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

Extensiones de Homomorfismos

TESIS

Para optar el Título Profesional de Licenciada en Matemática

AUTOR

Jessica Yuneiri LÉVANO MENDOZA

ASESOR

Dr. Gabriel Armando MUÑOZ MÁRQUEZ

Lima, Perú

2023

Referencia bibliográfica

Lévano, J. (2023). *Extensiones de Homomorfismos*. [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	Jessica Yuneiri Lévano Mendoza
Tipo de documento de identidad	DNI
Número de documento de identidad	73895813
URL de ORCID	https://orcid.org/0009-0008-2853-9397
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	Carlos Alberto Peña Miranda
Tipo de documento	DNI
Número de documento de identidad	10699143
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 10:30 horas del viernes 06 de octubre del 2023, se reunieron los docentes designados como Miembros del Jurado Evaluador (PROGRAMA DE TITULACIÓN PROFESIONAL 2023): Dr. Carlos Alberto Peña Miranda (PRESIDENTE), Dr. Leonardo Henry Alejandro Aguilar (MIEMBRO) y el Dr. Gabriel Armando Muñoz Márquez (MIEMBRO ASESOR), para la sustentación de la Tesis titulada: "**EXTENSIONES DE HOMOMORFISMOS**", presentado por la señorita **Bachiller JESSICA YUNEIRI LÉVANO MENDOZA**, para optar el Título Profesional de Licenciada en Matemática.

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

Realizada la evaluación correspondiente por los Miembros del Jurado Evaluador, la expositora mereció la aprobación ..Sobresaliente..... con un calificativo promedio de ..dieciocho (18)..

A continuación, los Miembros del Jurado Evaluador dan manifiesto que la participante **Bachiller JESSICA YUNEIRI LÉVANO MENDOZA**, en vista de haber aprobado la sustentación de su Tesis, será propuesto para que se le otorgue el Título Profesional de Licenciada en Matemática.

Siendo las 11:10 horas se levantó la sesión firmando para constancia la presente Acta.

Dr. Carlos Alberto Peña Miranda
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° 001545-2023-D-FCM/UNMSM de la tesis, cuyo título es EXTENSIONES DE HOMOMORFISMOS, presentado por el bachiller Jessica Yuneiri Lévano Mendoza 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 12 % 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

Agradecimientos

Agradezco en primer lugar a mi papá (*in memoriam*), por todo el amor y apoyo para realizar mis sueños. Él era, y para siempre será, el mayor ejemplo de mi vida y mi inspiración.

A mi mamá y a mi hermana, que me incentivaron y aconsejaron en los momentos difíciles. Gracias por su paciencia, confianza y apoyo incondicional. Sin su apoyo este trabajo no hubiera sido posible.

A mi tío Jacinto, por enseñarme matemática en mis años de colegio y creer en mis capacidades desde mi infancia hasta hoy. Mi amor por la matemática es gracias a él.

A mi enamorado Alexander, por todo el amor, comprensión y apoyo, muchas gracias por haber estado a mi lado en esta etapa importante de mi vida.

Quiero agradecer también a mi orientador Gabriel Armando Muñoz Márquez, por la paciencia y momentos dedicados a aclarar las dudas que surgieron a lo largo de este trabajo contribuyendo en mi formación académica.

Índice general

Resumen III

Abstract IV

Introducción V

1. Preliminares **1**

1.1. Anillos 1

1.1.1. Conceptos Básicos 1

1.1.2. Ideales y Anillos Cocientes 4

1.1.3. Homomorfismos de anillos 9

1.1.4. Localización 12

1.2. Extensiones de Cuerpos 19

1.2.1. Conceptos Básicos 19

1.2.2. Cerradura Algebraica 24

2. Extensiones de Anillos **28**

3. Extensiones de Homomorfismos **33**

Conclusiones **42**

Referencias **44**

Resumen

En este trabajo presentaremos varios resultados fundamentales que establecen las condiciones necesarias para la extensión de homomorfismos de anillos.

En la primera parte, sentamos las bases teóricas sobre la teoría de anillos y sus principales resultados. Además, introducimos el procedimiento algebraico de la localización que es una herramienta poderosa para extender anillos y por ende para extender homomorfismos entre estos.

En la segunda parte, dirigimos nuestra atención hacia el estudio de las extensiones de anillos, explorando sus propiedades y características esenciales, pues estas son la base para nuestros resultados principales sobre extensiones de homomorfismos.

Palabras clave: Extensión de homomorfismos, extensión de anillos, extensión de cuerpos, localización, anillos locales.

Abstract

In this work, we will present several fundamental results that establish the necessary conditions for the extension of ring homomorphisms.

In the first part, we lay down the theoretical foundations of ring theory and its main results. Additionally, we introduce the algebraic procedure of localization, which is a powerful tool for extending rings and, consequently, for extending homomorphisms between them.

In the second part, we turn our attention to the study of extension of rings, exploring their properties and essential characteristics, as these form the basis for our main results regarding extension of homomorphism.

Key words: Extension of homomorphisms, extension of rings, extension of fields, localization, local rings.

Introducción

La historia de las extensiones de homomorfismos de anillos está estrechamente ligada al desarrollo de la teoría de anillos y al álgebra abstracta en general. A medida que los matemáticos exploraban las propiedades de las estructuras algebraicas, surgieron preguntas sobre cómo extender los homomorfismos entre anillos a estructuras más grandes o más generales.

La teoría de anillos comenzó a tomar forma en el siglo XIX con los trabajos de matemáticos como Richard Dedekind y Ernst Eduard Kummer. Dedekind introdujo el concepto de ideales en anillos y sentó las bases para el estudio de extensiones de anillos y cuerpos. Kummer trabajó en la factorización única en anillos de números enteros y contribuyó al desarrollo de la teoría de números algebraicos.

A principios del siglo XX, Emil Artin, un matemático destacado del siglo XX, realizó importantes investigaciones en álgebra abstracta y teoría de números. En particular, sus contribuciones a la teoría de extensiones de cuerpos y anillos fueron fundamentales. Artin y sus colaboradores estudiaron extensiones de anillos y cuerpos con un enfoque en la teoría de Galois.

Más adelante, en la década de 1930 Wolfgang Krull, otro influyente matemático del siglo XX, desarrolló la teoría de anillos y módulos, así como la teoría de cuerpos. Krull trabajó en la teoría de anillos locales y contribuyó al estudio de las extensiones de anillos y homomorfismos en ese contexto.

Desde la década de 1950 en adelante, con el avance de la teoría de módulos y la teoría de anillos conmutativos, matemáticos como Serge Lang y Oscar Zariski realizaron investigaciones fundamentales en el campo. La noción de "homomorfismo integral"se introdujo para estudiar propiedades locales de anillos y sus extensiones.

A medida que avanzó el siglo XX, la teoría de anillos y homomorfismos se convirtió en una parte esencial del álgebra abstracta.

En el primer capítulo, presentamos algunos conceptos importantes de la teoría de anillos, como ideales, anillos cocientes, homomorfismos de anillos, presentamos también el proceso algebraico de la localización que permite extender un anillo al incluir elementos inversibles que no eran inversibles en el anillo original. Finalizamos este capítulo introduciendo las extensiones de cuerpos y estudiando sus principales resultados.

En el segundo capítulo, introducimos las extensiones de anillos y presentamos el concepto de homomorfismo integral que relaciona un anillo, su extensión, y una propiedad importante entre estos anillos, este homomorfismo jugará un papel importante a la hora de extender homomorfismos.

En el tercer capítulo, presentamos los resultados principales de este trabajo. Establecemos las condiciones necesarias que deben verificar ciertos anillos, para que homomorfismos definidos en estos puedan ser extendidos.

Capítulo 1

Preliminares

1.1. Anillos

Las referencias para esta sección son (Gonçalves, 1979), (Dorronsoro y Hernández, 1996) y (Herstein y Lluis, 1970).

1.1.1. Conceptos Básicos

Definición 1.1.1. Sea A un conjunto no vacio donde se definen dos operaciones

$$\begin{aligned} + : A \times A &\to A & \cdot : A \times A &\to A \\ (a, b) &\mapsto a + b & (a, b) &\mapsto a \cdot b \end{aligned}$$

llamadas *suma* y *producto* respectivamente. Decimos que $(A, +, \cdot)$ es un *anillo* si verifica las siguientes propiedades:

A1) $(a + b) + c = a + (b + c)$, para todo $a, b, c \in A$ (asociatividad de la suma)

A2) $a + b = b + a$, para todo $a, b \in A$ (conmutatividad de la suma)

A3) Para todo $a \in A$, existe $0 \in A$ tal que $a + 0 = 0 + a = a$ (existencia del elemento neutro para la suma)

A4) Para cada $a \in A$, existe un único elemento en A, denotado por $-a$, tal que $a+(-a) = (-a) + a = 0$ (existencia del inverso aditivo)

A5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in A$ (asociatividad del producto)

A6) $a \cdot (b+c) = a \cdot b + a \cdot c$ y $(a+b) \cdot c = a \cdot c + b \cdot c$, para todo $a, b, c \in A$ (distributividad a la izquierda y a la derecha)

Note que en la definición de anillo, no se precisa que el producto sea conmutativo, pero si este fuera el caso, decimos que A es un *anillo conmutativo* (esto es, $a \cdot b = b \cdot a$ para todo $a, b \in A$).

Si existe un elemento en A, denotado por 1 ($0 \neq 1$), tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$, decimos que A es un *anillo con unidad* 1. Además, si $a \cdot b = 0$, implica que $a = 0$ o $b = 0$, para $a, b \in A$, decimos que A es un *anillo sin divisores de cero*.

Definición 1.1.2. Sea $(A, +, \cdot)$ un anillo.

i) Si A es un anillo conmutativo, con unidad y sin divisores de cero, decimos que A es un *dominio de integridad*.

ii) Si A es un anillo conmutativo, con unidad y para cada $a \in A$, $a \neq 0$, existe un elemento en A, denotado por a^{-1}, tal que $a.a^{-1} = a^{-1}.a = 1$, decimos que A es un *cuerpo*.

Note que si A es un cuerpo, esto implica que A es un dominio de integridad. En efecto, sea $a \cdot b = 0$ para $a, b \in A$. Si $a \neq 0$, entonces $b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$. De forma similar, si $b \neq 0$, entonces $a = 0$.

Ejemplo 1.1.3. Con las operaciones usuales de suma y producto se tiene que $\mathbb{Z}$ es un dominio de integridad que no es un cuerpo y además que $\mathbb{Q}$, $\mathbb{R}$, y $\mathbb{C}$ son cuerpos.

Ejemplo 1.1.4. Si p es un número primo, entonces $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\} \subset \mathbb{R}$ es un cuerpo con las operaciones usuales $+$ y $\cdot$ en $\mathbb{R}$.

En efecto, como $\mathbb{R}$ es un cuerpo, entonces los elementos de $\mathbb{Q}[\sqrt{p}]$ verifican las propiedades $A1), A2), A5), A6)$ de la Definición 1.1.1 y la conmutatividad del producto. Además, $\mathbb{Q}[\sqrt{p}]$ es cerrado con las operaciones $+$ y $\cdot$, esto es,

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$$
$$(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pbd) + (bc + ad)\sqrt{p}.$$

Luego,

- Para todo $x = a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, existe $0 = 0 + 0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ tal que $x + 0 = 0 + x = x$.

- Para cada $x = a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, existe un único elemento $-x = -a - b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ tal que $x + (-x) = (-x) + x = 0$.
- Para todo $x = a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, existe un único elemento $1 = 1 + 0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ tal que $x \cdot 1 = 1 \cdot x = x$.
- Para cada $x = a + b\sqrt{p} \neq 0 \in \mathbb{Q}[\sqrt{p}]$, existe un elemento $x^{-1} = (a - b\sqrt{p})/(a^2 - pb^2) \in \mathbb{Q}[\sqrt{p}]$ tal que $x.x^{-1} = x^{-1}.x = 1$.

Definición 1.1.5. Sean $(A, +, \cdot)$ un anillo y B un subconjunto no vacio de A tal que B es cerrado con las operaciones $+$ y $\cdot$ de A, esto es,

a) si $a, b \in B$, entonces $a + b \in B$,

b) si $a, b \in B$, entonces $a \cdot b \in B$.

Si $(B, +, \cdot)$ es un anillo con las operaciones de A, decimos que B es un *subanillo* de A.

Ejemplo 1.1.6. $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, $\mathbb{Q}$ es un subanillo de $\mathbb{R}$ y $\mathbb{R}$ es un subanillo de $\mathbb{C}$.

Ejemplo 1.1.7. $\mathbb{Q}$ es un subanillo de $\mathbb{Q}[\sqrt{p}]$ y $\mathbb{Q}[\sqrt{p}]$ es un subanillo de $\mathbb{R}$, para todo p primo.

