valoración, de hecho, los lugares sobre subcuerpos C del cuerpo donde estan definidos corresponden a anillos de valoración conteniendo a C.*

Demostración. Dado s lugar de K en F se tiene que $V = s^{-1}(F)$ es un anillo de valoración:

Dado $x \in K^*$, $x \notin V$ si y solo si $s(x) = \infty$ que implica $s(x^{-1}) = 0 \in V$. Luego por el lema 2.4 se tiene que es un anillo de valoración.

Dado un anillo de valoración V tomamos M su ideal maximal y consideramos V/M 8que es el cuerpo residual del ideal macimal) y el homomorfismo natural n entre V y V/M. Definimos entonces:

$$s(x) = \begin{cases} n(x) & \text{si } x \in V \\ \infty & \text{si } x \notin V \end{cases}$$

que resulta ser un lugar.

La última afirmación se debe a que un lugar estará sobre C si $C \subset V$. □

Nota. Por lo tanto, será indiferente hablar de valoraciones, valores absolutos no arquimedianos, anillos de valoración o lugares.

Capítulo 3

Dominios de Dedekind

3.1. Familias de valoraciones y propiedad de aproximación fuerte.

Definición. Sea K cuerpo sobre el que esta definida la familia de valoraciones S que suponemos no triviales y no equivalentes 2 a 2. Dados los correspondientes anillos de valoración A_p definimos $\mathcal{O} = \cap A_p$ que llamaremos el anillo integral.

Podemos asi dar una divisibilidad relativa S en K a través de la regla: $x|y$ si y solo si $v_p(y) \geq v_p(x)$ para todo p en S.

Definición. Un elemento x de K será integral respecto a la valoracion p si $v_p(x) \geq 0$.

Definición. Sea K cuerpo sobre el que esta definida la familia de valoraciones S que suponemos no triviales, normailizados y no equivalentes 2 a 2. Diremos que S satisface la condición de aproximación fuerte si cumple:

1. Las valoraciones son principales.
2. Dado $x \in K$, $v_p(x) \geq 0$ para casi todo $p \in S$.
3. Dadas $p, p' \in S$, distintas y $N > 0$, existe $x \in K$ tal que $v_p(x-1) > N$, $v_{p'}(x) > N$ y $v_q \geq 0$ para cualquier $q \in S$, $q \neq p, p'$.

Nota. Con estas condiciones se busca de alguna manera imitar el caso de $\mathbb{Z}$ y $\mathbb{Q}$. En este, se puede ver como el conjunto que es integral para todas las valoraciones discretas sobre $\mathbb{Q}$ y a su vez $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$. En pocos resultados veremos que el conjunto $\mathfrak{a}$ cumple ciertas propiedades de divisibilidad a nivel de ideales que son deseables.

Lema 3.1. *Sea K cuerpo sobre el que esta definida la familia de valoraciones S que cumple la condición de aproximación fuerte, se tiene que $v_p(u) = 0$ para casi toda valoración $v_p \in S$ y para todo $u \in K$.*

Demostración. Basta usar la segunda propiedad, si existiese un elemento $u \in K$ tal que $v_p(u) > 0$ en un conjunto infinito de valoraciones de S se tendría que su inverso sería negativo en todas esas valoraciones, lo que contradice la segunda propiedad. □

Teorema 3.1. *Sea K un cuerpo con una familia de valoraciones S que satisface la condición de aproximación fuerte. Entonces, para cualesquiera $p_1, \ldots, p_n \in S$, $a_1, \ldots, a_n \in K$ y $N > 0$, existe $a \in K$ tal que:*

$$v_{p_i}(a - a_i) > N, \text{ para } i = 1, \ldots, n,$$

$$v_q(a) \geq 0, \text{ para } q \neq p_1, \ldots, p_n.$$

Demostración. Podemos suponer que se cumple $v_q(a_i) \geq 0$ ya que a lo mucho fallará en una familia finita que podemos añadir a nuestras $p_1, \ldots, p_n$ completando con 0 los a_i. Tambien podemos suponer que n>1, pues el caso n=1 es trivial.

Sea $M > 0$, por la tercera parte de la condición de aproximación fuerte se tiene que existe para cada $i = 2, ..., n$ c_i tal que:

$$v_{p_1}(c_i - 1) > M,\ v_{p_i}(c_i) > M.$$

Con los c_i integrales también en las otras valoraciones, luego $c_i \in \mathcal{O}$ y definiendo $b_1 = c_2 \ldots c_n$ se tiene que $b_1 \in \mathcal{O}$ y $v_{p_i}(b_1) = \sum_j v_{p_i}(c_j) > M$. Es más,

$$b_1 - 1 = (c_2 - 1)c_3 \ldots c_n + (c_3 - 1)c_4 \ldots c_n + \ldots + c_n - 1$$

Con lo que $v_{p_1}(b_1 - 1) \geq min\{v_{p_1}(c_2 - 1), \ldots, v_{p_1}(c_n - 1) > M$.

