BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

Nullstellensatz

Tesis Presentada al

Colegio de Matemáticas

como requisito para la obtención del grado de

Licenciatura

por

José Arturo Ramos Ramos

asesorado por

Dr. Iván Fernando Vilchis Montalvo

Puebla, Pue.

2022

In memoriam

Arturo Ramos Cuautle

Agradecimientos

A mis padres Gloria y Arturo por su apoyo, paciencia, esfuerzos, amor incondicional y sobretodo, su gran ejemplo.

A Darlen y Kevin por los hermosos momentos que me han regalado. Además, por ser mi inspiración y felicidad todos estos años.

A todos mis profesores que a lo largo de mi formación académica me han enseñado, sin ustedes nada de esto sería posible. En particular, al Dr. Iván Fernando Vilchis Montalvo por aceptar ser mi director de tesis y por haber impartido el curso de teoría de anillos, pues éste último hecho fue la motivación.

Finalmente, a todas las personas que directa o indirectamente me han brindado una mano.

Introducción

Desde Descartes, geometría coordenada, una de las ideas mas fructíferas en matematicas ha sido la de la dualidad entre el álgebra y la geometría; es decir, para cada concepto o afirmación en el álgebra se tiene un concepto o afirmación correspondiente en geometría. La formulación precisa de esta dualidad es por medio de una equivalencia entre las categorías asociadas.

Mencionado lo anterior, el presente trabajo tiene como objetivos demostrar el teorema de los ceros de Hilbert, Nullstellensatz, y mostrar que la categoría de variedades algebraicas afines sobre un campo algebraicamente cerrado K es equivalente a la categoría opuesta de K-álgebras conmutativas finitamente generadas sin elementos nilpotentes; es decir, álgebras reducidas.

En el capítulo 1 se expone la definición de categoría, funtor, transformación natural y equivalencia de categorías, lo suficiente para demostrar la dualidad antes mencionada.

En el capítulo 2 se exponen las definiciones y resultados necesarios del álgebra conmutativa para demostrar el Nullstellensatz. Entre otros temas, se da la definición de anillo conmutativo con uno, subanillo, morfismos entre anillos, ideales, y como caso particular, se definen los ideales máximos e ideales primos; estos últimos son de suma importancia en geometría algebraica. Además, se construye el anillo de polinomios en varias variables, anillo ambiente en la geometría algebraica, y se enuncian sus principales propiedades. Finalmente, se demuestra el teorema de la base de Hilbert, el cual versa que si A es un anillo noetheriano, entonces el anillo de polinomios en n variables con coeficientes en A es noetheriano, es decir, todo ideal es finitamente generado.

En el capítulo 3 se dan las principales definiciones y construcciones de geometría algebraica, espacio afín, conjunto algebraico, ideal asociado a un conjunto algebraico, y se demuestran las principales propiedades de estas dos últimas construcciones. Posteriormente se demuestran dos resultados

puramente algebraicos, Lema de normalización de Noether y Teorema de Zariski, los cuales nos ayudarán con la demostración del Nullstellensatz. Por último, se define el anillo de coordenas de una variedad algebraica, se definen las aplicaciones polinomiales y la ley de composición entre estas, para que posteriormente se defina la categoría de variedades algebraicas y aplicaciones polinomiales, para así demostrar la equivalencia antes mencionada.

Índice

Capítulo 1

Preliminares

1.1 Categorías, funtores y transformaciones naturales

Definición 1.1. *Una **categoría** $\mathcal{C}$ consiste de lo siguiente:*

1. *Una clase $|\mathcal{C}|$, cuyos elementos los llamaremos **objetos** de la categoría.*
2. *Para cualquier par A, B de objetos de $\mathcal{C}$, un conjunto $\mathcal{C}(A, B)$, cuyos elementos los llamaremos **morfismos** de A a B.*
3. *Para cualquier terna A, B, C de objetos de $\mathcal{C}$, una ley de **composición***

$$\begin{array}{ccc} \mathcal{C}(A,B) \times \mathcal{C}(B,C) & \longrightarrow & \mathcal{C}(A,C) \\ (f,g) & \longmapsto & g \circ f \end{array}$$

4. *Para cualquier objeto A de $\mathcal{C}$, un morfismo $1_A \in \mathcal{C}(A, A)$, llamado morfismo **identidad** en A.*

Con 3. y 4. sujetos a los siguientes axiomas:

(i) ***Asociatividad**: dados $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$ y $h \in \mathcal{C}(C, D)$, se cumple:*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(ii) ***Identidad**: dados $f \in \mathcal{C}(A, B)$ y $g \in \mathcal{C}(B, C)$, se cumplen:*

$$1_B \circ f = f \text{ y } g \circ 1_B = g.$$

Notación 1.1. *Si $\mathcal{C}$ es una categoría, un morfismo $f \in \mathcal{C}(A, B)$ lo denotaremos por $A \xrightarrow{f} B$; A es llamado* ***dominio*** *de f y B* ***codominio*** *de f.*

Observación 1.1. *Sean $\mathcal{C}$ una categoría y $A \xrightarrow{f} B$, $B \xrightarrow{g} D$, $A \xrightarrow{h} C$ y $C \xrightarrow{k} D$ morfismos en $\mathcal{C}$. Ahora, consideremos el diagrama:*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[k]{} & D \end{array}$$

Diremos que el diagrama ***conmuta*** *si $g \circ f = k \circ h$. Una terminología análoga se aplica para diagramas de forma arbitraria.*

En cada uno de los siguientes ejemplos entenderemos por (I) la clase de objetos, por (II) los conjuntos $\mathcal{C}(A, B)$, con A y B objetos, y por (III) la ley de composición.

Ejemplos 1.1. *1.* ***Set*** *= Categoría de conjuntos:*

(I) La clase de todos los conjuntos.

(II) El conjunto de todas las funciones de A a B.

(III) Composición usual de funciones.

2. ***Top*** *= Categoría de espacios topológicos:*

(I) La clase de todos los espacios topológicos.

(II) El conjunto de todas las funciones continuas de A a B.

(III) Composición usual de funciones continuas.

3. ***Rng*** *= Categoría de anillos:*

(I) La clase de todos los anillos.

(II) El conjunto de todos los homomorfismos de anillos de A a B.

(III) Composición usual de homomorfismos de anillos.

4. ***Ring*** *= Categoría de anillos con elemento unitario:*

(I) La clase de todos los anillos con elemento unitario.

(II) *El conjunto de todos los homomorfismos de anillos de A a B que preservan elemento unitario.*

(III) *Composición usual de homomorfismos de anillos.*

5. **Gr** = *Categoría de grupos:*

(I) *La clase de todos los grupos.*

(II) *El conjunto de todos los homomorfismos de grupos de A a B.*

(III) *Composición usual de homomorfismos de grupos.*

Proposición 1.1. *Sean $\mathcal{C}$ una categoría y $A \in |\mathcal{C}|$. Entonces, $A \xrightarrow{1_A} A$ es único.*

Demostración. En efecto, sea $A \xrightarrow{i_A} A$ otro morfismo en $\mathcal{C}$ tal que cumple (ii) de la **Definición 1.1** Entonces, $1_A = 1_A \circ i_A = i_A$. Por tanto, $A \xrightarrow{1_A} A$ es único. †

Definición 1.2. *Sean $\mathcal{A}$ y $\mathcal{B}$ categorías. Diremos que $\mathcal{A} \xrightarrow{F} \mathcal{B}$ es un **funtor covariante** si consiste de lo siguiente:*

1. *Una regla,*

$$|\mathcal{A}| \longrightarrow |\mathcal{B}| \ ,$$

tal que asigna a cada objeto A de $\mathcal{A}$ exactamente un objeto $F(A)$ de $\mathcal{B}$.

2. *Para cualquier par A, A' de objetos de $\mathcal{A}$, una regla,*

$$\mathcal{A}(A, A') \longrightarrow \mathcal{B}(F(A), F(A')) \ ,$$

tal que asigna a cada morfismo $f \in \mathcal{A}(A, A')$ exactamente un morfismo $F(f) \in \mathcal{B}(F(A), F(A'))$. De tal forma que se cumplen los siguientes axiomas:

(i) *Para cualquier par de morfismos $f \in \mathcal{A}(A, A')$ y $g \in \mathcal{A}(A', A'')$,*

$$F(g \circ f) = F(g) \circ F(f).$$

(ii) *Para cualquier A objeto de $\mathcal{A}$,*

$$F(1_A) = 1_{F(A)}.$$

Notación 1.2. *Sea $\mathcal{A} \xrightarrow{F} \mathcal{B}$ un funtor covariante. Denotaremos la acción de F tanto en objetos como en morfismos por:*

$$F(A \xrightarrow{f} A') = F(A) \xrightarrow{F(f)} F(A')$$

Sean $\mathcal{A}, \mathcal{B}$ categorías y $\mathcal{A} \xrightarrow{F} \mathcal{B}$ un funtor. En cada uno de los siguientes ejemplos entenderemos por (I) la regla que manda objetos de $\mathcal{A}$ en objetos de $\mathcal{B}$ y por (II) la regla que manda morfismos de $\mathcal{A}$ en morfismos de $\mathcal{B}$.

Ejemplos 1.2. *1.* $Set \xrightarrow{\mathcal{P}} Set$ *, llamado funtor conjunto potencia:*

(I)
$$\begin{array}{ccc} |Set| & \longrightarrow & |Set| \\ A & \longmapsto & \mathcal{P}(A) \end{array}$$

(II) Si $A, A' \in |Set|$*, entonces:*
$$\begin{array}{ccc} Set(A, A') & \longrightarrow & Set(\mathcal{P}(A), \mathcal{P}(A')) \\ A \xrightarrow{f} A' & \longmapsto & \mathcal{P}(A) \xrightarrow{\mathcal{P}(f)} \mathcal{P}(A') \\ & & X \longmapsto f[X] \end{array}$$

2. Sea $\mathcal{C}$ *una categoría.* $\mathcal{C} \xrightarrow{Id_{\mathcal{C}}} \mathcal{C}$ *, llamado funtor identidad en* $\mathcal{C}$*:*

(I)
$$\begin{array}{ccc} |\mathcal{C}| & \longrightarrow & |\mathcal{C}| \\ A & \longmapsto & A \end{array}$$

(II) Si $A, B \in |\mathcal{C}|$*, entonces:*
$$\begin{array}{ccc} \mathcal{C}(A, B) & \longrightarrow & \mathcal{C}(A, B) \\ A \xrightarrow{f} B & \longmapsto & A \xrightarrow{f} B \end{array}$$

3. Sean $\mathcal{A}$*,* $\mathcal{B}$*,* $\mathcal{C}$ *categorías y consideremos los funtores* $\mathcal{A} \xrightarrow{F} \mathcal{B}$ *,* $\mathcal{B} \xrightarrow{G} \mathcal{C}$ *.* $\mathcal{A} \xrightarrow{G \circ F} \mathcal{C}$ *, llamado funtor composición:*

(I)
$$\begin{array}{ccc} |\mathcal{A}| & \longrightarrow & |\mathcal{C}| \\ A & \longmapsto & G(F(A)) \end{array}$$

(II) Si $A, A' \in |\mathcal{A}|$*, entonces:*
$$\begin{array}{ccc} \mathcal{A}(A, A') & \longrightarrow & \mathcal{C}(G(F(A)), G(F(A'))) \\ A \xrightarrow{f} A' & \longmapsto & G(F(A)) \xrightarrow{G(F(f))} G(F(A')) \end{array}$$

Definición 1.3. *Sean* $\mathcal{A}$ *y* $\mathcal{B}$ *categorías. Diremos que* $\mathcal{A} \xrightarrow{F} \mathcal{B}$ *es un* ***funtor contravariante*** *si consiste de lo siguiente:*

1. Una regla,

$$|\mathcal{A}| \longrightarrow |\mathcal{B}| \ ,$$

tal que asigna a cada objeto A de $\mathcal{A}$ exactamente un objeto $F(A)$ de $\mathcal{B}$.

