Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Matemática

Anillos de valuación y sus aplicaciones

TESIS

Para optar el Título Profesional de Licenciado en Matemática

AUTOR

César Ronald Osmar VILLALTA CUETO

ASESOR

Dr. Gabriel Armando MUÑOZ MÁRQUEZ

Lima, Perú

2023

Referencia bibliográfica

Villalta, C. (2023). *Anillos de valuación y sus aplicaciones*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Matemática]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	César Ronald Osmar Villalta Cueto
Tipo de documento de identidad	DNI
Número de documento de identidad	71430849
URL de ORCID	No aplica
Datos de asesor	
Nombres y apellidos	Gabriel Armando Muñoz Márquez
Tipo de documento de identidad	DNI
Número de documento de identidad	44444774
URL de ORCID	https://orcid.org/0000-0001-5064-1250
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Alfonso Pérez Salvatierra
Tipo de documento	DNI
Número de documento de identidad	06445739
Miembro del jurado 1	
Nombres y apellidos	Leonardo Henry Alejandro Aguilar
Tipo de documento	DNI
Número de documento de identidad	43069051
Datos de investigación	
Línea de investigación	A.3.1.3. Álgebra

Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	Universidad Nacional Mayor de San Marcos País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Coordenadas geográficas Latitud: -12.058333 Longitud: -77.083333
Año o rango de años en que se realizó la investigación	Mayo 2023 – octubre 2023
URL de disciplinas OCDE	Matemáticas puras https://purl.org/pe-repo/ocde/ford#1.01.01 Matemáticas aplicadas https://purl.org/pe-repo/ocde/ford#1.01.02

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE CIENCIAS MATEMÁTICAS
ESCUELA PROFESIONAL DE MATEMÁTICA

ACTA DE SUSTENTACIÓN DE TESIS PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE LICENCIADO(A) EN MATEMÁTICA (PROGRAMA DE TITULACIÓN PROFESIONAL 2023)

En la UNMSM – Ciudad Universitaria – Facultad de Ciencias Matemáticas, siendo las 10:00 horas del viernes 27 de octubre del 2023, se reunieron los docentes designados como Miembros del Jurado Evaluador (PROGRAMA DE TITULACIÓN PROFESIONAL 2023): Dr. Alfonso Pérez Salvatierra (PRESIDENTE), Dr. Leonardo Henry Alejandro Aguilar (MIEMBRO) y el Dr. Gabriel Armando Muñoz Márquez (MIEMBRO ASESOR), para la sustentación de la Tesis titulada: "**ANILLOS DE VALUACIÓN Y SUS APLICACIONES**", presentado por el señor **Bachiller CÉSAR RONALD OSMAR VILLALTA CUETO**, para optar el Título Profesional de Licenciado en Matemática.

Luego de la exposición de la Tesis, el Presidente invitó al expositor a dar respuesta a las preguntas formuladas.

Realizada la evaluación correspondiente por los Miembros del Jurado Evaluador, el expositor mereció la aprobación Sobresaliente, con un calificativo promedio de Dieciocho (18)

A continuación, los Miembros del Jurado Evaluador dan manifiesto que el participante **Bachiller CÉSAR RONALD OSMAR VILLALTA CUETO** en vista de haber aprobado la sustentación de su Tesis, será propuesto para que se le otorgue el Título Profesional de Licenciado en Matemática.

Siendo las 10:45 horas se levantó la sesión firmando para constancia la presente Acta.

Dr. Alfonso Pérez Salvatierra
PRESIDENTE

Dr. Leonardo Henry Alejandro Aguilar
MIEMBRO

Dr. Gabriel Armando Muñoz Márquez
MIEMBRO ASESOR

Yo Gabriel Armando Muñoz Márquez en mi condición de asesor acreditado con la Resolución Decanal N° 001653-2023-D-FCM/UNMSM de la tesis, cuyo título es ANILLOS DE VALUACIÓN Y SUS APLICACIONES, presentado por el bachiller César Ronald Osmar Villalta Cueto para optar el título Profesional de Licenciado en Matemática de la Facultad de Ciencias Matemáticas.

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 6 % de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título correspondiente.

Firma del Asesor ____________________

DNI: 44444774

Nombres y apellidos del asesor:
Gabriel Armando Muñoz Márquez

Agradecimiento

Agradezco, principalmente a Dios, por ayudarme
a mantenerme firme hasta la finalización del trabajo;
a mi madre Cecilia por siempre darme los ánimos necesarios para continuar
asimismo, agradezco a mi asesor, el Dr. Gabriel Muñoz,
por sus enseñanzas, consejos y sugerencias
que me sirvieron para terminar este proyecto.

Índice general

Resumen

En este trabajo, presentamos el concepto de anillo de valuación y estudiamos sus principales propiedades.
Además, presentamos un resultado muy importante sobre la existencia de anillos de valuación que contienen un anillo dado. Como consecuencia de la teoría de anillos de valuación, presentaremos diversas aplicaciones, principalmente relacionadas a extensiones de cuerpos.
Palabras clave: Anillos de valuación, anillos locales, extensiones de cuerpos, cuerpos de funciones.

Abstract

In this paper, we present the concept of valuation ring and study its main properties. In addition, we present a very important result about the existence of valuation rings that contain a given ring. As a consequence of the valuation ring theory, we will present various applications, mainly related to field extensions.

Keywords: Valuation rings, local rings, field extensions, function fields.

Introducción

Los anillos de valuación representan un interesante y relevante tema dentro del Álgebra. Estas estructuras algebraicas despiertan el interés debido a sus propiedades únicas y aplicaciones en diversas áreas del conocimiento.

Un anillo de valuación puede obtenerse a partir de una función cuyo dominio es un cuerpo, la cual asigna a cada elemento un valor en un conjunto ordenado, el cual puede ser, por ejemplo, el conjunto de los números enteros. Esta función de valuación mide el tamaño relativo de los elementos del anillo, lo que resulta fundamental en el estudio de propiedades algebraicas y aritméticas.

El concepto de anillos de valuación encuentra sus raíces en la teoría de números, específicamente en la búsqueda de extensiones de cuerpos y la clasificación de campos valuados completos. Además, estos anillos encuentran aplicaciones en la geometría algebraica, teoría de cuerpos, ecuaciones diferenciales y otras áreas de las matemáticas.

En esta investigación, nos adentraremos en la teoría de anillos de valuación, explorando sus fundamentos, características y propiedades principales. Además, abordaremos ejemplos, destacando sus implicaciones en la resolución de problemas matemáticos y su influencia en el desarrollo de otras ramas de la Matemática.

En el estudio de los anillos de valuación, podemos apreciar la elegancia y profundidad del Álgebra, así como la versatilidad y aplicabilidad de estas estructuras matemáticas. La comprensión de este tema nos abrirá las puertas para abordar desafíos matemáticos más complejos y, al mismo tiempo, nutrirá nuestra capacidad para analizar y resolver problemas en contextos teóricos y prácticos.