De manera análoga podemos construir b_i y poniendo $a = \sum_i a_i b_i$ llegamos a:

$$v_{p_i}(a - a_i) = v_{p_i}((b_i - 1)a_i + \sum_{j \neq i} a_i b_i) \geq mín_j\{v_{p_i}(a_j + M)$$

Y se llega al resultado tomando $M > N - mín_{i,j}\{v_{p_j}(a_i)\}$ y $v_q(a) \geq 0$. □

Corolario 3.1. *Dado K cuerpo y S una familia que cumple la propiedad de aproximación fuerte se tiene que K es precisamente el cuerpo de fracciones de $\mathcal{O}$.*

Demostración. Dado $a \in K^*$ $v_p(a) \geq 0$ para casi todos los $p \in S$, sea $p_1, \ldots, p_n$ aquellos donde no se cumple y sea $N = -mín\{v_{p_i}(a)\}$, por el teorema 3.1 se sigue que existe $b \in k$ tal que $b \in \mathcal{O}$, $v_{p_i}(b) > N$ Por lo tanto, $ab \in \mathcal{O}$ y $a = \frac{c}{b}$ para cierto $c \in \mathcal{O}$. □

De hecho, el teorema 3.1 nos permite decretar que existen elementos en K que toman los valores que nosotros queramos en una familia finita de valoraciones:

Lema 3.2. *Sea K un cuerpo y S una familia de valoraciones sobre él que cumple la propiedad de aproximación fuerte. Entonces, para cualquier conjunto finito de valoraciones $\{p_1, \ldots, p_n\} \in S$ de S y enteros $a_1, \ldots, a_n$ existe un elemento $c \in K$ tal que:*

$$v_{p_i}(c) = a_i,\ y\ v_q(c) \geq 0\ para\ q \neq p_i\ i = 1, \ldots, n.$$

Demostración. Por estar las valoraciones normalizadas existe para cada i un $b_i \in K$ tal que $v_{p_i}(b_i) = a_i$. Por el teorema 3.1 existe $c \in K$ tal que

$$v_{p_i}(c - b_i) > a_i,\ v_q(c) \text{ para todo } q \neq p_i.$$

Luego $v_{p_i}(c) \geq mín\{v_{p_i}(b_i), v_{p_i}(c - b_i)\}$ y se tiene la igualdad a a_i ya que $v_{p_i}(b_i) = a_i < v_{p_i}(c - b_i)$. □

3.2. Ideales fraccionarios y grupo de divisores.

Definición. Sea K cuerpo y R un subanillo de K. Llamaremos ideal fraccionario de R a un R-módulo U de K tal que

$$uR \subseteq U \subseteq vR, \text{ para ciertos } u, v \in k^*$$

Nota. Los ideales fraccionarios asi definidos no son necesariamente ideales.

Lema 3.3. *Dado K cuerpo y R subanillo de K, se tiene que un ideal U de R es fraccionario si no es el nulo.*

Demostración. Llamando al ideal I y notando que, por no ser el nulo, tendrá algún elemento distinto del 0 (a), se sigue que:

$$aR \subseteq I \subseteq 1R.$$

□

Definición. Dado K cuerpo y R subanillo de K, llamaremos ideales enteros a los ideales fraccionarios que sean también ideales en R.

Proposición 3.1. *Dado K cuerpo y R subanillo de K, se tiene el que el conjunto de ideales fraccionarios de R (F) junto a la multiplicación dada por:*

$$U_1U_2 = \{\sum x_1x_2 / x_1 \in U_1, x_2 \in U_2\}.$$

Es un monoide.

Demostración. Veamos primero que la multiplicación asi definida es una operación binaria interna:
Sean $U_1, U_2 \subset K$ ideales fraccionarios de $\mathfrak{a}$.

$$a_iR \subseteq U_i \subseteq b_iR, \text{ para } a_i, b_i \in K \text{ e } i = 1, 2.$$

Entonces, es claro que:

$$a_1a_2R \subseteq U_1U_2 \subseteq b_1b_2R.$$

Por la definición de esta operación, es asociativa y tiene elemento neutro: R. Por lo tanto F junto a esta operación es un monoide. □

Definición. Dado K cuerpo y R subanillo de K, definimos la inversa generalizada de U ideal fraccionario como:

$$(R : U) = \{x \in K | xU \subseteq R\}$$

Lema 3.4. *Dado K cuerpo y R subanillo de K, la inversa generalizada definida sobre F es una operación interna.*

Demostración. Sea $U \in F$, se tiene que existen $a, b \in K^*$ de manera que

$$aR \subseteq U \subseteq bR,$$

luego:

$$b^{-1}R \subseteq (R : U) \subseteq a^{-1}R.$$

Y dado $c \in R$ se tiene que $cxU \subseteq R$ para cualquier $x \in (R : U)$ y es un R-módulo.
Por lo tanto es un ideal fraccionario. □

Corolario 3.2. *Dado K cuerpo y R subanillo de K, se tiene que:*

$$(R : U)U \subseteq R.$$

Demostración. Por el lema anterior sabemos que la operación $(R:U)$ es interna, luego el producto $(R:U)U$ esta bien definido y el resultado es inmediato teniendo en cuenta la definicíon de $(R:U)$. □

Definición. Llamaremos a $U \in F$ invertible si cumple que:

$$(R:U)U = R.$$

En ese caso usaremos la notación: $U^{-1} = (R:U)$.

Ya estamos en condiciones de comenzar a definir relaciones de divisibilidad sobre los ideales fraccionarios, a continuación definiremos el grupo de divisores que nos servirá de fulcro para definir una relación de divisibilidad a nivel de ideales fraccionarios.