2. *Para cualquier par A, A' de objetos de $\mathcal{A}$, una regla,*

$$\mathcal{A}(A, A') \longrightarrow \mathcal{B}(F(A'), F(A)) \ ,$$

tal que asigna a cada morfismo $f \in \mathcal{A}(A, A')$ exactamente un morfismo $F(f) \in \mathcal{B}(F(A'), F(A))$. De tal forma que se cumplen los siguientes axiomas:

(i) Para cualquier par de morfismos $f \in \mathcal{A}(A, A')$ y $g \in \mathcal{A}(A', A'')$,

$$F(g \circ f) = F(f) \circ F(g).$$

(ii) Para cualquier A objeto de $\mathcal{A}$,

$$F(1_A) = 1_{F(A)}.$$

Ejemplos 1.3. 1. $Set \xrightarrow{\mathcal{P}^*} Set$ *, llamado funtor imagen inversa:*

(I)
$$\begin{array}{ccc} |Set| & \longrightarrow & |Set| \\ A & \longmapsto & \mathcal{P}(A) \end{array}$$

(II) Si $A, A' \in |Set|$, entonces:
$$\begin{array}{ccc} Set(A, A') & \longrightarrow & Set(\mathcal{P}(A'), \mathcal{P}(A)) \\ A \xrightarrow{f} A' & \longmapsto & \mathcal{P}(A') \xrightarrow{\mathcal{P}^*(f)} \mathcal{P}(A) \\ & & Y \longmapsto f^{-1}[Y] \end{array}$$

2. *Sean $\mathcal{A}$ una categoría y $A \in |\mathcal{A}|$ fijo arbitrario.* $\mathcal{A} \xrightarrow{\mathcal{A}(-A)} Set$ *:*

(I)
$$\begin{array}{ccc} |\mathcal{A}| & \longrightarrow & |Set| \\ B & \longmapsto & \mathcal{A}(B, A) \end{array}$$

(II) Si $B, B' \in |\mathcal{A}|$, entonces:
$$\begin{array}{ccc} \mathcal{A}(B, B') & \longrightarrow & Set(\mathcal{A}(B', A), \mathcal{A}(B, A)) \\ B \xrightarrow{f} B' & \longmapsto & \mathcal{A}(B', A) \xrightarrow{\mathcal{A}(-A)(f)} \mathcal{A}(B, A) \\ & & B' \xrightarrow{g} A \longmapsto B \xrightarrow{g \circ f} A \end{array}$$

Convención 1.1. *De aquí en adelante la palabra* ***funtor (funtores)*** *significará* ***funtor covariante (funtores covariantes)****.*

Definición 1.4. *Sean* $F, G : \mathcal{A} \rightrightarrows \mathcal{B}$ *dos funtores. Una* ***transformación natural***

$$\alpha : F \Longrightarrow G$$

entre los funtores F y G es una clase de morfismos $(\alpha_A : F(A) \longrightarrow G(A))_{A\in\mathcal{A}}$ de $\mathcal{B}$ indexada por los objetos de $\mathcal{A}$ de tal forma que para cada morfismo $f : A \longrightarrow A'$ de $\mathcal{A}$, $\alpha_{A'} \circ F(f) = G(f) \circ \alpha_A$.

$$\begin{array}{ccc} F(A) & \xrightarrow{\alpha_A} & G(A) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(A') & \xrightarrow{\alpha_{A'}} & G(A') \end{array}$$

Proposición 1.2. *Sean $F, G, H : \mathcal{A} \rightrightarrows \mathcal{B}$ tres funtores y $\alpha : F \Longrightarrow G$, $\beta : G \Longrightarrow H$ dos transformaciones naturales. Entonces, la fórmula $(\beta \circ \alpha)_A = \beta_A \circ \alpha_A$ define una nueva transformación natural $\beta \circ \alpha : F \Longrightarrow H$.*

Demostración. Sea $f : A \longrightarrow A'$ un morfismo de $\mathcal{A}$. Observemos el siguiente diagrama:

$$\begin{array}{ccccc} F(A) & \xrightarrow{\alpha_A} & G(A) & \xrightarrow{\beta_A} & H(A) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} & & \downarrow{\scriptstyle H(f)} \\ F(A') & \xrightarrow{\alpha_{A'}} & G(A') & \xrightarrow{\beta_{A'}} & H(A') \end{array}$$

En efecto, para cada A objeto de $\mathcal{A}$, sea $(\beta \circ \alpha)_A = \beta_A \circ \alpha_A : F(A) \longrightarrow H(A)$. Así, tenemos:

$$(\beta \circ \alpha)_{A'} \circ F(f) = (\beta_{A'} \circ \alpha_{A'}) \circ F(f) = \beta_{A'} \circ (\alpha_{A'} \circ F(f)) = \beta_{A'} \circ (G(f) \circ \alpha_A) =$$
$$(\beta_{A'} \circ G(f)) \circ \alpha_A = (H(f) \circ \beta_A) \circ \alpha_A = H(f) \circ (\beta_A \circ \alpha_A) = H(f) \circ (\beta \circ \alpha)_A.$$

Por tanto, $(\beta \circ \alpha)_A = \beta_A \circ \alpha_A$ define una nueva transformación natural $\beta \circ \alpha : F \Longrightarrow H$.

†

Definición 1.5. *Sean $F, G : \mathcal{A} \rightrightarrows \mathcal{B}$ dos funtores contravariantes. Una* ***transformación natural***

$$\alpha : F \Longrightarrow G$$

entre los funtores F y G es una clase de morfismos $(\alpha_A : F(A) \longrightarrow G(A))_{A\in\mathcal{A}}$ de $\mathcal{B}$ indexada por los objetos de $\mathcal{A}$ de tal forma que para cada morfismo $f : A \longrightarrow A'$ de $\mathcal{A}$, $G(f) \circ \alpha_{A'} = \alpha_A \circ F(f)$.

$$\begin{array}{ccc} F(A') & \xrightarrow{\alpha_{A'}} & G(A') \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(A) & \xrightarrow{\alpha_A} & G(A) \end{array}$$

Definición 1.6. *1. Sean $F, G : \mathcal{A} \rightrightarrows \mathcal{B}$ dos funtores. Una transformación natural $\alpha : F \Longrightarrow G$ se dice que es una **equivalencia natural** si existe otra transformación natural $\psi : G \Longrightarrow F$ tal que para todo A objeto de $\mathcal{A}$, $\alpha_A : F(A) \longrightarrow G(A)$ es un isomorfismo con inverso $\psi_A : G(A) \longrightarrow F(A)$.*

*2. Si existen funtores $F : \mathcal{A} \longrightarrow \mathcal{B}$ y $G : \mathcal{B} \longrightarrow \mathcal{A}$ tales que $F \circ G$ es naturalmente equivalente al funtor identidad $Id_{\mathcal{B}} : \mathcal{B} \longrightarrow \mathcal{B}$ y $G \circ F$ es naturalmente equivalente al funtor identidad $Id_{\mathcal{A}} : \mathcal{A} \longrightarrow \mathcal{A}$, diremos que las categorías $\mathcal{A}$ y $\mathcal{B}$ son **equivalentes**.*

Capítulo 2

Álgebra Conmutativa

2.1 Anillos, morfismos e ideales

El concepto de anillo se modeló a partir de las propiedades familiares del conjunto de enteros $\mathbb{Z}$ y sus propiedades aritméticas elementales, la suma y el producto. Otro modelo importante fue el conjunto de polinomios con coeficientes en $\mathbb{Q}$ (o en $\mathbb{R}$ o en $\mathbb{Z}$) con la suma y producto usuales. Por tanto, aquí damos la definición de anillo conmutativo con uno y todo nuestro trabajo posterior estará basado en ella. Dicho lo anterior, hacemos la siguiente:

Convención 2.1. *En este trabajo la palabra* ***anillo*** *significará* ***anillo conmutativo con uno****.*

Definición 2.1. *Un* ***anillo*** $(A, +, \cdot)$ *es un conjunto no vacío* A *junto con dos operaciones, suma* $(+)$ *y producto* $(\cdot)$*,*

$$+ : A \times A \to A$$

y

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

que satisfacen las propiedades siguientes:

1. $(A, +)$ *es un grupo abeliano.*

2. *El producto $\cdot$ es asociativo.*

3. *El producto $\cdot$ es conmutativo.*

4. *La suma y el producto se relacionan mediante la siguiente propiedad distributiva:*

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

para cualesquiera $a, b, c \in A$.

5. *Existe un elemento, denotado por 1, en A tal que*

$$1 \cdot a = a,$$

para todo $a \in A$.

Notación 2.1. *Si $(A, +, \cdot)$ es un anillo, generalmente, lo expresaremos solo escribiendo A es un anillo. Además, si $a, b \in A$, para el producto, escribiremos ab en lugar de $a \cdot b$.*

Ejemplos 2.1. 1. *$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son anillos, donde $+$ y $\cdot$ son la suma y producto usales, correspondientes.*

2. *Sea $n > 1$ un entero. Decimos que $a, b \in \mathbb{Z}$ son **congruentes módulo** n, denotado por $a \equiv b$ mód n, si $n|a - b$. Afirmamos que la congruencia módulo n es una relación de equivalencia. En efecto, es **reflexiva** porque si $a \in \mathbb{Z}$, $n|a - a = 0$, es decir, $a \equiv a$ mód n. Es **simétrica**, pues si $a, b \in \mathbb{Z}$ con $a \equiv b$ mód n, se tiene que $n|a - b$, entonces $a - b = ln$, para algún $l \in \mathbb{Z}$, y esto implica que $-(ln) = -(a - b) = b - a = (-l)n$, con $-l \in \mathbb{Z}$, entonces se cumple que $n|b - a$, es decir, $b \equiv a$ mód n. Es **transitiva** porque si $a, b, c \in \mathbb{Z}$ son tales que $a \equiv b$ mód n y $b \equiv c$ mód n, que es equivalente a que $n|a - b$ y $n|b - c$, que a su vez equivale a que $a - b = rn$ para algún $r \in \mathbb{Z}$ y $b - c = sn$ para algún $s \in \mathbb{Z}$, entonces $(r + s)n = rn + sn = a - b + b - c = a - c$, con $r + s \in \mathbb{Z}$, entonces $n|a - c$, es decir, $a \equiv c$ mód n. Por tanto, la congruencia módulo n particiona a $\mathbb{Z}$ en subconjuntos disjuntos, llamados **clases residuales de enteros módulo** n. Así, si $a \in \mathbb{Z}$, a la clase residual módulo n a la que pertenece la denotaremos por $\overline{a}$, con $\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \text{ mód } n \} = \{x \in \mathbb{Z} \mid n|x - a \} = \{x \in \mathbb{Z} \mid x - a = rn \text{ para algún } r \in \mathbb{Z} \} = \{a + rn \mid r \in \mathbb{Z}\}$. Además, $\overline{a} = \overline{b}$ sii $a \equiv b$ mód n. Luego, con $\mathbb{Z}/n\mathbb{Z}$ denotemos al conjunto que contiene a estas clases residuales módulo n. Ahora, se afirma que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, pues si $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, entonces $a \in \overline{a}$ y por el algoritmo de la división, existen únicos $q, r \in \mathbb{Z}$ tales que $a = qn + r$, con $0 \leq r < n$, lo que implica que $a - r = qn$, con $0 \leq r < n$, entonces $a \equiv r$ mód n, con $0 \leq r < n$; es decir,*

$\overline{a} = \overline{r}$, *con* $0 \leq r < n$, *entonces* $\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. *Por último, definimos una suma y un producto en* $\mathbb{Z}/n\mathbb{Z}$ *de la siguiente forma:*

Suma:

$$\begin{array}{rccc} + : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} + \overline{b} = \overline{a+b} \end{array}$$

Producto:

$$\begin{array}{rccc} \cdot : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a}\overline{b} = \overline{ab} \end{array}$$

Así, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *es un anillo.*

3. *Sean* X *un conjunto no vacío y* A *un anillo. Definimos el conjunto* A^X *como:*

$$A^X = \{f : X \to A \mid f \text{ es función }\}.$$

Ahora, definimos una suma y un producto en A^X *como sigue:*

Suma:

$$\begin{array}{rccc} + : & A^X \times A^X & \longrightarrow & A^X \\ & (f, g) & \longmapsto & (f+g)(x) = f(x) + g(x) \end{array}$$

Producto:

$$\begin{array}{rccc} \cdot : & A^X \times A^X & \longrightarrow & A^X \\ & (f, g) & \longmapsto & (fg)(x) = f(x)g(x) \end{array}$$

Así, $(A^X, +, \cdot)$ *es un anillo.*

Demostración. Solo se demostrará 3.

(i) $+$ está bien definida:

Es claro.

(ii) $+$ es asociativa:

Sean $f, g, h \in A^X$. Luego, si $x \in X$, entonces $((f+g)+h)(x) = (f+g)(x) + h(x) = (f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x)) = f(x) + (g+h)(x) = (f + (g+h))(x)$. Por tanto, $(f+g)+h = f + (g+h)$.

(iii) $+$ es conmutativa:

Sean $f, g \in A^X$. Ahora, si $x \in X$, se tiene que $(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$. Luego, $f+g = g+f$.

(iv) Existe neutro aditivo, 0:

Sea $0 : X \longrightarrow A$, $x \longmapsto 0$. Entonces, $0 \in A^X$. Ahora, si $f \in A^X$ y $x \in X$, se tiene que $(f+0)(x) = f(x)+0(x) = f(x)+0 = f(x)$. Por tanto, $f+0 = f$.

(v) Existe inverso aditivo para cualquier $f \in A^X$:

Sea $f \in A^X$. Ahora, si $-f : X \longrightarrow A$, $x \longmapsto -f(x)$, entonces $-f \in A^X$ y $f+(-f) = 0$. En efecto, que $-f \in A^X$ es claro. Ahora, si $x \in X$, se tiene que $(f+(-f))(x) = f(x)+(-f)(x) = f(x)+(-f(x)) = 0$ y $0(x) = 0$, entonces $(f+(-f))(x) = 0(x)$. Luego, $f+(-f) = 0$.