La siguiente proposición nos proporciona una caracterización para subanillos.

Proposición 1.1.8. *Sean $(A, +, \cdot)$ un anillo y B un subconjunto de A. Entonces, B es un subanillo de A si y solamente si se verifica:*

i) $0 \in B$

ii) Si $a, b \in B$, entonces $a - b \in B$

iii) Si $a, b \in B$, entonces $a \cdot b \in B$

Si un subanillo B de un cuerpo $(K, +, \cdot)$ es un cuerpo, decimos que B es un *subcuerpo* de K.

Ejemplo 1.1.9. $\mathbb{Q}$ es un subcuerpo de $\mathbb{Q}[\sqrt{p}]$ y $\mathbb{Q}[\sqrt{p}]$ es un subcuerpo de $\mathbb{R}$, para todo p primo.

1.1.2. Ideales y Anillos Cocientes

Definición 1.1.10. Sean A un anillo e I un subanillo de A.

i) Si $\forall a \in A$ y $\forall x \in I$ se tiene que $a \cdot x \in I$ (esto es, $A \cdot I \subseteq I$), decimos que I es un *ideal a la izquierda* de A.

ii) Si $\forall a \in A$ y $\forall x \in I$ se tiene que $x \cdot a \in I$ (esto es, $I \cdot A \subseteq I$), decimos que I es un *ideal a la derecha* de A.

iii) Si I es un ideal simultaneamente a la derecha y a la izquierda de A, decimos que I es un *ideal* de A.

Note que si A es un anillo conmutativo, entonces las tres definiciones anteriores coinciden.

Es claro que $\{0\}$ es un ideal de A y será llamado *ideal trivial* de A. Los ideales de A distintos de A y $\{0\}$ son llamados *ideales propios* de A. Además, si $1 \in I$, entonces $I = A$.

Sea A un anillo conmutativo y sean $a_1, ..., a_n$ elementos de A. Se verifica que el subconjunto de A definido por

$$(a_1, ..., a_n) = \{x_1 \cdot a_1 + ... + x_n \cdot a_n : x_i \in A\},$$

es un ideal de A, el cual es llamado *ideal generado* por $a_1, ..., a_n$. En efecto,

i) $0 = 0 \cdot a_1 + ... + 0 \cdot a_n \in (a_1, ..., a_n)$.

ii) Si $x = x_1 \cdot a_1 + ... + x_n \cdot a_n, y = y_1 \cdot a_1 + ... + y_n \cdot a_n \in (a_1, ..., a_n)$, entonces

$$x - y = (x_1 - y_1) \cdot a_1 + ... + (x_n - y_n) \cdot a_n \in (a_1, ..., a_n) \quad ; \quad x_i - y_i \in A.$$

iii) Si $a \in A$ y $x = x_1 \cdot a_1 + ... + x_n \cdot a_n \in (a_1, ..., a_n)$, entonces

$$a \cdot x = (a \cdot x_1) \cdot a_1 + ... + (a \cdot x_n) \cdot a_n \in (a_1, ..., a_n) \quad ; \quad a \cdot x_i \in A.$$

En particular, si $I = (a)$ para algún $a \in A$, decimos que I es un *ideal principal*.

En general, sean I y J ideales de A. De forma similar al caso anterior, se verifica que el subconjunto de A definido por

$$IJ = \{x_1 \cdot y_1 + ... + x_n \cdot y_n : x_i \in I \text{ e } y_i \in J\},$$

es también un ideal de A, el cual es llamado *ideal generado* por I y J.

Definición 1.1.11. Sean A un anillo conmutativo con unidad e I un ideal de A. Decimos que I es *maximal* si $I \neq A$ y si los únicos ideales de A conteniendo I son I y A.

Definición 1.1.12. Sean A un anillo conmutativo con unidad y P un ideal de A. Decimos que P es *primo* si $P \neq A$ y si $x \cdot y \in P$ implica que $x \in P$ o $y \in P$.

Ejemplo 1.1.13. Si p es un número primo, entonces el ideal principal $(p) \subset \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$. En efecto, sean $a, b \in \mathbb{Z}$. Si $ab \in (p)$, entonces ab es divisible por p. Como p es primo, entonces a es divisible por p o b es divisible por p, esto es, $a \in (p)$ o $b \in (p)$. Por lo tanto, (p) es primo.

Ejemplo 1.1.14. Si K es un cuerpo, entonces $\{0\}$ es un ideal maximal de K. En efecto, supongamos que $\{0\} \neq J$ es un ideal de K. Luego, existe un $0 \neq a \in J$. Como K es un cuerpo, existe $a^{-1} \in K$ tal que $a.a^{-1} = 1$. Entonces, $1 \in J$ y por lo tanto $J = K$. Como $\{0\} \subset J$, concluímos que $\{0\}$ es un ideal maximal de K.

Por otro lado, sea A un anillo y J un ideal de A. Consideramos en A la relación

$$x \equiv x'(\text{mod } J) \;\Leftrightarrow\; x - x' \in J.$$

Luego, podemos verificar que esta es una relación de equivalencia en A.

En efecto, para cualquier $x, x', x'' \in A$ tenemos:

i) $x \equiv x(\text{mod } J)$ pues $0 = x - x \in J$. (Propiedad Reflexiva)

ii) $x \equiv x'(\text{mod } J)$, entonces $x - x' = -(x' - x) \in J$. Luego, $x' - x \in J$ y por lo tanto $x' \equiv x(\text{mod } J)$. (Propiedad Simétrica)

iii) $x \equiv x'(\text{mod } J)$ y $x' \equiv x''(\text{mod } J)$, entonces $x - x' \in J$ y $x' - x'' \in J$. Luego, $x - x'' = (x - x') + (x' - x'') \in J$ y por lo tanto $x \equiv x''(\text{mod } J)$. (Propiedad Transitiva)

La *clase de equivalencia* de $x \in A$ en relación a $\equiv (\text{mod } J)$ es denotada por

$$x + J = \{y \in A : y \equiv x(\text{mod } J)\} = \{x + z : z \in J\}.$$

Además, definimos el *conjunto cociente de A por J* como

$$A/J = \{x + J : x \in A\}.$$

Proposición 1.1.15. *Sean A un anillo y J un ideal de A. El conjunto A/J con las siguientes operaciones*

$$\begin{aligned} +: A/J \times A/J &\to A/J & \cdot: A/J \times A/J &\to A/J \\ (x+J, y+J) &\mapsto (x+y)+J & (x+J, y+J) &\mapsto (x\cdot y)+J \end{aligned}$$

tiene una estructura de anillo.

Demostración: Veamos que $+$ y $\cdot$ están bien definidos, esto es, que la clase de la suma y la clase del producto no dependen de los representantes de las clases de los sumandos ni de las clases de los factores, respectivamente.

En efecto, si $x' \in x+J$ y $y' \in y+J$, entonces existen $a, b \in J$ tal que $x' = x+a$ y $y' = y+b$. Luego,

- $x'+y' = x+y+(a+b) \in (x+y)+J$, pues $a+b \in J$. Entonces, $(x+y)+J = (x'+y')+J$.
- $x' \cdot y' = x \cdot y + (x \cdot b + a \cdot y + a \cdot b) \in (x \cdot y) + J$, pues $x \cdot b + a \cdot y + a \cdot b \in J$. Entonces, $(x \cdot y) + J = (x' \cdot y') + J$.

Resta probar que $(A/J, +, \cdot)$ verifica las 6 propiedades de la definición 1.1.1: Sean $x+J, y+J, z+J \in A/J$

A1) Asociatividad de la suma.

$$\begin{aligned} ((x+J)+(y+J))+(z+J) &= ((x+y)+J)+(z+J) \\ &= ((x+y)+z)+J \\ &= (x+(y+z))+J \\ &= (x+J)+((y+z)+J) \\ &= (x+J)+((y+J)+(z+J)) \end{aligned}$$

A2) Conmutatividad de la suma.

$$\begin{aligned} (x+J)+(y+J) &= (x+y)+J \\ &= (y+x)+J \\ &= (y+J)+(x+J) \end{aligned}$$

A3) Existencia del elemento neutro para la suma.
Tenemos que $(x+J)+(0+J) = (0+J)+(x+J) = x+J$. Por lo tanto, $0+J$ es el elemento neutro para la suma en A/J.

A4) Existencia del inverso aditivo.
Tenemos que $(x+J)+(-x+J) = (-x+J)+(x+J) = 0+J$. Por lo tanto, $-x+J$ es el inverso aditivo de $x+J$.

A5) Asociatividad del producto.

$$\begin{aligned}((x+J)\cdot(y+J))\cdot(z+J) &= ((x\cdot y)+J)\cdot(z+J)\\ &= ((x\cdot y)\cdot z)+J\\ &= (x\cdot(y\cdot z))+J\\ &= (x+J)\cdot((y\cdot z)+J)\\ &= (x+J)\cdot((y+J)\cdot(z+J))\end{aligned}$$

A6) Distributividad.

$$\begin{aligned}(x+J)\cdot((y+J)+(z+J)) &= (x+J)\cdot((y+z)+J)\\ &= (x\cdot(y+z))+J\\ &= (x\cdot y+x\cdot z)+J\\ &= (x\cdot y+J)+(x\cdot z+J)\\ &= (x+J)\cdot(y+J)+(x+J)\cdot(z+J)\end{aligned}$$

De forma análoga, se verifica que

$$((x+J)+(y+J))\cdot(z+J) = (x+J)\cdot(z+J)+(y+J)\cdot(z+J).$$

□

Además, si 1 es la unidad de A, entonces $1+J$ es la unidad de A/J pues

$$(1+J)\cdot(x+J) = 1\cdot x+J = x+J = x\cdot 1+J = (x+J)\cdot(1+J) \quad , \quad \forall x\in A.$$

Más aún, si A es conmutativo, entonces A/J es conmutativo pues

$$(x+J)\cdot(y+J) = x\cdot y+J = y\cdot x+J = (y+J)\cdot(x+J) \quad , \quad \forall x,y\in A.$$

Teorema 1.1.16. *Sean A un anillo conmutativo con unidad $1\in A$ y J un ideal propio de A. Entonces, tenemos lo siguiente:*

a) J es primo si y solamente si A/J es un dominio de integridad.

b) J es maximal si y solamente si A/J es un cuerpo.

Demostración:

a) ($\Rightarrow$) Sean $(x+J),(y+J) \in A/J$ tal que $(x+J)\cdot(y+J) = 0+J$. Luego,

$$xy + J = 0 + J \Leftrightarrow xy \in J.$$

Por hipótesis, J es un ideal primo, lo que implica que $x \in J$ o $y \in J$. Entonces,

$$x + J = 0 + J \ \text{ o } \ y + J = 0 + J.$$

Por lo tanto, A/J es un dominio de integridad.

($\Leftarrow$) Sean $x, y \in A$ tal que $xy \in J$. Luego, $xy + J = 0 + J$. Por hipótesis, A/J es un dominio de integridad. Entonces,

$$x + J = 0 + J \ \text{ o } \ y + J = 0 + J,$$

lo que implica que $x \in J$ o $y \in J$. Por lo tanto, J es un ideal primo.

b) ($\Rightarrow$) Sea $0 + J \neq a + J \in A/J$ y sea $I = J + a \cdot A = \{x + ay : x \in J \text{ e } y \in A\}$. Veamos que I es un ideal. En efecto,

- $0 = 0 + a \cdot 0 \in I$.
- Si $x + ay, \bar{x} + a\bar{y} \in I$, entonces $(x + ay) - (\bar{x} + a\bar{y}) = (x - \bar{x}) + a(y - \bar{y}) \in I$ pues $x - \bar{x} \in J$ y $y - \bar{y} \in A$.
- Si $z \in A$ y $x + ay \in I$, entonces $(x + ay)z = xz + a(yz) \in I$ pues $xz \in J$ y $yz \in A$.

Para cada $x \in J$, tenemos que $x = x + a \cdot 0 \in I$, esto es, que J está contenido en I. Más aún, $a = 0 + a \cdot 1 \in I$ y $a \notin J$, pues caso contrario $a + J = 0 + J$. Entonces, $J \neq I$.

Por hipótesis, J es un ideal maximal, entonces $I = A$. Luego, existen $u \in J$ y $b \in A$ tales que $1 = u + ab$. Así, $1 + J = u + ab + J = ab + J$, pues $u \in J$. Finalmente, existe $b + J \in A/J$ tal que $1 + J = (a + J)\cdot(b + J)$. Por lo tanto, A/J es un cuerpo.