Definición. Sea K un cuerpo sobre el que se ha definido una familia de valoraciones S, y sea $\mathscr{O}$ su anillo de enteros. Llamamos grupo de divisores de K (D), al grupo abeliano libre generado por los lugares asociadas a las valoraciones de S. Si denotamos por $\mathfrak{p}$ a los lugares tenemos que los elementos de D son de la forma:

$$\mathfrak{b} = \prod \mathfrak{p}^{a_\mathfrak{p}}, \text{ con } a_\mathfrak{p} \in \mathbb{Z}, \text{ casi todos ellos nulos.}$$

Llamaremos a los elementos de D divisores y a los elementos de S divisores primos.

De aquí en adelante suponderemos que S cumple la propiedad de aproximación fuerte.

Lema 3.5. *Sea K un cuerpo sobre el que se ha definido una familia de valoraciones S, y sea $\mathscr{O}$ su anillo de enteros y F los ideales fraccionarios de $\mathscr{O}$. Dada $v_p \in S$ podemos extender a F v_p a través de:*

$$v_p(U) = min\{v_p(x) | x \in U\}, \text{ para } U \in F.$$

Además es compatible con el producto de ideales fraccionarios en el sentido de que, dados $U,V \in F$, $v_p(UV) = v_p(U)v_p(V)$.

Demostración. Por ser U ideal fraccionario se tiene que existen $a,b \in K^*$ tales que:

$$a\mathscr{O} \subseteq U \subseteq b\mathscr{O},$$

luego $v_p(a) \geq v_p(U) \geq v_p(b)$ ya que:

$$v_p(c\mathscr{O}) = mín\{v_p(cx) | x \in \mathscr{O}\} = mín\{v_p(c) + v_p(x) | x \in \mathscr{O}\} = v_p(c).$$

Por lo que esta bien definido.

Para ver que es compatible con el producto notamos que $c \in UV$ puede ser expresado como $c = \sum a_i b_i$ con $a_i \in U$, $b_i \in V$, luego:

$$v_p(c) \geq mín_i\{v_p(a_i) + v_p(b_i)\} \geq v_p(U) + v_p(V),$$

Por lo tanto $v_p(UV) \geq v_p(U) + v_p(V)$ y se alcanza la igualdad tomando c el producto de dos elementos que minimicen v_U y $v_p(V)$ respectivamente. □

Nota. Observamos en la demostración anterior se deduce que debe ser 0 para casi todo p, ya que deben ser 0 en casi todo p en u y v.

Proposición 3.2. *La aplicación ϕ que va de los ideales fraccionarios al grupo de divisores dada por:*

$$\phi(U) = \prod p^{v_p(U)}$$

Esta bien definida y es un homomorfismo de monoides.

Demostración. Por la nota anterior sabemos que $v_p(U)$ es nulo para casi todo $p \in S$, luego la aplicación esta bien definida ya que el productorio tendra casi todos sus elementos 1's.

Por otra parte, teniendo en cuenta que v_p es compatible con el producto por el Lema 3.5, se sigue que es homomorfismo. □

Nota. Si probamos que ϕ es un isomorfismo habremos logrado concluir que F es un grupo en el que podemos dar las relaciones de divisibilidad referentes a las de D. Para ello, necesitaremos el siguiente lema:

Lema 3.6. *Dado un cuerpo K sobre el que esta definido una familia de valoraciones S que cumple la propiedad de la aproximación fuerte, y denotando por $\mathcal{O}$ al anillo de enteros asociado. Se tiene que, dado un ideal fraccionario U de $\mathcal{O}$ en K, para todo $x \in K$:*

$$x \in U \text{ si y solo si } v_p(x) \geq v_p(U) \text{ para toda valoración } p \in S.$$

Demostración. La implicación a derechas es inmediata por la defínción de $v_p(U)$. Para ver la otra sea x que cumple la condición, entonces:

$$v_p(x^{-1}U) \leq 0$$

Y usando que, si intersecamos $x^{-1}U$ con $\mathcal{O}$ obtenemos un nuevo conjunto sobre el que podemos definir nuestra extensión de la valoración:

Si $V \in F$ es un ideal fraccionario, $a\mathcal{O} \subseteq V \subseteq b\mathcal{O}$ para $a, b \in K^*$, $(V \cap \mathcal{O})$ es un $\mathcal{O}$-módulo cumpliendo $V \cap \mathcal{O} \subseteq \mathcal{O}$. Por lo que $v_p(V \cap \mathcal{O}) = min\{v_p(x) | x \in V \cap \mathcal{O}\} \geq 0$ y esta bien definido.

Tenemos que los elementos de $x^{-1}U$ toman valores no positivos en las valoraciones. Se sigue que: $v_p(x^{-1}U \cap \mathcal{O}) = 0$.

Sea ahora $c \in x^{-1}U \cap \mathcal{O}^*$, si c es una unidad se tendría que $1 \in x^{-1}U \cap \mathcal{O} \subset x^{-1}U$ y por lo tanto $x \in U$. Sino es una unidad $v_p(c)$ será cero salvo un número finito de valoraciones $p_1, \ldots, p_n \in S$.