(vi) $\cdot$ está bien definido:

Es claro.

(vii) $\cdot$ es asociativo:

Sean $f, g, h \in A^X$. Luego, si $x \in X$, entonces $((fg)h)(x) = (fg)(x)h(x) = (f(x)g(x))h(x) = f(x)(g(x)h(x)) = f(x)(gh)(x) = (f(gh))(x)$. Por tanto, $(fg)h = f(gh)$.

(viii) $\cdot$ es conmutativo:

Sean $f, g \in A^X$. Ahora, si $x \in X$, se tiene que $(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$. Luego, $fg = gf$.

(ix) Existe neutro multiplicativo, 1:

Sea $1 : X \longrightarrow A$, $x \longmapsto 1$. Entonces, $1 \in A^X$. Ahora, si $f \in A^X$ y $x \in X$, se tiene que $(f1)(x) = f(x)1(x) = f(x)1 = f(x)$. Por tanto, $f1 = f$.

(x) $\cdot$ se distribuye sobre $+$:

Sean $f, g, h \in A^X$. Luego, si $x \in X$, se tiene que $(f(g+h))(x) = f(x)(g+h)(x) = f(x)(g(x)+h(x)) = f(x)g(x)+f(x)h(x) = (fg)(x)+(fh)(x)$. Luego, $f(g+h) = fg+fh$.

Por tanto, $(A^X, +, \cdot)$ es un anillo.

†

Ahora unas propiedades que cumplen los elementos de un anillo:

Proposición 2.1. *Sea A un anillo. Entonces para todo $a, b \in A$, se cumplen:*

1. $a0 = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. $(-1)a = -a$.
5. *Para todo $n \in \mathbb{Z}^+$,* $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

Definición 2.2. *Sea A un anillo.*

1. *Un elemento $a \in A \setminus \{0\}$ se llama un **divisor de cero** si existe $b \in A \setminus \{0\}$ tal que $ab = 0$.*
2. *Un elemento $u \in A \setminus \{0\}$ se llama una **unidad** de A si existe $v \in A$ tal que $uv = 1$.*
3. *Un **campo** k es un anillo tal que todos sus elementos distintos de cero son unidades y $1 \neq 0$.*
4. *Un **dominio entero** D es un anillo tal que no tiene divisores de cero y $1 \neq 0$.*

Ejemplos 2.2.

1. *El anillo $\mathbb{Z}$ no tiene divisores de cero y sus unidades son solo 1 y -1.*
2. *Los anillos $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son campos.*
3. *En el anillo $\mathbb{Z}/4\mathbb{Z}$, $\overline{2}$ es un divisor de cero; $\overline{2} \neq \overline{0}$ y $\overline{2} \cdot \overline{2} = \overline{0}$.*
4. *En el anillo $\mathbb{R}^{[0,1]} = \{f : [0,1] \longrightarrow \mathbb{R} \mid f \text{ es función}\}$ sus unidades son las funciones que no son cero en todo elemento de su dominio, pues si $f(x) \neq 0$ para todo $x \in [0,1]$, entonces si $g : [0,1] \longrightarrow \mathbb{R}$ es tal que $g(x) = (f(x))^{-1}$ para todo $x \in [0,1]$, se tiene que $f(x)g(x) = f(x)(f(x))^{-1} = 1 = 1(x)$, para todo $x \in [0,1]$. Además, si $h \in \mathbb{R}^{[0,1]}$ es tal que $h(x) \neq 0$ para algún $x \in [0,1]$, entonces h es un divisor de cero, pues si $l \in \mathbb{R}^{[0,1]}$ la definimos como* $l(x) = \begin{cases} 0 & si \quad h(x) \neq 0 \\ \\ 1 & si \quad h(x) = 0 \end{cases}$, *se tiene que l no es la función cero y $hl(x) = 0$, para todo $x \in [0,1]$, entonces h es un divisor de cero.*

Notación 2.2. *Si A es un anillo y $a \in A \setminus \{0\}$ es una unidad, entonces su inverso multiplicativo es único, pues si $u, u' \in A$ son tales que $au = 1 = au'$, entonces $u = 1u = (u'a)u = u'(au) = u'1 = u'$, y lo denotaremos por a^{-1}.*

Ahora veamos una caracterización de los dominios enteros:

Proposición 2.2. *Sea D un anillo no cero. D es un dominio entero si y solo si para cualesquiera $a, b \in D\backslash\{0\}$, $ab \neq 0$.*

Demostración. ($\Longrightarrow$) Si $a, b \in D\backslash\{0\}$ son fijos arbitrarios, entonces, en particular, a no es un divisor de cero, por lo que $ab \neq 0$.
($\Longleftarrow$) Por contradicción. En efecto, si $a \in D\backslash\{0\}$ fuera un divisor de cero, existiría $b \in D\backslash\{0\}$ tal que $ab = 0$, pero por hipótesis, $ab \neq 0$, porque $a, b \in D\backslash\{0\}$, entonces $0 \neq 0$, contradicción. Así, D no tiene divisores de cero; es decir, D es un dominio entero.

†

Proposición 2.3. *Sea $p > 1$ un entero. El anillo $\mathbb{Z}/p\mathbb{Z}$ es un dominio entero si y solo si p es un número primo.*

Demostración. ($\Longrightarrow$) Por contradicción. Si $p = ab$, con $1 < a < p$ y $1 < b < p$, entonces $\overline{a} \neq \overline{0}$ y $\overline{b} \neq \overline{0}$. Luego, $\overline{0} = \overline{m} = \overline{ab} = \overline{a}\overline{b}$. Así, $\overline{a}$ (o $\overline{b}$) es un divisor de cero de $\mathbb{Z}/p\mathbb{Z}$, contradicción. Por tanto, p es un número primo.
($\Longleftarrow$) Supongamos que p es un número primo y sean $\overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ tales que $\overline{a}\overline{b} = \overline{0}$. Así, $\overline{ab} = 0$ y por tanto $p|ab$, pero como p es un número primo, $p|a$ o $p|b$, es decir, $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$. Por tanto, por la **Proposición** 2.2, $\mathbb{Z}/p\mathbb{Z}$ es un dominio entero.

†

Proposición 2.4. *Sea A un anillo. Si $a \in A$ es un divisor de cero, entonces a no es una unidad de A.*

Demostración. Por contradicción. En efecto, supongamos que $a \in A\backslash\{0\}$ es una unidad, entonces $au = 1$ para algún $u \in A$. Además, existe $b \in A\backslash\{0\}$ tal que $ab = 0$. Luego, $ab = 0$ implica que $0 = u0 = u(ab) = (ua)b = 1b = b$, entonces $b = 0$, contradicción. Por tanto, a no es una unidad de A.

†

Corolario 2.1. *Si k es un campo, entonces k es un dominio entero.*

El recíproco del corolario anterior en general no es cierto, pues $\mathbb{Z}$ es un dominio entero y no es campo, pero si D es dominio entero finito, se cumple:

Proposición 2.5. *Si D es un dominio entero finito, entonces D es un campo.*

Demostración. Sea $a \in D\backslash\{0\}$. Ahora, consideremos la función $f_a : D \longrightarrow D$ tal que $f_a(x) = ax$, para todo $x \in D$. f_a es inyectiva, pues si $x, x' \in D$ son tales que $f_a(x) = f_a(x')$, se cumple que $a(x - x') = 0$, por lo que $x = x'$, por la **Proposición 2.2**. f_a es sobreyectiva, de lo contrario, si $f_a[D] \neq D$, entonces $f_a|^{f_a[D]} : D \longrightarrow f_a[D]$ sería una biyección, por lo que D tendría un subconjunto propio con la misma cardinalidad, entonces D es infinito, contradicción. Así, f_a es biyectiva. Luego, para $1 \in D$ existe un único $x \in D$ tal que $1 = f_a(x) = ax$. Así, a es una unidad. Por tanto, D es un campo.

†

Proposición 2.6. *Sea $p > 1$ un entero. El anillo $\mathbb{Z}/p\mathbb{Z}$ es un campo si y solo si p es un número primo.*

Demostración. ($\Longrightarrow$) Si $\mathbb{Z}/p\mathbb{Z}$ es un campo, por el **Corolario 2.1**, $\mathbb{Z}/p\mathbb{Z}$ es un dominio entero, y por la **Proposición 2.3**, p es un número primo.
($\Longleftarrow$) Si p es un número primo, por la **Proposición 2.3**, $\mathbb{Z}/p\mathbb{Z}$ es un dominio entero, que es finito, entonces por la **Proposición 2.5**, $\mathbb{Z}/p\mathbb{Z}$ es un campo.

†

Definición 2.3. *Sea A un anillo. Un subconjunto S de A es un **subanillo** si:*

1. $1 \in S$.
2. *Si $a, b \in S$, entonces $a - b \in S$.*
3. *Si $a, b \in S$, entonces $ab \in S$.*

Ejemplos 2.3.
1. *Si A es un anillo, A es un subanillo de si mismo.*
2. *Se sabe que $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, inclusión de subanillos.*

Observación 2.1. *Si A es un anillo y $\{S_j\}_{j\in\Lambda}$ es una familia de subanillos de A, entonces $A := \bigcap_{j\in\Lambda} S_j$ si $\Lambda = \emptyset$.*

Proposición 2.7. *Sean A un anillo y $\{S_j\}_{j\in\Lambda}$ una familia de subanillos de A. Entonces, $\bigcap_{j\in\Lambda} S_j$ es un subanillo de A.*

Demostración. Si $\Lambda = \emptyset$, $\bigcap_{j\in\Lambda} S_j = A$, que claramente es un subanillo de A. Ahora, supongamos que $\Lambda \neq \emptyset$. En efecto, primero, $\bigcap_{j\in\Lambda} S_j \subseteq A$ porque si $x \in \bigcap_{j\in\Lambda} S_j$, se tiene que $x \in S_j$ para toda $j \in \Lambda$, pero $S_j \subseteq A$ para toda $j \in \Lambda$, entonces $x \in A$. Ahora, $1 \in \bigcap_{j\in\Lambda} S_j$, pues como S_j es un subanillo de A, para toda $j \in \Lambda$, $1 \in S_j$ para toda $j \in \Lambda$. Luego, si $a, b \in \bigcap_{j\in\Lambda} S_j$, se cumple que $a, b \in S_j$ para toda $j \in \Lambda$, entonces $a - b \in S_j$ para toda $j \in \Lambda$; es decir, $a - b \in \bigcap_{j\in\Lambda} S_j$. Por último, si $a, b \in \bigcap_{j\in\Lambda} S_j$, se cumple que $a, b \in S_j$ para toda $j \in \Lambda$, entonces $ab \in S_j$ para toda $j \in \Lambda$, con lo que $ab \in \bigcap_{j\in\Lambda} S_j$. Por tanto, $\bigcap_{j\in\Lambda} S_j$ es un subanillo de A.

†

Corolario 2.2. *Sea A un anillo y B un subconjunto de A. Entonces, existe un anillo más pequeño que contiene a B.*

Demostración. Sea $\mathcal{F}_B := \{S \subseteq A \mid S \text{ es subanillo de } A \text{ y } B \subseteq S\}$. Ahora, $\mathcal{F}_B \neq \emptyset$; $A \in \mathcal{F}_B$. Luego, por la proposición anterior, $\bigcap \mathcal{F}_B$ es un subanillo de A y contiene a B. Además, es claro que es el anillo más pequeño que contiene a B.

†

Al anillo que hace refencia el corolario anterior le llamaremos subanillo de A **generado** por B.

Definición 2.4. *Sean A un anillo, S un subanillo de A y R un subconjunto de A. Ahora, sea $\mathcal{F} = \{S' \subseteq A \mid S' \text{ es un subanillo de } A \text{ y } S, R \subseteq S'\}$. Definimos el subanillo de A **generado por** S y R, denotado por $S[R]$, como*

$$S[R] = \bigcap \mathcal{F}.$$

Observación 2.2.

