FACULTAD DE MATEMÁTICAS

DEPARTAMENTO DE ÁLGEBRA

TRABAJO DE FIN DE GRADO:

INTRODUCCIÓN A LA TEORÍA DE VALORACIONES

Realizado por Ramón Piedra de la Cuadra

Supervisado por:
Miguel Ángel Olalla Acosta

Abstract

This paper makes an introduction to the theory of valuations on fields, we try to analyse the extension of valuations in transcendental extensions and the application on the irreducibility of polynomials showing the criterion of irreducibility of Eisenstein and noting that other many criteria of irreducibility of polynomials can be demonstrated through this theory.
In this work we have relied on the work already done by Michel VAQUIÉ in *Valuations* (August 17, 1998) [1] and by Saunders MacLane in *A construction for absolute values in polynomial rings* (1936) [2] .

Índice general

Índice general **5**

Introducción **7**

1. Anillos de valoración **11**

2. Valoraciones **15**

3. Altura de una valoración **21**

4. Prolongación de una valoración **29**
Centro de una valoración 31

5. Construcción de valoraciones en anillos de polinomios **33**
Introducción 33
Valoración de primera etapa 34
Valoraciones aumentadas 35
Propiedades de las valoraciones aumentadas 39
Valoraciones inductiva y límite 40
Completitud 46

6. Criterios de Irreducibilidad **49**

A. Grupos y anillos **53**

Bibliografía **57**

Introducción

Este trabajo consiste en una introducción a la teoría de valoraciones sobre cuerpos. Comenzamos por la definición y propiedades básicas de lo que entendemos por anillo de valoración V y valoración ν sobre un anillo A. Más adelante haremos la construcción de valoraciones en anillos de polinomios definiendo las valoraciones inductivas y límites, ayudándonos de unos polinomios especiales $\phi(x)$ que llamaremos polinomios claves. Y por último veremos que toda esta teoría se puede utilizar para demostrar criterios de irreducibilidad de polinomios, como el de Eisenstein, e incluso para generalizar estos criterios.
En el capítulo 1 trataremos los anillos de valoraciones, definiendo y demostrando su existencia. Al no ser una definición muy constructiva y que puede no entenderse bien, probaremos un resultado (Teorema 1.3) que caracteriza a los anillos de valoración de un cuerpo K. Finalmente para poder visualizar todo ello trabajaremos un ejemplo, el primero que se nos puede ocurrir que no sea trivial, como es el anillo de series formales que lo trataremos en el ejemplo 1.8.
En el capítulo 2 estudiaremos las valoraciones propiamente, denotando como Γ un grupo con una relación de orden total compatible con la suma (podemos pensar en un subgrupo de $\mathbb{Z}$), entonces definimos valoración como una aplicación ν de un anillo A en Γ que cumple las siguientes propiedades

- $\nu(x \cdot y) = \nu(x) + \nu(y) \quad \forall x, y \in A,$
- $\nu(x + y) \geq \text{ínf}(\nu(x), \nu(y)) \quad \forall x, y \in A,$
- $\nu(1) = 0$ y $\nu(0) = +\infty$

Observando que $\nu(-x) = \nu(x)$. También podemos ver que tienen una cierta relación estas tres condiciones con las propiedades de los grados de polinomios y que veremos a lo largo del trabajo y en especial en los ejemplos. En este mismo capítulo podremos prolongar la valoración ν sobre un anillo A

que sea dominio de integridad a su cuerpo de fracciones K y recíprocamente a partir de una valoración ν de K encontraremos su anillo de valoración.
En los dos siguientes capítulos (3 y 4) daremos algunas definiciones relacionadas con las valoraciones como segmento, rango o altura, ideales, prolongación y centro; dando propiedades de cada una de ellas.
El capítulo 5 finaliza toda la parte teórica y hace de introducción de la aplicación que veremos en el siguiente capítulo. En esta parte, supondremos que $\Gamma \subset \mathbb{R}$ y construiremos valoraciones en anillos de polinomios, definimos la extensión al cuerpo de fracciones de una valoración ν tal que $\nu(\frac{a}{b}) = \nu(a) - \nu(b)$ con b no nulo.
Partiendo de una valoración ν_0 sobre K queremos construir valoraciones de $K[x]$ que la prolonguen. Para ello primero tomamos lo que denominaremos valoración de primera etapa o ν_1, por un resultado (Teorema 5.6) veremos que determinar las valoraciones del anillo $K[x]$ a partir de las de K, es equivalente a determinar las del cuerpo $K(x)$. Y las construiremos por etapas. Para la primera tomaremos ν_0 valoración de K y $\mu \in \mathbb{R}$ y definiremos la valoración de primera etapa como

$$\nu_1(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0) = \text{mín}[\nu_0(a_n) + n\mu, \nu_0(a_{n-1}) + (n-1)\mu, \ldots, \nu_0(a_0)].$$

Para construir las siguientes etapas nos ayudaremos de los polinomios "clave" que los definiremos en el trabajo (definición 5.11). A este polinomio le asignaremos una nueva valoración $\nu(\phi) = \mu$ y para el resto de polinomios los escribiremos en forma de combinación de potencias de ϕ y la nueva valoración para el polinomio será el mínimo de $(W(f_i(x)) + i\mu)$ con i las potencias de ϕ en la expresión de f, donde W es la valoración de etapa anterior, $f_i(x)$ el coeficiente i-ésimo de f. Así podemos hacerlo repetidas veces, las valoraciones resultantes son lo que llamaremos valoraciones inductivas y si lo hicieramos una infinidad de veces valoración límite (cumpliendo una serie de condiciones). Finalmente llegaremos a que toda valoración de $K[x]$ se puede representar como valoración inductiva o límite (Teorema 5.25)
Por último, el capítulo 6 estudiamos algunos criterios de irreducibilidad de polinomios. Comenzamos por el criterio de Eisenstein demostrándolo a través de las valoraciones en vez del modo clásico. Para demostrarlo usamos la valoración p-ádica $\nu_0(p) = n$ con $n \in \mathbb{Z}$ y su valoración de primera etapa $\nu_1 = [\nu_0, \nu_1(x) = 1]$. Mencionaremos que de igual modo tomando otra valoración de primera etapa podremos demostrar el criterio de Schönemann, además de para muchos otros que mencionaremos. Como cúlmen del trabajo daremos el enunciado de un teorema que generaliza todos los criterios de irreducibilidad que mencionamos en el trabajo y dando un ejemplo aplicándolo sobre un polinomio para el que no se pueda usar el criterio de

Eisenstein pero que sí sea irreducible.
Para este trabajo nos hemos apoyado en los trabajos ya realizados por Michel Vaquié en *Valuations* (17 agosto 1998) [1] y en el realizado por Saunders MacLane en *A construction for absolute values in polynomial rings* [2](1936) y *The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals* [4] (1938).

Capítulo 1

Anillos de valoración

Antes de comenzar vamos a definir unos pequeños conceptos que nos van a servir a lo largo de todo el trabajo y a dar algunas notaciones.
Sean A y B dos anillos locales (definición A.14), cuyos ideales maximales (definición A.13) son respectivamente $max(A)$ y $max(B)$, decimos que B domina a A si $A \subset B$ y $max(A) = A \cap max(B)$.
Suponiendo la primera condición, la segunda es equivalente a que $max(A) \subset max(B)$.
La relación B domina a A es una relación de orden sobre el conjunto de anillos locales y lo notamos $A \preceq B$. Si tenemos la relación $A \preceq B$, entonces la inyección de A en B define un isomorfismo entre el cuerpo residual de A ($k(A) = A/max(A)$, véase apéndice definición A.17) y un subcuerpo del cuerpo residual de B. Con esto ya podemos dar la definición de anillo de valoración.

Definición 1.1 *Sea V un dominio de integridad (definición A.8) contenido en el cuerpo K, entonces V es un anillo de valoración de K si K es el cuerpo de fracciones de V y V es un elemento maximal del conjunto de subanillos locales de K ordenado por la relación de dominación, es decir, V es un anillo local y si W es un subanillo local de K que domina a V entonces $W = V$.*
Sea V un dominio de integridad, V es un anillo de valoración si V es un anillo de valoración de su cuerpo de fracciones.

Teorema 1.2 *(De Cohen-Seidenberg) Sean A y B dos anillos tales que $A \subset B$ y B entero sobre A (definición A.21) entonces para todo ideal primo $\mathcal{P}$ (definición A.12) de A existe un ideal primo $\mathcal{Q}$ de B tal que $\mathcal{P} = A \cap \mathcal{Q}$.*

Teorema 1.3 *Sea V un DDI (dominio de integridad) contenido en K, entonces las condiciones siguientes son equivalentes:*

1. *V es un anillo de valoración de K.*

2. *Sea x un elemento de K, si $x \notin V \Longrightarrow x^{-1} \in V$.*

3. *K es el cuerpo de fracciones de V y el conjunto de ideales de V está totalmente ordenado por la relación de inclusión.*

Demostración:
1. $\Rightarrow$ 2.: Sea $x \in K$ distinto de 0, demostraremos que x o x^{-1} pertenecen a V.
-Si x es entero sobre V, tomamos el anillo $W = V[x]$. Por el Teorema de Cohen-Seidenberg, existe un ideal primo $\mathcal{Q}$ de W tal que $max(V) = V \cap \mathcal{Q}$. Por tanto, el anillo local $W_{\mathcal{Q}}$ domina a V, de donde $W \subset W_{\mathcal{Q}} = V$ y $x \in V$
-Si x no es entero sobre V, tomamos el anillo $W = V[x^{-1}]$.
Como x no es entero sobre V, x^{-1} no es una unidad de W. En efecto, toda relación de la forma $x^{-1}w = 1$, $w \in W = V[x^{-1}]$, i.e., $w = \sum a_j x^{-j}$, dando una relación de dependencia íntegra de x sobre V. Por tanto, existe un ideal maximal $\mathcal{Q}$ de W conteniendo a x^{-1}, sea V' el localizado (definición A.16) $V' = W_{\mathcal{Q}}$. Como $x^{-1} \in \mathcal{Q}$, el morfismo compuesto $V \to W = V[x^{-1}] \to k = W/\mathcal{Q}$ es sobreyectivo y su núcleo $V \cap \mathcal{Q}$ es el ideal maximal de V. Deducimos que V' es un subanillo de K que domina a V, luego $V' = V$ y $x^{-1} \in V$.
2. $\Rightarrow$ 3.: Sean $\mathcal{I}$ y $\mathcal{J}$ dos ideales de V y supongamos que $\mathcal{J}$ no está incluído en $\mathcal{I}$.
Entonces existe un elemento x de $\mathcal{J}$ tal que $x \notin \mathcal{I}$ y $\forall y \in \mathcal{I}$, $y \neq 0$, tenemos $x \notin (y)V$; en consecuencia x/y es un elemento de K que no pertenece a V y se deduce que $y/x \in V$ ($y \in (x)V$ de donde $y \in \mathcal{J}$).
Luego $\mathcal{I} \subset \mathcal{J}$ y K es el cuerpo de fracciones de V.
3. $\Rightarrow$ 1.: Como el conjunto de ideales de V está totalmente ordenado por la inclusión, V posee un solo ideal maximal $max(V)$.
Sea W un subanillo local de K que domina a V y sea $x \in W$, vamos a demostrar que también $x \in V$. Podemos escribir $x = a/b$ con $a \in V$, $b \in V$.
Si $(a)V \subset (b)V$ entonces $x \in V$.
Si $(b)V \subset (a)V$ entonces $x^{-1} \in V$.
Deducimos que x y x^{-1} pertenecen a W de donde $x^{-1} \notin max(W)$ y $x^{-1} \notin max(V)$ puesto que W domina a V. El elemento x^{-1} de K verifica entonces que $x^{-1} \in V$ y $x^{-1} \notin max(V)$, en consecuencia como V es local, $x \in V$.
Luego V es un anillo de valoración de K. $\square$

Observación 1.4 *En 1. $\Rightarrow$ 2. hemos demostrado que todo anillo de valoración es integramente cerrado (definición A.21).*
También podemos reemplazar la propiedad 3. por una equivalente:

3'. K es el cuerpo de fracciones de V y el conjunto de ideales principales de V está totalmente ordenado por la relación de inclusión (en particular, todo ideal finitamente generado de V es un ideal principal).

Vamos a ver ahora la existencia de los anillos de valoración.