Como $v_p(x^{-1}U \cap \mathcal{O}) = 0$ para toda $p \in S$, se tiene que existen $a_i \in x^{-1}U$ tales que $v_{p_i}(a_i) = 0$ y por el teorema 3.1 para cada p_i existirá $b_i \in K$ tal que:

$$v_{p_i}(a_i^{-1} - b_i) \geq v_{p_i}(c), \text{ además } v_q(b_i) \geq v_q(c) \text{ con } q \neq p_i.$$

Ya que $v_q(c) = 0$ salvo en una familia finita de valoraciones. Deducimos que $b_i \in \mathcal{O}$ para las $i = 1, \ldots, n$ ya que la c tomaba valores no negativos en cualquier valoración de S.

Así se tiene que $a = \sum_i a_i b_i \in x^{-1}U$ y es tal que:

$$v_{p_j}(1-a) = v_{p_j}(1 - a_j b_j - \sum_{i \neq j} a_i b_i) \geq v_{p_j}(c),\ j = 1, \ldots, n.$$

De manera que $1 - a \in \mathcal{O}$.

Por lo tanto $c^{-1}(1-a) = d \in \mathcal{O}$ y $1 = a + cd \in x^{-1}U$, luego $x \in U$. □

Teorema 3.2. *Sea K cuerpo sobre el que esta definida una familia de valoraciones S que cumple la propiedad de aproximación fuerte. Sea $\mathcal{O}$ el anillo de enteros de S y F sus ideales fraccionarios. Entonces F junto al producto de ideales fraccionarios y la inversión es un grupo abeliano libre que tiene como base los ideales enteros. Es más, es ismoformo al grupo de divisores de S.*

Demostración. Procedemos a definir una función χ del grupo D en F que veremos es inversa de ϕ:

$$\chi(\prod_p p^{a_p}) = \{x \in K | v_p(x) \geq a_p, \text{ para todo } p \in S\}.$$

Ya que todos los elementos de $\mathcal{O}$ son no negativos se tiene que $\chi(\prod_p p^{a_p})$ será un $\mathcal{O}$-módulo. Por otra parte, como $a_p = 0$ salvo en un número finito de casos, si tomamos $u, v \in K$ tales que $v_p(u) = a_p$, $v_p(v) = -a_p$ para los que no se anulan y no negativo en el resto (tales números existen en virtud del lema 3.2). Se sigue que:

$$u\mathcal{O} \subseteq \chi(\prod_p p^{a_p}) \subseteq v^{-1}\mathcal{O}.$$

Por lo que la aplicación asi definida efectivamente va de D en F.

Para ver que son inversas la una de la otra usamos que:

$$U \subseteq \chi(\phi(U)), \text{ para } U \in F.$$

Y la igualdad se sigue del lema anterior.

Si tomamos ahora $a = \prod_p p^{a_p}$ y $U = \chi(a)$, se tiene por el lema 3.2 que existe $x \in U$ tal que $v_p(x) = a_p$ para todas las valoraciones (recordar que son casi todas nulas). Por lo tanto:

$$v_p(U) = a_p, \text{ para toda } p \in S.$$

Luego $\phi(U) = a$, es decir:

$$\phi(\chi(a)) = a.$$

Y se tiene que ambas son inversas.

La segunda parte es inmediata teniendo en cuenta que la inversión existirá siempre y se podrá hallar a través de las aplicaciones ϕ y χ. Por último, que se pueda tomar como base una familia de ideales enteros se deduce tomando $\chi(p) = \{x \in K | v_p(x) \geq 1, v_q(x) \geq 0 \text{ con } p \neq q \in S\}$ que es un ideal en $\mathcal{O}$. □

3.3. Dominios de Dedekind y equivalencia de definiciones.

Definición. Un dominio integral cuyos ideales fraccionarios forman junto al producto de ideales es un grupo se llamará Dominio de Dedekind.

Por el momento se ha visto que un anillo de enteros de un cuerpo que tiene un conjunto de valoraciones satisfaciendo la propiedad de aproximación fuerte es un dominio de Dedekind. Mostramos a continuación que no es un ejemplo sino una equivalencia, pero para ello debemos definir el concepto de anillo Noetheriano.

Definición. Un anillo A es Noetheriano si todo conjunto no vacio de ideales en A tiene un elemento maximal.

Lema 3.7. *Sea A anillo, es Noetheriano si y solo si todo ideal es finitamente generado.*

Demostración. Sea I un ideal que no es finitamente generado, entonces consideramos la familia de ideales:

$$(a_1) \subset (a_1,a_2) \subset \ldots (a_1,\ldots,a_n) \subset \ldots \text{ donde } a_i \in I \text{ para } i = 1,\ldots,n.$$

Existe por no ser I finitamente generado pero debe haber un elemento maximal, lo cual lleva a contradicción. Por lo tanto deben ser todos los ideales finitamente generados.