1. *La familia $\mathcal{F}$, de la definición anterior, es no vacía porque $A \in \mathcal{F}$.*
2. *Por la **Proposición 2.7**, $S[R]$ es un subanillo de A. Además, $S, R \subseteq S[R]$, por definición. Así, $S[R]$ es el subanillo más pequeño que contiene a S y R.*

Notación 2.3. *Si A es un anillo, S un subanillo de A y $R = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ un subconjunto finito de A, denotaremos a $S[R]$ como $S[\alpha_1, \alpha_2, \ldots, \alpha_n]$.*

Proposición 2.8. *Si A es un anillo, S un subanillo de A y $\alpha \in A$, entonces*

$$S[\alpha] = \{s_0\alpha^0 + s_1\alpha^1 + \cdots + s_n\alpha^n \mid n \in \mathbb{Z}^+ \cup \{0\}\ y\ s_0, \ldots, s_n \in S\}.$$

Demostración. Ver [Sha00, 1.11 Lema]

†

Definición 2.5. *Sean K un campo y k un subconjunto de K. Diremos que k es un **subcampo de** K si:*

1. *k es un subanillo de K.*
2. *$a^{-1} \in k$ siempre que $a \in k\backslash\{0\}$.*

Ejemplos 2.4. 1. *$\mathbb{Q}$ es un subcampo de $\mathbb{R}$.*

2. *$\mathbb{R}$ es un subcampo de $\mathbb{C}$.*

3. *Si $K := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, entonces $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$, inclusión de subcampos.*

Definición 2.6. *Si K es un campo y k es un subcampo de K, diremos que K es una **extensión** de k, lo cual será denotado por K/k.*

Observación 2.3. 1. *Por la definición anterior, se observa que K es un k-espacio vectorial. En efecto, como K, en particular, es un anillo, K es un grupo abeliano aditivo. Luego, al multiplicar por un escalar $\lambda \in k$, un elemento $v \in K$, se considera $\lambda \in K$, entonces $\lambda v \in K$ será el producto de K, por lo que se cumplen los axiomas de espacio vectorial.*

2. *Si K/k es una extensión de campos, entonces a la dimensión de K como k-espacio vectorial le llamaremos **grado de la extensión**, lo cual se denotará por $[K : k]$. Así, $[K : k]$ puede ser finita o infinita.*

Ejemplos 2.5. 1. *$[\mathbb{R} : \mathbb{Q}] = \infty$.*

2. *$[\mathbb{C} : \mathbb{R}] = 2$.*

3. *Si $K := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, entonces $[K : \mathbb{Q}] = 2$.*

Proposición 2.9. *Sean K un campo y $\{F_j\}_{j\in\Lambda}$ una familia de subcampos de K. Entonces, $\bigcap_{j\in\Lambda} F_j$ es un subcampo de K.*

Demostración. En efecto, por la **Proposición 2.7**, $\bigcap_{j\in\Lambda} F_j$ es un subanillo de K. Luego, si $\Lambda = \emptyset$, $\bigcap_{j\in\Lambda} F_j = K$, que es campo. Ahora, supongamos que $\Lambda \neq \emptyset$. En efecto, si $a \in \bigcap_{j\in\Lambda} F_j$, $a \in F_j$

para toda $j \in \Lambda$, por lo que $a^{-1} \in F_j$ para toda $j \in \Lambda$, entonces $a^{-1} \in \bigcap_{j\in\Lambda} F_j$. Por lo anterior, $\bigcap_{j\in\Lambda} F_j$ es un subcampo de K.

†

Definición 2.7. *Sea K un campo.*

1. *A la intersección k de todos los subcampos de K le llamaremos el **campo primo de** K.*

2. *Si k es un subcampo de K, X es un subconjunto de K y $\mathcal{F} := \{F \subseteq K \mid F$ es un subcampo de K y $k, X \subseteq F\}$, entonces se define el subcampo de K obtenido **adjuntando** X a k, denotado por $k(X)$, como*

$$k(X) = \bigcap \mathcal{F}.$$

Observación 2.4. 1. *La familia $\mathcal{F}$, de 2. de la definición anterior, es no vacía porque $K \in \mathcal{F}$.*

2. *Por la **Proposición 2.9** $k(X)$ es un subcampo de K. Luego, $k(X)$ es el subcampo más pequeño que contiene a k y X. Además, si X es un subconjunto finito de K, con más de un elemento, $k(X)/k$ será llamada extensión **finitamente generada** de k y si X contiene exactamente un elemento, $k(X)/k$ será llamada extensión **simple** de k.*

Notación 2.4. *Si K es un campo, k un subcampo de K y $X = \{\alpha_1, \ldots, \alpha_n\}$ un subconjunto finito de K, denotaremos a $k(X)$ como $k(\alpha_1, \ldots, \alpha_n)$.*

Más adelante, una vez que hayamos introducido el anillo de polinomios, continuaremos con nuestra exposición sobre extensiones de campos.

Ahora, lo que nos ocupa es relacionar anillos, es decir, dados A y B anillos, los relacionaremos mediante funciones que "respeten" su estructura. A tales funciones les llamaremos homomorfismos de anillos. Dicho lo anterior, comenzamos con la siguiente:

Definición 2.8. *Sean A y B dos anillos. Diremos que una función $f : A \longrightarrow B$ es un **homomorfismo de anillos**, más brevemente **morfismo de anillos**, si:*

1. *$f(a + a') = f(a) + f(a')$, para todo $a, a' \in A$.*

2. *$f(aa') = f(a)f(a')$, para todo $a, a' \in A$.*

3. $f(1) = 1$.

Ejemplos 2.6. 1. *La función cero,* $0 : A \longrightarrow \{0\}$*, es un homomorfismo de anillos, el homomorfismo* ***cero****.*

2. *Si* B *es un subanillo de* A*, la función inclusión,* $\iota : B \longrightarrow A$ *definida por* $\iota(x) = x$*, es un homomorfismo de anillos. Así, en particular, la función identidad en* A*,* $Id_A : A \longrightarrow A$*, es un homomorfismo de anillos.*

4. *La función conjugación compleja,* $\overline{()} : \mathbb{C} \longrightarrow \mathbb{C}$ *definida por* $\overline{()}(a + ib) = \overline{a + ib} = a - ib$*, es un homomorfismo de anillos.*

5. *Sea* $n \geq 2$ *un entero. La función* $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$*, definida por* $f(m) = \overline{m}$*, es un homomorfismo de anillos.*

6. *Sea* A *un anillo. La función* $g : \mathbb{Z} \longrightarrow A$*, definida por*

$$g(n) = \begin{cases} n1 & si \quad n > 0 \\ 0 & si \quad n = 0 \\ (-n)(-1) & si \quad n < 0 \end{cases}$$

, es un homomorfismo de anillos.

Proposición 2.10. *Sea* $f : A \longrightarrow B$ *un morfismo de anillos. Entonces:*

1. $f(0) = 0$.

2. *Para todo* $a \in A$*,* $f(-a) = -f(a)$.

3. *Para todo* $n \in \mathbb{Z}$ *y todo* $a \in A$*,* $f(na) = nf(a)$.

4. *Para todo* $n \in \mathbb{Z}^+$ *y todo* $a \in A$*,* $f(a^n) = f(a)^n$.

5. *Si* $a \in A$ *es una unidad, entonces* $f(a)$ *es una unidad y* $f(a^{-1}) = f(a)^{-1}$*. Más aún, si* $a \in A$ *es una unidad, entonces* $f(a^{-n}) = f(a)^{-n}$ *para todo* $n \geq 1$ *entero.*

6. *Si* $g : B \longrightarrow C$ *es un homomorfismo de anillos,* $g \circ f : A \longrightarrow C$ *es un homomorfismo de anillos.*

Definición 2.9. *Sean* A, B *anillos y* $f : A \longrightarrow B$ *un morfismo.*

1. *Diremos que* f *es un* ***isomorfismo*** *si existe un morfismo* $f^{-1} : B \longrightarrow A$ *tal que* $f^{-1} \circ f = Id_A$ *y* $f \circ f^{-1} = Id_B$.

2. *Diremos que A y B son **isomorfos**, lo cual se denotará por $A \cong B$, si existe un isomorfismo entre ellos.*

3. *El **núcleo** de f, denotado por $ker(f)$, es el conjunto*

$$ker(f) = \{a \in A \mid f(a) = 0\}.$$

4. *La **imagen** de A bajo f, denotada por $f[A]$, es el conjunto*

$$f[A] = \{b \in B \mid b = f(a) \text{ para algún } a \in A\}.$$

Proposición 2.11. *Sea $f : A \longrightarrow B$ un morfismo de anillos. Se cumplen:*

1. *f es isomorfismo si y solo si $f$es biyectivo.*

2. *f es inyectivo si y solo si $ker(f) = \{0\}$*

3. *$f[A]$ es un subanillo de B.*

Demostración. 1. ($\Longrightarrow$): Si f es un isomorfismo, entonces f, por definición, tiene inverso izquierdo e inverso derecho, por lo que f es inyectivo y suprayectivo. Luego, f es biyectivo. ($\Longleftarrow$): Si f es biyectivo, entonces existe una función inversa $f^{-1} : B \longrightarrow A$ tal que $f \circ f^{-1} = Id_B$ y $f^{-1} \circ f = Id_A$. Demostremos que f^{-1} es morfismo. En efecto, si $x, y \in B$, entonces $f^{-1}(x + y) = f^{-1}(f(f^{-1}(x)) + f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x) + f^{-1}(y))) = f^{-1}(x) + f^{-1}(y)$, $\quad f^{-1}(xy) = f^{-1}(f(f^{-1}(x))f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x)f^{-1}(y))) = f^{-1}(x)f^{-1}(y)$ y $f(1) = 1$ implica que $1 = f^{-1}(f(1)) = f^{-1}(1)$. Así, f^{-1} es morfismo. Por tanto, f es isomorfismo.

2. ($\Longrightarrow$): Si $a \in ker(f)$, entonces $f(a) = 0$, pero también $f(0) = 0$, entonces $f(a) = f(0)$, pero f es inyectivo, entonces $a = 0$. Luego, $ker(f) \subseteq \{0\}$. Así, $ker(f) = \{0\}$. ($\Longleftarrow$): Si $a, b \in A$ y $f(a) = f(b)$, entonces $0 = f(a) - f(b) = f(a - b)$, es decir, $a - b \in ker(f) = \{0\}$, entonces $a - b = 0$, es decir, $a = b$. Por tanto, f es inyectivo.

3. Primero, por definición, $f[A] \subseteq B$. Ahora, como $f(1) = 1$, entonces $1 \in f[A]$. Luego, si $x, y \in f[A]$, entonces $x = f(a)$, para algún $a \in A$, y $y = f(b)$, para algún $b \in B$. Así, $x - y = f(a) - f(b) = f(a - b)$, con $a - b \in A$, y $xy = f(a)f(b) = f(ab)$, con $ab \in A$, entonces $x - y \in f[A]$ y $xy \in f[A]$. Por tanto, $f[A]$ es un subanillo de B.

†

Ejemplos 2.7. *1. Si B es un subanillo de A, entonces el morfismo inclusión, $\iota : B \longrightarrow A$, $b \longmapsto b$, es inyectivo.*

2. Si A es un anillo, entonces el morfismo identidad en A, $Id_A : A \longrightarrow A$ es un isomorfismo.

3. Consideremos el morfismo conjugación compleja, $\overline{()} : \mathbb{C} \longrightarrow \mathbb{C}$, $a + ib \longmapsto a - ib$. Entonces, $\overline{()}$ es un isomorfismo.

Ahora definiremos un tipo especial de subconjuntos de un anillo A.

Definición 2.10. *Sea A un anillo. Diremos que un subconjunto I de A es un **ideal** de A si:*

1. $0 \in I$.

2. Si $a, b \in I$, entonces $a + b \in I$.

3. Si $a \in A$ y $b \in I$, entonces $ab \in I$.

Ejemplos 2.8. *1. Si A es un anillo, entonces A y $\{0\}$ son ideales de A, llamados ideales **triviales** de A.*

2. Si $f : A \longrightarrow B$ es un morfismo de anillos y J es un ideal de B, entonces $f^{-1}[J] := \{a \in A \mid f(a) \in J\}$ es un ideal de A.

3. Si $f : A \longrightarrow B$ es un morfismo de anillos sobreyectivo e I es un ideal de A, entonces $f[I] := \{f(a) \in B \mid a \in I\}$ es un ideal de B.

4. Si $f : A \longrightarrow B$ es un morfismo de anillos, $ker(f)$ es un ideal de A.

5. Si $n \in \mathbb{Z}$, entonces $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ es un ideal de $\mathbb{Z}$.

Demostración. 1. Es claro.

2. En efecto, $0 \in f^{-1}[J]$ porque $f(0) = 0 \in J$. Ahora, si a y $b \in f^{-1}[J]$, entonces $f(a)$ y $f(b) \in J$, pero como J es un ideal de B y f es un morfismo de anillos, $f(a + b) = f(a) + f(b) \in J$, así $a + b \in f^{-1}[J]$. Por último, si $a \in A$ y $b \in f^{-1}[J]$, entonces $f(a) \in B$ y $f(b) \in J$, pero como J es un ideal de B y f es un morfismo de anillos, $f(ab) = f(a)f(b) \in J$ lo que implica que $ab \in f^{-1}[J]$. Por tanto, $f^{-1}[J]$ es un ideal de A.

3. Por definición, $f[I] \subseteq B$. $0 \in f[I]$ porque $f(0) = 0$ y $0 \in I$. Si $f(a), f(b) \in f[I]$ para algunos $a, b \in I$, entonces $f(a) + f(b) = f(a + b) \in I$ porque $a + b \in I$. Por último, si

$b \in B$ y $f(a) \in f[I]$, entonces existe $a' \in A$ tal que $f(a') = b$ y $f(a) \in f[I]$, por lo que $bf(a) = f(a')f(a) = f(a'a) \in f[I]$ porque $a'a \in I$. Por tanto, $f[I]$ es un ideal de B.