Proposición 1.5 *Sea A un subanillo de un cuerpo K y sea $h : A \to L$ morfismo con L un cuerpo algebraicamente cerrado entonces existe un anillo de valoración V de K y un morfismo h' de V en L tal que V contiene a A, h' prolonga a h y $max(V) = h'^{-1}(0)$.*

Demostración:
Consideremos el conjunto $\mathcal{H}$ formado por (B, f) donde B es un subanillo de K que contiene a A y f es un morfismo de B en L que prolonga a h. El conjunto $\mathcal{H}$ es no vacío porque contiene a (A, h).
Definimos sobre $\mathcal{H}$ la relación de orden $(B, f) \preceq (C, g)$ por $B \subset C$ y g prolonga a f.
El conjunto $\mathcal{H}$ dotado de esta relación de orden es un conjunto inductivo, i.e. todo subconjunto totalmente ordenado admite una cota superior (si tenemos el subconjunto $\{(B_\alpha, f_\alpha)\}$, basta tomar como cota superior a (B, f) donde $B = \bigcup B_\alpha$ y f está definido por las restricciones de f_α).
Por el lema de Zorn (lema A.23) deducimos que $\mathcal{H}$ admite un elemento maximal (W, g).
Si llamamos $\mathcal{P}$ al núcleo del morfismo $g : W \to L$, el anillo V buscado es el localizado $V = W_{\mathcal{P}}$. □

Corolario 1.6 *Todo subanillo local A de un cuerpo K está dominado por al menos un anillo de valoración de K.*

Demostración:
Es suficiente aplicar la proposición anterior a $h : A \to L$, donde L es una clausura algebraica del cuerpo residual $A/max(A)$. □

Observación 1.7 *La mayoría de las veces empezaremos con un cuerpo base k y consideraremos únicamente los cuerpos K que son extensiones de k y los subanillos A que son k-álgebras. Y encontramos el resultado de existencia como antes:*
Sea A una sub k-álgebra de K y sea h un k-morfismo de A en un cuerpo algebraicamente cerrado L, existen un anillo de valoración V de K que es una k-álgebra y un k-morfismo h' de V en L tales que V contiene a A, h' prolonga a h y $max(V) = h'^{-1}(0)$.

Ejemplo 1.8 *Sea $V = \mathbb{C}[[x]]$ el anillo de series formales en una variable x con coeficientes complejos. Es un anillo local, con ideal maximal (x). De hecho, todas las series formales $f(x) = a_0 + a_1x + a_2x^2 + \ldots$ con $a_0 \neq 0$ son unidades. En efecto, sea $f(x) = a_0 + a_1x + a_2x^2 + \ldots$ con $a_0 \neq 0$, entonces puedo encontrar un $g(x) \in \mathbb{C}[[x]]$ tal que $f(x)g(x) = 1$ comparando grados a izquierda y derecha, sea $g(x) = b_0 + b_1x + b_2x^2 + \ldots$, entonces*

$$\begin{aligned} a_0b_0 &= 1 && \textit{(grado 0)} \\ a_0b_1 + a_1b_0 &= 0 && \textit{(grado 1)} \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 && \textit{(grado 2)} \\ &\vdots \end{aligned}$$

Despejando los b_i por cada grado (se puede hacer porque conocemos los a_i y hemos calculado para un b_j fijo todos los anteriores y además $a_0 \neq 0$), así por inducción probaríamos que existen esos b_i y por tanto $g(x)$.
Por tanto, cualquier serie con término independiente no nulo es una unidad y (x) es el ideal maximal.
Además, también observamos que V es un anillo de ideales principales, cualquier ideal I es de la forma $I = (x^n)$, para cierto $n \in \mathbb{N}$. En efecto, sea $I = (f(x))$ suponemos que $f(x)$ no es unidad porque sino $I = V = (1)$, luego $f(x)$ no tiene término independiente, sacamos factor común la mayor potencia de x, y tendremos

$$f(x) = x^n[a_0 + a_1x + a_2x^2 + \ldots] \qquad a_0 \neq 0,$$

es decir, $f(x) = ux^n$ con u unidad pues tiene término independiente no nulo. Por tanto $I = (f(x)) = (x^n)$. Ahora si $I = (f_1(x), f_2(x), \ldots, f_s(x))$, hacemos lo mismo para cada f_i y tenemos que $I = (x^{n_1}, x^{n_2}, \ldots, x^{n_s})$, tomamos $n = \min\{n_1, n_2, \ldots, n_s\}$ entonces $I = (x^n)$. Una adaptación simple del Teorema de la Base de Hilbert (A.24) permite probar que $\mathbb{C}[[x]]$ es un anillo noetheriano (A.22). Luego V es anillo de ideales principales.
Su cuerpo de fracciones $K = \mathbb{C}((x))$, está formado por los cocientes de series $f(x)/g(x)$, con $g(x) \neq 0$. Podemos suponer que $g(x)$ es un simple monomio x^n, $n \in \mathbb{N}$, por el argumento utilizado con los ideales principales.
Por la propiedad 3 del Teorema 1.3, V es un anillo de valoración, pues el conjunto de ideales de V está totalmente ordenado por la relación de inclusión.

Capítulo 2

Valoraciones

A partir de ahora Γ es un grupo conmutativo totalmente ordenado, es decir, grupo con una relación de orden total compatible con la suma ($a > b, c > d \Rightarrow a + c > b + d$), en particular Γ es un grupo sin torsión.
Escribimos $\Gamma^+ = \{x \in \Gamma : x \geq 0\}$ se tiene que:

$$\Gamma = \Gamma^+ \cup \Gamma^-, \ \ \Gamma^+ \cap \Gamma^- = \{0\} \ \ y \ \ \alpha \geq \beta \Longleftrightarrow \alpha - \beta \in \Gamma^+.$$

Adjuntamos al grupo Γ un elemento $+\infty$ y llamamos Γ_∞ al conjunto obtenido. A este conjunto le dotamos de una relación de orden imponiendo que para todo α en Γ, $\alpha < +\infty$, $(+\infty) + \alpha = (+\infty)$ y $(+\infty) + (+\infty) = (+\infty)$.

Definición 2.1 *Sea A un anillo, llamamos valoración de A con valores en Γ a una aplicación ν: $A \longrightarrow \Gamma_\infty$ verificando las siguientes condiciones:*

1. $\nu(x \cdot y) = \nu(x) + \nu(y) \quad \forall x, y \in A,$
2. $\nu(x + y) \geq \text{ínf}\{\nu(x), \nu(y)\} \quad \forall x, y \in A,$
3. $\nu(1) = 0$ *y* $\nu(0) = +\infty.$

Observación 2.2 *Suponiendo que ν verifica 1. y 2. y no toma únicamente el valor $+\infty$ entonces tenemos que $\nu(1) = 0$. En general, si tenemos un elemento z en A tal que $z^n = 1$ con $n \in \mathbb{N}^*$, tenemos que $\nu(z) = 0$ ya que Γ no tiene torsión. En particular $\nu(-1) = 0$ y también $\nu(-x) = \nu(x)$.*

Definición 2.3 *La única valoración ν de A que verifica que $\nu(x) = 0$ para todo x en A^* se llama valoración impropia de A.*

Proposición 2.4 *Sea ν una valoración de un anillo A, para toda familia finita $\{x_1, \ldots, x_n\}$ de elementos de A tenemos la desigualdad siguiente:*

$$\nu\left(\sum_{i=1}^{n} x_i\right) \geq \inf_{1\leq i\leq n}\{\nu(x_i)\},$$

Es más, si existe un índice j tal que para todo $i \neq j$ tenemos la desigualdad estricta $\nu(x_i) > \nu(x_j)$, entonces tenemos la igualdad:

$$\nu\left(\sum_{i=1}^{n} x_i\right) = \inf_{1\leq i\leq n}\{\nu(x_i)\} = \nu(x_j).$$

Demostración:
La primera parte de la proposición se demuestra por inducción en n utilizando la condición 2. de la Definición 2.1 de valoración. Para la segunda parte basta probarlo para $n = 2$ y si x e y son dos elementos tales que $\nu(x) < \nu(y)$ deducimos del axioma 2. que $\nu(x+y) \geq \nu(x)$ y $\nu(x) \geq \text{ínf}\{\nu(x+y), \nu(-y)\}$ y como $\nu(y) = \nu(-y) > \nu(x)$ tenemos la igualdad que buscábamos. □

Observación 2.5 *Si ν es una valoración de A con valores en Γ y si $f : B \to A$ es un morfismo de anillos, la composición $\nu \circ f : B \to \Gamma_\infty$ define una valoración de B con valores en Γ.*

Observación 2.6 *Para toda valoración ν de un anillo A con valores en Γ, la imagen recíproca $\nu^{-1}(+\infty)$ es un ideal primo $\mathcal{P}$ de A. La aplicación $\bar{\nu} : A/\mathcal{P} \to \Gamma_\infty$ deducida de ν por paso al cociente define una valoración del dominio de integridad $A/\mathcal{P}$ tal que la imagen recíproca de $+\infty$ se reduce al 0.*

Proposición 2.7 *Sea A un dominio de integridad con cuerpo de fracciones K y una valoración ν de A con valores en Γ, tal que para todo $x \neq 0$ tenemos $\nu(x) \neq +\infty$. Entonces existe una única valoración μ de K que prolonga a ν. Además $\mu(K^*)$ es el subgrupo de Γ generado por $\nu(A^*)$.*

Demostración:
Para todo x en K^* existen y y z pertenecientes a A^* tales que $x = y/z$, basta entonces poner que $\mu(x) = \nu(y) - \nu(z)$.
Se verifica fácilmente que $\mu(x)$ no depende de los elementos y y z tomados y que la aplicación μ así definida es una valoración de K que prolonga a ν y es única.

Por construcción está claro que $\mu(K^*)$ es el subgrupo de Γ generado por el semigrupo $\nu(A^*)$. $\square$
Veamos ahora la relación que existe entre las valoraciones de un cuerpo K y los anillos de valoración de dicho cuerpo.

Proposición 2.8 *Sea ν una valoración del cuerpo K con valores en el grupo Γ. Entonces el conjunto A de elementos x de K que verifiquen $\nu(x) \geq 0$ es un anillo de valoración de K, cuyo ideal maximal $max(A)$ es el conjunto de sus elementos positivos x que verifican $\nu(x) > 0$. Recíprocamente, si V es un anillo de valoración de K podemos asociarle una valoración ν de K con valores en un grupo Γ_V tal que el anillo V sea la imagen recíproca $\nu^{-1}(\Gamma_V^+)$.*

Demostración:
Deducimos de los axiomas de una valoración que el conjunto A de elementos x de K que verifican $\nu(x) \geq 0$ es un subanillo de K y deducimos de la parte 2. del Teorema 1.3 que es un anillo de valoración de K.
Es más, como A es local, un elemento x de K es tal que $\nu(x) = 0$ si y sólo si x y x^{-1} pertenecen a A, es decir x pertenece a $A \setminus max(A)$.
Para el recíproco, más generalmente consideramos C un DDI de cuerpo de fracciones K; el conjunto $U(C)$ de unidades de C es un subgrupo multiplicativo K^* y notamos como $\Gamma_C = K^*/U(C)$ el grupo cociente. La relación de divisibilidad en C : $x|y \iff y \in (x)C$, define una estructura de grupo ordenado sobre Γ_C. Más precisamente, si denotamos respectivamente $\bar{x}$ y $\bar{y}$ las clases de x e y de K^* en el grupo cociente Γ_C, entonces la relación esta definida por $\bar{x} \leq \bar{y} \iff \exists z \in C$ tal que $y = zx$.
La relación $\leq$ está bien definida sobre el espacio cociente ya que no depende de los representantes elegidos.
Esta relación es de orden sobre el grupo Γ_C, compatible con la estructura de grupo y que corresponde a la relación de orden definida por la inclusión sobre el conjunto de ideales principales del anillo C.
Deducimos de la Observación 1.4 que el grupo Γ_C está totalmente ordenado si y sólo si C es un anillo de valoración de K. Como C es un anillo local tenemos la siguiente igualdad

$$U(C) = C \setminus max(C).$$

La aplicación canónica $\nu : K^* \to \Gamma_C = K^*/U(C)$ es entonces una valoración de K tal que el anillo C es igual al anillo de valoración asociado $\{x \in K | \nu(x) \geq 0\}$. $\square$

Definición 2.9 *El anillo de valoración V de K asociado a la valoración ν se llama anillo de la valoración ν y el cuerpo $k(V) = V/max(V)$ es llamado el cuerpo residual de la valoración.*
El subgrupo $\nu(K^*)$ de Γ se llama grupo de órdenes o grupo de valores de ν. Deducimos de esto que es isomorfo al grupo cociente $\Gamma_V = K^*/U(V)$.

Para toda valoración ν de un cuerpo K, denotaremos R_ν su anillo de valoración, k_ν su cuerpo residual y Γ_ν su grupo de valores.

Definición 2.10 *Decimos que dos valores ν y ν' de K son equivalentes si tienen el mismo anillo.*

Proposición 2.11 *Dos valoraciones ν y ν' de un cuerpo K son equivalentes si y sólo si existe un isomorfismo de grupos ordenados λ de $\nu(K^*)$ en $\nu'(K^*)$ tal que $\nu' = \lambda \circ \nu$.*

Demostración:
Basta darse cuenta de que por definición la valoración determina el anillo V y recíprocamente el anillo V de la valoración determina el grupo de valores $\Gamma = K^*/U(V)$, así como el subconjunto de elementos "positivos" $\Gamma^+ = V^*/U(V)$. $\square$

Ejemplo 2.12 *Completando el Ejemplo 1.8 del capítulo anterior con el anillo de valoración $V = \mathbb{C}[[x]] \subset K = \mathbb{C}((x))$, aquí la valoración ν está definida en V como el orden de las series formales:*
$\nu(a_0x^n + a_1x^{n+k_1} + a_2x^{n+k_2} + \ldots) = n$ con $a_0 \neq 0$ y $0 < k_1 < k_2, \ldots$ enteros.
Y en K: $\nu(f/g) = \nu(f) - \nu(g)$. El cuerpo residual es $\mathbb{C}$ y $\Gamma = \mathbb{Z}$.