Sean ahora todos los ideales finitamente generados y supongamos que existe una familia de ellos en la que no existe elemento maximal. Necesariamente dado un ideal cualquiera de esa familia existirá otro que lo contendrá y reiterando obtendremos una cadena de ideales dentro de esa familia:

$$I_1 \subset \ldots \subset I_n \subset \ldots$$

Se tiene entonces que $\bigcup_{n\geq 1} I_n$ es un ideal que, por hipótesis, es finitamente generado: $\bigcup_{n\geq 1} I_n = (a_1,\ldots,a_n)$ y por ser la cadena ascendiente cada a_i estará en algún I_i, por lo que $I_n = (a_1,\ldots,a_n)$ y se llega a contradicción (la cadena no puede continuar). □

Teorema 3.3. *Sea $\mathcal{O}$ un dominio integral con cuerpo de fracciones K de manera que sus ideales fraccionarios forman un grupo junto al producto de ideales (es un dominio de Dedekind). Entonces $\mathcal{O}$ puede expresarse como la intersección de una familia de anillos de valoraciónes con la familia de valoraciones cumpliendo la propiedad de aproximación fuerte.*

Demostración. Veamos que $\mathcal{O}$ es Noetheriano:

Dado un ideal no nulo I de $\mathcal{O}$ se tiene que es invertible, luego $II^{-1} = \mathcal{O}$, por lo que:

$$1 = \sum_i a_i b_i \text{ donde } a_i \in I, b_i \in I^{-1}.$$

De lo que deducimos que cualquier elemento $x \in I$ puede escribirse como:

$$x = \sum_i a_i (b_i x),$$

Con $b_i x \in \mathcal{O}$, por lo que I está generado por $a_1,\ldots,a_n$.

Sean $P_1,\ldots$ los ideales maximales de $\mathcal{O}$, tenemos que si tomamos una familia finita de $a_i \geq 0$

$$\prod P_i^{a_i} \subseteq \mathcal{O},$$

Donde suponemos que $P^0 = \mathcal{O}$.

Llamemos F' a este grupo generado por el producto de ideales maximales con exponentes nulos salvo un conjunto finito y veamos que de hecho es el grupo de los ideales fraccionarios:

F' contiene a los ideales enteros ya que, si no fuera así, bastaría tomar un ideal maximal de ese conjunto (V) y se tendría que $V \subseteq P_i \subset \mathcal{O}$ para algún ideal P_i. Entonces, $V \subset VP_i^{-}1 \subseteq \mathcal{O}$ y por la maximalidad de V se tiene que $VP_i^{-1} \in F'$. Y por estar los productos con otros ideales: $V = VP_i^{-1}P_i^{-1} \in$

F que es una contradicción. F' contiene tambien a todos los ideales principales puesto que si $c = \frac{a}{b}$ se sigue que $a\mathcal{O}$, $b\mathcal{O} \in F'$ y por lo tanto $c\mathcal{O} = (a\mathcal{O})(b^{-1}\mathcal{O}) \in F'$.

Finalmente, F' contiene a los ideales fraccionarios ya que si V es un ideal fraccionario existirá u de manera que $uV = B \in \mathcal{O}$ es entero, luego $V = u^{-1}B = (u^{-1}\mathcal{O})B \in F'$.

Por lo tanto el grupo de ideales fraccionarios es libre y generado por los maximales. Con lo que cualquier elemento $a\mathcal{O} \in K^*$ puede se llevado al ideal principal asociado $a\mathcal{O}$ que admite una única representación:

$$a\mathcal{O} = \prod_P P^{a_P}$$

Se tiene entonces, que la función v_P que a cada $a \in K^*$ le asigna $v_P(a) = a_P$ es una valoración discreta añadiendo que $v_P(0) = \infty$: que toma valores discretos y que al producto le asigna la suma es directo. Que la suma sea mayor o igual que el mínimo de ambos proviene de que $a\mathcal{O}, b\mathcal{O} \subseteq a\mathcal{O} + b\mathcal{O}$.

Veamos ahora que este conjunto de valoraciones posee pla propiedad de aproximación fuerte:

-Ya hemos visto que las valoraciones son discretas.

-Dado $a \in K$, $a\mathcal{O} = \prod_P P^{a_P}$ donde casi todas las a_P son nulas, luego no negativas.

-Dados dos ideales maximales P y Q se tiene que $P + Q = \mathcal{O}$, luego para cualquier $N > 0$ $\mathcal{O} = (P+Q)^{2N} = \sum_i P^{2N-i}Q^i \subseteq P + Q$. Por lo tanto podemos descomponer $1 = p + q$ donde $p \in P^n$, $q \in Q^n$ por lo que:

$$v_P(a) \geq N,\ v_Q(1-a) \geq N \text{ y } v_T(a) = 0 \text{ para cualquier ideal maximal } P, Q \neq T.$$

□

Veamos que nuestra definición de dominio de Dedekind es equivalente a la usual, para ello definimos previamente el concepto de integralmente cerrado.

Definición. Dado un dominio integral A diremos que un elemento es integral sobre A si es solución de un polinomio mónico con coeficientes en A. Se dirá que A es integralmente cerrado si toda solución de un polinomio mónico con coeficientes en A pertenece a A.

Lema 3.8. *Dado A subanillo del cuerpo K se tiene que un elemento $c \in K$ es integral sobre A si y solo si existe un A-módulo no nulo finitamente generado M tal que $cM \subseteq M$.*

Demostración. Si el elemento es integral sobre A será solución de una ecuación $x^n + a_1x^{n-1} + \ldots + a_n = 0$ y se tendrá que el A-módulo generado por $1, c, \ldots, c^{n-1}$ cumple las condiciones.