4. Notemos que $\{0\}$ es un ideal de B, por 1., y $ker(f) = f^{-1}[\{0\}]$, entonces, por 2., se tiene que $ker(f)$ es un ideal de A.

5. Es claro.

†

Observación 2.5. *Si $f : A \longrightarrow B$ es un morfismo de anillos e I es un ideal de A, en general $f[I]$ no es un ideal de B, pues basta considerar al morfismo inclusión $\iota : \mathbb{Z} \longrightarrow \mathbb{Q}$ y al ideal $2\mathbb{Z}$ de $\mathbb{Z}$. En efecto, $\iota[2\mathbb{Z}] = \{2n \mid n \in \mathbb{Z}\}$. Ahora, si $\frac{1}{3} \in \mathbb{Q}$ y $2n \in \iota[2\mathbb{Z}]$, para algún $n \in \mathbb{Z}$, entonces $\frac{1}{3}2n = 2\frac{n}{3}$, pero $\frac{n}{3} \notin \mathbb{Z}$, entonces $\frac{1}{3}2n \notin \iota[2\mathbb{Z}]$. Luego, $\iota[2\mathbb{Z}]$ no es un ideal de $\mathbb{Q}$.*

Notación 2.5.

1. *Si A es un anillo e I es un ideal de A, entonces con $I \leq A$ denotaremos que I es un ideal de A y con $I < A$ denotaremos que I es un ideal propio de A.*

2. *Dado A un anillo, con 0 denotaremos a $\{0_A\}$ y con 1 denotaremos a $\{1\}$.*

Proposición 2.12. *Sea A un anillo e I un ideal de A. Entonces, para todo $n \in \mathbb{Z}^+$, $a_1, \ldots, a_n \in A$ y $b_1, \ldots, b_n \in I$, $\sum_{i=1}^{n} a_i b_i \in I$. En particular, $\sum_{i=1}^{n} b_i \in I$.*

Observación 2.6. *Sean A un anillo e I un ideal de A. Ahora, si $1 \in I$, entonces $I = A$. Más aún, si $u \in I$ es una unidad de A, entonces $I = A$. En efecto, para la primera parte, si $1 \in I$, entonces para cada $a \in A$, $a = a1 \in I$. Así, $A \subseteq I$. Luego, $A = I$. Por último, si $u \in I$ es una unidad de A, existe $u^{-1} \in A$ tal que $1 = u^{-1}u \in I$. Así, por lo anterior, $A = I$.*

Convención 2.2. *Si A es un anillo y Γ es la familia vacía de ideales de A, entonces $\bigcap \Gamma := A$.*

Proposición 2.13. *Sean A un anillo y Γ una familia de ideales de A. Entonces, $\bigcap \Gamma$ es un ideal de A.*

Definición 2.11. *Sean A un anillo y X un subconjunto de A. Sea $\Gamma := \{I \subseteq A \mid I$ es un ideal de A y $X \subseteq I\}$. Definimos el **ideal generado** por X, denotado por (X), como*

$$(X) = \bigcap \Gamma.$$

Observación 2.7. *Por la **Proposición 2.13** (X) es un ideal de A. Además, como $X \subseteq I$ para todo $I \in \Gamma$, $X \subseteq (X)$. Por último, (X) es el ideal más pequeño que contiene a X.*

Proposición 2.14. *Sean A un anillo y $X \subseteq A$. Se cumple:*

$$(X) = \begin{cases} \left\{ \sum_{finita} a_j x_j | a_j \in A, x_j \in X \right\} & si \quad X \neq \emptyset \\ \\ 0 & si \quad X = \emptyset \end{cases}$$

Notación 2.6. *Si $X = \{x_1, x_2, ..., x_n\}$ es un subconjunto finito de A, denotaremos a (X) como $(x_1, \ldots, x_n)$ y lo llamaremos ideal generado por $x_1, x_2, ..., x_n$. En particular, si $X = \{x_1\}$, entonces $(X) = (x_1)$ tiene un nombre especial, ideal **principal** generado por x_1.*

Observación 2.8. *Sea A un anillo. Entonces, A y 0 siempre son ideales principales, ya que $A = (1)$ y $0 = (0)$.*

Proposición 2.15. *Consideremos al anillo $\mathbb{Z}$. Entonces, todo ideal I de $\mathbb{Z}$ es principal.*

Demostración. Sea I un ideal de $\mathbb{Z}$. Ahora, si $I = 0$, entonces I es principal. Supongamos que $I \neq 0$, entonces existe $m \in \mathbb{Z}^+ \cap I$. Luego, por el principio del buen orden, I tiene elemento menor, digamos n. Así, se afirma que $I = (n)$. ($\subseteq$): Si $x \in I$, entonces, por el algoritmo de la división, existen únicos $q, r \in \mathbb{Z}$ tales que $x = qn + r$, con $0 \leq r < n$. Ahora, si $0 < r < n$, entonces $r = x - qn \in I$, lo cual no puede pasar, pues n es el elemento menor de I. Así, $r = 0$ y por tanto $x = qn \in (n)$. ($\supseteq$): Si $ln \in (n)$, para algún $l \in \mathbb{Z}$, entonces, como $n \in I$ e I es ideal de $\mathbb{Z}$, entonces $ln \in I$. Luego, $I = (n)$. Por tanto, todo ideal I de $\mathbb{Z}$ es principal.

†

Definición 2.12. *Sea A un anillo.*

1. *Si I y J son ideales de A, definimos el **producto** de I y J, denotado por IJ, como*

$$IJ := (\{ab \mid a \in I, b \in J\}).$$

2. *Si $\{I_j\}_{j \in \Lambda}$ es una familia de ideales de A, definimos la **suma** de la familia, denotada por $\sum_{j \in \Lambda} I_j$, como*

$$\sum_{j \in \Lambda} I_j := \left(\bigcup_{j \in \Lambda} I_j \right).$$

Proposición 2.16. *Sea A un anillo. Se cumplen:*

1. *Si I y J son ideales de A, entonces*

$$IJ = \begin{cases} \left\{ \sum_{finita} a_j b_j \,|\, a_j \in I, b_j \in J \right\} & si \quad \{ab \,|\, a \in I, b \in J\} \neq \emptyset \\ \\ 0 & si \quad \{ab \,|\, a \in I, b \in J\} = \emptyset \end{cases}$$

2. *Si $\{I_j\}_{j\in\Lambda}$ es una familia arbitraria de ideales de A, entonces*

$$\sum_{j\in\Lambda} I_j = \begin{cases} \left\{ \sum_{j=1}^{n} a_{i_j} x_{i_j} \,|\, n \in \mathbb{Z}^+,\ a_{i_j} \in A, x_{i_j} \in I_{i_j} \right\} & si \quad X \neq \emptyset \\ \\ 0 & si \quad X = \emptyset \end{cases}$$

Observación 2.9. *Sea A un anillo.*

1. *Si I y J son ideales de A, entonces $IJ \subseteq I,\ J$ y por lo tanto $IJ \subseteq I \cap J$.*
2. *Si $\{I_j\}_{j\in\Lambda}$ es una familia arbitraria de ideales de A, entonces $I_j \subseteq \sum_{j\in\Lambda} I_j$, para todo $j \in \Lambda$.*

Definición 2.13. *Sea A un anillo y $\mathcal{F} := \{I_j\}_{j\in\mathbb{Z}^+}$ una familia de ideales de A. Diremos que $\mathcal{F}$ es una* ***cadena ascendente en*** *A, si $\mathcal{F}$ es una cadena en $(A, \subseteq)$ e $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$.*

Proposición 2.17. *Sea A un anillo y $\{I_j\}_{j\in\mathbb{Z}^+}$ una familia de ideales de A tal que es una cadena ascendente, entonces $J := \bigcup_{n\geq 1} I_n \leq A$.*

Demostración. (i) $0 \in J$.

Porque $0 \in I_j$, para todo $j \in \mathbb{Z}^+$.

(ii) Si $a, b \in J$, entonces $a + b \in J$.

Si $a, b \in J$, existen $l, m \in \mathbb{Z}^+$ tales que $a \in I_l$ y $b \in I_m$. Ahora, $l \leq m$ o $m \leq l$. Sin pérdida de generalidad, supongamos que $l \leq m$. Entonces, $I_l \subseteq I_m$. Así, $a, b \in I_m$, entonces $a + b \in I_m$. Por tanto, $a + b \in J$.

(iii) Si $a \in A$ y $b \in J$, entonces $ab \in J$.

En efecto, si $a \in A$ y $b \in J$, entonces $a \in A$ y $b \in I_k$, para algún $k \in \mathbb{Z}^+$. Luego, $ab \in I_k$, para algún $k \in \mathbb{Z}^+$. Así, $ab \in J$.

Por tanto, $J = \bigcup_{n\geq 1} I_n \leq A$.

†

Definición 2.14. *Sea A un anillo e $I \leq A$. Definimos el* ***radical*** *de I, denotado por $\sqrt{I}$, como*

$$\sqrt{I} = \{a \in A \mid \text{existe } k \in \mathbb{Z}^+ \text{ con } a^k \in I\}.$$

Proposición 2.18. *Sean A un anillo e $I \leq A$. Entonces, $I \subseteq \sqrt{I}$ y $\sqrt{I} \leq A$.*

Demostración. Primero, $I \subseteq \sqrt{I}$ porque si $a \in I = I \cap A$,entonces $a \in A$ y $a^1 \in I$. Ahora, veamos que $\sqrt{I} \leq A$. En efecto, por la definición de $\sqrt{I}$, $\sqrt{I} \subseteq A$. Además, como $I \subseteq \sqrt{I}$, $0 \in \sqrt{I}$. Ahora, sean $a, b \in \sqrt{I}$ y $c \in A$, entonces existen k y l enteros positivos tales que $a^k, b^l \in I$. Supongamos, sin pérdida de generalidad, que $k \leq l$. Así,

(i) $a + b \in \sqrt{I}$:

Afirmamos que $(a+b)^{k+l} \in I$. En efecto, por 5. de la **Proposición 2.1**

$$(a+b)^{k+l} = \sum_{i=0}^{k+l} \binom{k+l}{i} a^i b^{k+l-i}.$$

Ahora, si $i < k$, tenemos que $l < k + l - i$, entonces se cumple que $a^i b^{k+l-i}$ $= (a^i b^{k-i}) b^l \in I$. Luego, por la **Proposición 2.12**

$$\sum_{i=0}^{k-1} \binom{k+l}{i} a^i b^{k+l-i} \in I.$$

Ahora, si $k \leq i$, tenemos que $a^i b^{k+l-i} = a^k a^{i-k} b^{k+l-i} = a^k (a^{i-k} b^{k+l-i}) \in I$. Así, por la **Proposición 2.12**

$$\sum_{i=k}^{k+l} \binom{k+l}{i} a^i b^{k+l-i} \in I.$$

Luego,

$$\sum_{i=0}^{k-1} \binom{k+l}{i} a^i b^{k+l-i} + \sum_{i=k}^{k+l} \binom{k+l}{i} a^i b^{k+l-i} \quad \in I.$$

Por tanto, $(a+b)^{k+l} \in I$.

(ii) $bc \in \sqrt{I}$:

Porque $(bc)^l = b^l c^l \in I$.

Así, $bc \in \sqrt{I}$.

Por tanto, $\sqrt{I} \leq A$.

†

Observación 2.10. *Sea A un anillo y consideremos $0 \leq A$. En particular,*

$$\sqrt{0} = \{a \in A \mid \text{existe } k \in \mathbb{Z}^+ \text{ con } a^k \in 0\} = \{a \in A \mid \text{existe } k \in \mathbb{Z}^+ \text{ con } a^k = 0\}$$

*lo llamaremos **nilradical** de A, lo denotaremos por $nil\ A$ y a sus elementos los llamaremos elementos **nilpotentes** de A.*

Definición 2.15. *Sea A un anillo.*

1. *Si I es un ideal de A, diremos que I es un ideal **radical** si $I = \sqrt{I}$.*
2. *Si A no tiene elementos nilpotentes no nulos, diremos que A es **reducido**.*

Proposición 2.19. *Sea A un anillo e $I \leq A$. Entonces, se cumplen:*

1. *$\sqrt{I}$ es un ideal radical.*
2. *$\sqrt{I}$ es el menor ideal radical que contiene a I.*

Demostración. 1. Veamos que $\sqrt{I} = \sqrt{\sqrt{I}}$.

($\subseteq$) Por 1. la **Proposición 2.18**, $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$.