Ejemplo 2.13 *Sea A un dominio de ideales principales y $p \in A$ un elemento irreducible. Entonces*

$$A_p = \left\{ \frac{a}{b}, b \text{ no es múltiplo de } p \right\},$$

es un anillo local, de ideal maximal

$$M_p = \left\{ \frac{a}{b}, b \text{ no es múltiplo de } p \text{ y } a \text{ es múltiplo de } p \right\} \subset A_p,$$

pues para todo $\frac{a}{b} \in A_p$ tal que a no sea múltiplo de p tiene inverso $\frac{b}{a} \in A_p$, por lo tanto es unidad.

Es claro que M_p es el ideal principal generado por $\frac{p}{1}$.
Se tiene la cadena de ideales:

$$A_p \supsetneq M_p = \left(\frac{p}{1}\right) \supsetneq M_p^2 = \left(\frac{p}{1}\right)^2 \supsetneq \dots \qquad con \bigcap_{\forall n \geq 0} M_p^n = \{0\}.$$

Definimos la valoración p-ádica ν_p en K= cuerpo de fracciones de A, como sigue:
Si $a \in A \setminus \{0\}$, $\nu_p(a) = n$ si $a \in M_p^n \setminus M_p^{n+1}$, $\nu(0) = +\infty$ y si $\frac{a}{b} \in K$, $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.
El anillo de valoración de ν_p es el conjunto de elementos con valores positivos o no nulos de K, es R_p, ya que si

$$\forall \frac{a}{b} \in K, \nu_p\left(\frac{a}{b}\right) \geq 0 \Longrightarrow \nu_p(a) = r \geq \nu_p(b) = s, \quad con \ p^r \mid a, p^s \mid b$$

$$a = p^r a', \ \ b = p^s b', \quad con \ p \nmid a', p \nmid b' \Longrightarrow \frac{a}{b} = \frac{p^r a'}{p^s b'} = \frac{p^{r-s} a'}{b'} \in A_p.$$

Y podemos comprobar que ν_p es un valoración.
En el caso más simple, $A = \mathbb{Z}$, p=número primo, si $a \in \mathbb{Z}$, $\nu_p(a)$ = máxima potencia de p que divide a a.
Si $\frac{a}{b} \in \mathbb{Q}$, $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.
Más generalmente, si la valoración anterior $\nu_p : \mathbb{Q} \to \mathbb{Z}$, la componemos con la multiplicación por m (para cualquier entero $m \neq 0$) $\mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z}$, se puede obtener otra valoración p-ádica tal que $\nu_p(p) = m$, que también es valoración equivalente.

Capítulo 3

Altura de una valoración

Veamos ahora algunas definiciones y propiedades de las valoraciones.

Definición 3.1 *Sea Γ un grupo aditivo totalmente ordenado, un subconjunto Δ de Γ se llama segmento si para todo elemento $\alpha \in \Delta$ y $\beta \in \Gamma$ tal que $-\alpha \leq \beta \leq \alpha$ o bien $\alpha \leq \beta \leq -\alpha$, entonces $\beta \in \Delta$.*
Un subgrupo Γ' de Γ se dice aislado si Γ' es a la vez subgrupo propio de Γ y un segmento.
Un homomorfismo entre grupos ordenados $\Phi : \Gamma \to \Delta$ se dice homomorfismo creciente si $a, b \in \Gamma, a \geq b \Longrightarrow \Phi(a) \geq \Phi(b)$.

Proposición 3.2 *El núcleo de un homomorfismo creciente de Γ en un grupo ordenado es un subgrupo aislado de Γ.*
Recíprocamente si Γ' es un subgrupo aislado de Γ, el grupo cociente Γ/Γ' posee una estructura natural de grupo ordenado tal que $\Gamma \to \Gamma/\Gamma'$ es un homomorfismo creciente.

Demostración:
Sea $\Phi : \Gamma \to \Delta$ homomorfismo creciente.
Sea $\alpha \in \ker(\Phi)$ y $\beta \in \Gamma$ tal que $-\alpha \leq \beta \leq \alpha$.
Como $\Phi(\alpha) = \Phi(-\alpha) = 0$ por ser Φ homomorfismo y α estar en su núcleo, entonces por la desigualdad anterior $\beta \in Ker(\Phi)$.
Por tanto el núcleo del homomorfismo es un subgrupo aislado.
Sea ahora $\Gamma' \subset \Gamma$ un subgrupo aislado.
En Γ/Γ' definimos el orden inducido por el de Γ: $\alpha + \Gamma' \geq \beta + \Gamma' \Leftrightarrow \alpha \geq \beta$.
Veamos que el orden está bien definido, es decir, que no depende de la elección del representante en cada clase.
Sean $\alpha + \Gamma'$, $\beta + \Gamma'$ dos elementos de Γ/Γ' distintos. Supongamos que $\alpha > \beta$,

entonces:

$$\alpha + \gamma_1 > \beta + \gamma_2 \qquad \forall \gamma_1, \gamma_2 \in \Gamma'.$$

En efecto, por R.A. supongamos que no, sean $\gamma_1, \gamma_2 \in \Gamma'$ tales que

$$\alpha + \gamma_1 \leq \beta + \gamma_2 \to \alpha - \beta \leq \gamma_2 - \gamma_1.$$

Además, $\alpha > \beta \to \alpha - \beta > 0$.
Luego $-(\gamma_2 - \gamma_1) < 0 < \alpha - \beta \leq \gamma_2 - \gamma_1$. Como $\gamma_2 - \gamma_1, \gamma_1 - \gamma_2 \in \Gamma'$ y Γ' es un subgrupo aislado, entonces $\alpha - \beta \in \Gamma'$. Lo que implica que $\alpha + \Gamma' = \beta + \Gamma'$.
Esto es contradicción, pues hemos tomado $\alpha + \Gamma' \neq \beta + \Gamma'$.
Por tanto Γ/Γ' es un grupo ordenado. Por la construcción del orden se deduce que $\Gamma \to \Gamma/\Gamma'$ es un homomorfismo creciente. $\square$

Consideremos una valoración ν de un cuerpo K con valores en el grupo Γ, con Γ igual al grupo de órdenes, i.e. suponemos que ν es sobreyectiva, y sea V el anillo de la valoración ν.
Para todo subconjunto A de V que contenga el 0 definimos el subconjunto Δ_A de Γ como el complementario en Γ_∞ de $(\nu(A)) \cup (-\nu(A))$.

Teorema 3.3 *Si $\mathcal{I}$ es un ideal propio de V, el subconjunto $\Delta_\mathcal{I}$ es un segmento de Γ. La aplicación $\mathcal{I} \longmapsto \Delta_\mathcal{I}$ es una biyección del conjunto de ideales de V sobre el conjunto de segmentos de Γ, y tenemos la siguiente equivalencia:*
$\mathcal{I} \subset \mathcal{J} \Leftrightarrow \Delta_\mathcal{J} \subset \Delta_\mathcal{I}$.
El segmento $\Delta_\mathcal{I}$ es un subgrupo aislado de Γ si y sólo si $\mathcal{I}$ es un ideal primo de V.

Demostración:
Sea $b \in \Gamma^+$ que no pertenezca al subconjunto $\Delta_\mathcal{I}$, basta demostrar que para todo a en Γ se tiene que : $a \geq b \implies a \notin \Delta_\mathcal{I}$ (Por la definición (3.1) de segmento).
Por la hipótesis sobre b existe un elemento x del ideal $\mathcal{I}$ tal que $b = \nu(x)$, como la aplicación ν es sobreyectiva se deduce de $a \geq b$ que existe un elemento y del anillo V tal que $a - b = \nu(y)$.
Entonces xy pertenece al ideal $\mathcal{I}$ de V y $a = \nu(xy)$ no pertenece a $\Delta_\mathcal{I}$.
Recíprocamente si Δ es un segmento de Γ, hay que demostrar que el subconjunto $\{x \in V | \nu(x) \notin \Delta\}$ es un ideal de V:

$$\begin{aligned} x \in \mathcal{I}, y \in V &\Rightarrow \nu(x) \notin \Delta, \nu(x), \nu(y) \geq 0 \\ &\Rightarrow \nu(x) + \nu(y) \notin \Delta \\ &\Rightarrow xy \in \mathcal{I}, \end{aligned}$$

$$\begin{aligned} x, y \in \mathcal{I} &\Rightarrow \nu(x), \nu(y) \notin \Delta \\ &\Rightarrow \nu(x+y) \geq \text{ínf}\{\nu(x), \nu(y)\} \\ &\Rightarrow \nu(x+y) \notin \Delta \\ &\Rightarrow x+y \in \mathcal{I}. \end{aligned}$$

La relación $\mathcal{I} \subset \mathcal{J} \Leftrightarrow \Delta_{\mathcal{J}} \subset \Delta_{\mathcal{I}}$ es evidente. De donde se obtiene la biyección, pues el conjunto de los ideales de V y el conjunto de segmentos de Γ están totalmente ordenados por la inclusión.
El ideal $\mathcal{I}$ de V es un ideal primo si y sólo si el complementario $V \setminus \mathcal{I}$ es estable para la multiplicación, es decir, si y sólo si su imagen $\nu(V \setminus \mathcal{I})$ es estable para la suma lo cual es equivalente a decir que $\Delta_{\mathcal{I}}$ es subgrupo de Γ. □

Definición 3.4 *El rango de un grupo totalmente ordenado Γ, notado rango(Γ), es igual al número de sus subgrupos aislados, si es finito, y es infinito, si no. La altura o rango de la valoración ν de un cuerpo K es el rango del grupo de valores Γ y lo notamos altura(ν) o rango(ν).*

Observación 3.5 *En vez de considerar los segmentos del grupo Γ, se pueden considerar los subconjuntos mayores M, es decir, los subconjuntos M de Γ que verifican: $x \in M$ e $y \geq x \Rightarrow y \in M$.*
Se obtiene una biyección creciente entre el conjunto de subconjuntos mayores M de Γ y conjunto de sub V-módulos $\mathcal{M}$ de K, biyección definida por $M \longmapsto \mathcal{M} = \{x \in K | \nu(x) \in M \cup \{+\infty\}\}$.

Definición 3.6 *Para todo elemento α del grupo $\Gamma = \Gamma_\nu$, podemos definir los ideales $\mathcal{P}_\alpha(R_\nu)$ y $\mathcal{P}_{\alpha+}(R_\nu)$ del anillo de valoración $V = R_\nu$ por*

$$\mathcal{P}_\alpha(R_\nu) = \{x \in R_\nu | \nu(x) \geq \alpha\}$$

$$\mathcal{P}_{\alpha+}(R_\nu) = \{x \in R_\nu | \nu(x) > \alpha\}.$$

Corolario 3.7 *La altura de una valoración ν es igual a la dimensión del anillo de valoración V asociado a ν.*

Demostración:
En efecto la altura de la valoración ν es igual al número de subgrupos aislados de Γ, luego al número de ideales primos propios de V.
Como el conjunto de estos ideales está totalmente ordenado por la inclusión, este número si es finito, es la dimensión del anillo V. □

Proposición 3.8 *Sean K un cuerpo y V un anillo de valoración de K.*

a) Todo anillo local R verificando $V \subset R \subset K$ es un anillo de valoración de K. El ideal maximal $max(R)$ de R está contenido en el anillo V y es un ideal primo de V.

b) La aplicación $\mathcal{P} \to V_{\mathcal{P}}$ es una biyección decreciente del conjunto de ideales primos $\mathcal{P}$ de V en el conjunto de anillos locales R tales que $V \subset R \subset K$. La biyección recíproca está definida por $R \to max(R)$.

Demostración:
De la condición 2 del Teorema 1.3 deducimos que el anillo R es un anillo de valoración y que su ideal maximal $max(R)$ está incluido en V (si $x \in max(R) \Rightarrow x^{-1} \notin R \Rightarrow x^{-1} \notin V \Rightarrow x \in V$). Como $max(R)$ es un ideal primo de R, es también un ideal primo de V.
Para todo ideal primo $\mathcal{P}$ del anillo V, el anillo localizado $V_{\mathcal{P}}$ verifica que $V \subset V_{\mathcal{P}} \subset K$, y la aplicación $\mathcal{P} \to V_{\mathcal{P}}$ es estrictamente decreciente. Además se verifica que el ideal maximal $\mathcal{P}V_{\mathcal{P}}$ del localizado es igual al ideal primo $\mathcal{P}$ de V. $\square$

Así vemos que el estudio de ideales primos $\mathcal{P}$ de V, es decir, el estudio de los subgrupos aislados del grupo de valores Γ, nos lleva al estudio de los anillos R verificando $V \subset R \subset K$.

Notación 3.9 *Sea V el anillo de valoración asociado a una valoración ν de K de grupo de valores Γ, y supongamos que ν es de rango finito r.*
Notamos $\mathcal{P}_i$,V_i y Δ_i, $0 \leq i \leq r$, respectivamente a los ideales primos de V, a los subanillos de K que contienen a V y a los subgrupos aislados de Γ, con las relaciones: $\mathcal{P}_i = max(V_i)$ y $V_i = V_{\mathcal{P}_i}$; $\Delta_i = \Delta_{\mathcal{P}_i}$, es decir, el complementario de $(\nu(\mathcal{P}_i)) \cup (-\nu(\mathcal{P}_i))$ en Γ.
Notamos por Γ_i al grupo cociente Γ/Δ_i, que es un grupo totalmente ordenado.