Equivalentemente, si M es un A-módulo cumpliendo esas propiedades, pongamos que M esta generado por $a_1, \ldots, a_n$, se sigue que:

$$ca_i = \sum_j b_{i,j}a_j \text{ con los } b_{i,j} \in A.$$

Y como M es no nulo alguna a_i deberá no ser nula. Si llamamos B a la matriz cuyos elementos son $(b_{i,j})$ se tiene que:

$$det(cI - B) = 0$$

Y c será solución de la ecuación mónica anterior asociada (extendiendo el determinante). □

Teorema 3.4. *Sea $\mathcal{O}$ un dominio integral cuyo cuerpo de fracciones es K. Se tiene que es un dominio de Dedekind si y solo si cumple las siguientes tres propiedades:*

1. *$\mathcal{O}$ es Noetheriano.*
2. *$\mathcal{O}$ es integralmente cerrado en K.*
3. *Todo ideal primo no nulo de $\mathcal{O}$ es maximal.*

Demostración. Sea $\mathscr{O}$ un dominio de Dedekind, en la prueba del teorema anterior hemos visto que $\mathscr{O}$ es Noetheriano.

Como $\mathscr{O} = \cap A_p$, para ver que es integralmente cerrado bastará ver que todo número que sea solucíon de una ecuación mónica con coeficientes en $\mathscr{O}$ pertenece a todo anillo de valoración:

Sea $f \in K$ solución de la ecuación con coeficientes en $\mathscr{O}$:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0.$$

Sea $\pi \in \mathscr{O}$ tal que $v_p(\pi) = 1$ y $v_q \geq 0$ para el resto de valoraciones, se tiene que $f = \pi^r d$ donde $r \in \mathbb{Z}$ y $v_p(d) = 0$ y sustituyendo en la ecuación que cumple f vemos que d debe cumplir:

$$d^n + a_1 d^{n-1}\pi^{-r} + \ldots + a_n \pi^{-rn} = 0.$$

Y si $r < 0$ se llegaría a que $v_p(d) = \frac{v_p(d^n)}{n} \geq -r > 0$ que es una contradicción. Por lo tanto $f \in \cap A_p = \mathscr{O}$.

Como todo ideal fraccionario se puede poner como producto de los ideales maximales $\prod_P P^{a_P}$ observamos que un ideal de $\mathscr{O}$ admitirá una expresión con coeficientes no negativos (recordar que un ideal es un ideal fraccionario) y claramente será primo si y solo si es maximal.

Supongamos ahora que se cumplen las tres propiedades y veamos que es un dominio de Dedekind:

Sabemos que lo único que requiere el conjunto de ideales fraccionarios para ser grupo es tener inversa para todos sus elementos, puesto que el producto entre ideales fraccionarios es nuevamente ideal fraccionario y tenemos elemento neutro ($\mathscr{O}$). Veamos entonces que todos los elementos tienen inversa en tres pasos:

Los ideales de $\mathscr{O}$ contienen un producto de primos ideales puesto que sino fuese cierto, por ser Noetheriano, existiría un elemento maximal en ese conjunto M. Se tiene entonces que este ideal no puede ser primo por lo que existen $a, b \in \mathscr{O}$ tales que $a, b \notin M$ pero $ab \in M$. Por lo tanto:

$$M \subset M + b_i\mathscr{O}, \text{ para } i = 1, 2.$$

Y por la maximalidad de M deducimos que existen $p_1, \ldots, p_{n+m}$ tales que $p_1 \cdots p_n \subseteq M + b_1\mathscr{O}$ y $p_{n+1} \cdots p_{n+m} \subseteq M + b_2\mathscr{O}$. Por lo tanto:

$$p_1 \cdots p_{n+m} \subseteq (M + b_1\mathscr{O})(M + b_2\mathscr{O}) \subseteq M.$$

Lo que observamos es una contradicción con la definición de M.

Veamos ahora que los ideales maximales son invertibles:

Dado P un ideal maximal podemos tomar un elemento cualquiera $a \in P$ de manera que:

$$a\mathscr{O} \subseteq P,$$

Y sabemos que $a\mathscr{O}$ contendrá un producto finito de ideales primos que supondremos ya mínimo $P_1 \cdots P_r \subseteq a\mathscr{O} \subseteq P$. Por ser P maximal se tiene que es primo luego alguno de los $P_i \subseteq P$, supongamos sin perdida de generalidad que es el P_1. Por ser P_1 primo es también maximal por hipótesis de lo que deducimos $P = P_1$.

Hay ahora dos casos, si $r = 1$ ó $r > 1$:

Si $r = 1$ se tiene $P = P_1 \subseteq a\mathscr{O} \subseteq P$ por lo que $P = a\mathscr{O}$ es principal y tendrá como inverso $a^{-1}\mathscr{O}$.