($\supseteq$) Sea $a \in \sqrt{\sqrt{I}}$. Demostremos que $a \in \sqrt{I}$; es decir, $a \in A$ y $a^k \in I$ para algún $k \in \mathbb{Z}^+$. En efecto, $a \in \sqrt{\sqrt{I}}$ implica que $a \in A$ y $a^l \in \sqrt{I}$ para algún $l \in \mathbb{Z}^+$, entonces $a \in A$, $a^l \in A$ y $(a^l)^n \in I$ para algún $n \in \mathbb{Z}^+$, pero $(a^l)^n = a^{ln}$ y $ln \in \mathbb{Z}^+$, entonces $a \in A$ y $a^{ln} \in I$ con $ln \in \mathbb{Z}^+$. Así, $a \in \sqrt{I}$. Luego, $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$.

Por tanto, $\sqrt{I}$ es un ideal radical.

2. Sea J un ideal radical tal que $I \subseteq J$. Ahora, si $a \in \sqrt{I}$, entonces $a^k \in I$ para algún $k \in \mathbb{Z}^+$, entonces $a^k \in J$ para algún $k \in \mathbb{Z}^+$; es decir, $a \in \sqrt{J} = J$. Por tanto, $\sqrt{I} \subseteq J$.

†

Ahora, generalicemos 2. de **Ejemplos 2.1**

Proposición 2.20. *Sean A un anillo e I un ideal de A. Definimos la relación* ***congruencia módulo*** I *en* A *como:* $a \equiv b$ *mód* I *sii* $a - b \in I$. *Entonces, la relación* ***congruencia módulo*** I *es de equivalencia.*

Demostración. En efecto, es **reflexiva** porque si $a \in A$, $a - a = 0 \in I$, es decir, $a \equiv a$ mód I. Es **simétrica**, pues si $a, b \in A$ son tales que $a \equiv b$ mód I, entonces $a - b \in I$ implica que $I \ni (-1)(a - b) = b - a$, es decir, $b \equiv a$ mód I. Es **transitiva** porque si $a, b, c \in A$ y pasa que $a \equiv b$ mód I y $b \equiv c$ mód I, se tiene que $a - b \in I$ y $b - c \in I$, entonces $I \ni (a - b) + (b - c) = a - c$, es decir, $a \equiv c$ mód I. Por tanto, la congruencia módulo I es una relación de equivalencia en A.

†

Notación 2.7. *Sean A un anillo e I un ideal de A.*

1. *Si $a \in A$, denotamos a su clase residual módulo I, como $a + I$. Así, $a + I = \{b \in A \mid b - a \in I\} = \{b \in A \mid s = b - a \text{ para algún } s \in I\} = \{a + s \mid s \in I\}$.*
2. *Con A/I denotaremos al conjunto cociente de A por la relación congruencia módulo I.*

Proposición 2.21. *Sean A un anillo e I un ideal de A. Entonces, A/I es un anillo con las operaciones:*

$$\begin{array}{rccc} +: & A/I \times A/I & \longrightarrow & A/I \\ & (a+I, a'+I) & \longmapsto & a + a' + I \end{array} \qquad \begin{array}{rccc} \cdot: & A/I \times A/I & \longrightarrow & A/I \\ & (a+I, a'+I) & \longmapsto & aa' + I \end{array}$$

Demostración. (i) $+$ está bien definida:

Sean $(a + I, a' + I), (b + I, b' + I) \in A/I \times A/I$ tales que $(a + I, a' + I) = (b + I, b' + I)$. Demostremos que $a + a' + I = b + b' + I$. En efecto, como $a + I = b + I$ y $a' + I = b' + I$, se tiene que $a - b \in I$ y $a' - b' \in I$, entonces $I \ni (a - b) + (a' - b') = (a + a') - (b + b')$, es decir, $a + a' + I = b + b' + I$.

(ii) $+$ es asociativa:

Sean $a + I, b + I, c + I \in A/I$. Luego, $(a + I + b + I) + c + I = (a + b) + I + c + I = ((a + b) + c) + I = (a + (b + c)) + I = a + I + (b + c) + I = a + I + (b + I + c + I)$.

(iii) $+$ es conmutativa:

Sean $a + I, b + I \in A/I$. Entonces, $a + I + b + I = a + b + I = b + a + I = b + I + a + I$.

(iv) Existe neutro aditivo, 0:

Sea $0 := 0 + I$. Ahora, si $a + I \in A/I$, entonces $a + I + 0 + I = a + 0 + I = a + I$. Por tanto, $0 := 0 + I$ es el neutro aditivo de A/I.

(v) Existe inverso aditivo para cualquier $a + I \in A/I$:

Sea $a+I$. Ahora, si $-(a+I) := (-a)+I$, entonces $a+I+(-a)+I = a+(-a)+I = 0+I$. Luego, $-(a + I) := (-a) + I$ es el inverso aditivo de $a + I$.

(vi) $\cdot$ está bien definido:

Sean $(a+I, a'+I), (b+I, b'+I) \in A/I \times A/I$ tales que $(a+I, a'+I) = (b+I, b'+I)$. Demostremos que $aa'+I = bb'+I$. En efecto, como $a+I = b+I$ y $a'+I = b'+I$, se tiene que $a-b \in I$ y $a'-b' \in I$, entonces $I \ni a'(a-b) = aa'-a'b$ e $I \ni b(a'-b') = a'b-bb'$, lo que implican que $I \ni (aa'-a'b)+(a'b-bb') = aa'-bb'$, es decir, $aa'+I = bb'+I$.

(vii) $\cdot$ es asociativo:

Sean $a+I, b+I, c+I \in A/I$. Luego, $(a+I\cdot b+I)\cdot c+I = (ab)+I\cdot c+I = ((ab)c)+I = (a(bc))+I = a+I\cdot bc+I = a+I\cdot(b+I\cdot c+I)$.

(viii) $\cdot$ es conmutativo:

Sean $a+I, b+I \in A/I$. Entonces, $a+I\cdot b+I = ab+I = ba+I = b+I\cdot a+I$.

(ix) Existe neutro multiplicativo, 1:

Sea $1 := 1+I$. Ahora, si $a+I \in A/I$, entonces $1+I\cdot a+I = 1a+I = a+I$. Por tanto, $1 := 1+I$ es el neutro multiplicativo de A/I.

(x) $\cdot$ se distribuye sobre $+$:

Sean $a+I, b+I, c+I \in A/I$. Luego, $a+I\cdot(b+I+c+I) = a+I\cdot(b+c+I) = a(b+c)+I = ab+ac+I = ab+I+ac+I = (a+I\cdot b+I)+(a+I\cdot c+I)$

Por tanto, de lo anterior, $(A/I, +, \cdot)$ es un anillo.

†

Observación 2.11. *Sean A un anillo e I un ideal de A. Al anillo A/I le llamaremos **anillo cociente** de A **módulo** I.*

Proposición 2.22. *Sean A un anillo e I un ideal de A. La función $A \xrightarrow{\pi} A/I$, $a \longmapsto a+I$, es un morfismo de anillos suprayectivo. Además, $ker(\pi) = I$.*

Demostración. i) π es morfismo:

Sean $a, b \in A$. Entonces:

- $\pi(a+b) = (a+b)+I = (a+I)+(b+I) = \pi(a)+\pi(b)$.

- $\pi(ab) = (ab) + I = a + I \cdot b + I = \pi(a) \cdot \pi(b)$.
- $\pi(1_A) = 1_A + I = 1_{A/I}$.

Por tanto, π es morfismo.

ii) π es suprayectivo:

Sea $x + I \in A/I$, para algún $x \in A$. Así, $\pi(x) = x + I \in \pi[A]$. Por tanto, $\pi[A] = A/I$.

Por tanto, π es suprayectivo.

iii) $ker(\pi) = I$:

$$ker(\pi) = \{a \in A \mid \pi(a) = 0 + I\} = \{a \in A \mid a + I = 0 + I\}$$

$$= \{a \in A \mid a \in I\} = A \cap I = I.$$

Luego, $ker(\pi) = I$.

†

Observación 2.12. *Sean A un anillo e I un ideal de A. Al morfismo $A \xrightarrow{\pi} A/I$ le llamaremos morfismo* ***natural****.*

Proposición 2.23 (Propiedad universal del anillo cociente). *Sean A un anillo e I un ideal de A. Consideremos al morfismo natural $A \xrightarrow{\pi} A/I$. Si $\varphi : A \longrightarrow B$ es un morfismo de anillos tal que $I \subseteq ker(\varphi)$, entonces existe un único morfismo*

$$\bar{\varphi} : A/I \longrightarrow B$$

tal que $\bar{\varphi} \circ \pi = \varphi$.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \bar{\varphi}} & \\ A/I & & \end{array}$$

Demostración. Definamos $\bar{\varphi}$ como:

$$\bar{\varphi} : A/I \longrightarrow B$$

$$a + I \longmapsto \varphi(a)$$

(i) $\bar{\varphi}$ está bien definido:

Sean $a+I, a'+I \in A/I$ tales que $a+I = a'+I$. Luego, $a-a' \in I \subseteq ker(\varphi)$, por lo que $0 = \varphi(a-a') = \varphi(a) - \varphi(a')$, entonces $\bar{\varphi}(a+I) = \varphi(a) = \varphi(a') = \bar{\varphi}(a'+I)$.

(ii) $\bar{\varphi}$ es morfismo:

Pues φ es morfismo.

(iii) $\bar{\varphi}$ es único:

Sea $\psi : A/I \longrightarrow B$ morfismo tal que $\psi \circ \pi = \varphi$. Demostremos que $\psi = \bar{\varphi}$. En efecto, sea $a+I \in A/I$, entonces $\bar{\varphi}(a+I) = \varphi(a) = \psi(\pi(a)) = \psi(a+I)$. Luego, $\bar{\varphi} = \psi$. Por tanto, $\bar{\varphi}$ es único.

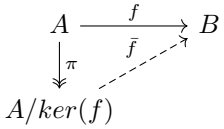
†

Corolario 2.3 (Primer teorema de isomorfismo). *Si $f : A \longrightarrow B$ es un morfismo de anillos, entonces $A/ker(f) \cong f[A]$.*

Demostración. $ker(f)$ es un ideal de A y consideremos el morfismo natural $A \xrightarrow{\pi} A/ker(f)$, entonces, por la propiedad universal del anillo cociente, existe un único morfismo

$$\bar{f} : A/ker(f) \longrightarrow B$$

tal que $\bar{f} \circ \pi = f$.



Se afirma que $\bar{f}$ es inyectivo. En efecto, si $a+ker(f), a'+ker(f) \in A/ker(f)$ son tales que $\bar{f}(a+I) = \bar{f}(a'+I)$, se tiene que $f(a) = f(a')$, entonces $f(a-a') = 0$, es decir, $a-a' \in ker(f)$, de lo cual se implica que $a+ker(f) = a'+ker(f)$. Ahora, $\bar{f}[A/ker(f)] = \{\, b \in B \mid b = \bar{f}(a+ker(f)) = f(a)$ para algún $a \in A \,\} = \{\, b \in B \mid b = f(a)$ para algún $a \in A \,\} = f[A]$. Así, $\bar{f}|^{f[A]} : A/ker(f) \longrightarrow f[A]$ es un isomorfismo. Por tanto, $A/ker(f) \cong f[A]$.

†

Teorema 2.1 (Tercer teorema de isomorfismo). *Sean A un anillo e I, J ideales de A tales que $I \subseteq J$. Se cumplen:*

1. $J/I := \{a + I \mid a \in J\}$ *es un ideal en el anillo cociente* A/I.
2. $(A/I)/(J/I) \cong A/J$.

Demostración. 1. Si $a+I \in J/I$, para algún $a \in J$, entonces, como $J \subseteq A$, se tiene que $a+I \in A/I$. Luego, $J/I \subseteq A/I$. Ahora, como $0 \in J$, entonces $0 + I \in J/I$. Sean $a + I, a' + I \in J/I$, para algunos $a, a' \in J$, entonces $(a + I) + (a' + I) = (a + a') + I$, con $a +' a \in J$, entonces $(a+I)+(a'+I) \in J/I$. Por último, si $a+I \in A/I$, para algún $a \in A$, y $a'+I \in J/I$, para algún $a' \in J$, tenemos que $(a + I)(a' + I) = (aa') + I$, con $aa' \in J$, entonces $(a + I)(a' + I) \in J/I$. Por tanto, J/I es un ideal del anillo cociente A/I.