Tenemos entonces las siguientes inclusiones:

$$(0) = \mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_{r-1} \subset \mathcal{P}_r = max(V)$$

$$V = V_r \subset V_{r-1} \subset \ldots \subset V_1 \subset V_0 = K$$

$$(0) = \Delta_r \subset \Delta_{r-1} \subset \ldots \subset \Delta_1 \subset \Delta_0 = \Gamma.$$

El grupo de valores de la valoración ν_i asociado al anillo de valoración $V_i = V_{\mathcal{P}_i}$ es entonces el grupo cociente $\Gamma_i = \Gamma/\Delta_i$ y la aplicación $\nu_i : K^* \to \Gamma_i$ es la composición de la aplicación $\nu : K^* \to \Gamma$ y la aplicación canónica $\Gamma \to \Gamma_i$. Se verifica también que la inclusión de $U(V) = V \setminus \mathcal{P}_r$ en $U(V_i) = V_i \setminus \mathcal{P}_i$ define la aplicación canónica del grupo $\Gamma = K^*/U(V)$ en el grupo cociente $\Gamma_i = K^*/U(V_i)$.

Ejemplo 3.10 *La valoración impropia de K, es decir, la valoración ν que es cero para cualquier valor de K^*, es la única valoración de altura 0.*

Ejemplo 3.11 *La valoración ν es una valoración discreta de K si Γ su grupo de valores es un grupo discreto de rango finito, i.e. isomorfo a un subgrupo de $\mathbb{Z}^n$. En particular decimos que la valoración ν es discreta de rango 1 si su grupo de valores es isomorfo a un subgrupo de $\mathbb{Z}$, podemos suponer siempre que es igual a $\mathbb{Z}$; decimos entonces que el anillo asociado V es un anillo de valoración discreto de rango 1.*

Ejemplo 3.12 *Sea $A = \mathbb{C}[[x, y, z]]$ el anillo de series formales en 3 variables con coeficientes complejos. En este anillo local con ideal maximal $< x, y, z >$, se define ν, como $\nu(f) = \min \nu(\text{monomios de } f)$ para el orden lexicográfico, con $\nu(x^a y^b z^c) = (a, b, c) \in \mathbb{Z}^3$ luego $\Gamma = \mathbb{Z}^3$ (valoración discreta de orden 3). Así definido ν verifica las 3 propiedades de la definición 2.1. La proposición 2.7 nos permite extender ν al cuerpo de fracciones de A, $K = \mathbb{C}((x, y, z))$, mediante la definición $\nu(f/g) = \nu(f) - \nu(g)$. La proposición 2.8 nos garantiza que $V = \left\{ \frac{f(x)}{g(x)} \middle| \nu\left(\frac{f(x)}{g(x)}\right) \geq 0 \right\}$ es un anillo de valoración.*
Los subgrupos aislados son

$$\{0\}^3 = \Delta_3 \subset \{0\}^2 \oplus \mathbb{Z} = \Delta_2 \subset \{0\} \oplus \mathbb{Z}^2 = \Delta_1 \subset \mathbb{Z}^3 = \Delta_0.$$

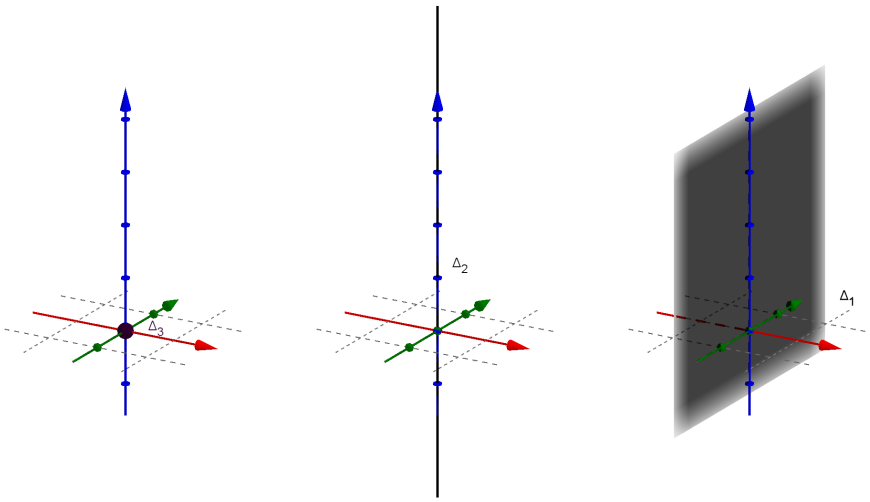
Y sus ideales asociados son

$$\mathcal{P}_0 = \left\{ \frac{f(x)}{g(x)} \middle| \nu\left(\frac{f(x)}{g(x)}\right) \notin \Delta_0 \right\} = \{0\},$$

$$\mathcal{P}_1 = \left\{ \frac{f(x)}{g(x)} \middle| \nu\left(\frac{f(x)}{g(x)}\right) \notin \Delta_1 \right\} =< x >,$$

$$\mathcal{P}_2 = \left\{ \frac{f(x)}{g(x)} \middle| \nu\left(\frac{f(x)}{g(x)}\right) \notin \Delta_2 \right\} =< x, y >,$$

$$\mathcal{P}_3 = \left\{ \frac{f(x)}{g(x)} \middle| \nu\left(\frac{f(x)}{g(x)}\right) \notin \Delta_3 \right\} =< x, y, z >= max(V).$$



Luego $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \mathcal{P}_2 \subset \mathcal{P}_3$.

Proposición 3.13 *Sea A un anillo local DDI distinto de su cuerpo de fracciones K. Entonces las condiciones siguiente son equivalentes:*

a) A es un anillo de valoración discreta de rango 1;

b) A es un dominio de ideales principales;

c) el ideal maximal $max(A)$ es principal y el anillo A es noetheriano;

d) A es un anillo de valoración noetheriano.

Demostración:
a) $\Rightarrow$ b): Por hipótesis el grupo de valores es isomorfo a $\mathbb{Z}$, los únicos segmentos son entonces de la forma $[-n, n]$, para $n \in \mathbb{N}$. Por tanto todo ideal I de A es un ideal del tipo $\mathcal{P}_n$ y está generado por un elemento x del anillo A que verifica $\nu(x) = n$, donde $n = \nu(I) = \text{ínf}\{\nu(y)|y \in I\}$.
b) $\Rightarrow$ c): Evidente
c) $\Rightarrow$ d): Vamos a definir una valoración ν sobre A llamada valoración $\mathcal{M}$-ádica, donde $\mathcal{M}$ es el ideal maximal $max(A)$ de A.
Como A es noetheriano tenemos $\bigcap_{n\geq 0} \mathcal{M}^n = (0)$, luego para todo elemento no nulo $x \in A$ podemos definir $\nu(x)$ como el mayor entero n tal que $x \in \mathcal{M}^n$, es decir $\nu(x) \geq n \Longleftrightarrow x \in \mathcal{M}^n$.
Si llamamos u a un generador del ideal maximal $\mathcal{M}$ de A, todo elemento x de A se escribe de la forma $x = yu^n$ con $n = \nu(x)$ y donde y es una unidad

de A.
Todo elemento z de K se escribe por tanto como $z = yu^n$ con $n \in \mathbb{Z}$ e y es una unidad de A, de donde deducimos que ν es una valoración discreta de rango 1 de K y que A es el anillo asociado.
d) $\Rightarrow$ a): Si A es noetheriano, toda sucesión creciente de ideales de A se estabiliza, luego toda sucesión decreciente de elementos de Γ^+ debe también estabilizarse. Entonces el grupo Γ es isomorfo a $\mathbb{Z}$. □

Observación 3.14 *Si ν es una valoración discreta de rango 1, suponiendo que su grupo de valores Γ es igual a $\mathbb{Z}$, es decir, que la valoración ν es también la valoración $\mathcal{M}$-ádica definida anteriormente, donde $\mathcal{M}$ es el ideal maximal del anillo de valoración A. Entonces todo elemento u de K verificando $\nu(u) = 1$ es un generador del ideal maximal $\mathcal{M}$ de A. A ese elemento u se le llama uniformizante. Es más, los únicos ideales de A son los ideales $(u^n)A$.*

Capítulo 4

Prolongación de una valoración

Sean K un cuerpo y L una extensión de K.
Si μ es una valoración de L, la restricción de μ a K es una valoración ν de K cuyo grupo de valores, Γ_ν, es un subgrupo del de μ, Γ_μ. Además, el anillo de valoración de ν, V, es igual a $W \cap K$ donde W es el anillo de valoración de μ, y W domina a V.

Definición 4.1 *En la situación anterior, se dice que la valoración μ de L prolonga a la valoración ν de K, o que μ es una prolongación de ν.*

Observación 4.2 *Sean V y W dos anillos de valoración de K y L, respectivamente, donde L extiende a K. Entonces W domina a V si y sólo si $V = W \cap K$. En efecto, si W domina a V entonces $V \subset W \cap K$; y si x es un elemento de K que no está en V su inverso x^{-1} pertenece a $max(V)$, luego a $max(W)$, en consecuencia $x \notin max(W)$.*
Recíprocamente, si $V = W \cap K$ en particular $V \subset W$; y si $x \in max(V)$, su inversa x^{-1} no pertenece a V, luego $x^{-1} \notin W$ y $x \in max(W)$.

Observación 4.3 *Para toda valoración ν de K existe al menos una valoración μ de L que prolonga a ν.*
En efecto, el anillo de valoración V de ν es un subanillo local de L y por el Corolario 1.6 existe un anillo de valoración W de L que domina a V. Por la observación anterior se deduce que la valoración ν asociada a W prolonga a ν.

Nos proponemos estudiar las extensiones Γ_μ y k_μ respectivamente del grupo de valores Γ_ν y del cuerpo residual k_ν, correspondientes a una prolongación μ de ν en una extensión L de K dada.
Para empezar estudiaremos el caso en que L es una extensión algebraica de K. Notaremos respectivamente Γ_ν y Γ_μ, y V y W, a los subgrupos de valores y a los anillos de valoración, asociados a ν y μ.
Notaremos k_ν y k_μ a los cuerpos residuales respectivos de las valoraciones ν y μ, es decir, los cuerpos definidos por $k_\nu = V/max(V)$ y $k_\mu = W/max(W)$.

Definición 4.4 *El índice de ramificación de μ respecto de ν es igual al índice del grupo de valores Γ_ν en Γ_μ:*

$$e(\mu/\nu) = [\Gamma_\mu : \Gamma_\nu].$$

El grado residual de μ respecto de ν es igual al grado de la extensión del cuerpo residual k_ν en k_μ:

$$f(\mu/\nu) = [k_\mu : k_\nu].$$

El índice de ramificación y el grado residual son elementos de $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$.

Observación 4.5 *Si L' es una extensión de L y si μ' es una valoración de L' que prolonga a μ, entonces μ' prolonga a ν y tenemos las igualdades:*

$$e(\mu'/\nu) = e(\mu'/\mu)e(\mu/\nu),$$

$$f(\mu'/\nu) = f(\mu'/\mu)f(\mu/\nu).$$

En particular $e(\mu'/\nu)(resp. f(\mu'/\nu))$es finito si y sólo si $e(\mu'/\mu)$ y $e(\mu/\nu)$ $(resp. f(\mu'/\mu)$ y $f(\mu/\nu))$ son finitos.

Proposición 4.6 *Si L es una extensión finita de K de grado n se tiene la desigualdad:*

$$e(\mu/\nu)f(\mu/\nu) \leq n.$$

En particular, el índice de ramificación y el grado residual son finitos.

Demostración:
Sean r y s dos enteros tales que $r \leq e(\mu/\nu)$ y $s \leq f(\mu/\nu)$; basta demostrar que se tiene $rs \leq n$.
Por hipótesis existen r elementos $x_1, x_2, \ldots, x_r$ de L tales que para todo (i, j) con $i \neq j$, $\mu(x_i) \not\equiv \mu(x_j) \bmod \Gamma_\nu$.

Análogamente existen s elementos $y_1, y_2, \ldots, y_s$ de W cuyas imágenes $\bar{y_1}, \bar{y_2}, \ldots, \bar{y_s}$ en k_μ son linealmente independientes sobre k_ν.
Basta demostrar que los rs elementos $x_i y_j$, $1 \leq i \leq r$ y $1 \leq j \leq s$, son independientes sobre K. Supongamos que no es el caso y que existe una relación lineal no trivial entre ellos:

$$(*) \sum a_{i,j} x_i y_j = 0,$$

con $a_{i,j} \in K$. Escogemos un índice (l, m) tal que $\forall (i, j)$,

$$\mu(a_{l,m} x_l y_m) \leq \mu(a_{i,j} x_i y_j),$$

en particular $a_{l,m} \neq 0$.
Para $i \neq l$, tenemos la desigualdad $\mu(a_{l,m} x_l y_m) \neq \mu(a_{i,j} x_i y_j)$; en efecto si tuviéramos la igualdad, $\mu(x_l) - \mu(x_i)$ sería igual a $\nu(a_{i,j}) - \nu(a_{l,m})$ ya que $\mu(y_j)$ es nulo para todo y_j verificando $\bar{y_j} \neq 0$ y porque μ prolonga ν y tenemos la relación $\mu(x_l) \equiv \mu(x_i) \mathrm{mod} \Gamma_\nu$, lo que es imposible para $i \neq l$.
Multiplicando la relación $(*)$ por $(a_{l,m} x_l)^{-1}$, obtenemos la relación:

$$\sum b_j y_j + z = 0, \text{ con } b_j = a_{l,j}/a_{l,m} \in W \cap K \text{ y } z \in max(W).$$

Obtenemos así en el cuerpo $k_\mu = W/max(W)$ la relación $\sum \bar{b_j} \bar{y_j} = 0$ con $\bar{b_m} = 1$. Es una relación no trivial de dependencia lineal sobre k_ν de los $\bar{y_j}$, lo que es imposible por las hipótesis de los y_j. □

Centro de una valoración

Sea K un cuerpo dotado de una valoración ν, llamamos R_ν al anillo de valoración de ν y $\mathcal{M}_\nu$ su ideal maximal.