Si $r > 1$ se tiene que, por minimalidad, $P_2 \cdots P_r \nsubseteq a\mathscr{O}$ y existe $b \in P_2 \cdots P_n$ tal que $b \notin a\mathscr{O}$. Por otro lado $bP \subseteq a\mathscr{O}$ de lo que deducimos que $a^{-1}b \in (\mathscr{O} : P)$ pero $a^{-1}b \notin \mathscr{O}$. Y se tiene que $(\mathscr{O} : P) \neq \mathscr{O}$. Se tiene la cadena de contenidos:

$$P \subseteq P(\mathscr{O} : P) \subseteq \mathscr{O},$$

Y P es maximal por lo tanto $P(\mathscr{O} : P)$ es ó P ó $\mathscr{O}$. Si fuese $P = P(\mathscr{O} : P)$ por el lema 3.8 se tendría que $(\mathscr{O} : P)$ es integral (recordar que por ser Noetheriano los ideales son finitamente generados y P será el $\mathscr{O}$-módulo de ese lema), pero por ser $\mathscr{O}$ integralmente cerrado necesariamente $(\mathscr{O} : P) \subseteq \mathscr{O}$ que no puede ser. Por lo tanto necesariamente $P(\mathscr{O} : P) = \mathscr{O}$ y se tiene que P es invertible.

Veamos que todo ideal entero es invertible:

Si no fuera así podriamos tomar un elemento maximal M de ese conjunto M y necesariamente estará contenido en algún elemento maximal P de $\mathscr{O}$, $M \subseteq P \subset \mathscr{O}$. Luego $M \subseteq MP^{-1} \subseteq \mathscr{O}$. Como todos los ideales son finitamente generados (por ser Noetheriano el anillo) se tiene que M es un $\mathscr{O}$-módulo. Por otro lado $\mathscr{O} \subset P^{-1}$ y se deduce por el lema 3,8 que $M \subset MP^{-1}$ (en caso contrario P^{-1} sería integral pero $\mathscr{O} \subset P^{-1} \subseteq \mathscr{O}$ es una contradicción). Por lo tanto $MP^{-1} \in \mathscr{O}$ más grande que M implica necesariamente que posee inverso C, luego $MP^{-1}C = \mathscr{O}$ y se tiene que CP^{-1} es inversa de M.

Para el caso de ideales fraccionarios basta tener en cuenta que si $a\mathscr{O} \subseteq U \subseteq b\mathscr{O}$, entonces $b^{-1}U \subseteq \mathscr{O}$ es un ideal entero que tiene inversa V, por lo tanto $b^{-1}V$ es la inversa del ideal fraccionario U. □

Por el momento no hemos visto realmente ningún dominio de Dedekind de manera explícita, para ver ejemplos y encuadrar los dominios de Dedekind en la jerarquía de estructuras damos el siguiente corolario:

Corolario 3.3. *Todo dominio de ideales principales es un dominio de Dedekind.*

Demostración. Los ideales serán generados por un único elemento, por lo que los ideales enteros serán invertibles y se sigue que también lo serán los ideales fraccionarios que construyamos sobre este dominio de ideales principales. □

De esta manera $\mathbb{Z}$ es un ejemplo de dominio de Dedekind.

Continuamos con una propiedad de interés sobre los dominios de Dedekind, la permanencia bajo extensión finita separable.

Definición. Dado K cuerpo diremos que el cuerpo L es una extensión separable algebraica de K si todo elemento de L tiene polinomio mínimo separable, es decir, si sus raices son distintas en su clausura algebraica.

Definición. Llamaremos clausura integral de un conjunto en una extensión suya al conjunto formado por todos los elementos integrales del conjunto inicial que pertenezcan a la extensión.

Requerimos el siguiente resultado que daremos sin demostración:

Lema 3.9. *Sea K cuerpo sobre el que existe una valoración v y L otro cuerpo que extiende a K y sobre el que esta definida la valoración w que extiende a v. Si L/K es finito se tiene que el ideal maximal asociado a la valoración se escinde en un número finito de ideales sobre la extensión y que la extensión de la valoración (w) será trivial o discreta si lo era v.*

Demostración. Teorema 1.1 pagina 44 de [1]. □

Teorema 3.5. *Sea $\mathscr{O}$ un dominio de Dedekind con cuerpo de fracciones K, sea L una extensión finita separable y sea $\mathscr{Q}$ la clausura integral de $\mathscr{O}$ en L. Entonces $\mathscr{Q}$ es de nuevo un dominio de Dedekind.*

Demostración. Por el teorema 3.3 podemos definir $\mathscr{O}$ a través de una familia de valoraciones con la propiedad de la aproximación fuerte, llamemos a esta familia S_K.

$$\mathscr{O} = \cap_{p \in S_K} A_p,$$

con la notación habitual.

Consideramos ahora el conjunto de todas las valoraciones que extienden a L alguna de S_k y lo denotamos por S_L. Veamos que $\mathscr{Q} = \cap_{p \in S_L} A_p$:

Dado $a \in \mathscr{Q}$, por ser este clausura integral de $\mathscr{O}$, podremos expresarlo como la solución de una ecuación mónica con términos en $\mathscr{O}$,

$$a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0.$$

Supongamos que existe un anillo de valoración de aquellas que extienden a las originales al cual a no pertenece. Entonce a^{-1} lo hará y se tendrá que:

$$a = -(\alpha_1 + \dots \alpha_n a^{1-n}),$$

y el término de la derecha pertenecería al anillo de valoración puesto que los términos α_i son elementos de $\mathscr{O}$ que pertenecen a los anillos de valoración previos a su extensión (es claro que si un elemento tiene valor no negativo es una valoración seguira teniéndolo en su extensión como aplicación) y se llega a contradicción.