($\Leftarrow$) Sea M un ideal de A tal que $M \neq J$ y $J \subset M \subseteq A$, entonces existe $a \in M \setminus J$. Por hipótesis, A/J es un cuerpo, entonces para $0 + J \neq a + J \in A/J$, existe $b + J \in A/J$ tal que $(a + J) \cdot (b + J) = 1 + J$. Luego,

$$ab + J = 1 + J \Leftrightarrow ab - 1 \in J,$$

entonces existe $u \in J$ tal que $ab - 1 = u$. Como $a \in M$, se sigue que $ab \in M$ y además $u \in J \subset M$. Luego, $1 \in M$ y por lo tanto $M = A$. Así queda probado que J es un ideal maximal.

□

Observación 1.1.17. Si A es un anillo conmutativo con unidad 1 y J es un ideal maximal de A, entonces J es un ideal primo de A. En efecto, si J es un ideal maximal de A, entonces A/J es un cuerpo, lo que implica que A/J es un dominio de integridad. Luego, J es un ideal primo de A.

El recíproco no siempre se cumple. Basta considerar el anillo $\mathbb{Z}$ y el ideal $\{0\}$ de $\mathbb{Z}$. Se cumple que

$$\mathbb{Z}/\{0\} = \{x + \{0\} : x \in \mathbb{Z}\} = \{x : x \in \mathbb{Z}\} = \mathbb{Z}.$$

Como $\mathbb{Z}$ es un dominio de integridad que no es un cuerpo, por el Teorema 1.1.16 se tiene que $\{0\}$ es primo pero no maximal.

Definición 1.1.18. Sea A un anillo conmutativo. Decimos que A es *local* si tiene un único ideal maximal.

Ejemplo 1.1.19. Todo cuerpo K es un anillo local. En efecto, como todo ideal de K contiene al ideal $\{0\}$ y $\{0\}$ es maximal por el Ejemplo 1.1.14, entonces los únicos ideales de K son $\{0\}$ y K. Luego, $\{0\}$ es el único ideal maximal de K.

1.1.3. Homomorfismos de anillos

Sean A y B dos anillos. Vamos a denotar las operaciones en estos anillos por los mismos símbolos $+$ y $\cdot$, además denotaremos el elemento neutro de A por 0 (resp. elemento neutro de B por $0'$) y, en caso exista, a la unidad en A (resp. en B) la denotamos por 1 (resp. por $1'$).

Definición 1.1.20. Un *homomorfismo* de A en B es una función $f : A \to B$ que verifica las siguientes condiciones:

a) $f(x + y) = f(x) + f(y)$, para todo $x, y \in A$

b) $f(x \cdot y) = f(x) \cdot f(y)$, para todo $x, y \in A$

En todo homomorfismo se verifica fácilmente que $f(0) = 0'$ y $f(-a) = -f(a)$ para todo $a \in A$. Además, si A y B son anillos con unidad, de aquí en adelante vamos a suponer que $f(1) = 1'$.

Si $f : A \to B$ es un homomorfismo biyectivo, decimos que f es un isomorfismo de A sobre B. Decimos que dos anillos A y B son isomorfos (y denotamos por $A \simeq B$) si existe un isomorfismo de A sobre B.

Ejemplo 1.1.21. Sean A y B anillos tal que $A \subseteq B$. Claramente la función inclusión $i : A \to B$ tal que $i(x) = x \ \forall x \in A$, es un homomorfismo de A en B. Además, si J es un ideal de A, la proyección canónica $\pi : A \to A/J$ definida por $\pi(x) = x + J \ \forall x \in A$ también es un homomorfismo de A en A/J, ya que para todo $x, y \in A$ se cumple:

$$\pi(x + y) = (x + y) + J = (x + J) + (y + J) = \pi(x) + \pi(y)$$
$$\pi(x \cdot y) = x \cdot y + J = (x + J) \cdot (y + J) = \pi(x) \cdot \pi(y).$$

A continuación presentamos el Primer Teorema de Homomorfismos.

Teorema 1.1.22. *Sean A y B anillos y $f : A \to B$ un homomorfismo. Entonces, se cumple lo siguiente:*

1) $Imf = \{f(a) : a \in A\}$ es un subanillo de B.

2) $Kerf = \{a \in A : f(a) = 0'\}$ es un ideal de A. Además, f es inyectiva $\Leftrightarrow Kerf = \{0\}$.

3) Los anillos $A/Kerf$ e Imf son isomorfos.

Demostración:

1) Tenemos que:

   i) $0' = f(0) \in \mathrm{Im}f$.

   ii) Si $f(a), f(b) \in \mathrm{Im}f$, entonces $f(a) - f(b) = f(a - b) \in \mathrm{Im}f$ pues $a - b \in A$.

   iii) Si $f(a), f(b) \in \mathrm{Im}f$, entonces $f(a) \cdot f(b) = f(a \cdot b) \in \mathrm{Im}f$ pues $a \cdot b \in A$.

   Luego, por la Proposición 1.1.8, $\mathrm{Im}f$ es un subanillo de B.

2) Primero vamos a probar que $\mathrm{Ker}f$ es un ideal de A. En efecto,

   i) $0 \in \mathrm{Ker}f$, pues $f(0) = 0'$.

ii) Si $a, b \in \text{Ker}f$, entonces $f(a-b) = f(a) - f(b) = 0' - 0' = 0'$. Luego, $a - b \in \text{Ker}f$.

iii) Si $x \in A$ y $a \in \text{Ker}f$, entonces $f(x \cdot a) = f(x) \cdot f(a) = f(x) \cdot 0' = 0'$. Luego, $x \cdot a \in \text{Ker}f$. De forma análoga, se prueba que $a \cdot x \in \text{Ker}f$.

Ahora, si f es inyectiva y $0 \neq x \in \text{Ker}f$, luego $f(x) = f(0) = 0'$. Por la inyectividad de f, se sigue que $x = 0$, lo que es una contradicción. Así, $\text{Ker}f = \{0\}$. Por otro lado, si $\text{Ker}f = \{0\}$ y $f(x) = f(y)$, se tiene que $x - y \in \text{Ker}f$ pues $f(x-y) = f(x) - f(y) = 0'$. Así, se concluye que $x = y$ y por lo tanto f es inyectiva.

3) Definimos la función:

$$\begin{aligned} F : A/\text{Ker}f &\to \text{Im}f \\ x + \text{Ker}f &\mapsto f(x) \end{aligned}$$

Luego, dados $x + \text{Ker}f, y + \text{Ker}f \in A/\text{Ker}f$, tenemos:

i) $F((x + \text{Ker}f) + (y + \text{Ker}f)) = F((x+y) + \text{Ker}f) = f(x+y) = f(x) + f(y) = F(x + \text{Ker}f) + F(y + \text{Ker}f)$,

ii) $F((x + \text{Ker}f) \cdot (y + \text{Ker}f)) = F(x \cdot y + \text{Ker}f) = f(x \cdot y) = f(x) \cdot f(y) = F(x + \text{Ker}f) \cdot F(y + \text{Ker}f)$.

De $i)$ y $ii)$, F es un homomorfismo de anillos.

Observe que,

$$\begin{aligned} F(x + \text{Ker}f) = F(y + \text{Ker}f) &\Leftrightarrow f(x) = f(y) \\ &\Leftrightarrow f(x-y) = 0 \\ &\Leftrightarrow x - y \in \text{Ker}f \\ &\Leftrightarrow x \in y + \text{Ker}f \\ &\Leftrightarrow x + \text{Ker}f = y + \text{Ker}f. \end{aligned}$$

Lo que verifica que F está bien definida y también que es inyectiva.

Finalmente, $\text{Im}F = \{F(x + \text{Ker}f) : x + \text{Ker}f \in A/\text{Ker}f\} = \{f(x) : x \in A\} = \text{Im}f$. Luego, $A/\text{Ker}f \simeq \text{Im}f$.

□

El subanillo $\text{Im}f$ de B se dice *imagen* de f y el ideal $\text{Ker}f$ de A se dice *núcleo* de f.

1.1.4. Localización

En esta sección introduciremos un procedimiento algebraico llamado localización, que nos servirá para construir anillos locales a partir de anillos. La referencia para esta subsección es (Carballo Rodríguez, s.f.).

Sea A un anillo conmutativo con unidad 1.

Definición 1.1.23. Decimos que S es un *subconjunto multiplicativo* de A si $S \subseteq A$ tal que

a. $1 \in S$,

b. si $x, y \in S$, entonces $xy \in S$.

Consideramos en $A \times S$ la relación

$$(a, s) \sim (a', s') \Leftrightarrow \text{existe } s_1 \in S \text{ tal que } s_1(s'a - sa') = 0.$$

Luego, podemos verificar que esta es una relación de equivalencia en $A \times S$.
En efecto, para cualquier $(a, s), (a', s'), (\tilde{a}, \tilde{s}) \in A \times S$ tenemos:

- $(a, s) \sim (a, s)$ pues $1 \in S$ y $1(sa - sa) = 0$. (Propiedad Reflexiva).
- $(a, s) \sim (a', s')$, luego existe $s_1 \in S$ tal que $s_1(s'a - sa') = s_1(sa' - s'a) = 0$. Entonces, $(a', s') \sim (a, s)$. (Propiedad Simétrica)
- $(a, s) \sim (a', s')$ y $(a', s') \sim (\tilde{a}, \tilde{s})$, entonces existen s_1 y s_2 tales que $s_1(s'a - sa') = 0$ y $s_2(\tilde{s}a' - s'\tilde{a}) = 0$. Luego,

  $$s_1 s'a = s_1 sa' \quad \text{y} \quad s_2 \tilde{s}a' = s_2 s'\tilde{a}.$$

  Multiplicando las igualdades anteriores por $s_2\tilde{s}$ y $s_1 s$ respectivamente, se tiene

  $$(s_1 s_2 s')\tilde{s}a = s_1 s_2 \tilde{s} s a' = (s_1 s_2 s')s\tilde{a}.$$

  Como $s_1 s_2 s' \in S$, entonces $(a, s) \sim (\tilde{a}, \tilde{s})$. (Propiedad Transitiva)

La *clase de equivalencia* de $(a, s) \in A \times S$ en relación a $\sim$ es denotada por

$$a/s = \{(a', s') \in A \times S : (a', s') \sim (a, s)\}.$$

Además, definimos el conjunto

$$S^{-1}A = \{a/s : a \in A \text{ y } s \in S\}.$$

Proposición 1.1.24. *Sea S un subconjunto multiplicativo de A. El conjunto $S^{-1}A$ con las siguientes operaciones*

$$+ : S^{-1}A \times S^{-1}A \to S^{-1}A \qquad \cdot : S^{-1}A \times S^{-1}A \to S^{-1}A$$
$$(a/s, a'/s') \mapsto (s'a + sa')/ss \qquad (a/s, a'/s') \mapsto aa'/ss'$$

tiene una estructura de anillo.

Demostración: Veamos que $+$ y $\cdot$ están bien definidos.

En efecto, si $(a_1, s_1) \in a/s$ y $(a'_1, s'_1) \in a'/s'$, entonces $(a_1, s_1) \sim (a, s)$ y $(a'_1, s'_1) \sim (a', s')$. Luego, existen $s_2, s_3 \in S$ tal que

$$s_2(sa_1 - s_1a) = 0,$$
$$s_3(s'a'_1 - s'_1a') = 0.$$

- Multiplicamos la primera ecuación por $(s_3s'_1)$ y la segunda ecuación por (ss_1s_2), luego sumamos ambas ecuaciones y obtenemos:

  $$s_2s_3[ss'(s'_1a_1 + s_1a'_1) - s_1s'_1(s'a + sa')] = 0$$

  Como $s_2s_3 \in S$, entonces

  $$((s'_1a_1 + s_1a'_1), s_1s'_1) \sim ((s'a + sa'), ss').$$

  Luego, $(s'_1a_1 + s_1a'_1)/s_1s'_1 = (s'a + sa')/ss'$.

- Multiplicamos la primera ecuación por $(s_3s'a'_1)$ y la segunda ecuación por (s_1s_2a), luego sumamos ambas ecuaciones y obtenemos:

  $$s_2s_3[ss'a_1a'_1 - s_1s'_1aa'] = 0$$

  Como $s_2s_3 \in S$, entonces

  $$(a_1a'_1, s_1s'_1) \sim (aa', ss').$$

  Luego, $a_1a'_1/s_1s'_1 = aa'/ss'$.