Este trabajo estará organizado de la siguiente forma: en el Capítulo 1 presentamos definiciones y resultados previos necesarios para la posterior comprensión de los anillos de valuación; en el Capítulo 2 estudiaremos precisamente los anillos de valuación dando a conocer su definición, algunos resultados importantes, pero sobre todo el teorema de existencia de anillos de valuación; en el Capítulo 3 presentamos algunas aplicaciones correspondientes a los anillos de valuación, precisamente fundamentados en el teorema de existencia de anillos de valuación. Así, para nuestro objetivo planteado, primero definiremos los anillos de valuación y demostramos la existencia de los anillos de valuación. Finalmente mostramos algunas aplicaciones sobre nuestros resultados, así como también proyectos a futuro sobre el tema.

Capítulo I

Preliminares

En este capítulo daremos a conocer un breve y resumido repaso sobre las herramientas principales y necesarias que se deben conocer para tener un mejor entendimiento de los anillos de valuación y con ello sus diversas aplicaciones.

1.1. Anillos

Definición 1.1. *Decimos que A es un anillo (conmutativo unitario), si es un conjunto con dos operaciones binarias (adición y multiplicación)*

$$+, \cdot : A \times A \to A$$

que cumple las siguientes condiciones; para todo $a, b, c \in A$

1) $a + (b + c) = a + (b + c)$

2) $a + b = b + a$

3) Existe $0 \in A$ tal que $0 + a = a$.

4) Existe $-a \in A$ tal que $a + (-a) = 0$.

Del 1) al 4) decimos que $(A, +)$ es un grupo abeliano.

5) $a(bc) = (ab)c$.

6) Existe $1_A \in A$ tal que $1_A \cdot a = a \cdot 1_A = a$.

7) $a(b + c) = ab + ac$.

8) $(a+b)c = ac + bc$.

10) $ab = ba$

Por simplicidad denotaremos $1 = 1_A$ *cuando el anillo* A *está sobreentendido.*

Proposición 1.2. *Si* A *es un anillo y* $a \in A$ *entonces se cumple:*

1) $0a = a0 = 0$.

2) $(-1)(-a) = (-a)(-1) = a$.

3) $(-1)a = a(-1) = -a$.

4) El 1 es único.

Ejemplo 1.3. *1)* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *y* $\mathbb{C}$ *son anillos conmutativos unitarios.*

2) Dado $n \in Z$, $n > 1$, *tenemos que* $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$ *y* $\mathbb{C}^n$ *son anillos conmutativos.*

3) Si $x, y \in \mathbb{R}$ *con* $x < y$ *entonces* $C^\infty(x,y)$ *es un anillo conmutativo unitario.*

Donde $C^\infty(x,y)$ *es el conjunto de funciones reales infinitamente diferenciables en el intervalo* (x,y).

1.1.1. Subanillos

Ahora veremos la difiniión y resultados sobre subanillos.

Definición 1.4. *Sea* A *un anillo, un subanillo* S *es un subconjunto* $S \subset A$ *tal que* S *es un anillo bajo las operaciones de* A, *donde* $1_S = 1_A$.

Proposición 1.5. *Dado* $S \subset A$ *subconjunto,* S *es subanillo si cumple lo siguiente*

1) $1 \in S$.

2) $a, b \in S$ *entonces* $a - b \in S$.

3) $a, b \in S$ *entonces* $ab \in S$.

Ejemplo 1.6. *1) Tenemos que* $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

2) Si $xy, \in \mathbb{R}$ *con* $x < y$, *entonces para todo* $k \in \mathbb{Z}$, $k \geq 0$, $C^\infty(x,y)$ *y* $C^{k+1}(x,y)$ *son subanillos de* $C^k(x,y)$.

1.2. Ideales

Ahora veremos ña definición y resultados sobre ideales.

Definición 2.7. *Sea A un anillo. Decimos que un ideal I de A es un subconjunto $I \subset A$ tal que cumple lo siguiente:*

1) I es un subgrupo aditivo de A.

2) Para todo $a \in A$ y $i \in I$, entonces $ai \in I$.

Además, si $I \neq A$ decimos que I es un ideal propio.

Definición 2.8. *Sea I un ideal de A. Decimos que I es un ideal primo, si $I \subset A$ y para $x, y \in A$: $xy \in I$ entonces $x \in I$ o $y \in I$.*

Definición 2.9. *Sea I un ideal de A. Decimos que I es un ideal maximal, si $I \subset A$ y para todo J ideal de A: $I \subset J$ implica $J = I$ o $J = A$.*

Definición 2.10. *Sea A un anillo ; decimos que el ideal generado por un elemento i está dado por:*

$$(i) = \{ai : \quad a \in A\}.$$

Definición 2.11. *Sea I un ideal de A. Decimos I que es un ideal principal, si existe $a \in A$ tal que I es generado por a.*

Definición 2.12. *Sea A un anillo; decimos que A es dominio integral si no tiene divisores de cero; es decir si:*

$$ab = 0 \text{ entonces } a = 0 \text{ o } b = 0$$

Proposición 2.13. *Sea A un anillo e I un ideal propio de A, tenemos que I es primo si y solo si A/I es dominio integral.*

Definición 2.14. *Decimos que K es un cuerpo; si es un conjunto no vacío con las operaciones de adición y multiplicación que cumplen con las siguientes condiciones; para todo $a, b, c \in K$.*

1) $a + (b + c) = a + (b + c)$

2) $a + b = b + a$

3) Existe $0 \in K$ *tal que* $0 + a = a$.

4) Existe $-a \in K$ *tal que* $a + (-a) = 0$.

Del 1) al 4) decimos que $(K, +)$ *es un grupo abeliano.*

5) $a(bc) = (ab)c$.

6) Existe $1 \in K$ *tal que* $1 \cdot a = a \cdot 1 = a$.

7) $ab = ba$.

8) Para todo $a \in K$ *existe* $a^{-1} \in K$ *tal que* $aa^{-1} = a^{-1}a = 1$.

Del 5) al 8) decimos que $(K^*; \cdot)$ *es un grupo abeliano. Nota* $K^* = K - \{0\}$.

9) $a(b + c) = ab + ac$.

Proposición 2.15. *Sea* A *un anillo e* I *un ideal propio de* A*, tenemos que* I *es maximal si y solo si* A/I *es un cuerpo.*

Proposición 2.16. *Sea* A *un anillo e* I *un ideal propio de* A*; tenemos que si* I *es maximo entonces es maximal.*

Proposición 2.17. *Sea un anillo* A *e* I *un ideal propio de* A*; tenemos que si* I *es maximal entonces* I *es primo.*

Teorema 2.18. *Sea* $A \neq \emptyset$ *anillo, se tiene que al menos un ideal es maximal.*

Definición 2.19. *Sea* A *un anillo;* I *y* J *ideales de* A*; decimos que* $I + J$ *está dado por:* $I + J := \{i + j : \quad i \in I, j \in J\}$.

Teorema 2.20. *Sea* I *y* J *ideales de* A*; entonces* $I + J$ *es un ideal de* A.