2. Consideremos la función $\psi : A/I \longrightarrow A/J, a+I \longmapsto a+J$. Se afirma que ψ es un morfismo suprayectivo. Primero, ψ está bien definida porque si $a+I, b+I \in A/I$, para algunos $a, b \in A$, son tales que $a+I = b+I$, entonces $a-b \in I$, pero como $I \subseteq J$, entonces $a-b \in J$ lo que implica que $\psi(a+I) = a+J = b+J = \psi(b+I)$. Segundo, ψ es morfismo, pues si $a+I, b+I \in A/I$, entonces $\psi((a+I)+(b+I)) = \psi((a+b)+I) = (a+b)+J = (a+J)+(b+J) = \psi(a+I)+\psi(b+I)$, $\psi((a + I)(b + I)) = \psi((ab) + I) = (ab) + J = (a + J)(b + J) = \psi(a + I)\psi(b + I)$ y $\psi(1 + I) = 1 + J = 1_{A/J}$. Ahora, ψ es suprayectivo porque si $a + J \in A/J$, para algún $a \in A$, entonces $a + I \in A/I$ y $\psi(a + I) = a + J$. Además, $ker(\psi) = \{ a + I \in A/I \mid \psi(a + I) = 0 + J \} = \{ a + I \in A/I \mid a + J = 0 + J \} = \{ a + I \in A/I \mid a \in J \} = J/I$. Así, por el **Primer teorema de isomorfismo**, $(A/I)/(J/I) \cong A/J$

†

Ejemplos 2.9. *Sea A un anillo.*

1. *Consideremos el morfismo $Id_A : A \longrightarrow A$. Ahora, sabemos que Id_A es suprayectivo y $ker(Id_A) = \{0\}$, entonces, por el **Primer teorema de isomorfismo**, $A/0 \cong A$.*
2. *Consideremos el morfismo $0 : A \longrightarrow \{0\}$. Entonces, 0 es suprayectivo y $ker(0) = A$, entonces, por el **Primer teorema de isomorfismo**, $A/A \cong \{0\}$.*

Proposición 2.24. *Sea A un anillo.Entonces, son equivalentes:*

1. *A es un campo.*

2. *Los únicos ideales de A son A y 0.*

3. *Todo morfismo $f : A \to B$, con $B \neq 0$, es inyectivo.*

Demostración. ($1. \implies 2.$): Si I fuera un ideal de A tal que $I \neq 0$ e $I \neq A$, existiría $u \in I$ una unidad de A, que por la **Observación** 2.6, implicaría que $I = A$, contradicción. Así, los únicos ideales de A son A y 0.

($2. \implies 3.$): En efecto, sea $f : A \to B$ un morfismo, con $B \neq 0$. Luego, por 4. de los **Ejemplos** 2.8, $ker(f)$ es un ideal de A. Así, por hipótesis, $ker(f) = 0$ o $ker(f) = A$. Luego, se afirma que $ker(f) \neq A$, pues como f es morfismo y $B \neq 0$, entonces $f(1) = 1 \neq 0$, por lo que $1 \notin ker(f)$. Así, $ker(f) = 0$. Por tanto, por 1. de la **Proposición** 2.11, f es inyectiva.

($3. \implies 1.$): Primero, $A \neq 0$, pues de lo contrario $0 = 1 \in A$, entonces, para todo morfismo $f : A \to B$, con $B \neq 0$, $f(1) = 1_B$, $f(1) = 0_B$ y $0_B \neq 1_B$, f no sería función, contradicción. Ahora, demostremos que para todo $a \in A$, $a \neq 0$, existe $u \in A$ tal que $au = 1$. Supongamos lo contrario, es decir, supongamos que existe $a \in A$, $a \neq 0$, tal que para todo $u \in A$, $au \neq 1$. Así, $1 \notin (a)$, entonces (a) es un ideal propio de A y por tanto $A/(a) \neq 0$. Luego, si consideramos al morfismo natural $A \xrightarrow{\pi} A/(a)$, entonces π será inyectivo, es decir, $ker(f) = 0$. Así, por la **Proposición** 2.22, $(a) = 0$, entonces $a = 0$, contradicción. Por tanto, se cumple que para todo $a \in A$, $a \neq 0$, existe $u \in A$ tal que $au = 1$. Luego, A es un campo.

†

Proposición 2.25. *Sean A un anillo e I un ideal de A. Entonces, A/I es reducido si y solo si I es un ideal radical.*

Demostración. ($\implies$): Supongamos que A/I es reducido. En efecto, $a \in \sqrt{I}$ implica que existe $r \in \mathbb{Z}^+$ tal que $a^r \in I$, entonces $0 + I = a^r + I = (a + I)^r$. Así, por hipótesis, $a + I = 0 + I$, entonces $a \in I$. Luego, $\sqrt{I} \subseteq I$. Por tanto, $\sqrt{I} = I$.

($\impliedby$): Supongamos que $\sqrt{I} = I$. Ahora, si $a^r + I = (a + I)^r = 0 + I$ para algún $a \in A$ y algún $r \in \mathbb{Z}^+$, entonces $a^r \in I$. Así, por hipótesis, $a \in I$, entonces $a + I = 0 + I$. Luego, el único nilpotente de A/I es $0 + I$. Por tanto, A/I es reducido.

†

Teorema 2.2 (Teorema de la correspondencia). *Sean A un anillo e I un ideal de A. Consideremos al morfismo natural $A \xrightarrow{\pi} \twoheadrightarrow A/I$. Entonces, existe una biyección*

$$\begin{array}{ccc} \{J \subseteq A | J \leq A, I \subseteq J\} & \longleftrightarrow & \{\overline{J} \subseteq A/I | \overline{J} \leq A/I\} \\ J & \longmapsto & J/I := \pi[J] \\ \pi^{-1}[\overline{J}] & \longleftarrow & \overline{J}. \end{array}$$

Esta biyección preserva las inclusiones:

(i) Si $I \subseteq J_1 \subseteq J_2 \subseteq A$, entonces $J_1/I \subseteq J_2/I \subseteq A/I$.

(ii) Si $\overline{J}_1 \subseteq \overline{J}_2 \subseteq A/I$, entonces $I \subseteq \pi^{-1}[\overline{J}_1] \subseteq \pi^{-1}[\overline{J}_2] \subseteq A$.

Demostración. Primero, como π es suprayectivo, entonces, si J es un ideal de A, $\pi[J] = \{x + I \mid x \in J\} = J/I$ es un ideal de A/I, por 3. de los **Ejemplos 2.8**. Así, en particular, si J es un ideal de A que contiene a I, $\pi[J]$ es un ideal de A/I. Segundo, si $\overline{J}$ es un ideal de A/I, entonces, $\pi^{-1}[\overline{J}]$ es un ideal de A, por 2. de los **Ejemplos 2.8** e $I \subseteq \pi^{-1}[\overline{J}]$, pues si $x \in I$, $x + I = \pi(x) = 0 + I \in \overline{J}$. Ahora, veamos que las funciones $J \longmapsto \pi[J]$ y $\pi^{-1}[\overline{J}] \longleftarrow \overline{J}$ son mutuamente inversas. Primero, demostremos que si $\overline{J}$ es un ideal de A/I, entonces $\pi[\pi^{-1}[\overline{J}]] = \overline{J}$. ($\subseteq$): $y \in \pi[\pi^{-1}[\overline{J}]]$ implica que $y = \pi(x)$, para algún $x \in \pi^{-1}[\overline{J}] = \{x \in A \mid \pi(x) \in \overline{J}\}$, entonces $y \in \overline{J}$. ($\supseteq$): $y \in \overline{J} \subseteq A/I$ implica que existe $x \in A$ tal que $y = \pi(x) \in \overline{J}$, entonces $y \in \pi[\pi^{-1}[\overline{J}]] = \{\pi(x) \mid x \in \pi^{-1}[\overline{J}]\}$. Así, $\pi[\pi^{-1}[\overline{J}]] = \overline{J}$. Ahora, demostremos que si J es un ideal de A, con $I \subseteq J$, entonces $\pi^{-1}[\pi[J]] = J$. En efecto, $\pi^{-1}[\pi[J]] = \{a \in A | \ \pi(a) \in \pi[J] \ \} = \{a \in A | \ \pi(a) = \pi(a')$ para algún $a' \in J\} = \{a \in A | \ a - a' \in ker(\pi) = I$ para algún $a' \in J\} = J$, usando que $I \subseteq J$. Es claro que las dos aplicaciones preservan inclusiones.

†

2.1.1 Ideales primos e ideales máximos

En esta sección definiremos una clase importante de ideales, los ideales **máximos** y los ideales **primos**. Además, se enunciarán y demostrarán sus principales propiedades.

Definición 2.16. *Sea A un anillo.*

1. *Diremos que* $\mathfrak{p}$ *es un ideal* ***primo*** *de* A *si cumple las siguientes condiciones:*

   (i) $\mathfrak{p} \neq A$.

   (ii) Para todo $a, b \in A$ *tal que* $ab \in \mathfrak{p}$*, entonces* $a \in \mathfrak{p}$ *o* $b \in \mathfrak{p}$.

2. *Diremos que* $\mathfrak{m}$ *es un ideal* ***máximo*** *de* A *si cumple las siguientes condiciones:*

   (i) $\mathfrak{m} \neq A$.

   (ii) Para todo ideal I *de* A *tal que* $\mathfrak{m} \subseteq I \subseteq A$ *se cumple que* $\mathfrak{m} = I$ *o* $I = A$.

Veamos que existen los "entes" matemáticos antes definidos.

Proposición 2.26. *Si* A *es un anillo tal que* $1 \neq 0$*, entonces* A *tiene al menos un ideal máximo.*

Demostración. Sea $\mathcal{I} := \{I \subseteq A \mid I < A\}$. Notemos que $\mathcal{I} \neq \emptyset$, ya que $\{0\} < A$, y sabemos que $(\mathcal{I}, \subseteq)$ es un **COPO**, entonces $(\mathcal{I}, \subseteq)$ es un COPO no vacío. Ahora, sea $\mathcal{C}$ una cadena en $(\mathcal{I}, \subseteq)$. Afirmamos que $M = \bigcup \mathcal{C}$ es una cota superior de $\mathcal{C}$ en $\mathcal{I}$. Demostremos este último hecho:

- Para todo $I \in \mathcal{C}$, se tiene que $I \subseteq M$.

- M es un ideal de A.

  (i) $0 \in M$ ya que $0 \in I$, para todo ideal I de A.

  (ii) M es cerrado bajo adición, ya que si $a, b \in M$, entonces existen I_1 e $I_2 \in \mathcal{C}$ tales que $a \in I_1$ y $b \in I_2$, pero como $\mathcal{C}$ es una cadena en $(\mathcal{I}, \subseteq)$, entonces $I_1 \subseteq I_2$ o $I_2 \subseteq I_1$. Si suponemos que $I_1 \subseteq I_2$, entonces $a, b \in I_2$ y como es un ideal de A, entonces $a+b \in I_2$, y así $a + b \in M$. De igual forma obtenemos que $a + b \in M$ si suponemos que $I_2 \subseteq I_1$. Por tanto, M es cerrado bajo adición.

  (iii) M es cerrado bajo multiplicación por todos los elementos de A, ya que si $a \in A$ y $b \in M$, entonces existe $I \in \mathcal{C}$ tal que $b \in I$ y como I es un ideal de A, entonces $ab \in I$.Así $ab \in M$.

  Por tanto, de (i), (ii) y (iii) $M = \bigcup \mathcal{C}$ es un ideal de A.

- $M < A$, ya que $1 \notin M$, de lo contrario existiría $I \in \mathcal{C}$ tal que $1 \in I$, y por la **Observación 2.6**, tendríamos que $I = A$, pero $I < A$. Por tanto, $M < A$.

Así, por lo anterior, tenemos que toda cadena en $(\mathcal{I}, \subseteq)$ es acotada superiormente, entonces por el **Lema de Zorn**, $\mathcal{I}$ tiene un elemento $\subseteq$-máximo $\mathfrak{m}$.

†

Observación 2.13. *Si A es un campo, entonces $1 \neq 0$. Así, 0 es el único ideal máximo que tiene A.*

Proposición 2.27. *Sea A un anillo. Entonces, $\mathfrak{p}$ es un ideal primo de A si y solo si $A/\mathfrak{p}$ es un dominio entero.*

Demostración. ($\Longrightarrow$): Si $\mathfrak{p}$ es un ideal primo de A, se tiene que $A/\mathfrak{p} \neq 0$. Además, si $a+\mathfrak{p}, b+\mathfrak{p} \in A/\mathfrak{p}$, para algunos $a, b \in A$, son tales que $(a+\mathfrak{p})(b+\mathfrak{p}) = 0+\mathfrak{p}$, entonces $ab \in \mathfrak{p}$, lo que implica que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, es decir, $a+\mathfrak{p} = 0+\mathfrak{p}$ o $b+\mathfrak{p} = 0+\mathfrak{p}$. Así, $A/\mathfrak{p}$ no tiene divisores de cero distintos de cero. Por tanto, $A/\mathfrak{p}$ es un dominio entero.

($\Longleftarrow$): Si $A/\mathfrak{p}$ es un dominio entero, se cumple que $A/\mathfrak{p} \neq 0$ y se sigue que $\mathfrak{p} \neq A$. Ahora, si $a, b \in A$ y $ab \in \mathfrak{p}$, se tiene que $0+\mathfrak{p} = ab+\mathfrak{p} = (a+\mathfrak{p})(b+\mathfrak{p})$, por lo que $a+\mathfrak{p} = 0+\mathfrak{p}$ o $b+\mathfrak{p} = 0+\mathfrak{p}$, entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Así, $\mathfrak{p}$ es un ideal primo de A.