Supongamos ahora que a es un elemento que pertenece a la intersección de todas las valoraciones extendidas y sea:

$$a^n + \alpha_1 a^{n-1} + \dots + \alpha_n = 0$$

la ecuación mínima sobre K, veamos que los α_i pertenecen a $\mathscr{O}$:

Primero vamos a ver que toda conjugación $\hat{a}$ de a (en la clausura normal de K) pertenece a su vez a la intersección de todas las valoraciones. Para ello, usamos el hecho de que dada una valoración $v_{p'}$ se tendrá que el valor que tome en $\hat{a}$ coincidirá con el que tome a en otra valoración v_p (demostración del teorema 3.4 de [1]), luego, por ser no negativa la a en cualquier valoración lo es a su vez cualquier conjugación.

De esta manera, tenemos que los α_i son los coeficientes resultantes del producto $\prod(x - a_i)$ por lo tanto son no negativos en cualquier valoración sobre $\mathscr{O}$ (puesto que son productos y sumas de elementos no negativos en cada valoración). Luego a está en $\mathscr{Q}$ por ser este la clausura integral de $\mathscr{O}$.

Por tanto tenemos que $\mathscr{Q}$ es intersección de los anillos de valoración de las extensiones. Veamos ahora que estas valoraciones cumplen la propiedad de aproximación fuerte.

Que sean principales se deriva directamente del lema anterior puesto que en S_K lo eran.

Sea ahora $a \in L$ cumpliendo la ecuación con coeficientes sobre K:

$$a^n + \alpha_1 a^{n-1} + \dots + \alpha_n = 0.$$

Cada α_i es negativa en un número finito de valoraciones de S_K y por el lema anterior se escinden cada una de ella en un número finito de valoraciones, por lo tanto deducimos que a será no negativa en casi todas las valoraciones de S_K.

Para ver que se cumple la tercera condición de la propiedad de aproximación fuerte tomamos dos valoraciones $q_1, q_2 \in S_L$, una base $u_1, \dots, u_n$ de la extensión L/K y sean $p_1, \dots, p_r \in S_k$ tales que: $v_q(u_i)$ para cualquier $q \in S_L$ que no extienda a p_j y sea distinto de q_1, q_2 con $j \neq i$ y q_1, q_2 extienden a alguna de las valoraciones.

Como la familia ya cumple las segunda propiedad se tiene que podemos exigirle estas condiciones: para la primera bastaría tomar la familia de valoraciones en S_L que son negativas sobre la base y tomar las $p \in S_K$ que extienden. La segunda se logra añadiendo a estas alguna que se extienda a q_1 y otra a q_2 ya que no rompen la primera condición.

Dada $N > 0$, por el teorema de aproximación, podemos tomar $B \in L$ tal que $v_{q_1}(B-1) > N$, $v_{q2}(B) > N$ y $v_q(B) \geq 0$ para las valoraciones que extienen a p_j fijo y que no coinciden con q_1 ni q_2. Expresando B en la base queda: $B = \sum_i y_i u_i$.

Dado $M > 0$, ya que S_k cumple la tercera condición de la propiedad de aproximación fuerte, se tiene que existen $x_i \in K$ tales que:

$$v_{p_j}(x_i - y_i) > M,\ v_p(x_i) \geq 0 \text{ para } p \text{ que no este en la familia, } i = 1, \dots, n \text{ y } j = 1, \dots, r.$$

Tomando ahora $\alpha = \sum_i x_i u_i$ llegamos a que:

$$v_q(\alpha - B) = v_q(\sum_i (x_i - y_i)u_i) \geq \mathit{mín}_i\{M + v_q(u_i)\}, \text{ para cualquier valoración que extienda a la familia.}$$

$$v_q(\alpha - B) = v_q(\sum_i (x_i - y_i)u_i) \geq 0, \text{ para cualquier valoración que no extienda a la familia.}$$

Basta tomar $M > N - v_q(u_i)$ para las valoraciones que extienden a las valoraciones iniciales y todos los elementos u_i de la base para llegar al resultado.

Por lo tanto la familia de valoraciones cumple la propiedad de aproximación fuerte y se tiene que es un dominio de Dedekind. □

Corolario 3.4. *Toda extensión integral separable de un dominio de ideales principales es un dominio de Dedekind.*

Demostración. Es inmediato de lo anterior y de que todo dominio de ideales principales es un dominio de Dedekind. □

De esta manera, llegamos finalmente a que toda extensión integral separable de $\mathbb{Q}$ será un dominio de Dedekind. Por lo que, aunque sea un trabajo más arduo, seremos capaces de establecer relaciones de divisibilidad sobre los ideales fraccionarios que pueden ser de utilidad en la busqueda de soluciones a ecuaciones.

Bibliografía

[1] P.M. COHN, *Algebraic numbers and algebraic functions*, Chapman & Hall mathematics.

[2] A. FRÖHLICH & M.J. TAYLOR, *Algebraic number theory* , Cambridge studies in advanced mathematics 27.

[3] PAULO RIBENBOIM, *The theory of classical valuations*, Springer monographs in mathematics.

[4] ATIYAH MACDONALD, *Introduction to commutative algebra*, Addison-Wesley.

[5] EDWIN WEISS, *Algebraic Number theory*, McGraw-Hill Book Company.

[6] HAROLD M. EDWARDS, *Divisor theory*, Birkhäuser.