Teorema 2.21. *La intersección de ideales es un ideal.*

Definición 2.22. *Sean* A*,* B *anillos; dada la aplicación* $f : A \to B$ *es homomorfismo de anillos si para todo* $a_1, a_2 \in A$ *se cumple lo siguiente :*

1) $f(a_1 + a_2) = f(a_1) + f(a_2)$.

2) $f(a_1 a_2) = f(a_1)f(a_2)$.

3) $f(1) = 1$.

Definición 2.23. *Sea $f : A \to B$ un homomorfimos de anillos; definimos el núcleo de f $(Ker(f))$ como*

$$Ker(f) := \{a \in A : \quad f(a) = 0\}$$

Teorema 2.24. *Sea $\varphi : A \to S$ un homomorfismo de anillos, entonces el $Ker\varphi$ es un ideal de A.*

Teorema 2.25. *Sea A un anillo, tenemos que A es un campo si y solo si sus únicos ideales son $\{0\}$ y A.*

Ejemplo 2.26. *Sea A un anillo y $a_1, a_2, \cdots, a_n \in A$ entonces:*

$$(a_1, a_2, \cdots, a_n) = \{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n : \quad x_i \in A\}$$

es un ideal de A.

1.3. Anillo local

Ahora veremos la definición y resultados sobre anillo local.

Definición 3.27. *Sea A un anillo, se dice que A es un anillo local si posee un único ideal maximal.*

Proposición 3.28. *Los siguientes enunciados son equivalentes a la definición anterior.*

1) *Si la suma de dos elementos cualesquiera de A que no seas unidades no es tampoco una unidad.*

2) *Si a un elemento que pertenece a A, entonces a o $1 - a$ es una unidad.*

3) *Si una suma finita es una unidad, entonces alguno de sus sumandos será unidad.*

Proposición 3.29. *Sea A un anillo y $I \neq A$ un ideal de A que cumple que para cada $x \in A - I$ es una unidad en A, entonces A es un anillo local y I su ideal maximal.*

Proposición 3.30. *Sea A un anillo y I un ideal maximal de A tal que cada elemento de $1 + I$ es una unidad en A; entonces A es un anillo local.*

Ejemplo 3.31. *Si C es un cuerpo y $n \in \mathbb{Z}$, $n > 0$, entonces el anillo cociente $C[x]/ < x^n >$ es local y su ideal maximal son las clases representadas por polinomios con término constante nulo.*

1.4. Extensiones Integrales

Ahora veremos la definición y resultados sobre extensiones integrales.

Definición 4.32. *Sea A un anillo, S un subanillo de A. Sea $x \in A$, se dice que x es integral sobre S, si x es una raiz de un polinomio mónico con coeficientes en S. Es decir, x satisface una ecuación de la forma $x^n + a_1x^{n-1}a_2x^{n-2} + \cdots + a_n = 0$ onde $a_i \in S$.*

Observación 4.33. *Todo elemento de S es integral sobre S.*

Definición 4.34. *Sea A un anillo; decimos que un A-módulo a la izquierda es un grupo abeliano $(M; +)$ on aplicación:*

$$A \times M \to M$$

$$(r, x) \to rx$$

para todo $r, s \in A$; para todo $x, y \in M$, que cumple lo siguiente:

1) $r(sx) = (rs)x$

2) $(r + s)x = rx + sx$

3) $r(x + y) = rx + ry$

4) $1 \cdot x = x$

Definición 4.35. *Sea A-módulo M; decimos que es finitamente generado si existe un subconjunto $S \subset M$ tal que*

$$\langle S\rangle = M$$

donde $\langle S\rangle := \{a_1x_1 + \cdots a_nx_n : \quad n \in \mathbb{N}, a_i \in A, x_i \in S, 1 \leq i \leq n\}$

Proposición 4.36. *Los siguientes enunciados son equivalentes.*

1) Si $x \in A$ es integral sobre S.

2) $S[x]$ es un módulo finitamente generado.

3) $S[x] \subset R$, donde R es un subanillo de A, tal que se tiene que R es un S-módulo finitamente generado.

4) Existe un $S[x]$-módulo M que se genera finitamente como un módulo S.

Corolario 4.37. *Sea el conjunto R de elementos de A que son integrales sore S, es un subanillo de A que contiene a S.*

Definición 4.38. *El anillo R anterior se llamará clausura integral de S en A.*

Definición 4.39. *Si $R = S$, entonces decimos que S es integralmente cerrado en A.*

Corolario 4.40. *Si se tiene que $S \subseteq A \subseteq R$ son anillos; además si A es integral sobre S y R es extensión sobre A; entonces R es extensión integral sobre S (transitividad de a extensión integral).*

Teorema 4.41. *Si $S \subseteq A$ dominios integrales, además A es integral sobre S, entonces A es un cuerpo si y solo si S es un cuerpo.*
Demostración. Ver [2]

Ejemplo 4.42. *Sea $S = \mathbb{Z}$ y $A = \mathbb{Q}$. Si un número racional $x = \dfrac{p}{q}$ es integral sobre $\mathbb{Z}$, donde p, q no tienen factor común, tenemos que*

$$p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0$$

donde a_i son enteros racionales.

Por tanto, q divide p^n, por tanto $q = \pm 1$, por tanto $x \in \mathbb{Z}$.

1.5. Dominio Integralmente Cerrado

Ahora veremos la definición y resultados sobre dominio integralmente cerrado.

Definición 5.43. *Decimos que un dominio integralmen es integralmente cerrado, si es integralmente cerrado en su campo de fracciones.*

Proposición 5.44. *Sea D un dominio integral, entonces decimos que los siguientes enunciados son equivalentes:*

1) D es integramente cerrado.

2) D_p es integralmente cerrado para cada ideal primo p.

3) D_m es integralmente cerrado para cada ideal maximal m.
Demostración. Ver [2]

Ejemplo 5.45. *$\mathbb{Z}$ es integralmente cerrado.*

1.6. Cuerpo de Funciones de una Variable

Ahora veremos la definición y resultados sobre un cuerpo de funciones de una variable.

Definición 6.46. *Tenemos que K/k es una extensión de campo, decimos que K es un campo de función de una variable sobre k si K/k es finitamente generado y además de grado de transcendencia 1.*

Observación 6.47. *Se tiene un caso importante, cuando $K = k(x)$ donde x es transcendental sobre k, es decir, cuando K/k puede ser generado por un solo elemento. Dicho campo de función se le llamará racional sobre k.*

Definición 6.48. *Sea $r(x) \in k(x)$ función racional, la cual podemos expresar como $r(x) = \dfrac{p(x)}{q(x)}$; donde p, q son polinomios coprimos en $k[x]$.*

El valor grado $(r) := \text{máx}\{grado(p), grado(q)\}$ se le llamará grado de $r(x)$.

Teorema 6.49. *Si $r(x) \in k(x)$ es una función racional no constante, entonces la extensión $k(x)/k(r(x))$ es finita de grado igual a grado(r).*
Demostración. Ver [2]

1.7. Extensiones Algebraicas de Cuerpos

Ahora veremos la definición y resultados sobre extensiones algebraicas de cuerpos.