Resta probar que $(S^{-1}A, +, \cdot)$ verifica las 6 propiedades de la Definición 1.1.1: Sean $a/s, a'/s', a''/s'' \in S^{-1}A$

A1) Asociatividad de la suma.

$$\begin{aligned}(a/s + a'/s') + a''/s'' &= (s'a + sa')/ss' + a''/s'' \\ &= (s''(s'a + sa') + ss'a'')/(ss')s'' \\ &= (s's''a + s(s''a' + s'a''))/s(s's'') \\ &= a/s + (s''a' + s'a'')/s's'' \\ &= a/s + (a'/s' + a''/s'')\end{aligned}$$

A2) Conmutatividad de la suma.

$$\begin{aligned}a/s + a'/s' &= (s'a + sa')/ss' \\ &= (sa' + s'a)/s's \\ &= a'/s' + a/s\end{aligned}$$

A3) Existencia del elemento neutro para la suma.
Tenemos que $a/s + 0/1 = 0/1 + a/s = a/s$. Por lo tanto, $0/1$ es el elemento neutro para la suma en $S^{-1}A$.

A4) Existencia del inverso aditivo.
Tenemos que $a/s + (-a)/s = (-a)/s + a/s = 0/s^2$, pero $0/s^2 = 0/1$ ya que $1(1 \cdot 0 - s^2 \cdot 0) = 0$. Por lo tanto, $(-a)/s$ es el inverso aditivo de a/s.

A5) Asociatividad del producto.

$$\begin{aligned}(a/s \cdot a'/s') \cdot a''/s'' &= aa'/ss' \cdot a''/s'' \\ &= (aa')a''/(ss')s'' \\ &= a(a'a'')/s(s's'') \\ &= a/s \cdot a'a''/s's'' \\ &= a/s \cdot (a'/s' \cdot a''/s'')\end{aligned}$$

A6) Distributividad.

$$\begin{aligned}a/s \cdot (a'/s' + a''/s'') &= a/s \cdot (s''a' + s'a'')/s's'' \\ &= a(s''a' + s'a'')/s(s's'') \\ &= (ss''aa' + ss'aa'')/ss'ss'' \\ &= aa'/ss' + aa''/ss'' \\ &= a/s \cdot a'/s' + a/s \cdot a''/s''\end{aligned}$$

De forma análoga, se verifica que

$$(a/s + a'/s') \cdot a''/s'' = a/s \cdot a''/s'' + a'/s' \cdot a''/s''.$$

□

Note que $1/1$ es la unidad de $S^{-1}A$ pues

$$1/1 \cdot a/s = 1 \cdot a/1 \cdot s = a/s = a \cdot 1/s \cdot 1 = a/s \cdot 1/1 \quad \forall a \in A \text{ y } \forall s \in S.$$

Además, como A es conmutativo, entonces $S^{-1}A$ también es conmutativo pues

$$a/s \cdot a'/s' = aa'/ss' = a'a/s's = a'/s' \cdot a/s \quad \forall a, a' \in A \text{ y } \forall s, s' \in S.$$

Observación 1.1.25. Si $a \in A$ y $s, s' \in S$, entonces $a/s = s'a/s's$ ya que

$$1(s'sa - ss'a) = 0.$$

Llamaremos *anillo de fracciones* de A por S al conjunto $S^{-1}A$ con las operaciones definidas en la Proposición 1.1.24.

Sean A un anillo conmutativo con unidad 1 y S un subconjunto multiplicativo de A, definimos la función:

$$\begin{aligned} \varphi_S : A &\to S^{-1}A \\ a &\mapsto a/1 \end{aligned}$$

Luego, dados $a, b \in A$, tenemos:

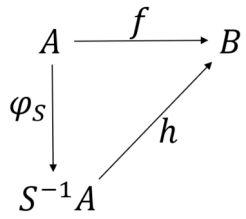
i) $\varphi_S(a+b) = (a+b)/1 = a/1 + b/1 = \varphi_S(a) + \varphi_S(b)$

ii) $\varphi_S(ab) = ab/1 = a/1 \cdot b/1 = \varphi_S(a) \cdot \varphi_S(b)$

Así, φ_S es un homomorfismo de anillos. Además, cada elemento de $\varphi_S(S)$ es inversible en $S^{-1}A$ (La inversa de $s/1$ es $1/s$).

Sean A y B anillos conmutativos con unidad, por simplicidad vamos a denotar por 1 a la unidad de A y B.

Proposición 1.1.26. *Sea S un subconjunto multiplicativo de A. Si $f : A \to B$ es un homomorfismo de anillos tal que cada elemento de $f(S)$ es inversible en B, entonces existe un único homomorfismo de anillos $h : S^{-1}A \to B$ tal que $f = h \circ \varphi_S$.*



Demostración: Definimos la función:

$$\begin{aligned} h : S^{-1}A &\to B \\ a/s &\mapsto f(a)f(s)^{-1} \end{aligned}$$

Veamos que h está bien definida.

En efecto, sea $(a', s') \in a/s$, entonces $(a', s') \sim (a, s)$. Luego, existe $s_1 \in S$ tal que

$$s_1(sa' - s'a) = 0.$$

Como f es un homomorfismo, se sigue que

$$\begin{aligned} 0 &= f(s_1(sa' - s'a)) \\ &= f(s_1)(f(s)f(a') - f(s')f(a)) \\ &= f(s_1)f(s)f(a') - f(s_1)f(s')f(a) \end{aligned}$$

multiplicando por $(f(s_1)^{-1}f(s')^{-1}f(s)^{-1})$, obtenemos

$$f(a')f(s')^{-1} = f(a)f(s)^{-1}.$$

Luego, dados $a/s, a'/s' \in S^{-1}/A$, tenemos:

i)

$$\begin{aligned} h(a/s + a'/s') &= h((s'a + sa')/ss') \\ &= f(s'a + sa')f(ss')^{-1} \\ &= (f(s')f(a) + f(s)f(a'))f(s)^{-1}f(s')^{-1} \\ &= f(a)f(s)^{-1} + f(a')f(s')^{-1} \\ &= h(a/s) + h(a'/s') \end{aligned}$$

ii)

$$\begin{aligned} h(a/s \cdot a'/s') &= h(aa'/ss') \\ &= f(aa')f(ss')^{-1} \\ &= f(a)f(s)^{-1}f(a')f(s')^{-1} \\ &= h(a/s) \cdot h(a'/s') \end{aligned}$$

De $i)$ y $ii)$, h es un homomorfismo de anillos, tal que

$$(h \circ \varphi_S)(a) = h(\varphi_S(a)) = h(a/1) = f(a).f(1)^{-1} = f(a) \quad \forall a \in A.$$

Resta probar la unicidad de h para que h sea el homomorfismo deseado.

Supongamos que existe un homomorfismo de anillos $h \neq h'$ tal que $f = h' \circ \varphi_S$.

Para $s \in S$, tenemos:

$$\begin{aligned} \varphi_S(s)\varphi_S(s)^{-1} &= 1/1 \\ h'(\varphi_S(s))h'(\varphi_S(s)^{-1}) &= 1 \\ f(s)h'(\varphi_S(s)^{-1}) &= 1. \end{aligned}$$

Entonces, $h'(\varphi_S(s)^{-1}) = f(s)^{-1}$. Analogamente, se prueba que $h(\varphi_S(s)^{-1}) = f(s)^{-1}$. Luego,

$$\begin{aligned} h'(\varphi_S(s)^{-1}) &= h(\varphi_S(s)^{-1}) \\ h'(1/s) &= h(1/s). \end{aligned}$$

Además, para $a \in A$, tenemos:

$$\begin{aligned} h'(\varphi_S(a)) &= h(\varphi_S(a)) \\ h'(a/1) &= h(a/1). \end{aligned}$$

Finalmente,

$$h(a/s) = h(a/1)h(1/s) = h'(a/1)h'(1/s) = h'(a/s) \quad \forall a/s \in S^{-1}A.$$

Lo que es una contradicción, por lo tanto h es único. □

Ejemplo 1.1.27. Sea A un dominio de integridad. Si S es el conjunto de todos los elementos de A diferentes de 0, entonces S es un conjunto multiplicativo de A, pues $1 \neq 0$ y para todo $a, b \neq 0$ se tiene que $ab \neq 0$. Luego, $S^{-1}A$ es un cuerpo.

En efecto, si $0 \neq a/s \in S^{-1}A$, entonces $0 \neq a \in S$. Luego, $s/a \in S^{-1}A$ y $a/s \cdot s/a = s/a \cdot a/s = 1/1$. Se sigue que s/a es el inverso multiplicativo de a/s.

En este caso, $S^{-1}A$ es llamado *cuerpo cociente* de A.

Ejemplo 1.1.28. Sea A un anillo conmutativo con unidad 1 y P un ideal primo de A. Si $S = A \setminus P$, entonces S es un subconjunto multiplicativo de A, pues $1 \notin P$ y para todo $x, y \notin P$, se tiene que $xy \notin P$. Luego, $A_P = S^{-1}A$ es un anillo local.

En efecto, sea el conjunto

$$M = \{p/s : p \in P \text{ y } s \notin P\} \subset A_P.$$

AFIRMACIÓN: M es el único ideal maximal de A_P.

Primero, vamos a ver que M es un ideal. En efecto, tenemos que se verifica:

i) $0/1 \in M$ pues $0 \in P$ y $1 \notin P$.

ii) Si $p/s, \tilde{p}/\tilde{s} \in M$, entonces $p/s + \tilde{p}/\tilde{s} = (\tilde{s}p + s\tilde{p})/s\tilde{s} \in M$ pues $\tilde{s}p + s\tilde{p} \in P$ y $s\tilde{s} \notin P$.

iii) Si $p/s \in M$ y $a/s' \in A_P$, entonces $p/s \cdot a/s' = pa/ss' \in M$ pues $pa \in P$ y $ss' \notin P$.

Supongamos que existe un ideal $\overline{M}$ conteniendo M tal que $\overline{M} \neq M$. Consideramos $a/s \in \overline{M} \setminus M$, esto es, $a, s \notin P$. Luego, $s/a \in A_P$, lo que implica que $a/s \cdot s/a = 1/1 \in \overline{M}$. Así, $\overline{M} = A_P$. Por lo tanto, M es maximal.

Resta probar que M es único . Supongamos que M no es único. Sea $a/s \notin M$ que no es inversible en A_P, entonces el ideal principal (a/s) debe estar contenido en algún ideal maximal $\widetilde{M} \neq M$, caso contrario $a/s \in M$. Como $a, s \notin P$, entonces $s/a \in A_P$, lo que es una contradicción pues a/s no es inversible. Por lo tanto, M es único.

Este ejemplo será de gran importancia más adelante.

1.2. Extensiones de Cuerpos

Las referencias para esta sección son (Morandi, 2012) y (Lang, 2012).

1.2.1. Conceptos Básicos

Sean E y F cuerpos.

Definición 1.2.1. Si F es un subcuerpo de E, decimos que E es una *extensión de cuerpo* de F y denotamos E/F.

Ejemplo 1.2.2. $\mathbb{R}$ es una extensión de cuerpo de $\mathbb{Q}[\sqrt{p}]$ y $\mathbb{Q}[\sqrt{p}]$ es una extensión de cuerpo de $\mathbb{Q}$, para todo p primo.

Consideramos E/F como un E espacio vectorial sobre F y denotamos la dimensión de este espacio vectorial como $[E : F]$.

Definición 1.2.3. Sea E una extensión de cuerpo de F. Decimos que E es una *extensión finita* de F si $[E : F] < \infty$. Caso contrario, decimos que E es una *extensión infinita* de F.

Definición 1.2.4. Sea E una extensión de cuerpo de F. Decimos que un elemento $\alpha \in E$ es *algebraico* sobre F si existe un polinomio mónico diferente de cero $f(X) \in F[X]$ tal que $f(\alpha) = 0$. En el caso que α no sea algebraico, decimos que α es *trascendental* sobre F. Si cada elemento de E es algebraico sobre F, decimos que E es *algebraico* sobre F.

Ejemplo 1.2.5. $\mathbb{R}/\mathbb{Q}$ es una extensión de cuerpo y $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, ya que $\sqrt{2}$ es una raiz de $f(X) = X^2 - 2 \in \mathbb{Q}[X]$.

Ejemplo 1.2.6. π y e son trascendentales sobre $\mathbb{Q}$. Para más detalles,ver (Baker, 2022).

Sean E/F una extensión de cuerpo y $\alpha \in E$. La función

$$\begin{aligned} \phi_\alpha : F[X] &\to E \\ f(X) &\mapsto f(\alpha), \end{aligned}$$

define un homomorfismo. En efecto, dados $f(X), g(X) \in F[X]$, se cumple:

i) $\phi_\alpha(f(X) + g(X)) = f(\alpha) + g(\alpha) = \phi_\alpha(f(X)) + \phi_\alpha(g(X))$.

ii) $\phi_\alpha(f(X) \cdot g(X)) = f(\alpha) \cdot g(\alpha) = \phi_\alpha(f(X)) \cdot \phi_\alpha(g(X))$.