Definición 4.7 *Sea A el subanillo de K sobre el cual la valoración es positiva, $A \subset R_\nu$, entonces el centro de la valoración ν en A es el ideal $\mathcal{P} = A \cap \mathcal{M}_\nu$.*

Observación 4.8 *El centro $\mathcal{P}$ de la valoración es un ideal primo de A. Si A es local, el centro de ν en A es su ideal maximal $\mathcal{M}_\nu$ si y sólo si el anillo de la valoración R_ν domina a A.*
En particular, el centro $\mathcal{P}$ de la valoración ν en A es el único ideal primo $\mathcal{Q}$ de A tal que el anillo de valoración R_ν domina al localizado $A_\mathcal{Q}$.

Capítulo 5

Construcción de valoraciones en anillos de polinomios

Introducción

En lo sucesivo consideramos valoraciones reales, es decir cuando el conjunto de valores $\Gamma \subset \mathbb{R}$. Sea una valoración ν de un anillo A,

Definición 5.1 *Dos elementos a, b del anillo A se dicen equivalentes en la valoración ν si y sólo si*

$$\nu(a-b) > \nu(a),$$

y lo notaremos $a \sim b$

Observación 5.2 *Las leyes producto y triangular nos demuestran que dos elementos equivalentes tienen el mismo valor y que es una relación de equivalencia (reflexiva, simétrica y transitiva) imponiendo que $0 \sim 0$.*
Además, dos equivalencias

$$a \sim b \quad y \quad c \sim d,$$

se pueden multiplicar para obtener

$$ac \sim bd.$$

Definición 5.3 *Un elemento b se dice que es divisible equivalente en ν por a si y sólo si existe $c \in A$ tal que*

$$b \sim ca.$$

Observación 5.4 *Si la relación anterior es cierta, también lo es al reemplazar a o b por cualquier elemento equivalente.*

Observación 5.5 *La ley producto implica que un anillo A con una valoración ν debe ser un dominio de integridad (sin divisores de cero). La valoración ν se extiende al cuerpo de fracciones de A definiendo*

$$\nu\Big(\frac{a}{b}\Big) = \nu(a) - \nu(b),$$

para cualesquiera elementos a de A y $b \neq 0$.

Teorema 5.6 *Sean A un dominio de integridad y K su cuerpo de fracciones. Si ν es una valoración de A, entonces la función definida anteriormente es una valoración de K. Recíprocamente, toda valoración de K se puede obtener de esta forma a partir de una única valoración de A.*

Demostración:
La demostración se obtiene aplicando la Definición 2.1 de valoración con la construcción que hemos hecho en la Observación 5.5 . □

Observación 5.7 *Cuando $A = K$ es un cuerpo, el conjunto de todos los números reales $\nu(a)$ para $a \neq 0$ en A es el grupo aditivo (totalmente ordenado) que denotamos en el capítulo 3 por Γ, lo llamaremos el grupo de valores de ν.*
Si los números positivos de Γ tienen un mínimo $\delta > 0$, entonces la valoración ν se dice discreta. En este caso Γ es el grupo cíclico generado por δ.

Valoración de primera etapa

El problema que motiva esta sección es construir, dadas todas las valoraciones de un cuerpo K, las valoraciones del anillo $K[x]$ de polinomios en x con coeficientes en K. Lo que es equivalente, gracias al Teorema 5.6, a determinar todas las valoraciones del cuerpo $K(x)$ de las funciones racionales.
Las valoraciones de $K[x]$ serán construidos por etapas.
Para el primer paso, tomamos cualquier valoración ν_0 de K y cualquier número real μ y definimos entonces la valoración de primera etapa ν_1 para cualquier polinomio como sigue:

$$\nu_1(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0) = \text{mín}[\nu_0(a_n) + n\mu, \nu_0(a_{n-1}) + (n-1)\mu, \ldots, \nu_0(a_0)].$$

En particular

$$\nu_1(x) = \mu,\ \nu_1(a) = \nu_0(a),$$

para cualquier $a \in K$.
Usaremos el símbolo $[\nu_0, \nu_1(x) = \mu]$ para la valoración ν_1.

Tenemos el siguiente resultado demostrado por T. Rella en 1927([6])

Teorema 5.8 *Si ν_0 es una valoración de K y μ un número real, la función $\nu_1 = [\nu_0, \nu_1(x) = \mu]$ definida anteriormente es una valoración de $K[x]$.*

Observación 5.9 *En el caso de $\mu = 0$ el valor ν_1 es fácil de calcular. Y si ν_0 es trivial (igual a cero) y $\mu < 0$, entonces*

$$\nu_1(a(x)) = \mu \cdot deg(a(x)).$$

Ejemplo 5.10 *Sea p primo, consideramos ν_0 la valoración p-ádica en $\mathbb{Q}$ con $\nu_0(p) = 4$.*
Extendemos ν_0 con ν_1 a $\mathbb{Q}[x]$ con $\nu_1(x) = 0$.
Si $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,
$\nu_1(f) = \text{mín}\{\nu_0(a_n), \nu_0(a_{n-1}), \ldots, \nu_0(a_1), \nu_0(a_0)\}$.
Por ejemplo, si $p = 3$ y $f(x) = x^8 + 4x^6 + 12x^4 + 25x^2 + 25$,

$$\nu_1(f) = \text{mín}\{\nu_0(1), \nu_0(4), \nu_0(12), \nu_0(25)\} = \text{mín}\{0, 0, 4, 0\} = 0.$$

Valoraciones aumentadas

Ahora procedemos a construir una valoración de segunda etapa sobre la base de una de primera etapa (ν_1). O, más generalmente una valoración de k-ésima etapa sobre la base de una de la etapa $(k-1)$-ésima.
Este proceso puede ser reformulado como sigue: Dada una valoración W de $K[x]$, construir una valoración "aumentada" ν asignando valores más grandes a ciertos polinomios "clave" $\phi(x)$ y sus múltiplos-equivalentes. Veamos ahora qué queremos decir con polinomio "clave".

Definición 5.11 *Se dice que un polinomio no nulo $\phi(x)$, de $K[x]$ es un polinomio clave sobre una valoración W de $K[x]$ si satisface las siguientes condiciones:*

1. *Irreducibilidad. Si un producto es divisible equivalente en W por $\phi(x)$, entonces uno de los factores es divisible equivalente por $\phi(x)$.*

II. *Grado mínimo. Cualquier polinomio no nulo divisible equivalente en W por $\phi(x)$ tiene grado mayor o igual que $\phi(x)$.*

III. *Mónico. El coeficiente líder de $\phi(x)$ es 1.*

Lema 5.12 *Si ϕ es un polinomio clave sobre la valoración W de $K[x]$, y si $f(x) \neq 0$ con su expresión cociente-resto al dividir por ϕ, i.e. $f = q\phi + r$, entonces:*

1. $W(r(x)) \geq W(f(x))$,
2. $W(q(x)\phi) \geq W(f(x))$.

La primera desigualdad estricta se tiene si y sólo si $f(x)$ es divisible equivalente por ϕ en W.

Demostración:
Para demostrar el primero hacemos reducción al absurdo, supongamos que $W(r(x)) < W(f(x))$, por la expresión cociente-resto y la Definición 5.3 de equivalente tenemos que

$$r(x) \sim (-q(x))\phi \qquad \text{(en } W\text{)}.$$

Entonces si $r(x) \neq 0$ es divisible equivalente por ϕ, que es una contradicción ya que el grado de $r(x)$ es estrictamente menor que el de ϕ.
La segunda parte se sigue de la primera y de la ley triangular. Usando de nuevo la expresión cociente-resto,

$$-q(x)\phi = r(x) - f(x).$$

Tomando valoración W y por la ley triangular,

$$W(-q(x)\phi) = W(q(x)\phi) \geq \text{mín}(W(r(x)), W(f(x))).$$

Por la primera parte tenemos que $W(r(x)) \geq W(f(x))$, concluímos por tanto que $W(q(x)\phi) \geq W(f(x))$.
Por último la conclusión del lema, que nos da un test para la división-equivalente en términos de la división ordinaria. Cuando $W(r(x)) > W(f(x))$, entonces por la expresión cociente-resto tenemos que $f(x)$ es divisible equivalente por ϕ. Recíprocamente, si $f(x)$ es divisible equivalente por ϕ en W, entonces existen polinomios $h(x)$ y $s(x)$ tal que

$$f(x) = h(x)\phi + s(x), \qquad W(s(x)) > W(f(x)).$$

Si se diera la igualdad $W(r(x)) = W(f(x))$, tendríamos que

$$r(x) = f(x) - q(x)\phi = (h(x) - q(x))\phi + s(x),$$

con

$$W(s(x)) > W(f(x)) = W(r(x))$$

haciendo que ϕ sea divisible equivalente de $r(x)$, llegando a una contradicción, por lo que la desigualdad es estricta. $\square$

A este polinomio clave $\phi(x)$ se le asignará una nueva valoración

$$\nu(\phi(x)) = \mu > W(\phi(x)).$$

Para encontrar las nuevas valoraciones del resto de polinomios usaremos expansiones en ϕ, es decir, expresiones en potencias de ϕ de la forma

$$f(x) = f_m(x)\phi^m + f_{m-1}\phi^{m-1} + \ldots + f_0(x)$$

en el que cada $f_i(x)$ es nulo o de menor grado de $\phi(x)$. Esta expansión es única para cada polinomio y se consigue dividiendo sucesivamente por ϕ. La nueva valoración $\nu(f(x))$ es:

$$\nu(f_m(x)\phi^m + f_{m-1}\phi^{m-1} + \ldots + f_0(x)) = \min_i[W(f_i(x)) + i\mu].$$

Teorema 5.13 *Si W es una valoración de $K[x]$, $\phi(x)$ es un polinomio clave sobre W y $\mu > W(\phi(x))$ es un número real, entonces la función ν definida arriba es una valoración de $K[x]$. Se dice que ν es una valoración aumentada y se denota por:*

$$\nu = [W, \nu(\phi) = \mu].$$

Demostración:
Las leyes producto y triangular para ν deben verificarse. Primero probaremos la ley triangular para una suma $f(x) + g(x)$. Se expresan f y g como polinomios en *phi*:

$$f = \sum f_i\phi^i, \qquad g = \sum g_i\phi^i.$$

Por la definición de ν y por la ley triangular de W,

$$\begin{aligned}
\nu(f+g) = \min_i[W(f_i + g_i) + i\mu] &\geq \min_i[\min(W(f_i), W(g_i)) + i\mu] \\
&= \min_i[\min(W(f_i) + i\mu, W(g_i) + i\mu)] \\
&= \min[\min_i(W(f_i) + i\mu), \min_i(W(g_i) + i\mu)] \\
&= \min[\nu(f), \nu(g)].
\end{aligned}$$

Para probar la ley producto usamos la expresión cociente-resto del algoritmo de la división de $f(x)$,

$$f(x) = q(x)\phi + r(x)$$

donde r es cero o de grado menor que $\phi(x)$.
Consideramos primero la ley producto para el caso de un producto de dos expansiones monomiales $a(x)\phi^t$ y $b(x)\phi^u$. Ya que los grados de $a(x)$ y $b(x)$ son menores que el grado de ϕ, el producto $a(x)b(x)$ tiene una expresión con no más de dos términos,

$$a(x)b(x) = c(x)\phi + d(x).$$

El producto $a(x)b(x)$ no es divisible-equivalente en W por ϕ, porque si lo fuera, la parte de la irreducibilidad de ϕ en la Definición 5.11, necesitaríamos que uno de los factores fuera divisible-equivalente por ϕ, contrario al grado mínimo. Por el Lema 5.12 y la desigualdad triangular tenemos que

$$W(c(x)\phi) \geq W(a(x)b(x)) = W(d(x)).$$

Como la nueva valoración ϕ excede a la anterior, $\mu > W(\phi)$,

$$W(c(x)) + \mu > W(a(x)b(x)) = W(d(x))$$

el producto en cuestión tiene por la expresión de $a(x)b(x)$ la expansión,

$$(a(x)\phi^t)(b(x)\phi^u) = c(x)\phi^{t+u+1} + d(x)\phi^{t+u}.$$

Luego por la definición de ν

$$\begin{aligned}\nu[(a(x)\phi^t)(b(x)\phi^u)] &= \text{mín}[W(c(x)) + \mu + (t+u)\mu, W(d(x)) + (t+u)\mu] \\ &= W(d(x)) + (t+u)\mu \\ &= W(a(x)) + t\mu + W(b(x)) + u\mu \\ &= \nu(a(x)\phi^t) + \nu(b(x)\phi^u).\end{aligned}$$

Esta es la ley producto para expresiones monomiales.
La ley producto para polinomios $f(x)$ y $g(x)$ del tipo

$$f_m(x)\phi^m + f_{m-1}\phi^{m-1} + \ldots + f_0(x)$$

y

$$g_n(x)\phi^n + g_{n-1}\phi^{n-1} + \ldots + g_0(x)$$

es una consecuencia inmediata. El producto $f(x)g(x)$ tiene una expresión obtenida por la suma de expansiones de productos monomiales, por tanto:

$$\nu(f(x)g(x)) \geq \nu(f(x)) + \nu(g(x)).$$

Para demostrar la igualdad, tomamos t y u como los máximos enteros con

$$\nu(f_t(x)\phi^t)) = \nu(f(x)), \qquad \nu(g_u(x)\phi^u) = \nu(g(x))$$

respectivamente. En el caso de monomios se demuestra que la expansión de $f(x)g(x)$ tiene un término $r(x)\phi^{t+u}$ con la valoración $\nu(f) + \nu(g)$, la igualdad por tanto se tiene. □

Propiedades de las valoraciones aumentadas

Veamos ahora algunas propiedades de la valoración aumentada.