Definición 7.50. *Tenemos que K un cuerpo. Si K es un subcuerpo de un cuerpo C, entonces también decimos que C es un cuerpo de extensión de K. Ahora, sea K un subcuerpo de un cuerpo C, se dice que un elemento $x \in C$ es algebraico sore K,* *si existen elementos* $a_0, a_1, \cdots, a_n \in K$ *no todos iguales a cero, tales que cumplen lo siguiente:*

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$$

Definición 7.51. *Diremos que una extensión* C *de* K *es extensión algebraica de cuerpos si a todo elemento de* C *es algebraico sobre* K*.*

Proposición 7.52. *Si* C *es una extensión finita sobre* K*, entonces* C *es algebraica sobre* K*.*

Capítulo II

Anillos de valuación

2.1. Hipótesis y consideraciones

Definición 1.1. *Sea K un campo. Decimos que un subanillo $O \subset K$ es un anillo de valoración (abr. VR) de K si:*

1. *$O \neq K$,*
2. *Para todo $x \in K \setminus O$, tenemos $x^{-1} \in O$.*

En caso de que k sea un subcampo de K, decimos que O es un VR de K/k si además $k \subset O$. El conjunto de anillos de valoración de K (resp. de K/k) se denotará por Σ_K (resp. $\Sigma_{K/k}$). Nótese que un VR O de K es en particular un dominio con campo fraccionario K.

Proposición 1.2. *Para $O \in \Sigma_K$, el conjunto $P = O \setminus O^* = \{x \in O \mid x^{-1} \notin O\}$ es un ideal maximal distinto de cero de O. En particular, O es un anillo local y P es su único ideal maximal. También nos referiremos al par (O, P) como un VR de K. El anillo cociente O/P es, por lo tanto, un campo, llamado campo residual. Si $O \in \Sigma_{K/k}$, entonces el campo k se incrusta isomórficamente en O/P bajo la función cociente.*

Prueba: Para empezar, si P fuera $\{0\}$, O sería un campo, necesariamente igual a K, lo cual es una contradicción. Sean $x \in P$ y $y \in P$. Entonces $xy \notin O^*$, de lo contrario, para alguna $z \in O$, tendríamos $xyz = 1$ y x también tendría una inversa en O. Esto prueba que $xy \in P$. Sean entonces $x, y \in P \setminus \{0\}$. Entonces, o bien $y/x \in O$ o bien $x/y \in O$, y podemos suponer, por simetría, que se cumple la primera opción. Por lo tanto, $x - y = x(1 - y/x) = xt$, con $t = 1 - y/x \in O$. Por lo tanto, en vista de lo que acabamos de ver, tenemos $x - y \in P$. Estas verificaciones muestran que P es un ideal. Como P es, por definición, el conjunto de elementos no invertibles de O, deducimos que P es el único ideal maximal de O, lo que implica que O es un anillo local. Finalmente, sea O un VR de K/k, entonces $k \subset O$. Dado que k es un campo, tenemos $k^* = k \setminus \{0\} \subset O^*$, de donde $k \cap P = \{0\}$, lo que prueba la última afirmación.

Definición 1.3. *Sea $x \in K$. Decimos que x tiene un cero en P (o en O) si $x \in P$, y que tiene un polo en P si $x^{-1} \in P$. Finalmente, decimos que x es regular en O si $x \in O$.*

Observación 1.4. *Esta definición ya anticipa la idea de ver los elementos de K como funciones en Σ_K. Sea $O \in \Sigma_K$. Sea ∞ un símbolo (asociado a O) y definamos un mapa $\varphi : K \to (O/P) \cup \{\infty\}$ enviando $x \in O$ a su clase módulo P, y $x \in K \setminus O$ (es decir, x con un polo en P) a ∞. Observa que si $x \in K \setminus O$, entonces $x^{-1} \in O \setminus O^* = P$; esto dice que φ es un 'homomorfismo' (en un sentido más amplio) si en $(O/P) \cup \{\infty\}$ adoptamos las reglas usuales $a \pm \infty = \infty$ cuando $a \in O/P$, y $a \cdot \infty = \infty$ si $a \neq 0$, $1/0 = \infty$, $1/\infty = 0$. Por otro lado, $\infty \pm \infty$ y $0 \cdot \infty$ no están definidos. La función φ se llama un lugar de K. Recíprocamente, no es difícil verificar que se puede obtener un VR O de K partiendo de un 'lugar', es decir, de un 'homomorfismo' (en un sentido más amplio) $\varphi : K \to \tilde{K} \cup \{\infty\}$, donde $\tilde{K}$ es un campo; en tal situación, se pone $O = \varphi^{-1}(\tilde{K})$. Por esta razón, vamos a ocasionalmente llamar a O en sí mismo un 'lugar de K'.*

Proposición 1.5. *El conjunto $P \subset K$ determina la VR $O \in \Sigma_K$.*

Prueba. Sean O, O' dos elementos en $\Sigma_{K/k}$ que tienen el mismo ideal maximal P. Sea $x \in O \setminus O'$. Entonces $\frac{1}{x} \in O'$, y de hecho, $\frac{1}{x}$ está en el ideal maximal de O', que es P (de lo contrario, $\left(\frac{1}{\frac{1}{x}}\right) = x$ estaría en O'. Pero entonces $1 = x \cdot \frac{1}{x} \in P$, lo cual es imposible.

Proposición 1.6. *Si $O \in \Sigma_K$, entonces O es integralmente cerrado en K. En particular, si $O \in \Sigma_{K/k}$, O contiene la clausura algebraica de k en K.*

Prueba. Sea $x \in K$, x integral sobre O, entonces existen $a_1, \ldots, a_n \in O$ tales que $x^n + a_1 x^{n-1} + \ldots + a_n = 0$. Si x no pertenece a O, tenemos $\frac{1}{x} \in O$ por definición. Pero entonces la ecuación $x = -(a_1 + \frac{a_2}{x} + \ldots + \frac{a_n}{x^{n-1}})$ muestra que $x \in O$, lo cual es absurdo. Por lo tanto, $x \in O$ en cualquier caso, demostrando la primera parte. Si, por otro lado, O es un VR de K/k, entonces contiene k. Dado que un elemento de K que es algebraico sobre k es automáticamente integral sobre k, obtenemos la parte restante de la declaración.

Un corolario importante de esta proposición se refiere a los campos de funciones de una variable, los cuales discutimos superficialmente antes.

Proposición 1.7. *Si K es un campo de función en una variable sobre el campo algebraicamente cerrado k, y si $(O, P) \in \Sigma_{K/k}$, entonces el campo residual O/P es isomorfo a k bajo la inclusión natural $k \to O$.*

Prueba. En lo que sigue identificaremos tácitamente k con su imagen isomórfica en O/P . Supongamos ahora que existe $x \in O$ tal que la imagen $\overline{x}$ de x en O/P no está en k, y por lo tanto es trascendental sobre k. Entonces $f(\overline{x}) \neq 0$ para todo polinomio distinto de cero $f \in k[X]$.