Además, si α es algebraico sobre F, entonces Ker $\phi_\alpha \neq \{0\}$ y si α es trascendental sobre F, entonces Ker $\phi_\alpha = \{0\}$.

Como F es un cuerpo, entonces $F[X]$ es un dominio de ideales principales. Luego, Ker ϕ_α es un ideal principal. Si α es algebraico sobre F, entonces existe $p(X) \in F[X]$ con $\text{gr}(p(X)) \geq 1$, el cual podemos suponer que es mónico, tal que Ker $\phi_\alpha = (p(X))$. Esto es, si $f(X) \in$ Ker ϕ_α, entonces $p(X)$ divide a $f(X)$ y $\text{gr}(p(X)) \leq \text{gr}(f(X))$. Si $\text{gr}(p(X)) = \text{gr}(f(X))$, entonces $f(X) = ap(X)$ para algún $a \in F$.

Supongamos que $p(X)$ no es irreducible, entonces existen $f(X), g(X) \in F[X]$, cada uno con grado estrictamente menor que el grado de $p(X)$, tal que $p(X) = f(X)g(X)$. Luego, $0 = \phi_\alpha(p(X)) = f(\alpha)g(\alpha) \in E$, lo que implica que $f(\alpha) = 0$ o $g(\alpha) = 0$, esto es, $p(X)$ divide a $f(X)$ o $p(X)$ divide a $g(X)$. Entonces, $\text{gr}(p(X)) \leq \text{gr}(f(X))$ o $\text{gr}(p(X)) \leq \text{gr}(g(X))$, lo cual es una contradicción. Así, obtenemos que $p(X)$ es irreducible. Decimos que $p(X)$ es el *polinomio irreducible* de α sobre F y lo denotamos por $Irr(\alpha, F, X)$.

Ejemplo 1.2.7. Sean E/F una extensión de cuerpo y $\alpha \in E$ algebraico sobre F. Si consideramos $\phi_\alpha : F[X] \to E$ definido como antes, entonces Ker $\phi_\alpha = (Irr(\alpha, F, X))$. Como $F[X]$ es un dominio de ideales principales y $Irr(\alpha, F, X)$ es irreducible sobre F, entonces $(Irr(\alpha, F, X))$ es un ideal maximal de $F[X]$, lo que implica que $F[X]/(Irr(\alpha, F, X))$ es un cuerpo que extiende a F.

Denotamos $F[\alpha] = \{f(\alpha) : f(X) \in F[X]\}$. Luego, $F[X]/(Irr(\alpha, F, X)) \simeq F[\alpha]$, lo que implica que $F[\alpha]$ también es un cuerpo.

Definición 1.2.8. Definimos una *torre* de cuerpos como una secuencia

$$F_1 \subset F_2 \subset ... \subset F_n$$

de extensiones de cuerpos. La torre es llamada *finita* si y solo sí F_{i+1}/F_i es una extensión finita para cada $1 \leq i < n$.

Proposición 1.2.9. *Sea E una extensión de cuerpo de F. Si E/F es una extensión finita, entonces E/F es una extensión algebraica.*

Demostración: Sea $\alpha \in E$ tal que $\alpha \neq \emptyset$. Como $[E : F] < \infty$, entonces las potencias de α,

$$1, \alpha, \alpha^2, ..., \alpha^n,$$

no son linealmente independientes para todo $n \in \mathbb{N}$. Luego, existen $a_0, a_1, ..., a_N \in F$, no todos nulos, para algún $N \in \mathbb{N}$ tal que

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_N\alpha^N = 0 \quad a_N \neq 0.$$

Multiplicando por a_N^{-1}, obtenemos

$$a_0a_N^{-1} + a_1a_N^{-1}\alpha + a_2a_N^{-1}\alpha^2 + ... + \alpha^N = 0.$$

Si $f(X) = a_0a_N^{-1} + a_1a_N^{-1}X + a_2a_N^{-1}X^2 + ... + X^N \in F[X]$, luego $f(\alpha) = 0$. Como $\alpha \in E$ fue arbitrario, entonces E es algebraico sobre F. □

Proposición 1.2.10. *Sea $K \subset F \subset E$ una torre de cuerpos. Entonces,*

$$[E : K] = [E : F][F : K].$$

Además, si $\{x_i\}_{i\in I}$ es una base para F sobre K y $\{y_j\}_{j\in J}$ es una base para E sobre F, entonces $\{x_iy_j\}_{(i,j)\in I\times J}$ es una base para E sobre K.

Demostración: Sea $z \in E$. Por hipótesis, existe una familia $\{\alpha_j\}_{j\in J}$ de elementos de F, donde casi todo $\alpha_j = 0$, tal que

$$z = \sum_{j\in J} \alpha_j y_j.$$

Luego, para cada $j \in J$, existe una familia $\{b_{ji}\}_{i\in I}$ de elementos de K, donde casi todo $b_{ji} = 0$, tal que

$$\alpha_j = \sum_{i\in I} b_{ji}x_i,$$

y por lo tanto

$$z = \sum_j \sum_i b_{ji}x_iy_j.$$

Esto prueba que x_iy_j es una familia de generadores para E sobre K. Resta probar que $\{x_iy_j\}_{(i,j)\in I\times J}$ es linealmente independiente. Sea $\{c_{ij}\}_{(i,j)\in I\times J}$ una familia de elementos de K, donde casi todos son 0, tal que

$$\sum_j \sum_i c_{ij}x_iy_j = 0.$$

Luego, para cada j

$$\sum_i c_{ij}x_i = 0,$$

porque los elementos y_j son linealmente independientes sobre F. Finalmente, $c_{ij} = 0$ $\forall i \in I$ y $\forall j \in J$, porque los elementos x_i son linealmente independientes sobre K, con lo cual queda probado. □

Definición 1.2.11. Sea E una extensión de cuerpo de K y sea $\alpha \in E$. Definimos $K(\alpha)$ como la intersección de todos los subcuerpos de E que contienen K y α.

Lema 1.2.12. *Sea E una extensión de cuerpo de K y sea $\alpha \in E$. Luego, $K(\alpha)$ es el menor subcuerpo de E conteniendo K y α. Además, $K(\alpha)$ es igual al cuerpo cociente de $K[\alpha]$, esto es,*

$$K(\alpha) = \{f(\alpha)/g(\alpha) : f, g \in K[x], g(\alpha) \neq 0\}.$$

Demostración: Supongamos que H es el menor subcuerpo de E que contiene K y α tal que $H \neq K(\alpha)$. Luego, por definición de $K(\alpha)$, se tiene que $K(\alpha) \subset H$, lo que contradice la minimalidad. Por lo tanto, $K(\alpha)$ es el menor subcuerpo de E que contiene K y α.

Por otro lado, definimos el conjunto

$$K' = \{f(\alpha)/g(\alpha) : f, g \in K[x], g(\alpha) \neq 0\}.$$

Vamos a probar que $K' = K(\alpha)$.

En efecto, sea $a \in K$ y sean $f(X) = aX$, $g(X) = X \in K[X]$. Luego,

$$a = f(\alpha)/g(\alpha) \in K'.$$

Así, $K \subseteq K'$. Además, sean $\tilde{f}(X) = cX, \tilde{g}(X) = c \in K[X]$ para algún $0 \neq c \in K$. Luego,

$$\alpha = \tilde{f}(\alpha)/\tilde{g}(\alpha) \in K'.$$

Como K' es un subcuerpo que contiene K y α, entonces $K(\alpha) \subseteq K'$.

Sea $a \in K'$, entonces existen $f(X), g(X) \in K[X]$ tal que $g(\alpha) \neq 0$ y

$$a = f(\alpha)/g(\alpha).$$

Además, para todo subcuerpo F de E conteniendo K y α, se tiene que $f(\alpha), g(\alpha) \in F$, lo que implica que $a \in F$. Luego, a pertenece a la intersección de todos los subcuerpos de E que contienen K y α.

Así, $K' \subseteq K(\alpha)$ como se quería probar. □

Proposición 1.2.13. *Sea α algebraico sobre K. Entonces, $K(\alpha) = K[\alpha]$ y $K(\alpha)/K$ es una extensión finita. Además, $[K(\alpha) : K]$ es igual al grado de $Irr(\alpha, K, X)$.*

Demostración:

Sea el homomorfismo ϕ_α de $K[X]$ en alguna extensión de cuerpo de K que contenga α. Como α es algebraico sobre K, entonces existe el polinomio irreducible $p(X) = Irr(\alpha, K, X)$ que genera Ker ϕ_α.

Sea $f(X) \in K[X]$ tal que $f(\alpha) \neq 0$, entonces $f(X) \notin$ Ker ϕ_α, esto implica que $p(X)$ no divide a $f(X)$. Entonces, existen polinomios $g(X), h(X) \in K[X]$ tal que

$$1 = g(X)p(X) + h(X)f(X).$$

Luego,

$$\begin{aligned} 1 &= g(\alpha)p(\alpha) + h(\alpha)f(\alpha) \\ 1 &= h(\alpha)f(\alpha), \end{aligned}$$

de aquí vemos que $f(\alpha)$ es inversible en $K[\alpha]$ por $h(\alpha)$. Por lo tanto, $K[\alpha]$ es un cuerpo.

Por definición, $K(\alpha) \subseteq K[\alpha]$. Además, $f(\alpha) = f(\alpha)/1 \in K(\alpha)$ para todo $f(X) \in K[X]$, entonces $K[\alpha] \subseteq K(\alpha)$. Así, hemos probado que $K[\alpha] = K(\alpha)$.

Sea $n = \text{gr}(p(X))$.

AFIRMACIÓN: El conjunto $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ es una base de $K[\alpha]$ como un espacio vectorial sobre K.

En efecto, supongamos que $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ no son linealmente independientes sobre K, entonces existen $a_0, a_1, ..., a_{n-1} \in K$ no todos 0, tal que

$$a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = 0.$$

Sea $g(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} \in K[X]$. Luego, $g(\alpha) = 0$, lo que implica que $p(X)$ dvide a $g(X)$. Entonces, $n = \text{gr}(p(X)) \leq \text{gr}(g(X)) = n - 1$, lo que es una contradicción. Por lo tanto, $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ son linealmente independientes en K.

Finalmente, sea $f(\alpha) \in K[\alpha]$ para algún $f(X) \in K[X]$. Luego, existen polinomios $q(X), r(X) \in K[X]$ tal que $\text{gr}(r(X)) < \text{gr}(p(X)) = n$ y

$$f(X) = q(X)p(X) + r(X).$$

Entonces,

$$\begin{aligned} f(\alpha) &= q(\alpha)p(\alpha) + r(\alpha) \\ f(\alpha) &= r(\alpha) \\ f(\alpha) &= b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} \quad ; \quad b_0, b_1, ..., b_{n-1} \in K. \end{aligned}$$

De ahí, tenemos que $K[\alpha]$ es generado por $1, \alpha, \alpha^2, ..., \alpha^{n-1}$, lo que prueba nuestra afirmación.

Se sigue que $K(\alpha)/K$ es una extensión finita y $[K(\alpha) : K] = n = \text{gr}(Irr(\alpha, K, X))$. □

Ejemplo 1.2.14. Sea $\mathbb{R}/\mathbb{Q}$ una extensión de cuerpo y $\sqrt{3}$ es algebraico sobre $\mathbb{Q}$. Definimos:

$$\begin{aligned} \varphi_{\sqrt{3}} : \mathbb{Q}[X] &\to \mathbb{R} \\ f(X) &\mapsto f(\sqrt{3}) \end{aligned}$$

Luego, $\text{Ker}(\varphi_{\sqrt{3}})$ es generado por $Irr(\sqrt{3}, \mathbb{Q}, X) = x^2 - 3$. Además, $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ y

$$\mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \ ; \ a, b \in \mathbb{Q}\}.$$

1.2.2. Cerradura Algebraica

Definición 1.2.15. Sea L un cuerpo. Decimos que L es *algebraicamente cerrado* si cada polinomio en $L[X]$ de grado ≥ 1 tiene raíces en L.

Ejemplo 1.2.16. El teorema fundamental del álgebra afirma que todo polinomio en $\mathbb{C}$ de grado $n \geq 1$ tiene, contando multiplicidades, n raíces en $\mathbb{C}$. Entonces, $\mathbb{C}$ es algebraicamente cerrado.

Teorema 1.2.17. *Si K es un cuerpo, entonces existe una extensión de cuerpo de K que es algebraicamente cerrado.*

Demostración: Ver (Lang, 2012).