Teorema 5.14 *(Monotonía) Dado la valoración aumentada* $\nu = [W, \nu(\phi) = \mu]$*, se verifica que*

$$\nu(f(x)) \geq W(f(x)),$$

para todo polinomio $f(x) \neq 0$*. La desigualdad es estricta si y sólo si* $f(x)$ *es divisible equivalente en* W *por* $\phi(x)$*. En particular, si el grado de* $\phi(x)$ *es mayor que el de* $f(x)$ *se verifica la igualdad.*

Demostración:
La prueba es por inducción en el grado m de la expansión de $f(x)$ en ϕ. Si $m = 0$, la definición de ν demuestra que $\nu(f(x))$ y $W(f(x))$ son iguales. Si $m > 0$, la expresión cociente-resto ($f(x) = q(x)\phi + r(x)$) indica que $q(x)$tiene una expresión de grado $m - 1$ en ϕ, por hipótesis de inducción tendremos

$$\nu(q(x)) \geq W(q(x)),$$

por lo que la valoración en el primer término de la derecha de la expresión cociente-resto, por la ley producto, la definición de ϕ (5.11) y el Lema 5.12, es

$$\nu(q(x)\phi) \geq W(q(x)) + \nu(\phi) > W(q(x)) + W(\phi) = W(q(x)\phi) \geq W(f(x)).$$

Para el segundo término, en el caso $m = 0$ y por el Lema 5.12

$$\nu(r(x)) = W(r(x)) \geq W(f(x)),$$

donde la desigualdad estricta se tiene si y sólo si $f(x)$ es divisible equivalente por ϕ en W. La ley triangular estricta nos da el resultado. □

Teorema 5.15 *Si en la expresión*

$$a(x) = a_n(x)\phi^n + a_{n-1}(x)\phi^{n-1} + \ldots + a_0(x)$$

los grados de los $a_i(x)$ no están acotados (es decir, no es una expansión), pero ningún $a_i(x)$ es divisible en W por ϕ, entonces la valoración aumentada $\nu = [W, \nu(\phi) = \mu]$ es

$$\nu(a(x)) = \min_i[W(a_i) + i\mu] \quad con \quad i = 0, 1, \ldots, n.$$

Demostración:
Hacemos la expresión cociente-resto en cada uno de los polinomios $a_i(x)$

$$a_i(x) = q_i(x)\phi + r_i(x) \quad con \quad i = 0, 1, \ldots, n$$

$$a(x) = \sum_{i=0}^{n} q_i(x)\phi^{i+1} + \sum_{i=0}^{n} r_i(x)\phi^i.$$

El Lema 5.12 nos demuestra que

$$\nu\Big(\sum_i r_i\phi^i\Big) = \min_i[W(r_i) + i\mu] = \min[W(a_i) + i\mu].$$

Y el primer sumando

$$\begin{aligned}\nu\Big(\sum_i q_i\phi^{i+1}\Big) &\geq \min_i[\nu(q_i) + \nu(\phi) + i\mu] \\ &> \min_i[W(q_i) + W(\phi) + i\mu] \\ &= \min_i[W(q_i\phi) + i\mu],\end{aligned}$$

gracias a la monotonía. Y finalmente aplicamos la ley triangular fuerte a la suma de los dos sumandos y obtenemos el resultado deseado. □

Valoraciones inductiva y límite

Queremos clasificar las valoraciones y los grupos de valores obtenidos al hacer sucesivamente valoraciones aumentadas.

Definición 5.16 *Una valoración inductiva de k-ésima etapa ν_k es cualquier valoración de $K[x]$ obtenida como una sucesión de valoraciones $\nu_1, \nu_2, \ldots, \nu_k$, donde $\nu_1 = [\nu_0, \nu_1(x) = \mu_1]$ es una valoración de primera etapa y cada ν_i se obtiene aumentando ν_{i-1},*

$$\nu_i = [\nu_{i-1}, \nu_i(\phi_i) = \mu_i] \quad con \quad i = 2, \ldots, k.$$

Además, para cada $i = 2, \ldots, k$, los polinomios clave $\phi_i(x)$ deben satisfacer:

I) *$deg(\phi_i(x)) \geq deg(\phi_{i-1}(x))$.*

II) *La equivalencia $\phi_i(x) \sim \phi_{i-1}(x)$ (en ν_{i-1}) es falsa.*

Se sobreentiende que el primer polinomio clave es $\phi_1(x) = x$.

La valoración inductiva se denotará por

$$\nu_k = [\nu_0, \nu_1(x) = \mu_1, \nu_2(\phi_2) = \mu_2, \ldots, \nu_k(\phi_k) = \mu_k]$$

Ejemplo 5.17 *Continuando con el Ejemplo 5.10.*
Sea $\phi_2 = x^2 + 1$ polinomio clave por ν_1 en $\mathbb{Q}[x]$ porque: es mónico, es irreducible y homogéneo para ν_1, es decir, todos los monomios de ϕ_2 tienen el mismo valor ν_1, $\nu_1(x^2) = \nu_1(1) = 0$.

Definimos $\nu_2(x^2+1) = 2 > 0 = \nu_1(x^2+1)$. Para el mismo f lo dividimos por el polinomio clave ϕ_2, para obtener una expresión de la forma

$$f(x) = (x^2+1)^4 + 6(x^2+1)^2 + 9(x^2+1) + 9 = \phi_2^4 + 6\phi_2^2 + 9\phi_2 + 9.$$

Luego

$$\begin{aligned} \nu_2(f) &= \text{mín}\{4\nu_2(\phi_2), 2\nu_2(\phi_2) + \nu_0(6), \nu_2(\phi_2) + \nu_0(9), \nu_0(9)\} \\ &= \text{mín}\{8, 8, 10, 8\} = 8. \end{aligned}$$

Elegimos ahora el nuevo polinomio clave $\phi_3 = (x^2+1)^2 + 3$ para ν_2 porque: es mónico, es irreducible y homogéneo para ν_2, pues $\nu_2((x^2+1)^2) = 4 = \nu_2(3) = \nu_0(3) = 4$.
Definimos ν_3 tal que $\nu_3(\phi_3) = 5 > 4 = \nu_2(\phi_3)$, $f(x) = [(x^2+1)^2 + 3]^2 + 9(x^2+1) = \phi_3^2 + 9(x^2+1)$. Por tanto

$$\nu_3(f) = \text{mín}\{2 \cdot 5, \nu_2[9(x^2+1)]\} = 10$$

ya que $\nu_2[9(x^2+1)] = \nu_0(9) + \nu_2(x^2+1) = 2 \cdot 4 + 2 = 10$.
Nótese que se verifican las condiciones I) y II) de la definición 5.16.

Dada una sucesión infinita $\nu_1, \nu_2, \ldots, \nu_k, \ldots$ de valoraciones inductivas, se define la función

$$\nu_\infty(f(x)) = \lim_{k \to \infty} \nu_k(f(x)).$$

El carácter monótono de ν_k indica que este límite, si no es finito, es $+\infty$.
La función ν_∞ satisface la ley producto para valoraciones, se demuestra

tomando límites en la ley producto para ν_k. En cuanto a la suma $f(x)+g(x)$, vemos que la ley triangular en ν_k nos indica una de las desigualdades

$$\nu_k(f(x)+g(x)) \geq \nu_k(f(x)) \qquad \nu_k(f(x)+g(x)) \geq \nu_k(g(x))$$

se cumple para una infinidad de k's. Concluimos que

$$\nu_\infty(f(x)+g(x)) \geq \nu_\infty(f(x)) \qquad \nu_\infty(f(x)+g(x)) \geq \nu_\infty(g(x))$$

por lo que tenemos la ley triangular para ν_∞. Por consiguiente, se verifica el siguiente teorema:

Teorema 5.18 *Sean $\{\phi_k(x)\}$ y $\{\mu_k\}$ sucesiones infinitas tales que cada función ν_k es una valoración inductiva. Entonces la función $\nu_\infty f(x)$ definida anteriormente es una valoración de $K[x]$, aceptando que algunos polinomios puedan tomar el valor $+\infty$. Llamaremos valoración límite a esta función ν_∞.*

Estudiemos el caso en el que los polinomios clave tienen el mismo grado.

Lema 5.19 *Si en la valoración inductiva ν_k los polinomios clave $\phi_{t+1}(x), \phi_{t+2}(x), \ldots, \phi_k(x)$ tienen todos el mismo grado, para cierto t, $0 \leq t \leq k-1$, entonces*

1. *$\nu_t(\phi_{j+1} - \phi_j) = \mu_j$ para $j = t+1, t+2, \ldots, k-1$.*
2. *$\mu_k > \mu_{k-1} > \ldots > \mu_{t+1}$.*
3. *$\nu_t(\phi_k) = \nu_t(\phi_{k-1}) = \cdots = \nu_t(\phi_{t+1})$ si $t > 0$.*

Demostración:
Sea $j \in \{t+1, t+2, \ldots, k-1\}$ y sea

$$s_j(x) = \phi_{j+1}(x) - \phi_j(x).$$

Como ambos $\phi's$ tienen el primer coeficiente 1, el grado de $s_j(x)$ es menor que el de $\phi_j(x)$. Por lo tanto por el Teorema 5.14 de monotonía

$$\nu_t(s_j(x)) = \nu_{t+1}(s_j(x)) = \cdots = \nu_k(s_j(x)).$$

Si el apartado 1. fuera falso para algún j, tendríamos

$$\nu_t(s_j(x)) = \nu_t(\phi_{j+1} - \phi_j) > \mu_j = \nu_j(\phi_j)$$

la otra desigualdad no se puede dar por el Lema 5.12. Por tanto tenemos

$$\phi_{j+1} \sim \phi_j \quad (\text{en } \nu_j)$$

una contradicción por la Definición 5.16 de valoración inductiva. Luego 1. es cierto. Por monotonía, la ley triangular para la definición de s_j, tenemos 2., para

$$\mu_{j+1} = \nu_{j+1}(\phi_{j+1}) > \nu_j(\phi_{j+1}) \geq \text{mín}[\nu_j(\phi_j), \nu_t(s_j)] = \mu_j.$$

Suponemos ahora $t > 0$, por razones similares tenemos

$$\nu_t(s_j(x)) = \mu_j = \nu_j(\phi_j) > \nu_{j-1}(\phi_j) \geq \nu_t(\phi_j).$$

Por la ley triangular (fuerte) en la definición de s_j tenemos 3.

$$\nu_t(\phi_{j+1}) = \text{mín}[\nu_t(\phi_j), \nu_t(s_j(x))] = \nu_t(\phi_j). \quad \square$$

Una consecuencia interesante de este lema es la invarianza de las valoraciones para polinomios clave

Teorema 5.20 *Si la valoración inductiva de i-ésima etapa de*

$$\nu_k = [\nu_0, \nu_1(x) = \mu_1, \nu_2(\phi_2) = \mu_2, \ldots, \nu_k(\phi_k) = \mu_k]$$

usa un polinomio clave ϕ_i con valoración asignada μ_i, entonces

$$\nu_k(\phi_i(x)) = \nu_i(\phi_i(x)) = \mu_i.$$

Demostración:
Se sigue del Teorema 5.14 (Monotonía) si el grado de $\phi_{i+1}(x)$, y por tanto el de los posteriores polinomios claves, excede el grado de $\phi_i(x)$. El único caso restante es el del Lema 5.19, con $t = i - 1$. Pero por

$$s_j(x) = \phi_{j+1}(x) - \phi_j(x),$$

tenemos

$$\phi_i = \phi_k - s_{k-1}(x) - s_{k-2}(x) - \cdots - s_i(x).$$

El término de la derecha tenemos por el Lema anterior los ν_k valoraciones $\mu_k, \mu_{k-1}, \ldots, \mu_i$ respectivamente, el resultado lo obtenemos de la ley fuerte triangular. $\square$

Tanto este teorema como el lema anterior son también ciertos para las valoraciones límite.