De manera equivalente, $f(x) \notin P$ para cualquier polinomio de este tipo, de donde $k(x)$ sería contenido en O. Pero $K/k(x)$ es algebraico, porque K/k tiene grado de trascendencia 1 por supuesto. (Nótese, de hecho, que x es trascendental sobre k, ya que $\overline{x}$ lo es; o bien tenga en cuenta que $f(x) = 0$ implica $f(x) \in P$, que no es el caso). Por lo tanto, K sería integral sobre O y llevaría a $O = K$, una contradicción.

Observación 1.8.

1. *Si k no es algebraicamente cerrado, un argumento similar produce que O/P es algebraica sobre k y, de hecho, una extensión finita de k.*

2. *Tenga en cuenta que la conclusión no se cumple en general para los campos de función de variedades algebraicas, concretamente para los campos de extensión K/k con grado de trascendencia finito. (Considere por ejemplo $K = k(X, Y)$ y O la VR de K que consta de las funciones racionales cuyo denominador no es divisible por X.)*

Observación 1.9 (Anillos de valoración y puntos geométricos)**.** . *Se sigue que los elementos de un campo de función K/k pueden verse como funciones con valores en $P_1(k) = k \cup \{\infty\}$, cuyo dominio es el conjunto $\Sigma_{K/k}$ de VR de K/k: si $x \in K$, el valor de $x(O)$ será ∞ si $x \notin O$, o la clase de x en el campo residual O/P de lo contrario. (Tenga en cuenta que tal clase coincide con el único elemento $a \in k$ tal que $x - a \in P$. De esta manera, los elementos de $k \subset K$ dan lugar a funciones constantes.) De esta manera, los VR se ven como puntos. Este punto de vista coincide con el habitual cuando $K = k(t)$ es el campo de funciones racionales sobre k, se muestra que los VR* *corresponden precisamente a los puntos de $P_1(k)$). Incluso cuando K es el cuerpo de funciones de una curva, existe una interpretación geométrica de los anillos de valoración como puntos. Para tomar un ejemplo, suponga que $K = k(x, y)$, donde $F(x, y) = 0$ es una ecuación irreducible sobre k. Si O es un VR de K/k que contiene x, y, y si $a, b \in k$ son las clases respectivas de x, y módulo P, luego tomando la clase de $F(x, y)$ en O/P se encuentra $F(a, b) = F(x(O), y(O)) = 0$, de modo que O 'corresponde' al punto $(a, b) \in k^2$ sobre la curva plana $F = 0$ asociada a K. En las aplicaciones del Teorema 3.16 veremos cómo en general la geometría de los puntos siempre proviene de una VR adecuada, de la manera que acabamos de ilustrar. Sin embargo, hay que tener en cuenta que esta correspondencia no es biyectiva para campos de funciones generales. Es 'casi' biyectiva (hasta en un número finito de casos, en un sentido que se aclarará más adelante) en el caso de curvas. Vea a continuación para obtener más información sobre esto.*

2.2. Algunos ejemplos significativos

Ejemplo 2.10. *$K = \mathbb{Q}$. Sea $O \in \Sigma_{\mathbb{Q}}$. Entonces $P := P \cap \mathbb{Z}$ es un ideal de $\mathbb{Z}$, que es primo porque P es primo. Si tuviéramos $P = \{0\}$, entonces cada entero distinto de cero sería invertible en O; pero entonces O contendría $\mathbb{Q}$, una contradicción. Por lo tanto, P es un ideal maximal de $\mathbb{Z}$, generado por un número primo p: $P = p\mathbb{Z}$. Entonces los enteros coprimos con p son invertibles en O y deducimos que O contiene la localización $\mathbb{Z}_P := \left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z} \setminus P\right\}$. Sea entonces $x \in O \setminus \mathbb{Z}_P$; entonces existiría una potencia positiva p^r de p con $p^r x \in \mathbb{Z}_P^* \subset O^*$, lo cual es inconsistente, porque $p^r x \in p^r O \subset P$. Por lo tanto, $O = \mathbb{Z}_P$. Recíprocamente, inmediatamente vemos que $\mathbb{Z}_P$ es una VR para cada primo p. Esto describe todas las posibilidades para una VR de $\mathbb{Q}$. Permítanos observar que el campo residual O/P es $\mathbb{F}_p$, si P corresponde al primo p. El lugar correspondiente envía un número racional r a su clase de residuo módulo p si el denominador de r es primo con p, y envía r a ∞ (∞_p) en caso contrario.*

Observación 2.11. *Los números racionales pueden verse como funciones cuyo dominio es Spec($\mathbb{Z}$) (es decir, el conjunto de ideales primos de $\mathbb{Z}$). El 'valor' del número racional x en el ideal primo distinto de cero $p\mathbb{Z}$ será la clase de x en $\mathbb{F}_p$ si $x \in \mathbb{Z}_{(p)}$ y ∞ en caso contrario. El valor de x en el ideal cero (también llamado el punto genérico en este contexto) es simplemente x. Aquí, el espacio objetivo cambia de-*

pendiendo del punto, lo cual es una diferencia importante con el caso de campos de función (ver el siguiente ejemplo), donde dicho punto de vista devuelve la noción habitual de función.

Ejemplo 2.12. *$K = k(x)$, donde x es trascendental sobre k. Sea $O \in \Sigma_{K/k}$.*

1. Supongamos que empezamos con $x \in O$, entonces $O \supseteq k[x]$. Argumentando como en el caso $K = \mathbb{Q}$ (con $k[x]$ en lugar de $\mathbb{Z}$) uno encuentra que O es un anillo localizado $k[x]_P$, donde P es un ideal maximal de $k[x]$, por lo tanto, asociado biyectivamente a un polinomio mónico irreducible $p(x) \in k[x]$. Esto produce una primera lista de VR de $k(x)/k$.

Si O está asociado al polinomio $p(x)$, el campo residual es $k[x]_P/(p(x)) \cong k[x]/(p(x))$, que es una extensión algebraica de k, de grado deg p . Si ρ es una raíz de $p(x)$ en alguna extensión campo de k, el campo residual es isomorfo a $k(\rho)$ (sobre k); el lugar asociado $\varphi = \varphi_P$ envía $r(x)$ a $r(\rho)$ ($= \infty$ si ρ es un polo de r).

Supongamos ahora que O no contiene x. Entonces $y = x^{-1} \in O$ y en realidad $y \in P$ (ya que $y^{-1} = x \notin O$). Por otro lado (como hemos visto antes) $P \cap k[y]$ es un ideal maximal de $k[y]$, necesariamente generado por y, y O coincide con el anillo localizado $k[y]_{(y)}$. Tal anillo consiste en las funciones racionales de la forma $r(y) = a(y)/b(y)$ donde a, b son polinomios y $b(0) \neq 0$. El campo de residuos ahora es $k[y]/(y) \cong k$.