Proposición 1.2.18. *Sea K un cuerpo y sea α algebraico sobre K. Si $\sigma : K \to L$ es un homomorfismo inyectivo de K en un cuerpo algebraicamente cerrado L, entonces el número posible de homomorfismos inyectivos que extienden σ a $K(\alpha)$ es menor o igual al número de raíces del polinomio $Irr(\alpha, K, X)$.*

Demostración: Ver (Lang, 2012)

El siguiente teorema nos permite encontrar una extensión de un homomorfismo σ definido en un cuerpo K a un homomorfismo de una extensión algebraica arbitraria de K, para la demostración usaremos el Lema de Zorn.

Dado un conjunto C, una *relación de orden* en C es una relación binaria $\preceq$ que verifica las siguientes propiedades:

- $x \preceq x$ para todo $x \in C$. (Propiedad reflexiva)
- Si $x \preceq y$ e $y \preceq z$, entonces $x \preceq z$ para todo $x, y, z \in C$. (Propiedad transitiva)
- Si $x \preceq y$ e $y \preceq x$, entonces $x = y$ para todo $x, y \in C$. (Propiedad antisimétrica)

Luego $(C, \preceq)$ se llama un conjunto *parcialmente ordenado.*

Para cada subconjunto X de un conjunto parcialmente ordenado C, podemos definir una relación de orden restringiendo la relación de C en X, entonces X también es parcialmente ordenado.

Si C es un conjunto parcialmente ordenado y $X \subseteq C$, una *cota superior* de X en C es un elemento $a \in C$ tal que $x \leq a$ para todo $x \in X$ y un *máximo* en C es un elemento $a \in C$ tal que $c \leq a$ para todo $c \in C$.

Un conjunto parcialmente ordenado C se dice *totalmente ordenado* si para todo $a, b \in C$ se tiene que $a \preceq b$ o $b \preceq a$, y se dice *inductivamente ordenado* si cada subconjunto $X \subseteq C$ totalmente ordenado con el orden inducido tiene una cota superior en C.

Lema 1.2.19 (Zorn)**.** *Sea C un conjunto parcialmente ordenado. Si C es inductivamente ordenado, entonces tiene un elemento maximal.*

Demostración: Ver (Boyallían y Ovando, 1994).

Teorema 1.2.20. *Sean K un cuerpo y E una extensión algebraica de K. Si $\sigma : K \to L$ es un homomorfismo inyectivo de K en un cuerpo algebraicamente cerrado L, entonces existe una extensión de σ a un homomorfismo inyectivo λ de E en L.*

Demostración:

Sea C el conjunto de todos los pares (F, τ) donde F es un subcuerpo de E conteniendo K, y τ es un homomorfismo inyectivo de F en L que extiende σ.

Consideramos en C la relación

$$(F, \tau) \leq (F', \tau') \Leftrightarrow F \subseteq F' \text{ y } \tau'|F = \tau.$$

Luego, esta es una relación de orden parcial en C. En efecto, para cualquier (F, τ), (F', τ'), $(F'', \tau'') \in C$ tenemos:

i) $(F, \tau) \leq (F, \tau)$ pues $F \subseteq F$ y $\tau|F = \tau$.

ii) Si $(F, \tau) \leq (F', \tau')$ y $(F', \tau') \leq (F'', \tau'')$, entonces

$$F \subseteq F' \quad \wedge \quad \tau'|F = \tau \quad \text{y} \quad F' \subseteq F'' \quad \wedge \quad \tau''|F' = \tau'.$$

Luego,

$$F \subseteq F' \subseteq F'' \quad \text{y} \quad \tau''|F = \tau'|F = \tau.$$

Así, $(F, \tau) \leq (F'', \tau'')$.

iii) Si $(F, \tau) \leq (F', \tau')$ y $(F', \tau') \leq (F, \tau)$, entonces

$$F \subseteq F' \quad \wedge \quad \tau'|F = \tau \quad \text{y} \quad F' \subseteq F \quad \wedge \quad \tau|F' = \tau'.$$

Luego, $F = F'$ y por lo tanto $\tau = \tau'$. Así, $(F, \tau) = (F', \tau')$.

Entonces, $(C, \leq)$ es un conjunto parcialmente ordenado. Note que $C \neq \emptyset$ ya que $(K, \sigma) \in C$.

AFIRMACIÓN: C es inductivamente ordenado.

En efecto, sea $X = \{(F_i, \tau_i)\}$ un subconjunto totalmente ordenado. Definimos, $F = \bigcup F_i$ un subcuerpo de E que contiene K y τ en F tal que $\tau|F_i = \tau_i$. Luego, se cumple:

- $\tau : F \to L$ es un homomorfismo inyectivo que extiende σ.

Sean $x, y \in F$, entonces $x \in F_i$ e $y \in F_j$ para algunos i, j. Como X es totalmente ordenado, sin pérdida de generalidad podemos suponer que $(F_i, \tau_i) \leq (F_j, \tau_j)$, entonces $x, y \in F_j$. Luego,

$$\tau(x+y) = \tau_j(x+y) = \tau_j(x) + \tau_j(y) = \tau(x) + \tau(y),$$
$$\tau(x \cdot y) = \tau_j(x \cdot y) = \tau_j(x) \cdot \tau_j(y) = \tau(x) \cdot \tau(y)$$

y

$$\begin{aligned} \tau(x) &= \tau(y) \\ \tau(x-y) &= 0 \\ \tau_j(x-y) &= 0 \\ x-y &= 0 \\ x &= y. \end{aligned}$$

Además, como K está contenido en todo F_i se tiene que $\tau|K = \tau_i|K = \sigma$.

- $(F_i, \tau_i) \leq (F, \tau)$ para todo i.

  Es claro que $F_i \subseteq F$ para todo i y por definición $\tau|F_i = \tau_i$.

Luego, $(F, \tau) \in C$ y es una cota superior de X. Así, la afirmación queda probada.

Usando el Lema de Zorn, sea (H, λ) un elemento maximal en C. Supongamos que $H \neq E$, entonces existe $\alpha \in E \setminus H$. Luego, por la Proposición 1.2.18 existe un homomorfismo inyectivo $\tilde{\lambda} : K(\alpha) \to L$ que extiende λ. Como λ extiende σ, entonces $\tilde{\lambda}$ extiende σ. Luego, $(K(\alpha), \tilde{\lambda}) \in C$, lo que contradice la maximalidad de (H, λ). Por lo tanto, existe un homomorfismo inyectivo $\lambda : E \to L$ que extiende σ. □

Definición 1.2.21. Sea K un cuerpo. Decimos que E es una *clausura algebraica* de K si E es una extensión algebraica de K que es algebraicamente cerrada.

Capítulo 2

Extensiones de Anillos

Sean A y B anillos conmutativos con unidad. Siempre que A es subanillo de B, asumimos que la unidad de A es igual a la unidad de B. Más aún, asumimos que todo homomorfismo de anillos con unidad lleva la unidad en la unidad.

Definición 2.0.1. Si A es un subanillo de B, decimos que B es una *extensión de anillo* de A.

Definición 2.0.2. Sea A un subanillo de B. Decimos que un elemento $\alpha \in B$ es *integral* sobre A si existe un polinomio mónico diferente de cero $f(X) \in A[X]$ tal que $f(\alpha) = 0$. Si cada elemento de B es integral sobre A, decimos que B es *integral* sobre A.

Proposición 2.0.3. *Sea A un subanillo de B. Entonces, los elementos de B que son integrales sobre A forman un subanillo de B.*

Al conjunto de los elementos de B que son integrales sobre A se le llama *cerradura integral* de A en B.

Ejemplo 2.0.4. Sea K una extensión finita de $\mathbb{Q}$. La cerradura integral de $\mathbb{Z}$ en K se llama el anillo de los *enteros algebraicos* de K.

Proposición 2.0.5. *Sean A un dominio de integridad y K su cuerpo cociente. Si α es algebraico sobre K, entonces existe un elemento $c \neq 0$ en A tal que $c\alpha$ es integral sobre A.*

Demostración: Como α es algebraico sobre K, existen $b_0/c_0, b_1/c_1, ..., b_{n-1}/c_{n-1} \in K$ tal que

$$b_0/c_0 + b_1/c_1 \cdot \alpha + ... + b_{n-1}/c_{n-1} \cdot \alpha^{n-1} + \alpha^n = 0.$$

Escogemos, $c = c_0c_1...c_{n-1} \neq 0 \in A$. Multiplicando la ecuación por c^n, obtenemos

$$b_0/c_0 \cdot c^n + b_1/c_1 \cdot c^{n-1} \cdot (c\alpha) + ... + b_{n-1}/c_{n-1} \cdot c \cdot (c\alpha)^{n-1} + (c\alpha)^n = 0$$

con $b_i/c_i \cdot c^{n-i} \in A$. Por lo tanto, $c\alpha$ es integral sobre A. □

Si un dominio de integridad A es igual a su cerradura integral en K, donde K es su cuerpo cociente, decimos que A es *integralmente cerrado*.

Proposición 2.0.6. *Sean A un subanillo de B y h un homomorfismo de B. Si B es integral sobre A, entonces $h(B)$ es integral sobre $h(A)$.*

Demostración: Sea $h(\alpha) \in h(B)$. Como $\alpha \in B$ es integral sobre A, existen $a_0, a_1, ...a_{n-1} \in A$ tal que

$$a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Aplicando h, tenemos:

$$h(a_0) + h(a_1)h(\alpha) + ... + h(a_{n-1})h^{n-1}(\alpha) + h^n(\alpha) = 0.$$

Entonces, $h(\alpha)$ es integral sobre $h(A)$ y por lo tanto, $h(B)$ es integral sobre $h(A)$. □

Definición 2.0.7. Sea $f : A \to B$ un homomorfismo de anillos. Decimos que f es *integral* si B es integral sobre $f(A)$.

Sean $f : A \to B$ integral y S un subconjunto multiplicativo de A. Luego, $f(S)$ es un subconjunto multiplicativo de B, pues $1 = f(1) \in f(S)$ y para $s_1, s_2 \in S$ se tiene que $f(s_1)f(s_2) = f(s_1s_2) \in f(S)$. Definimos la función:

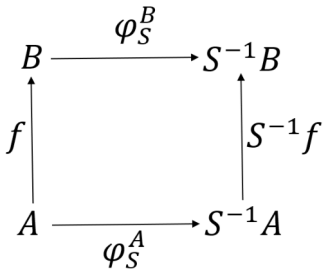
$$\begin{aligned} S^{-1}f : S^{-1}A \to S^{-1}B \ \ ; \ \ \text{donde } S^{-1}B = f(S)^{-1}B \\ x/s \mapsto f(x)/f(s) \end{aligned}$$

Si $x'/s' = x/s$, entonces $(x', s') \sim (x/s)$. Luego, existe $s_1 \in S$ tal que

$$\begin{aligned} s_1(sx' - s'x) = 0 \\ f(s_1)(f(s)f(x') - f(s')f(x)) = 0. \end{aligned}$$

Como $f(s_1) \in f(S)$, se sigue que $f(x')/f(s') = f(x)/f(s)$, lo que prueba la buena definición de $S^{-1}f$.

Luego, se verifica que $S^{-1}f$ es un homomorfismo y que el diagrama



es conmutativo, donde $\varphi_S^A(x) = x/1$ y $\varphi_S^B(y) = y/1$.

En efecto,

- Sean $x_1/s_1, x_2/s_2 \in S^{-1}A$. Luego,

$$\begin{aligned} S^{-1}f(x_1/s_1 + x_2/s_2) &= S^{-1}f((s_2x_1 + s_1x_2)/s_1s_2) \\ &= f(s_2x_1 + s_1x_2)/f(s_1s_2) \\ &= (f(s_2)f(x_1) + f(s_1)f(x_2))/f(s_1)f(s_2) \\ &= f(x_1)/f(s_1) + f(x_2)f(s_2) \\ &= S^{-1}f(x_1/s_1) + S^{-1}f(x_2/s_2) \end{aligned}$$

  y

$$\begin{aligned} S^{-1}f(x_1/s_1.x_2/s_2) &= S^{-1}f(x_1x_2/s_1s_2) \\ &= f(x_1x_2)/f(s_1s_2) \\ &= f(x_1)f(x_2)/f(s_1)f(s_2) \\ &= f(x_1)/f(s_1).f(x_2)/f(s_2) \\ &= S^{-1}f(x_1/s_1).S^{-1}f(x_2/s_2). \end{aligned}$$

  Entonces, $S^{-1}f$ es un homomorfismo.

- Sea $x \in A$. Luego,

$$\begin{aligned} \varphi_S^B(f(x)) &= f(x)/1 \\ &= f(x)/f(1) \\ &= S^{-1}f(x/1) \\ &= S^{-1}f(\varphi_S^A(x)). \end{aligned}$$

  Entonces, $\varphi_S^B \circ f = S^{-1}f \circ \varphi_S^A$.