Teorema 5.21 *Sea una valoración límite o inductiva construidos por las valoraciones $\nu_1, \nu_2, \ldots$. Entonces, para cualquier polinomio fijado $f(x) \neq 0$, o bien*

$$\nu_{k+1}(f(x)) > \nu_k(f(x)) \qquad (k = 1, 2, \ldots)$$

o bien existe un $i \geq 1$ tal que

$$\begin{aligned}\nu_1(f(x)) < \nu_2(f(x)) < \ldots < \nu_{i-1}(f(x)) \\ < \nu_i(f(x)) = \nu_{i+1}(f(x)) = \nu_{i+2}(f(x)) = \ldots\end{aligned}$$

En el último caso existe un $r(x)$ de grado menor que el de ϕ_{i+1} con

$$f(x) \sim r(x) \qquad (en \ \ \nu_k) \quad (k = i+1, i+2, \ldots).$$

Demostración:
Supongamos lo contrario a la primera alternativa, para algún i tenemos

$$\phi_{i+1}(f(x)) = \phi_i(f(x)).$$

La expresión resto-cociente

$$f(x) = q(x)\phi_{i+1} + r(x),$$

por el Teorema 5.14 (Monotonía) y el Lema 5.12 debemos obtener que $\nu_i(r) = \nu_i(f)$. Por lo tanto, para cualquier $k \geq i+1$,

$$\begin{aligned}\nu_k(f - r) &\geq \nu_{i+1}(f - r) \\ &= \nu_{i+1}(q\phi_{i+1}) > \nu_i(q\phi_{i+1}) \\ &\geq \nu_i(f) = \nu_i(r) = \nu_k(r).\end{aligned}$$

Por lo que $f(x)$ y $r(x)$ son equivalentes en ν_k y

$$\nu_k(f) = \nu_k(r) = \nu_i(r) = \nu_i(f),$$

luego $\nu_k(f(x))$ es constante para $k \geq i$, que es la segunda alternativa. □
Una valoración inductiva ν_k de $K[x]$ da por el Teorema 5.6 una valoración para el cuerpo $K(x)$ de funciones racionales. Esta valoración tiene un grupo de valores Γ_k (grupo de valores asociado con ν_k). Queda determinado por el siguiente teorema:

Teorema 5.22 *La valoración ν_k tiene grupo de valores Γ_k, que es el conjunto de los números de la forma*

$$\nu + m_1\mu_1 + m_2\mu_2 + \cdots + m_k\mu_k$$

donde los m_i son enteros y ν es un elemento del grupo de valores de ν_0.

Demostración:
Que cada número de Γ_k tenga esa forma se obtiene por inducción en la Definición de valoración aumentada. Inversamente, cualquier número con esa forma es, por el Teorema 5.20, la valoración en ν_k de la función racional

$$bx^{m_1}\phi_2^{m_2}\dots\phi_k^{m_k},$$

donde b es una constante en K. □

Definición 5.23 *Un número real μ se dice conmensurable con un grupo aditivo de números si algún múltiplo entero de μ está en el grupo.*

Teorema 5.24 *En una valoración inductiva ν_k cada valoración asignada μ_i, excepto quizás μ_k, es conmensurable con el grupo de valores Γ_{i-1} de la valoración precedente (el caso $i = 1$ incluído).*

Demostración:
Consideremos la expansión en ϕ_i del siguiente polinomio clave,

$$\phi_{i+1}(x) = f_m(x)\phi_i^m + f_{m-1}(x)\phi_i^{m-1} + \dots + f_0(x).$$

Si μ_i no es conmensurable con Γ_{i-1} no hay dos términos en la suma anterior que puedan tener la mismo valor en ν_i. Luego sólo un término, supongamos el j-ésimo, es el valor mínimo, y

$$\phi_{i+1}(x) \sim f_j(x)\phi_i^j.$$

Por la irreducibilidad de ϕ_{i+1}, al menos una de estas dos condiciones es cierta:

1. $f_j(x)$ es divisible equivalente en ν_i con ϕ_{i+1}.
2. $\phi_i(x)$es divisible equivalente en ν_i con ϕ_{i+1}.

Por la propiedad minimal (propiedad 2. de la definición de polinomio clave) de ϕ_{i+1} la primera condición se contradice con la Definición 5.16 I). Por las mismas razones la segunda condición implica que ϕ_{i+1} y ϕ_i tienen el mismo grado, mientras

$$s(x) = \phi_{i+1}(x) - \phi_i(x)$$

tiene menor grado. Debido a la segunda condición y al Lema 5.12 (en este caso la expresión cociente-resto del Lema es $\phi_i(x) = \phi_{i+1}(x) - s(x)$) aplicado a ν_i y al polinomio clave ϕ_{i+1} tenemos que $\nu_i(s(x)) > \nu_i(\phi_i(x))$. Luego

$$\phi_i(x) \sim \phi_{i+1}(x) \qquad (en\ \ \nu_i),$$

contradiciendo la segunda condición por tanto no puede ser ϕ_{i+1} polinomio clave. □

Completitud

El siguiente resultado demuestra que la clasificación de valoraciones sobre $K[x]$ es completa, es decir, que toda valoración de $K[x]$ es bien una valoración inductiva, bien una valoración límite obtenida de la correspondiente valoración de K.

Teorema 5.25 *(Completitud) Si cada valoración del cuerpo K es discreta, entonces cada valoración W del anillo $K[x]$ puede representarse o bien como una valoración inductiva o bien como una valoración límite.*

Demostración:
Dado W, construiremos por etapas su correspondiente valoración inductiva ν_k, con las siguientes 3 propiedades:

1. $W(f(x)) \geq \nu_k(f(x))(\forall f(x))$.
2. $grado(f(x)) < grado(\phi_k)$ entonces $W(f(x)) = \nu_k(f(x))$.
3. $W(\phi_i(x)) = \nu_k(\phi_i(x)) = \mu_i \quad (i = 1, 2, \ldots, k)$.

La valoración inicial ν_1 está definida por

$$\mu_1 = W(x), \;\; \nu_0(a) = W(a) \qquad (a \in K),$$

gracias a la propiedad triangular para W y a la definición de ν_1 (recordemos que $\nu_1(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0) = \text{mín}[\nu_0(a_n) + n\mu, \nu_0(a_{n-1}) + (n-1)\mu, \ldots, \nu_0(a_0)]$), entonces tenemos las propiedades anteriores cumplidas para $k = 1$. Supongamos ahora que ya tenemos construida una valoración inductiva ν_k con esas 3 propiedades, y que no tenemos igualdad siempre en la propiedad 1. Como posible polinomio clave, tomamos $\psi(x)$ el menor de menor grado tal que

$$W(\psi(x)) > \nu_k(\psi(x)).$$

Haciendo producto con alguna constante tenemos que el primer coeficiente de $\psi(x)$ es 1. Por tanto las dos propiedades siguientes son equivalentes

a) $W(f(x)) > \nu_k(f(x))$.

b) $f(x)$ es divisible-equivalente en ν_k por $\psi(x)$.

En efecto, si tenemos a) y si $f(x)$ tiene la expresión cociente-resto

$$q(x)\psi + r(x),$$

entonces

$$\nu_k(q\psi - f) = W(q\psi - f) \geq \text{mín}[W(q\psi), W(f)] > \text{mín}[\nu_k(q\psi), \nu_k(f)]$$

gracias a 2., al menor grado tomado por la elección de ψ y a la hipótesis de inducción de 1. en $q(x)$. Entonces la ley triangular fuerte demuestra que $f \sim q\psi$ en ν_k lo cual es b). Recíprocamente, si tenemos b) existen polinomios $h(x)$ y $s(x)$ con

$$f(x) = h(x)\psi + s(x), \qquad \nu_k(s(x)) > \nu_k(f(x)) = \nu_k(h(x)\psi).$$

Entonces, por la hipótesis de inducción en 1.

$$\begin{aligned} W(f) &\geq \text{mín}[W(h\psi), W(s)] \\ &\geq \text{mín}[\nu_k(h) + W(\psi), \nu_k(s)] \\ &> \nu_k(h) + \nu_k(\psi) = \nu_k(f), \end{aligned}$$

lo que nos da a). Luego tenemos la equivalencia entre a) y b).
Por esta equivalencia tenemos que $\psi(x)$ satisface la Definición 5.11 (de polinomio clave sobre ν_k). Finalmente podemos asignar a $\psi(x) = \phi_{k+1}$ el nuevo valor

$$\mu_{k+1} = W(\psi) > \nu_k(\psi),$$

satisfaciendo la desigualdad, y entonces construimos la valoración aumentada $\nu_{k+1} = [\nu_k, \nu_{k+1}\phi_{k+1} = \mu_{k+1}]$. Será una valoración inductiva si se verifican las condiciones I y II de la Definición 5.16.
Como hemos escogido $\phi_{k+1} = \psi$ y por la hipótesis de inducción en 2., el grado de $\phi_k(x)$ no puede ser mayor que el de ϕ_{k+1}, así que tenemos $deg(\phi_i(x)) \geq deg(\phi_{i-1}(x))$ (condición I de Definición 5.16).
Para la condición II, veamos que es falsa sólo si ϕ_{k+1} y ϕ_k son equivalentes en ν_k, en otras palabras sólo si

$$\nu_k(\phi_k - \phi_{k+1}) > \nu_k(\phi_k) = \nu_k(\phi_{k+1}).$$

Por 2. y 3., y la elección de ψ ($W(\psi(x)) > \nu_k(\psi(x))$), implica que

$$\begin{aligned} W(\phi_k) &\geq \text{mín}[W(\phi_{k+1}), W(\phi_k - \phi_{k+1})] \\ &> \text{mín}[\nu_k(\phi_{k+1}), \nu_k(\phi_k)] \\ &= \nu_k(\phi_k) = W(\phi_k). \end{aligned}$$

Contradicción, luego tendríamos la condición II.
La valoración inductiva ν_{k+1} así construida satisface condiciones análogas a

1., 2. y 3.. Las dos últimas consecuencias se obtienen a partir de $W(\psi(x)) > \nu_k(\psi(x))$ y de $\mu_{k+1} = W(\psi) > \nu_k(\psi)$, mientras que 1. se sigue de la definición de valoración aumentada ν_{k+1} (5.13) y del axioma triangular para W

$$W\left(\sum_{i=0}^{m} f_i(x)\psi^i\right) \geq \min_i[W(f_i(x)) + i\mu_{k+1}] = \nu_{k+1}\left(\sum_{i=0}^{m} f_i(x)\psi^i\right).$$

La construcción inductiva de la valoración ν_k asociada a W está completa. Este proceso o bien dará finalmente una valoración inductiva ν_k igual a W o dará una sucesión infinita de valoraciones inductivas con una valoración límite ν_∞ tal que

$$W(f(x)) \geq \nu_\infty(f(x)) = \lim_{k\to\infty} \nu_k(f(x)) \qquad (\forall f(x)).$$

En el caso discreto la desigualdad estricta nunca ocurre.
En efecto, supongamos que se cumple para algún $f(x)$; entonces ya que $\{\nu_k(f)\}$ es monótona no decreciente

$$W(f(x)) > \nu_k(f(x)) \qquad (k = 1, 2, \ldots).$$

La equivalencia entre a) y b) implica que $f(x)$ es divisible-equivalente en ν_k por $\phi_{k+1}(x)$. Por la monotonía del Teorema 5.14 tenemos que

$$\nu_{k+1}(f(x)) > \nu_k(f(x)) \qquad (k = 1, 2, \ldots).$$

Esto no es cierto si los grados de los polinomios clave $\phi_k(x)$ disminuyen indefinidamente, luego estamos en el caso donde $\phi_k(x)$ tenga grado fijo M para $k > t$. La sucesión monótona creciente $\{\nu_k(f(x))\}$ consta de todos los números del grupo discreto Γ_t, tal que

$$W(f(x)) \geq \nu_\infty(f(x)) = \lim_{k\to\infty} \nu_k(f(x)) = \infty.$$

Ésto solo ocurre si $f(x) = 0$, caso trivial. En consecuencia, $W = \nu_\infty$, y queda demostrado el teorema. $\square$

Capítulo 6

Criterios de Irreducibilidad

Vamos ahora a exponer algunas aplicaciones de las valoraciones sobre polinomios, más en particular vamos a estudiar algunos criterios de irreducibilidad de polinomios.
El criterio que vamos a estudiar más en profundidad va a ser el criterio de Eisenstein.
Consideramos las valoraciones sobre cualquier anillo $K[x]$ de polinomios en x con coeficientes en el cuerpo K, suponiendo que K tenga valoraciones discretas como las que hemos estudiado en el capítulo anterior.
Recordemos primero el Criterio:

Teorema 6.1 (Criterio de irreducibilidad de Eisenstein) *Si tenemos el siguiente polinomio con coeficientes enteros:*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

y un número primo p tal que

- *p divide a todo a_i para $i \neq n$*
- *p no divide a a_n*
- *p^2 no divide a a_0*

entonces $f(x)$ es irreducible sobre $\mathbb{Q}[x]$.

Demostración:
Sea p primo que cumple las condiciones del Teorema, consideramos ν_0 una valoración p-ádica (recordar definición ejemplo 2.13) sobre $\mathbb{Q}$, tal que $\nu_0(p) = n$.