Para leer esto en términos de x, pongamos $d = \text{máx}(\deg a, \deg b)$; entonces podemos escribir $r(y) = a(x^{-1})/b(x^{-1}) = A(x)/B(x)$ donde $A(x) = x^d a(x^{-1})$ y $B(x) = x^d b(x^{-1})$ son polinomios; observemos que ya que $b(0) \neq 0$, $\deg B = d$, mientras que en cualquier caso $\deg A \leq d$. En conclusión, O consta de las funciones racionales sin polo en el infinito, a saber, de la forma $A(x)/B(x)$ donde $\deg B \geq \deg A$. El lugar asociado envía una función a su valor en ∞. Esta única VR, sumada a la anterior lista, completa la clasificación.

Observación 2.13. .

i) Supongamos, por ejemplo, que k es algebraicamente cerrado. Entonces los ideales maximales de $k[x]$ están asociados biyectivamente a los polinomios $x - \alpha$, $\alpha \in k$, y por tanto a los elementos $\alpha \in k$. Por lo tanto, la clasificación muestra que los VR correspondientes corresponden a los puntos de k (en la primera lista) más el VR asociado a ∞. En otras palabras, los VR corresponden a puntos de $P_1(k)$. Un lugar $\varphi = \varphi_Q$ asociado a un punto $Q \in P_1$ envía el elemento

$r(x) \in k(x)$ a $\varphi(r) = r(Q)$, donde $r(Q)$ debe leerse como ∞ si Q es un polo de r.

Las extensiones finitas de $\mathbb{Q}$ o $k(x)$ se considerarán a continuación (los VR correspondientes amplían los del campo base).

ii) Para $K = k(x_1, \ldots, x_n)$, con x_i algebraicamente independiente sobre k, la clasificación ya es mucho más difícil para $n = 2$. A nuestro conocimiento, no ha sido formulado para $n > 2$.

Ejemplo 2.14. *$K = k((x))$. Este campo (que es el campo fraccionario del anillo formal de la serie de potencias $k[[x]]$, y se llama el campo de 'Laurent series') tiene un grado de trascendencia infinito sobre k, lo que hace que sea prácticamente imposible una clasificación general útil de los VRs de K/k. Por otro lado, existe un solo VR que contiene $k[[x]]$. De hecho, $k[[x]]$ tiene un único ideal primo $P \neq \{0\}$, generado por x, y este ideal es en realidad maximal. El VR es, como arriba, el anillo localizado, que ahora es el todo anillo: $O = k[[x]]_{((x))} = k[[x]]$, y el lugar correspondiente se asigna a una serie en $k((x))$ su valor en 0 (valor que es ∞ si la serie no está en $k[[x]]$).*

Ejemplo 2.15. *Sea D un subconjunto no vacío conexo abierto de $\mathbb{C}$ y sea K el campo de funciones meromórficas en D. Además, sea $z_0 \in D$. Entonces el conjunto $O = O_{z_0}$ de las funciones en K que son regulares en z_0 es un VR de $\mathbb{C}$. De hecho, O es un anillo diferente a K y si una función $f \in K$ no es en O, entonces tiene un polo en z_0 y por lo tanto $1/f \in O$. El ideal maximal P se compone de las funciones en K que se anulan en z_0 y $O/P \cong \mathbb{C}$. (En esta situación no es cierto que todos los VRs de K sean del tipo anterior.)*

2.3. Existencia y extensiones de anillos de valuación

El siguiente resultado será crucial en lo que sigue.

Teorema 3.16. *Sea K un campo, $A \subset K$ un subanillo y sea $I \neq \{0\}$ un ideal propio de A. Entonces existe un VR (O, P) de K tal que $A \subset O$ y $I \subset P$.*

Prueba. Ordenemos por inclusión los anillos $B \supset A$ en K tales que $IB \neq B$ (observando que A está entre ellos). Cada cadena (es decir, un subconjunto totalmente ordenado) tiene un elemento maximal, dado por la unión: de hecho, la unión

U de los anillos de la cadena es un subanillo de K que contiene A. Si tuviéramos $IU = U$, entonces 1 tendría la forma $\sum_{i=1}^{n} \omega_i u_i$, $\omega_i \in I$, $u_i \in U$. Pero entonces, tomando como B un anillo en la unión que contiene todas las u_i, tendríamos $IB = B$, una contradicción.

Por lo tanto, por el lema de Zorn, existe tal anillo O maximal bajo inclusión; contiene A y mostremos ahora que tiene las otras propiedades en la declaración. Sea $x \in O$, $x \equiv 1 \pmod{IO}$. Decimos que el anillo $\tilde{O} = O[x^{-1}]$ es tal que $IO \neq \tilde{O}$: en efecto, de lo contrario tendríamos una igualdad $1 = \sum_{i=1}^{n} \omega_i u_i x^{-m}$ para elementos $\omega_i \in I$, $u_i \in O$ y para un m suficientemente grande. Entonces $x^m = \sum_{i=1}^{n} \omega_i u_i$ y por lo tanto $1 = (1 - x^m) + \sum_{i=1}^{n} \omega_i u_i \in IO$, contra la suposición de que $IO \neq O$.

Entonces, por maximalidad, tenemos $\tilde{O} = O$ y por lo tanto x es invertible en O. Sea ahora $u \in K \setminus O$, de modo que $O[u]$ contenga a O propiamente; por maximalidad tenemos $1 \in IO[u]$, es decir, $1 = \sum_{i=0}^{m} \rho_i u^i$, para $\rho_i \in IO$ adecuado. Podemos suponer además que m (que debe ser > 0) es mínimo para las expresiones de este tipo. Haciendo $x = 1 - \rho_0$ tenemos $x \equiv 1 \pmod{IO}$; entonces x es invertible en O y tenemos entonces una igualdad $1 = \sum_{i=1}^{m} (\rho_i x^{-1}) u^i = \sum_{i=1}^{m} \nu_i u^i$, donde también los $\nu_i = \rho_i x^{-1}$ están en IO.

Queremos mostrar que $u^{-1} \in O$: si esto no se cumple, como antes obtendríamos elementos $\sigma_j \in IO$ tales que $1 = \sum_{j=1}^{n} \sigma_j u^{-j}$, donde de nuevo podemos suponer que n es mínimo. Demostremos que estas últimas dos expresiones (para u y para u^{-1}) son incompatibles, asumiendo por simetría que $m \geq n$. Multiplicando la segunda igualdad por u^m obtenemos $u^m = \sum_{j=1}^{n} \sigma_j u^{m-j}$ y por tanto, sustituyendo u^m en la anterior, obtenemos $1 = \sum_{i=1}^{m-1} \nu_i u^i + \sum_{j=1}^{n} \nu_m \sigma_j u^{m-j}$. Sin embargo, esta es una ecuación del primer tipo, donde se disminuye el exponente máximo de u, lo que produce la contradicción requerida por la minimalidad de m.

Resumiendo, hemos demostrado que $u \in O$ o bien $u^{-1} \in O$. Dado que $IO \neq O$ y como I es distinto de cero, O está estrictamente contenido en K (porque $IK = K$)

y por lo tanto es un VR de K que contiene A. Finalmente, si existe $x \in I \setminus P$, x sería invertible en O y por tanto IO contendría $x \cdot x^{-1} = 1$, contradicción que prueba que $I \subset P$, y el teorema.