Proposición 2.0.8. *Si $f : A \to B$ es integral y S es un subconjunto multiplicativo de A, entonces $S^{-1}f : S^{-1}A \to S^{-1}B$ es integral.*

Demostración: Sea $\alpha/f(s) \in S^{-1}B$. Como $\alpha \in B$, por hipotesis α es integral sobre $f(A)$. Luego, existen $a_0, a_1, ..., a_{n-1} \in A$ tal que

$$f(a_0) + f(a_1)\alpha + ... + f(a_{n-1})\alpha^{n-1} + \alpha^n = 0.$$

Aplicando φ_S^B y multiplicando por $1/f(s^n) \in S^{-1}B$, tenemos:

$$f(a_0)/f(s^n) + f(a_1)/f(s^{n-1}) \cdot \alpha/f(s) + ... + f(a_{n-1})/f(s) \cdot \alpha^{n-1}/f(s^{n-1}) + \alpha^n/f(s^n) = 0/1$$
$$f(a_0)/f(s^n) + f(a_1)/f(s^{n-1}) \cdot \alpha/f(s) + ... + f(a_{n-1})/f(s) \cdot (\alpha/f(s))^{n-1} + (\alpha/f(s))^n = 0/1$$
$$S^{-1}f(a_0/s^n) + S^{-1}f(a_1/s^{n-1}) \cdot \alpha/f(s) + ... + S^{-1}f(a_{n-1}/s) \cdot (\alpha/f(s))^{n-1} + (\alpha/f(s))^n = 0/1.$$

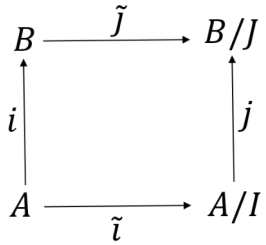
Como $a_0/s^n, a_1/s^{n-1}, ..., a_{n-1}/s \in S^{-1}A$, entonces $\alpha/f(s)$ es integral sobre $S^{-1}f(S^{-1}A)$.

Por lo tanto, $S^{-1}f$ es integral. □

Sean I un ideal primo de A, J un ideal primo de B y A subanillo de B. Si $I = J \cap A$, decimos que J *está sobre* I. En este caso, consideramos las inyecciones

$$\begin{aligned} i : A &\to B & \qquad j : A/I &\to B/J \\ x &\mapsto x & \qquad x + I &\mapsto x + J \end{aligned}$$

y obtenemos el diagrama conmutativo



donde $\tilde{i}(x) = x + I$ y $\tilde{j}(y) = y + J$. En efecto, es fácil ver que

$$(\tilde{j} \circ i)(a) = \tilde{j}(i(a)) = \tilde{j}(a) = a + J = j(a + I) = j(\tilde{i}(a)) = (j \circ \tilde{i})(a) \quad ; \forall a \in A.$$

Además, si B es integral sobre A, para qualquier $\alpha \in B$, existen $a_0, a_1, ..., a_{n-1} \in A$ tal que

$$a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Luego, si consideramos $a_0 + I, a_1 + I, ..., a_{n-1} + I \in A/I$ y $\alpha + J \in B/J$, se tiene

$$\begin{aligned}
&(a_0 + I) + (a_1 + I)(\alpha + J) + ... + (a_{n-1} + I)(\alpha + J)^{n-1} + (\alpha + J)^n \\
&= (a_0 + I) + (a_1 + I)(\alpha + J) + ... + (a_{n-1} + I)(\alpha^{n-1} + J) + (\alpha^n + J) \\
&= (a_0 + I) + (a_1\alpha + J) + ... + (a_{n-1}\alpha^{n-1} + J) + (\alpha^n + J) \\
&= (a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} + \alpha^n) + J \\
&= 0 + J.
\end{aligned}$$

De aquí, $\alpha + J \in B/J$ es integral sobre A/I. Entonces, B/J es integral sobre A/I.

Proposición 2.0.9. *Sean A un subanillo de B e I un ideal primo de A. Si B es integral sobre A, entonces $IB \neq B$ y existe un ideal primo J de B que está sobre I.*

Demostración: Ver (Lang, 2012).

Proposición 2.0.10. *Sea A un subanillo de B con B integral sobre A. Si J es un ideal primo de B que está sobre un ideal primo I de A, entonces J es maximal si y solo si I es maximal.*

Demostración:
($\Rightarrow$) Supongamos que J es un ideal maximal de B. Luego, por el Teorema 1.1.16 B/J es un cuerpo y su único ideal maximal es $\{0\}$. Además, B/J es integral sobre el dominio de integridad A/I. Si A/I no es un cuerpo, este tiene un ideal maximal $M \neq 0$ que también es primo. Por la Proposición 2.0.9, existe un ideal primo P de B/J que está sobre M, esto es, $M = A/I \cap P$. Luego, $P \neq \{0\}$ lo que es una contradicción. Por lo tanto, A/I es un cuerpo e I es un ideal maximal de A.

($\Leftarrow$) Supongamos que I es un ideal maximal de A, entonces se tiene que A/I es un cuerpo y B/J es un dominio de integridad por el Teorema 1.1.16. Además, B/J es integral sobre A/I, entonces $0 \neq \alpha \in B/J$ es algebraico sobre A/I. Por la Proposición 1.2.13 se tiene que $A/I[\alpha]$ es un cuerpo que contiene α y está contenido en B/J. Entonces, α es inversible en $A/I[\alpha]$ y por consiguiente es inversible en B/J. Así, B/J es un cuerpo y por lo tanto, J es un ideal maximal de B. □

Capítulo 3

Extensiones de Homomorfismos

Proposición 3.0.1. *Sea A un anillo conmutativo con unidad. Si $\varphi : A \to L$ es un homomorfismo de A en un cuerpo L y $P = Ker\ \varphi$, entonces φ tiene una extensión a un homomorfismo h del anillo local A_P en L tal que*

$$\begin{aligned} h : A_P &\to L \\ a/s &\mapsto \varphi(a)\varphi(s)^{-1} \end{aligned}$$

Demostración: Sea $P = \text{Ker } \varphi$. Por el Teorema 1.1.22, se tiene que $A/P \simeq \varphi(A)$, donde además $\varphi(A)$ es un dominio de integridad, pues es subanillo de L. Luego, A/P es un dominio de integridad y por el Teorema 1.1.16 se sigue que P es un ideal primo de A.

Consideramos el subconjunto multiplicativo $S = A \setminus P$ de A y el anillo local $A_P = S^{-1}A$. Note que $\varphi(s) \neq 0$ para todo $s \in S$, esto es que $\varphi(S)$ es inversible en L. Entonces, existe un único homomorfismo

$$\begin{aligned} h : A_P &\to L \\ a/s &\mapsto \varphi(a)\varphi(s)^{-1} \end{aligned}$$

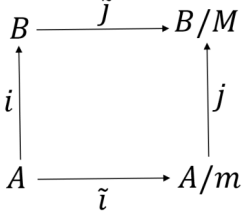
por la Proposición 1.1.26, que es una extensión de φ. □

Proposición 3.0.2. *Sea A subanillo de B tal que A es un anillo local con ideal maximal m y B es integral sobre A. Si $\varphi : A \to L$ es un homomorfismo de A en un cuerpo algebraicamente cerrado L con $Ker\ \varphi = m$, entonces φ tiene una extensión a un homomorfismo de B en L.*

Demostración: Como m es un ideal maximal de A, entonces m también es un ideal primo. Luego, por la Proposición 2.0.9 existe un ideal primo M de B tal que $m = M \cap A$.

Más aún, por la Proposicíón 2.0.10 tenemos que M es maximal.

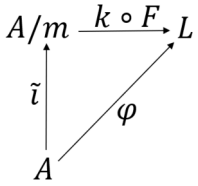
Se sigue de la Proposición 1.1.16 que tanto A/m como B/M son cuerpos. Note que B/M es una extensión algebraica sobre A/m ya que B/M es integral sobre A/m. Además el siguiente diagrama es conmutativo:



donde i,j son inyecciones, $\tilde{i}(x) = x + m$ y $\tilde{j}(y) = y + M$.
Por otro lado, existe un isomorfismo

$$\begin{aligned} F : A/m &\to \varphi(A) \\ a + m &\mapsto \varphi(a) \end{aligned}$$

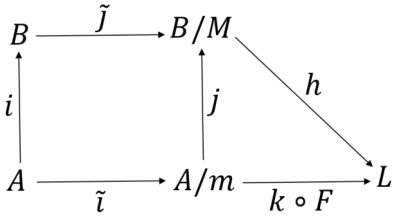
por el Teorema 1.1.22. Si $k : \varphi(A) \to L$ es la inclusión, el diagrama



conmuta, ya que

$$(k \circ F \circ \tilde{i})(a) = (k \circ F)(a + m) = k(\varphi(a)) = \varphi(a) \quad ; \quad \forall a \in A.$$

Finalmente, por el Teorema 1.2.20 existe una extensión de $k \circ F$ a un homomorfismo h de B/M en L que hace conmutativo el siguiente diagrama



ya que $h|A/m = k \circ F$. Por lo tanto, el homomorfismo $h \circ \tilde{j} : B \to L$ es una extensión para φ. □

Proposición 3.0.3. *Sea A un subanillo de B con B integral sobre A. Si $\varphi : A \to L$ es un homomorfismo de A en un cuerpo algebraicamente cerrado L, entonces φ tiene una extensión a un homomorfismo de B en L.*

Demostración:

Sean $P = \text{Ker } \varphi$ y $S = A \setminus P$ un subconjunto multiplicativo de A. Por la Proposición 3.0.1, φ tiene una extensión a un homomorfismo

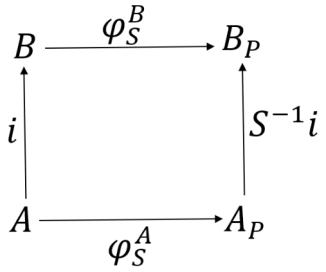
$$\begin{aligned} h : A_P &\to L \\ a/s &\mapsto \varphi(a)\varphi(s)^{-1} \end{aligned}$$

donde $A_P = S^{-1}A$ es un anillo local.

Como B es integral sobre A, entonces la inyección $i : A \to B$ es integral. Si $B_P = S^{-1}B$, entonces el homomorfismo

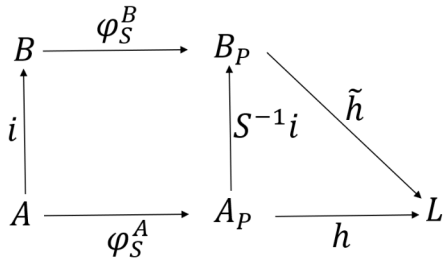
$$\begin{aligned} S^{-1}i : A_P &\to B_P \\ x/s &\mapsto i(x)/i(s) = x/s \end{aligned}$$

es una inyección. Más aún, por la Proposición 2.0.8 $S^{-1}i$ es integral, entonces B_P es integral sobre A_p. Además, el diagrama



es conmutativo, donde $\varphi_S^A(x) = x/1$ y $\varphi_S^B(y) = y/1$.

Además, Ker h es igual al ideal maximal $S^{-1}P$ de A_P. Luego, por la Proposición 3.0.2 h tiene una extensión a un homomorfismo $\tilde{h}$ de B_P en L que hace conmutativo el siguiente diagrama:



Note que

$$(h \circ \varphi_S^A)(a) = h(a/1) = \varphi(a)\varphi(1)^{-1} = \varphi(a) \ ; \ \forall a \in A.$$

Por lo tanto, el homomorfismo $\tilde{h} \circ \varphi_S^B : B \to L$ es una extensión para φ. □

Teorema 3.0.4. *Sea A subanillo de un cuerpo K y sea $0 \neq x \in K$. Si $\varphi : A \to L$ es un homomorfismo de A en un cuerpo algebraicamente cerrado L, entonces φ tiene una extension a un homomorfismo de $A[x]$ o $A[x^{-1}]$ en L.*

Demostración: Por la Proposición 3.0.1, podemos extender φ a un homomorfismo de un anillo local en L, además el núcleo de la extensión es igual al ideal maximal del anillo local. Entonces, sin perdida de generalidad podemos suponer que A es un anillo local con ideal maximal $m = \text{Ker } \varphi$.