Consideramos $\nu_1 = [\nu_0, \nu_1(x) = 1]$ la valoración de $\mathbb{Q}[x]$ como la construimos en el anterior capítulo. Vamos a calcular el valor de $f(x)$:

$$\begin{aligned}\nu_1(f(x)) &= \min_i\{\nu_0(a_i) + i\} \\ &= \min\{\nu_0(a_n) + n, \nu_0(a_{n-1}) + n - 1, \ldots, \nu_0(a_1) + 1, \nu_0(a_0)\}.\end{aligned}$$

Como p no divide a a_n y ν_0 es una valoración p-ádica tenemos que

$$\nu_0(a_n) = 0.$$

También como p divide al resto de los a_i

$$\nu_0(a_i) \geq n \qquad\qquad \forall i \in \{1, 2, \ldots, n-1\}.$$

Por último como p^2 no divide a a_0

$$\nu_0(a_0) = n.$$

Por tanto tenemos que

$$\nu_1(f(x)) = n.$$

Supongamos ahora por $\boxed{\text{R.A.}}$ que $f(x) = g(x)h(x)$ reducible con g y h no constantes en $\mathbb{Z}[x]$. Pongamos $g(x) = b_r x^r + \cdots + b_1 x + b_0$ y $h(x) = c_s x^s + \cdots + c_1 x + c_0$ ($r < n$ y $s < n$). Donde $p \nmid b_r, c_s$ y p divide a b_0 o c_0 pero no a los dos. Podemos suponer sin pérdida de generalidad que $p \mid b_0$ y $p \nmid c_0$, entonces

$$\nu_1(g(x)) = \min\{\nu_0(b_r) + r, \nu_0(b_{r-1}) + r - 1, \ldots, \nu_0(b_1) + 1, \nu_0(b_0)\} \leq r$$

y

$$\nu_1(h(x)) = \min\{\nu_0(c_s) + s, \nu_0(c_{s-1}) + s - 1, \ldots, \nu_0(c_1) + 1, \nu_0(c_0)\} = 0.$$

Luego

$$n = \nu_1(f(x)) = \nu_1(g(x)h(x)) = \nu_1(g(x)) + \nu_1(h(x)) = r + 0 < n.$$

Llegando a una contradicción. $\square$

Este criterio fue publicado de manera independiente por Eisenstein en 1850 y por Schönemann en 1846 como un corolario del siguiente criterio menos conocido (ver [5]):

Teorema 6.2 (Schönemann) *Supongamos que un polinomio $f(x) \in \mathbb{Z}[x]$ es de la forma $f(x) = \phi(x)^e + pM(x)$, donde p es un número primo, $\phi(x)$ es un polinomio irreducible módulo p y $M(x)$ es un polinomio relativamente primo con $\phi(x)$ módulo p, con $\deg(M) < \deg(f)$. Entonces $f(x)$ es irreducible sobre $\mathbb{Q}[x]$.*

Después de Eisenstein y Schöneman fueron muchos los matemáticos que dieron criterios de irreducibilidad que generalizan el de Eisenstein–Schöneman o que se basan en el uso del polígono de Newton. Desde Königsberger en 1895 hasta Ore en 1925, pasando por Netto, Dumas y Kurschak.
En 1938 MacLane ([3]) usó sus trabajos ([2, 4]) sobre la extensión de valoraciones de un cuerpo K a $K[x]$ para generalizar todos los criterios de irreducibilidad que acabamos de referir. El resultado es el siguiente:

Teorema 6.3 (MacLane 1938) *Si ν_k es un valor inductivo con un último polinomio clave ϕ_k, y si un polinomio $G(x)$ tiene expansión*

$$G(x) = g_m(x)\phi_k^m + g_{m-1}(x)\phi_k^{m-1} + \cdots + g_0(x),$$

en términos de ϕ_k tal que:

(I) $g_m(x) = 1$.

(II) $\nu_k(G) = \nu_k(\phi_k^m) = \nu_k(g_0)$.

(III) *Si $n < m$ es un entero positivo, entonces $n\mu_k$ no está en el grupo de valores Γ_{k-1}.*

Entonces $G(x)$ es un polinomio clave para ν_k y, en consecuencia, es irreducible.

Este resultado generaliza el criterio de Eisenstein, para $[\nu_0(p) = m, \nu_1(x) = 1]$, el de Schönemann, con $[\nu_0(p) = m, \nu_1(x) = 0, \nu_2(\phi) = 1]$, y el resto de criterios a los que nos hemos referido más arriba.
Incluso permite construir ejemplos de polinomios irreducibles para los que no pueden usarse los criterios anteriores. Por ejemplo:

Ejemplo 6.4 *La valoración inductiva*

$$[\nu_0(p) = 4, \nu_1(x) = 0, \nu_2(x^2+1) = 2, \nu_3((x^2+1)^2+p) = 5] \text{ con } (p = 3)$$

demuestra que el polinomio

$$f(x) = x^8 + 4x^6 + 12x^4 + 25x^2 + 25 = [(x^2+1)^2+p]^2 + p^2(x^2+1)$$

es irreducible sobre $\mathbb{Q}$.

Gracias a los ejemplos 5.10 y 5.17, hemos visto que,

$$\nu_3(f) = \nu_3(\phi_3^2) = \nu_3(f_0) = \nu_3(p^2(x^2+1)) = 10,$$

y está claro que $f_2 = 1$*, luego tenemos las dos primeras condiciones del Teorema de MacLane. Sólo falta ver la tercera condición.*
Como $m = 2$ *entonces* $n = 1$, $\mu_3 = \nu_3(\phi_3) = 5$. *Por tanto, tenemos que ver que* 5 *no está en el grupo de valores* Γ_2.
$\Gamma_0 =$ *grupo de valores de* $\nu_0 = Im(\nu_0) = \mathbb{Z}4$ *(Los múltiplos de 4)*
$\Gamma_1 =$ *grupo de valores de* $\nu_1 = Im(\nu_1)$*, como*

$$\nu_1(f) = \min_i\{\nu_0(a_i)\} \Longrightarrow Im(\nu_1) = \mathbb{Z}4.$$

$\Gamma_2 =$ *grupo de valores de* $\nu_2 = Im(\nu_2)$*, si* $f(x) = \sum a_i(x)\phi_2^i(x)$*, sabiendo que* $\nu_2(\phi_2) = 2$

$$\nu_2(f) = \min_i\{\nu_1(a_i) + i2\} \Longrightarrow Im(\nu_1) \subset \mathbb{Z}2.$$

Luego como $\Gamma_2 \subset \mathbb{Z}2$, $5 \notin \Gamma_2$. *Así se cumple la tercera condición y* $f(x)$ *es irreducible.*

Apéndice A

Grupos y anillos

En esta sección vamos a recordar algunas definiciones que supondremos conocidas en todo el trabajo.

Definición A.1 *Un grupo es un par $(G, *)$, donde $G \neq \emptyset$ es un conjunto y $*$ es una operación interna binaria que cumple las siguientes propiedades:*

1. *Propiedad asociativa*
2. *Elemento neutro*
3. *Elemento opuesto*

Además, el grupo G se dice abeliano si verifica lo siguiente

4. *Propiedad conmutativa*

Definición A.2 *Decimos que una aplicación entre dos grupos $f : (G, *) \to (H, \circ)$ es un homomorfismo si $f(a * b) = f(a) \circ f(b)$ $\forall a, b \in G$. Un isomorfismo es un homomorfismo biyectivo.*

Definición A.3 *Sea G un grupo. El orden de un elemento $a \in G$ es el menor entero positivo n tal que*

$$\underbrace{a * a * \ldots * a}_{n} = \varepsilon.$$

Donde ε es el elemento neutro.
Si n existe, se dice que a es un elemento de torsión . En otro caso, se dice que a tiene orden infinito.

Definición A.4 *Sea $(G, *)$ un grupo. Diremos que un subconjunto no vacío $H \subset G$ es un subgrupo de G si $(H, *)$ es un grupo. En este caso escribiremos $H \leq G$.*

Definición A.5 *Un anillo es una terna $(A, \cdot, +)$ donde $+$ y $\cdot$ son operaciones internas definidas en el conjunto A y que verifican*

1. *$(A, +)$ es un grupo abeliano.*
2. *$(A, \cdot)$ es un semigrupo.*
3. *Se tiene la propiedad distributiva (a izquierda y derecha) del producto respecto de la suma.*

Diremos que $B \subset A$ es un subanillo de A, si $(B, \cdot, +)$ es un anillo.

Definición A.6 *Un cuerpo es un anillo con elemento unidad tal que $A \backslash \{0\}$ también es grupo abeliano.*

Definición A.7 *Un elemento a en un anillo R es divisor de cero a izquierda si $\exists b \neq 0$ en R tal que $ab = 0$ y es divisor de cero a derecha si $\exists b \neq 0$ tal que $ba = 0$. Diremos que a es divisor de cero si lo es a izquierda y a derecha.*

Definición A.8 *Si R es un anillo conmutativo con unidad y no tiene divisores de cero decimos que R es un dominio íntegro o dominio de integridad.*

Definición A.9 *Sea A un anillo y $S \subset A$, decimos que S es un conjunto multiplicativo si $1 \in S$ y $st \in S$ $\forall s, t \in S$.*

Definición A.10 *Sea A un anillo y S un conjunto multiplicativo. Introducimos la siguiente relación en $A \times S$*

$$(a, s) \sim (b, t) \Leftrightarrow \exists u \in S \text{ tal que } u(at - bs) = 0,$$

$\sim$ es una relación de equivalencia. Escribimos a/s para la clase de (a, s). Notemos que la relación $at = bs$ no es de equivalencia. Entonces el anillo de fracciones de A con respecto a S es:

$$S^{-1}A = (A \times S)/\sim .$$

Con las operaciones definidas por las usuales en fracciones

$$a/s \pm b/t = (at \pm bs)/st \text{ y } a/s \cdot b/t = ab/st.$$

Definición A.11 *Un ideal en un anillo A es un subconjunto $I \subset A$ tal que $0 \in I$ y $af + bg \in I \quad \forall a, b \in A$ y $f, g \in I$.*

Definición A.12 *Decimos que un ideal P es un ideal primo si $P \neq A$ y $fg \in P \Rightarrow f \in P$ o $g \in P$.*

Definición A.13 *Decimos que un ideal I es un ideal maximal si $I \neq A$ y si los únicos ideales que los contienen son I y A.*

Definición A.14 *Un anillo A es local si tiene un único ideal maximal M*

Observación A.15 *A es local $\Leftrightarrow$ A tiene un único ideal maximal $\Leftrightarrow$ los no invertibles de A forman un ideal.*

Definición A.16 *Sea W anillo, Q su cuerpo de fracciones, $P \subset W$ ideal primo*

$$W_P = \{a/b : b \notin P\}$$

es el anillo localizado de W en P.

Definición A.17 *Sea A anillo local, se llama cuerpo residual a*

$$k(A) = A/max(A).$$

Definición A.18 *Subgrupo de torsión de un grupo abeliano consiste en el subgrupo formado por todos los elementos de orden finito.*

Definición A.19 *Un álgebra sobre un cuerpo K, o una K-álgebra, es un espacio vectorial A sobre K compatible con una estructura de anillo.*

Definición A.20 *Un cuerpo F se dice algebraicamente cerrado si cada polinomio de grado al menos 1, con coeficientes en F, tiene un cero en F.*

Definición A.21 *Sea $A \subset B$ una extensión de anillos. Un elemento $b \in B$ es llamado entero sobre A, si satisface una ecuación mónica*

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0, \quad n \geq 1$$

con coeficientes $a_i \in A$. El anillo B es llamado entero sobre A si todo elemento $b \in B$ es entero sobre A. Sea

$$\bar{A} = \{b \in B : b \text{ entero sobre } A\}.$$

A se dice que es integramente cerrado en B si $\bar{A} = A$.

Definición A.22 *Un anillo A es noetheriano si todos sus ideales son finitamente generados*

Lema A.23 (Lema de Zorn) *Si un conjunto A es inductivo, esto es, si toda cadena de A esta mayorada en A, entonces A admite al menos un elemento maximal.*

Teorema A.24 (Teorema de la base de Hilbert) *Si A es noetheriano, entonces el anillo $A[x]$ de polinomios es noetheriano. Mismo resultado para $A[[x]]$ anillo de series formales.*

La desmostración de este resultado en [7].

Bibliografía

[1] Vaquié, M., *Valuations*, 1998.

[2] MacLane, S., *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. 40 (1936), no. 3, 363–395.

[3] MacLane, S., *The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals*, Trans. Amer Math. Soc. 43 (1938) 226–239.

[4] MacLane, S., *Abstract absolute values which give new irreducibility criteria*, Trans. Amer Math. Soc., 21, págs. 472–474, 1935.

[5] N. C. Bonciocat, *Schönemann-Eisenstein-Dumas-type irreducibility conditions that use arbitrarily many prime numbers*, Comm. Algebra 43 (2015), no. 8, 3102–3122.

[6] T. Rella, *Ordnungsbestimmungen in Integritätsbereichen und Newtonsche Polygone*, Journal für die Mathematik, vol. 158 (1927), pp. 33-48.

[7] M.F. Atiyah, I. G. MacDonald *Introducción al álgebra conmutativa*, (1969), p. 90.

[8] `http://www.mate.unlp.edu.ar/~demetrio/Monografias/Materias/EA/24.%20Enteros%20Algebraicos%20-%20Gabriela%20Ravenna%20-%202008.pdf`