Observación 3.17. 1. *La condición de que el ideal I en el teorema es distinto de cero no puede ser omitida, como se ilustra con la elección $A = K$.*

2. *La última parte (crucial) de la prueba puede parecer un poco artificial; está inspirada en las dos relaciones básicas para u y u^{-1}, que muestran respectivamente que u^{-1} y u son integrales sobre IO. Si quisiéramos usar el hecho (no probado aquí) de que tales elementos integrales forman un subanillo, podríamos obtener de inmediato la contradicción $1 = uu^{-1} \in IO$, simplificando un poco el argumento.*

Capítulo III

Aplicaciones del Teorema de existencia y extensiones de anillos de valuación

3.1. Primera aplicación

Sea $K = k(x_1, \ldots, x_r)$ $(r \geq 1)$ una extensión de k que es propia (es decir, diferente de k) y finitamente generada, y sea J el ideal determinado por $(x_1, \ldots, x_r)$ en $k[X_1, \ldots, X_r]$. Entonces, si $(\xi_1, \ldots, \xi_r) \in k^r$ es un cero de J, existe un VR (O, P) de K/k tal que $x_i - \xi_i$ está en P.

Previo a la prueba de esta afirmación, recordemos que aquí J es el ideal que consiste en las $f(X)$ tales que $f(\xi) = 0$, es decir, J es el núcleo del homomorfismo $\phi : k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n]$ que asigna X_i a x_i. Un cero de J es, por definición, un cero común de todos los polinomios en J.

En cuanto a la demostración, apliquemos el Teorema 3.16 tomando $A = k[x_1, \ldots, x_r]$ y $I = \{f(x_1, \ldots, x_r) : f \in k[X_1, \ldots, X_n], f(\xi_1, \ldots, \xi_r) = 0\}$.

Se verifican los supuestos: seguramente I es un ideal, contiene $x_i - \xi_i$, $i = 1, \ldots, r$, y en particular es distinto de cero (porque $A \neq k$). Si tuviéramos $I = A$, entonces una igualdad $1 = f(x_1, \ldots, x_r)$ cumpliría con f siendo un polinomio nulo en $(\xi_1, \ldots, \xi_r)$. Ahora, en la igualdad $f(X_1, \ldots, X_r) - 1 \in J$, pero entonces, ya que $(\xi_1, \ldots, \xi_r)$ es un cero de J, obtendríamos $f(\xi_1, \ldots, \xi_r) - 1 = 0$, una contradicción.

Sea entonces (O, P) un VR de K como en la conclusión del teorema, a saber, que contiene A y tal que $I \subset P$; entonces, en vista del hecho de que $x_i - \xi_i \in I$, tenemos la afirmación.

3.2. Segunda aplicación

. Sea $K = k(x, y)$ un campo de función en una variable sobre k, y supongamos que $F(x, y) = 0$ para algún polinomio irreducible $F \in k[X, Y]$. Entonces, si $F(a, b) = 0$ para algún $(a, b) \in k^2$, existe un VR (O, P) de K/k con $x - a, y - b \in P$.

Este enunciado es un corolario fácil de la primera aplicación. De hecho, sea $J \subset k[X, Y]$ el ideal determinado por (x, y). Como F es irreducible y como x o y es trascendental sobre k por supuesto, J debe ser generado por F y, por lo tanto, (a, b) es un cero de J, lo que produce la afirmación.

Observación . En estos dos enunciados vemos cómo los puntos geométricos $(\xi_1, \ldots, \xi_r)$ (en el primer caso) y (a, b) (en el segundo) corresponden a la VR adecuada. (Esta correspondencia significa que $P \cap k[x_1, \ldots, x_r]$ es el ideal maximal generado por los $x_i - \xi_i$, asociado a $(\xi_1, \ldots, \xi_r)$.)

También se debe recordar que estos VRs no están determinados únicamente por el punto . Sin embargo, en el caso de las curvas y sus campos de funciones, esta correspondencia es esencialmente biyectiva (es decir, con un número finito de excepciones).

3.3. Tercera aplicación

.

Sea K/k una extensión de campo y sea $x \in K$ un elemento trascendente sobre k. Entonces x admite al menos un cero y al menos un polo (en VRs adecuados de K/k).

Como prueba, establezcamos en el Teorema 3.16 $A = k[x]$, $I = xA$. Dado que x es trascendente sobre k, I es distinto de cero y propio. Entonces la conclusión del teorema asegura la existencia de un VR (O, P) de K que contiene A y tal que $x \in P$, lo que dice que x tiene un cero en O . Considerando $1/x$ en lugar de x obtenemos la parte restante.

3.4. Cuarta aplicación

. Si K es una extensión trascendente de k, existen infinitas VRs de K/k.

De hecho, sea $x \in K$ trascendental sobre k; entonces existen infinitas VRs (O, P) de $k(x)/k$. (Existe un VR de este tipo para cada polinomio mónico irreducible;

existen infinitos polinomios de este tipo, porque una clausura algebraica de un campo no puede ser un campo finito). Ahora basta con extender a K cada uno de estos VRs, tomando por ejemplo $A = k[x]$, $I = P \cap A$ en el Teorema 3.16.

3.5. Quinta aplicación

.

Sea A un subanillo de un campo K. Entonces la clausura integral A en K es la intersección de los VRs de K que contienen a A.

Para una demostración, sea B el clausura integral en cuestión (es decir, el conjunto de elementos de K que son integrales sobre A). Sea $x \in B$ y sea (O, P) un VR de K que contiene a A; como x es integral sobre A, es a fortiori integral sobre O y por lo tanto está en O . Esto prueba la mitad de la afirmación.

Por el contrario, sea $x \in K \setminus B$. Entonces $y = x^{-1}$ no es invertible en $A[y]$ (porque de lo contrario tendríamos $x = y^{-1} \in A[y] = A[x^{-1}]$, lo que daría una ecuación integral para x sobre A). Por lo tanto, y se encuentra en un ideal maximal I de $A[y]$. Ciertamente, I es distinto de cero (contiene y) y, por lo tanto, podemos aplicar el Teorema 3.16 (con $A[y]$ en lugar de A), obteniendo la existencia de un VR (O, P) de K con $A[y] \subset O$ y $I \subset P$. Si tuviéramos $x \in O$, tendríamos también $1 = yx \in IO \subset P$, una contradicción. Por lo tanto, $x \notin O$ y x no está en la intersección en cuestión, concluyendo el argumento.

Observación . Tenga en cuenta que este resultado implica directamente que el cierre integral de un subanillo de un campo es en sí mismo un subanillo.

Ejemplo. El anillo $\mathbb{Z}$ es la intersección de los VRs de $\mathbb{Q}$) y, de hecho, $\mathbb{Z}$ es integralmente cerrado (como se deduce fácilmente de la factorización única). De manera similar, el anillo de enteros algebraicos (es decir, los números algebraicos integrales sobre $\mathbb{Z}$) en un campo numérico K coincide con la intersección de los VRs de K.

Otros ejemplos ocurren dentro de los campos de funciones; por ejemplo, el anillo polinomial $k[x]$ es la intersección de esos VRs de $k(x)/k$ que contienen x. (Aquí todo depende de la elección, no canónica, del generador x, al contrario del caso de $\mathbb{Q}$.)