Recordemos que $A[x^{-1}]$ es un subanillo de K tal que $A \subseteq A[x^{-1}] \subseteq K$. Es claro que

$$mA[x^{-1}] = \{m_1 p_1(x^{-1}) + ... + m_n p_n(x^{-1}) : m_i \in m \ \text{ y } \ p_i(x^{-1}) \in A[x^{-1}]\}$$

es un ideal de $A[x^{-1}]$ y además que $mA[x^{-1}] \subseteq m[x^{-1}]$, pues m es un ideal de A. Supongamos que

$$mA[x^{-1}] = A[x^{-1}].$$

Entonces, $1 \in mA[x^{-1}]$ y por lo mencionado anteriormente, podemos escribir

$$1 = a_0 + a_1 x^{-1} + ... + a_n x^{-n} \ \ ; \ \ a_i \in m.$$

Multiplicando por x^n, obtenemos

$$(1 - a_0)x^n + b_{n-1}x^{n-1} + ... + b_0 = 0 \ \ ; \ \ b_{n-i} = -a_i.$$

Supongamos que $1 - a_0$ no es inversible en A, entonces este genera un ideal propio que debe estar contenido en algún un ideal maximal de A. Como m es el único ideal maximal

de A, ya que estamos suponiendo que A es un anillo local, entonces $(1-a_0) \subseteq m$. Luego, $1-a_0 \in m$. Como $a_0 \in m$, se sigue que $1 = (a-a_0)+a_0 \in m$, lo que es una contradicción, pues m es un ideal maximal.

Multiplicando por $(1-a_0)^{-1}$ la ecuación anterior, obtenemos

$$x^n + b_{n-1}(1-a_0)^{-1}x^{n-1} + ... + b_0(1-a_0)^{-1} = 0.$$

De aquí, x es integral sobre A. Más aún, se cumple que $A[x]$ es integral sobre A. Luego, φ tiene una extensión de $A[x]$ en L por la Proposición 3.0.3.

Por otro lado, supongamos que

$$mA[x^{-1}] \neq A[x^{-1}].$$

Entonces, $mA[x^{-1}]$ está contenido en algún ideal maximal M de $A[x^{-1}]$. Como $m \subseteq mA[x^{-1}] \subseteq M$, se tiene que $m \subseteq M \cap A$. Además, $M \cap A$ es un ideal propio de A. Luego, como m es el único ideal maximal en A, se sigue que $m = M \cap A$.

Se sigue de la Proposición 1.1.16 que A/m y $A[x^{-1}]/M$ son cuerpos. Además, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} A[x^{-1}] & \xrightarrow{\tilde{j}} & A[x^{-1}]/M \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle j} \\ A & \xrightarrow[\tilde{i}]{} & A/m \end{array}$$

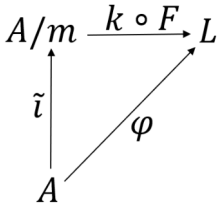
donde i,j son inclusiones, $\tilde{i}(a) = a + m$ y $\tilde{j}(b) = b + M$.

Por el Teorema 1.1.22, existe un isomorfismo

$$\begin{aligned} F : A/m &\to \varphi(A) \\ a + m &\mapsto \varphi(a) \end{aligned}$$

Si $k : \varphi(A) \to L$ es una inyeccion, entonces el siguiente diagrama conmuta:

Extendemos $k \circ F$ a un homomorfismo ψ de $A[x^{-1}]/M$, lo que podemos hacer si la imagen de x^{-1} en $A[x^{-1}]/M$ es trascendental o algebraico sobre A/m.



Finalmente, el homomorfismo $\psi \circ \tilde{j} : A[x^{-1}] \to L$ es una extensión para φ. □

Corolário 3.0.5. *Sean A un subanillo de un cuerpo K y $\varphi : A \to L$ un homomorfismo de A en un cuerpo algebraicamente cerrado L. Si B es un subanillo maximal de K para el cual φ tiene una extension a un homomorfismo en L, entonces B es un anillo local y si $0 \neq x \in K$ implica que $x \in B$ o $x^{-1} \in B$.*

Demostración:

Sea S el conjunto de todos los pares (C, ψ) donde C es un subanillo de K conteniendo A, y ψ es un homomorfismo C en L que extiende φ. Note que $S \neq \emptyset$ ya que $(A, \varphi) \in S$.

Consideramos en S la relación de equivalencia

$$(C, \psi) \leq (C', \psi') \Leftrightarrow C \subseteq C' \text{ y } \psi'|C = \psi.$$

Luego, $(C, \leq)$ es un conjunto parcialmente ordenado.

AFIRMACIÓN: S es inductivamente ordenado.

En efecto, sea $X = \{(C_i, \psi_i)\}$ un subconjunto totalmente ordenado. Definimos, $C = \bigcup C_i$ y el homomorfismo ψ en C tal que $\psi|C_i = \psi_i$. Luego, se cumple:

- C es un subanillo de K que contiene A.
- $\psi : C \to L$ extiende φ, pues $\psi|A = \psi_i|A = \varphi$.
- $(C_i, \psi_i) \leq (C, \psi)$ para todo i, pues $C_i \subseteq C$ y $\psi|C_i = \psi_i$ para todo i.

Entonces, $(C, \psi) \in S$ y es una cota superior de X. Así, la afirmación queda probada.

Usando el Lema de Zorn, existe (B, ψ_0) un elemento maximal en S, esto es que B es el mayor subanillo de K para el cual existe un homomorfismo $\psi_0 : B \to L$ que extiende φ. Luego, B tiene que ser un anillo local, pues caso contrario por la Proposición 3.0.1 existe un homomorfismo que extiende ψ_0 a el anillo local que surge de su núcleo, lo que contradice

la maximalidad de (B, ψ_0). Además, por el Teorema 3.0.4 existe un homomorfismo que extiende ψ de $B[x]$ o $B[x^{-1}]$, pero como (B, ψ_0) es maximal, entonces $B[x] = B$ o $B[x^{-1}] = B$. Finalmente, se sigue que $x \in B$ o $x^{-1} \in B$, como queríamos demostrar. □

Definición 3.0.6. Sea B un subanillo de un cuerpo K. Decimos que B es un *anillo de valuación* en K si para cada $0 \neq x \in K$, entonces $x \in B$ o $x^{-1} \in B$.

Sea F un cuerpo. Si $0 \neq a \in F$, definimos

$$a \pm \infty = \infty \quad , \quad a \cdot \infty = \infty \quad , \quad \infty \cdot \infty = \infty \quad , \quad \frac{1}{0} = \infty \quad \text{y} \quad \frac{1}{\infty} = 0.$$

Además, las siguientes expresiones:

$$\infty \pm \infty \quad , \quad 0 \cdot \infty \quad , \quad \frac{0}{0} \quad \text{y} \quad \frac{\infty}{\infty}$$

no están definidas.

Definición 3.0.7. Sean K y F cuerpos. Decimos que φ es un *lugar* de K en F si es una aplicación

$$\varphi : K \to \{F, \infty\}$$

que satisface

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b) \\ \varphi(1) &= 1, \end{aligned}$$

para todo $a, b \in K$, siempre que $\varphi(a) + \varphi(b)$, $\varphi(a) \cdot \varphi(b)$ estén definidas.

Decimos que $a \in K$ es *finito* bajo el lugar φ si $\varphi(a) \neq \infty$. Caso contrario, decimos que a es *infinito* bajo el lugar φ.

Como el lugar φ verifica las reglas usuales de un homomorfismo, es fácil ver que $\varphi(0) = 0$ y $\varphi(-a) = -\varphi(a)$ para todo $a \in K$.

Observación 3.0.8. A partir de un lugar φ de K en F, podemos obtener un anillo de valuación en K. Basta considerar el conjunto

$$A = \{x \in K : x \text{ es finito bajo el lugar } \varphi\}.$$

Más aún, el conjunto $m = \{x \in K : \varphi(x) = 0\}$ es un ideal maximal de A.

En efecto, A es un subanillo de K, ya que verifica:

i) $0 \in A$

ii) Si $x, y \in A$, entonces $\varphi(x - y) = \varphi(x) - \varphi(y) \neq \infty$. Luego, $x - y \in A$.

iii) Si $x, y \in A$, entonces $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \neq \infty$. Luego, $x \cdot y \in A$.

Luego, si $0 \neq x \in K$ puede suceder que $\varphi(x) \neq \infty$ ó que $\varphi(x) = \infty$. En el primer caso, se tiene que $x \in A$. Para el segundo caso,

$$\begin{aligned} \varphi(x^{-1}) \cdot \varphi(x) &= \varphi(1) \\ \varphi(x^{-1}) &= \frac{1}{\varphi(x)} \\ \varphi(x^{-1}) &= \frac{1}{\infty} \\ \varphi(x^{-1}) &= 0. \end{aligned}$$

Así, $x^{-1} \in A$. Entonces, A es un anillo de valuación en K.

Además, m es un ideal de A, pues verifica:

i) $0 \in m$

ii) Si $x, y \in m$, entonces $\varphi(x - y) = \varphi(x) - \varphi(y) = 0$ y $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = 0$. Luego, $x - y, x \cdot y \in A$.

iii) Si $x \in m$ y $a \in A$, entonces $\varphi(a \cdot x) = \varphi(a) \cdot \varphi(x) = \varphi(a) \cdot 0 = 0$. Luego, $a \cdot x \in m$.

Ahora supogamos que existe un ideal M de A tal que $m \subset M$. Entonces, existe $x \in M \setminus m$, esto es, $\varphi(x) \neq 0$ y $\varphi(x) \neq \infty$. Luego,

$$\varphi(x^{-1}) = \frac{1}{\varphi(x)} \neq \infty.$$

Se sigue que $x^{-1} \in A$, lo que implica que $1 = x \cdot x^{-1} \in M$. Entonces, $M = A$.

Por lo tanto, m es un ideal maximal de A como queríamos probar.

Ejemplo 3.0.9. Sea p un número primo. Sea (p) un ideal primo de $\mathbb{Z}$. Si $S = \mathbb{Z} \setminus (p)$ es un subconjunto multiplicativo de $\mathbb{Z}$, se tiene que

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : b \text{ no es divisible por } p \right\}$$

es un anillo local con ideal maximal

$$M = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} : a \text{ es divisible por } p \right\}.$$

Más aún, dado un elemento $0 \neq a/b \in \mathbb{Q}$ con a y b primos entre sí, tenemos dos posibilidades:

- Si b no es divisible por p, entonces $a/b \in \mathbb{Z}_{(p)}$.
- Si b es divisible por p, entonces a no es divisible por p, pues caso contrario a y b no son primos entre sí. Luego, $(a/b)^{-1} = b/a \in \mathbb{Z}_{(p)}$.

Entonces, $\mathbb{Z}_{(p)}$ es un anillo de valuación en $\mathbb{Q}$.

Conclusiones

- El proceso de localización es una técnica poderosa y fundamental en el álgebra conmutativa y la teoría de anillos, con ella no solo podemos extender anillos incluyendo elementos inversibles, sino que también podemos extender un anillo conmutativo con unidad a un anillo local usando apenas un ideal primo. La importancia de los anillos locales radica en las aplicaciones que tiene en las diversas áreas de las matemáticas, incluyendo la geometría algebraica, la teoría de números y la topología.

- La extensión de homomorfismo más simple es obtenida gracias al proceso de localización. Todo homomorfismo φ de un un anillo conmutativo con unidad A en un cuerpo, puede ser extendido a un homomorfismo del anillo local A_P que surge del ideal primo $P = \text{Ker } \varphi$.

- Las extensiones integrales de un anillo conmutativo con unidad son importantes para la extensión de homomorfismos, ya que cualquier homomorfismo de un anillo conmutativo con unidad A en un cuerpo algebraicamente cerrado puede ser extendido a un homomorfismo de una extensión integral de A.

- De forma general, cualquier homomorfismo de un anillo conmutativo con unidad A en un cuerpo algebraicamente cerrado puede ser extendido siempre que A esté contenido en un cuerpo K.

- Si un homomorfismo de un anillo conmutativo con unidad A en un cuerpo algebraicamente cerrado puede ser extendido de forma máxima a un homomorfismo de un subanillo B de un cuerpo, entonces se verifica que este anillo B no solo es un anillo local, sino que también es un anillo de valuación que al igual que los anillos locales poseen diversas aplicaciones en la teoría de números, la geometría algebraica, la teoría de cuerpos y otros campos de las matemáticas.

Referencias

Baker, A. (2022). *Transcendental number theory*. Cambridge university press.

Boyallían, C., y Ovando, G. (1994). El lema de zorn y algunas aplicaciones. *Revista de Educación Matemática (RevEM)*, *9*(1), 1.

Carballo Rodríguez, J. (s.f.). Localización de anillos conmutativos.

Dorronsoro, J., y Hernández, E. (1996). *Números, grupos y anillos* (n.º 512.7 D6).

Gonçalves, A. (1979). *Introdução à álgebra* (Vol. 7). Instituto de Matemática Pura e Aplicada.

Herstein, I., y Lluis, E. (1970). *Algebra moderna: grupos, anillos, campos, teoría de galois*. Trillas.

Lang, S. (2012). *Algebra* (Vol. 211). Springer Science & Business Media.

Morandi, P. (2012). *Field and galois theory* (Vol. 167). Springer Science & Business Media.