Observación . Si A es local con el ideal maximal M, la conclusión de la aplicación E se mantiene incluso si limitamos la intersección a aquellos VRs (O, P) de K con $A \subset O$ y $M \subset P$.

La primera parte de la demostración permanece sin cambios. En cuanto a la segunda parte, se puede proceder de manera similar: se comienza observando que si $x \in K \setminus B$ entonces $y = x^{-1}$ no es invertible en $A[y]/M[y]$. (De lo contrario, tendríamos $1 = m(y) + l(y)y, m \in M[y], l(y) \in A[y]$, de donde $1 = m_0 + l_1(y)y, m_0 \in M, l_1(y) \in A[y]$; pero $1 - m_0 \in A^*$ y por lo tanto y sería invertible en $A[y]$, y como antes x sería integral sobre A, una contradicción.) Entonces $M[y] + yA[y]$ está contenido en un ideal maximal I de $A[y]$ y ahora la prueba puede concluirse exactamente como arriba.

3.6. Sexta aplicación

.

Si un álgebra K/k finitamente generada es un campo, entonces es una extensión finita. La declaración es una de las varias versiones equivalentes del célebre Nullstellensatz de Hilbert. A continuación, presentamos una discusión y otros enfoques para una prueba del teorema de Hilbert.

Para probar la afirmación anterior, escribamos $K := k[x_1, \dots, x_m]$. Si la conclusión no se cumple, sean $z_1, \dots, z_r$ una base de trascendencia para K/k, con $r > 0$. Cada uno entre $x_1, \dots, x_m$ entonces satisface una ecuación algebraica no trivial con coeficientes en $A := k[z_1, \dots, z_r]$. Sea $f(z_1, \dots, z_r) \in A \setminus \{0\}$ el producto de los coeficientes principales de tales m polinomios.

Sea entonces I un ideal maximal de A distinto de cero, que no contenga a f. (Tal ideal existe, y es aquí donde usamos la condición $r > 0$: basta con tomar un ideal maximal de A que contenga $z_1 f + 1$, que tiene grado positivo y por lo tanto no es invertible. Alternativamente, si $\xi_1, \dots, \xi_r$ son elementos en una extensión algebraica k' de k y tales que $f(\xi_1, \dots, \xi_r) \neq 0$, basta tomar como I el conjunto de elementos de A que se anulan en $(\xi_1, \dots, \xi_r)$; I no contiene f, es distinto de cero - porque $r > 0$ y los ξ_i son algebraicos sobre k - y es maximal porque A/I es isomorfo a $k[\xi_1, \dots, \xi_r] = k(\xi_1, \dots, \xi_r)$.

Ahora sea, como en el Teorema 3.16, (O, P) un VR de K con $A \subset O$ y $I \subset P$. Como I no contiene f, vemos que P tampoco contiene f (porque de otro modo P contendría $I + (f)$, que es igual a A ya que I es maximal). Observa que, para $i = 1, \dots, m$, x_i satisface una ecuación sobre A con un coeficiente principal f. Por lo tanto, como f es invertible en O (porque f no está en P, como hemos visto), cada x_i es integral sobre O. Pero O es integralmente cerrado y, por tanto, $x_i \in O$ para todo $i = 1, \dots, m$, luego O contiene $k[x_1, \dots, x_m] = K$, una contradicción que finalmente prueba la afirmación.

Proposición 6.1. *Si L/K es una extensión de campo y (O, P) es un VR de L que no contiene K, entonces $(O \cap K, P \cap K)$ es un VR de K.*

Prueba . Sea $AO \cap K$ si $x \in K$, entonces $x \in O$, y por lo tanto $x \in A$, o $x^{-1} \in O \cap K = A$. Esto muestra que A es un VR de K. Si ahora $x \in A \setminus A^*$, tenemos $x = 0$ o $x^{-1} \notin O$, lo que implica que $x \in P$. Por lo tanto, $A \setminus A^* \subseteq P$. Finalmente, si $x \in P \cap K$, entonces $x \in A$; por otro lado, x no puede estar en A^*, porque x^{-1} no está en O. Esto prueba la implicación opuesta.

Proposición 6.2. *Sea L/K una extensión de campo y sean (O, P), (O', P') VR en K, L respectivamente, tales que $O \subseteq O'$ y $P \subseteq P'$. Entonces $O = O' \cap K$.*

Prueba. La inclusión $O \subseteq O' \cap K$ es clara. Sea ahora $x \in O' \cap K$, $x \notin O$. Entonces $yx^{-1} \in P$ y por lo tanto $y \in P'$, lo cual contradice el hecho de que $x = y^{-1}$ se encuentra en O'. Así, tenemos una contradicción que prueba la inclusión opuesta y el reclamo.

Observación 6.3. *Observa que la suposición $O \subseteq O'$ implica $P' \cap O \subseteq P$; sin embargo, que $P \subseteq P'$ no es automático: por ejemplo, sea $K = \mathbb{Q}$, $L = \mathbb{Q}(x)$, y sea (O, P) cualquier VR de $\mathbb{Q}$, siendo (O', P') el VR correspondiente al polinomio x. Tenemos $P' \cap \mathbb{Q} = \{0\}$.*

Conclusiones

En el presente trabajo, hemos desarrollado la teoría de anillos de valuación, presentando ejemplos concretos. Además, en dicho desarrollo, hemos establecido diversos resultados, aplicaciones e interpretaciones importantes, entre lo que podemos destacar:

- Hemos obtenido el Teorema de extensión de anillos de valuación, en el cual se establece que dado un subanillo de un cuerpo, siempre existe un anillo de valuación conteniendo al subanillo dado.
- Hemos dado una interpretación geométrica al Teorema de extensión de anillos de valuación, la cual nos dice que, dada una extensión de cuerpos finitamente generada, hay una correspondencia entre puntos geométricos y anillos de valuación.
- Hemos obtenido una de las versiones del Teorema de los Ceros de Hilbert, el cual es un resultado de mucha importancia en la Geometría Algebraica.
- Hemos establecido algunas conexiones entre anillos de valuación y el concepto de extensiones integrales de anillos.
- Hemos establecido que todo anillo de valuación es un anillo local, el cual es un tipo de anillo de mucha relevancia en la Geometría Algebraica, especialmente en la teoría de esquemas.

Bibliografía

[1] Scognamillo, R., & Zannier, U. (2014). *Introductory Notes on Valuation Rings and Function Fields in One Variable*. Edizioni della Normale.

[2] . Atiyah and I. MacDonald, *Commutative Algebra*, Addison Wesley, 1969.

[3] . Hartshorne, *Algebraic Geometry*, Springer-Verlag.

[4] . Lang, *Algebra*, Springer-Verlag.

[5] Atiyah, M. F., & MacDonald, I. G. (1969). *Introduction to Commutative Algebra*. Addison-Wesley.

[6] Lang, S. (1993). *Algebra*. Serie Graduate Texts in Mathematics, Springer.