†

Proposición 2.28. *Sea A un anillo. Entonces, $\mathfrak{m}$ es un ideal máximo de A si y solo si $A/\mathfrak{m}$ es un campo.*

Demostración. ($\Longrightarrow$): Si $\mathfrak{m}$ es un ideal máximo, $\mathfrak{m} \neq A$, por lo que $A/\mathfrak{m} \neq 0$. Ahora, si $\overline{I}$ es un ideal de $A/\mathfrak{m}$ y si consideramos al morfismo natural $A \xrightarrow{\pi} A/\mathfrak{m}$, entonces, por el **Teorema de la correspondencia**, $\pi^{-1}[\overline{I}]$ es un ideal de A con $\mathfrak{m} \subseteq \pi^{-1}[\overline{I}] \subseteq A$, pero entonces $\mathfrak{m} = \pi^{-1}[\overline{I}]$ o $\pi^{-1}[\overline{I}] = A$. Así, de nuevo, por el **Teorema de la correspondencia**, $\overline{I} = \pi[\mathfrak{m}] = 0$ o $\overline{I} = \pi[A] = A/\mathfrak{m}$. Luego, los únicos ideales de $A/\mathfrak{m}$ son 0 y $A/\mathfrak{m}$, entonces, por la **Proposición 2.24**, $A/\mathfrak{m}$ es un campo.

($\Longleftarrow$): Si $A/\mathfrak{m}$ es un campo, se tiene que $A/\mathfrak{m} \neq 0$, entonces $\mathfrak{m} \neq A$. Ahora, por la **Proposición 2.24**, los únicos ideales de $A/\mathfrak{m}$ son el mismo y 0. Así, si I es un ideal de A tal que $\mathfrak{m} \subseteq I \subseteq A$ y si consideramos al morfismo natural $A \xrightarrow{\pi} A/\mathfrak{m}$, entonces, por el **Teorema de la correspondencia**, $\pi[I] = 0$ o $\pi[I] = A/\mathfrak{m}$. Así, $I = \mathfrak{m}$ o $I = A$. Por tanto, $\mathfrak{m}$ es un ideal máximo de A.

†

Corolario 2.4. *Si A es un anillo y $\mathfrak{m}$ es un ideal máximo de A, entonces $\mathfrak{m}$ es un ideal primo.*

Demostración. Como $\mathfrak{m}$ es un ideal máximo de A, entonces, por la **Proposición 2.28**, $A/\mathfrak{m}$ es un campo, que por el **Corolario 2.1**, $A/\mathfrak{m}$ es un dominio entero, entonces, por la **Proposición 2.27**, $\mathfrak{m}$ es un ideal primo.

†

Proposición 2.29. *Sea $f : A \longrightarrow B$ un morfismo de anillos. Se cumplen:*

1. *Si $\mathfrak{p}$ es un ideal primo de B, entonces $f^{-1}[\mathfrak{p}]$ es un ideal primo de A.*

2. *Si f es suprayectivo y $\mathfrak{m}$ es un ideal máximo de B, entonces $f^{-1}[\mathfrak{m}]$ es un ideal máximo de B.*

Demostración. Primero, sea I un ideal de B. Ahora, consideremos el morfismo

$$A \xrightarrow{f} B \xrightarrow{\pi} B/I$$

Luego, $ker(\pi \circ f) = \{a \in A \mid f(a) \in I\} = f^{-1}[I]$. Así, por el **Primer teorema de isomorfismo**, $A/f^{-1}[I] \cong (\pi \circ f)[A]$

(1.): Si $I = \mathfrak{p}$ es primo, por la **Proposición 2.27**, $B/\mathfrak{p}$ es un dominio entero, pero como $(\pi \circ f)[A] \subseteq B/\mathfrak{p}$ es un subanillo, entonces $(\pi \circ f)[A]$ es un dominio entero. Así, $A/f^{-1}[\mathfrak{p}]$ es un dominio entero, entonces, por la **Proposición 2.27**, $f^{-1}[\mathfrak{p}]$ es un ideal primo de A.

(2.): Si f es suprayectivo, entonces $(\pi \circ f)[A] = B/I$. Ahora, si $I = \mathfrak{m}$ es máximo, entonces, por la **Proposición 2.28**, $B/\mathfrak{m}$ es un campo, y por tanto $(\pi \circ f)[A]$ es un campo. Así, $A/f^{-1}[\mathfrak{m}]$ es un campo, entonces, por la **Proposición 2.28**, $f^{-1}[\mathfrak{m}]$ es un ideal máximo de A.

†

Observación 2.14. *En general, si $f : A \longrightarrow B$ es un morfismo y si $\mathfrak{m}$ es un ideal máximo de B, entonces $f^{-1}[\mathfrak{m}]$ puede no ser un ideal máximo de A. Considere, por ejemplo, el morfismo inclusión $\iota : \mathbb{Z} \longrightarrow \mathbb{Q}$, que por la **Observación 2.13**, 0 es el único ideal máximo de $\mathbb{Q}$ e $\iota^{-1}[0] = 0$ es un ideal de $\mathbb{Z}$ que no es máximo, pues $0 \subsetneq (2) \subsetneq \mathbb{Z}$.*

Proposición 2.30. *Sean A un anillo e I un ideal de A. Consideremos al morfismo natural $A \xrightarrow{\pi} A/I$. La biyección*

$$\begin{array}{ccc} \{\, J \subseteq A \mid J \leq A,\ I \subseteq J \,\} & \longleftrightarrow & \{\, \overline{J} \subseteq A/I \mid \overline{J} \leq A/I \,\} \\ J & \longmapsto & J/I := \pi[J] \\ \pi^{-1}[\overline{J}] & \longmapsfrom & \overline{J}. \end{array}$$

se restringe a las biyecciones

$$\begin{array}{ccc} \{\, \mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ es primo e } I \subseteq \mathfrak{p} \,\} & \longleftrightarrow & \{\, \overline{\mathfrak{p}} \subseteq A/I \mid \overline{\mathfrak{p}} \text{ es primo}\} \\ \{\, \mathfrak{m} \subseteq A \mid \mathfrak{m} \text{ es máximo e } I \subseteq \mathfrak{m} \,\} & \longleftrightarrow & \{\, \overline{\mathfrak{m}} \subseteq A/I \mid \overline{\mathfrak{m}} \text{ es máximo}\} \end{array}$$

Demostración. $\{\, \mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ es primo e } I \subseteq \mathfrak{p} \,\} \longleftrightarrow \{\, \overline{\mathfrak{p}} \subseteq A/I \mid \overline{\mathfrak{p}} \text{ es primo}\}$:
($\longleftarrow$): Si $\overline{\mathfrak{p}}$ es un ideal primo de A/I, entonces, por 1. de la **Proposición 2.29**, $\pi^{-1}[\overline{\mathfrak{p}}]$ es un ideal primo de A y, por el **Teorema de la correspondencia**, $I \subseteq \pi^{-1}[\overline{\mathfrak{p}}]$. ($\longrightarrow$): Sea $\mathfrak{p}$ un ideal primo de A tal que $I \subseteq \mathfrak{p}$. Así, por el **Tercer teorema de isomorfismo**, $(A/I)/(\mathfrak{p}/I) \cong A/\mathfrak{p}$, con $A/\mathfrak{p}$ un dominio entero, por la **Proposición 2.27**, entonces $(\mathfrak{p}/I)$ es un ideal primo de A/I, por la **Proposición 2.27**.

Veamos $\{\, \mathfrak{m} \subseteq A \mid \mathfrak{m} \text{ es máximo e } I \subseteq \mathfrak{m} \,\} \longleftrightarrow \{\, \overline{\mathfrak{m}} \subseteq A/I \mid \overline{\mathfrak{m}} \text{ es máximo}\}$ ($\longleftarrow$): Si $\overline{\mathfrak{m}}$ es un ideal máximo de A/I, y como π es suprayectivo, entonces, por 2. de la **Proposición 2.29**, $\pi^{-1}[\overline{\mathfrak{m}}]$ es un ideal máximo de A y, por el **Teorema de la correspondencia**, $I \subseteq \pi^{-1}[\overline{\mathfrak{m}}]$. ($\longrightarrow$): Sea $\mathfrak{m}$ un ideal máximo de A tal que $I \subseteq \mathfrak{m}$. Así, por el **Tercer teorema de isomorfismo**, $(A/I)/(\mathfrak{m}/I) \cong A/\mathfrak{m}$, con $A/\mathfrak{m}$ un campo, por la **Proposición 2.28**, entonces $(\mathfrak{m}/I)$ es un ideal máximo de A/I, por la **Proposición 2.28**.

†

Corolario 2.5. *Sean A un anillo e I un ideal propio de A. Entonces, A posee un ideal máximo $\mathfrak{m}$ tal que $I \subseteq \mathfrak{m}$.*

Demostración. En efecto, sea I un ideal de A tal que $I \neq A$. Así, $A/I \neq 0$, entonces, por la **Proposición 2.26**, A/I posee un ideal máximo $\overline{\mathfrak{m}}$, que por la **Proposición 2.30**, corresponde a un ideal máximo $\mathfrak{m}$ de A tal que $I \subseteq \mathfrak{m}$. †

Proposición 2.31. *Sea A un anillo y P un ideal primo de A. Entonces, se cumplen:*

1. *P es un ideal radical.*
2. *Si I, J son ideales de A tal que $IJ \subseteq P$, entonces $I \subseteq P$ o $J \subseteq P$.*

Demostración. 1. Demostremos que $P = \sqrt{P}$.

($\subseteq$) Por 1. de la **Proposición 2.18**, $P \subseteq \sqrt{P}$.

($\supseteq$) Sea $a \in \sqrt{P}$, entonces $a \in A$ y $a^k \in P$ para algún $k \in \mathbb{Z}^+$. Luego, si $k = 1$ o $k = 2$, entonces es claro que $a \in P$. Ahora, para $k \geq 3$ basta con tomar a $k = \text{mín}\,\{n \in \mathbb{Z}^+ \mid a^n \in P\}$; $a^k = a^{k-1}a \in P$ y $a^{k-1} \notin P$, entonces $a \in P$. Luego, $\sqrt{P} \subseteq P$.

Por tanto, P es un ideal radical.

2. Procedamos por contradicción; es decir, existen $a \in I - P$ y $b \in J - P$. Luego, $ab \in IJ - P$; pues $IJ := (\{ab \mid a \in I, b \in J\})$ y P es ideal primo, pero por hipótesis, $IJ \subseteq P$. Así, $IJ \nsubseteq P$ y $IJ \subseteq P$, contradicción. Por tanto, $I \subseteq P$ o $J \subseteq P$.

†

2.1.2 Anillo de polinomios

Sean X un conjunto y A un anillo. Si $f : X \longrightarrow A$ es una función, definimos el **soporte** de f, que denotaremos por $Sop(f)$, como:

$$Sop(f) = \{\, x \in X \mid f(x) \neq 0 \,\}.$$

Sean A un anillo, $\mathbb{N}$ el conjunto de enteros no negativos y sea $n \in \mathbb{N}$ no cero. Consideremos el conjunto:

$$A^{(\mathbb{N}^n)} := \{\, f : \mathbb{N}^n \longrightarrow A \mid f \text{ es función y } Sop(f) \text{ es un conjunto finito } \}.$$

Ahora, definamos una suma y un producto en $A^{(\mathbb{N}^n)}$ de la siguiente forma:

Suma:

$$\begin{array}{rccc} + : & A^{(\mathbb{N}^n)} \times A^{(\mathbb{N}^n)} & \longrightarrow & A^{(\mathbb{N}^n)} \\ & (f, g) & \longmapsto & f(\nu) + g(\nu) \end{array}$$

Producto:

$$\begin{array}{rccc} \cdot : & A^{(\mathbb{N}^n)} \times A^{(\mathbb{N}^n)} & \longrightarrow & A^{(\mathbb{N}^n)} \\ & (f, g) & \longmapsto & \displaystyle\sum_{\mu+\rho=\nu} f(\mu)g(\rho)\text{'} \end{array}$$

donde $\mu, \nu, \rho \in \mathbb{N}^n$ y $\mu + \rho$ se efectúa coordenada a coordenada.

De lo anterior, podemos formular la siguiente:

Proposición 2.32. $(A^{(\mathbb{N}^n)}, +, \cdot)$ *es un anillo.*

Demostración. (i) $+$ está bien definida:

Si $f, g \in A^{(\mathbb{N}^n)}$ y $\nu \in Sop(f+g)$, se tiene que $0 \neq (f+g)(\nu) = f(\nu) + g(\nu)$, por lo que $f(\nu) \neq 0$ o $g(\nu) \neq 0$, es decir, $\nu \in Sop(f)$ o $\nu \in Sop(g)$. Así, $Sop(f+g) \subseteq Sop(f) \cup Sop(g)$, pero como $Sop(f)$ y $Sop(g)$ son conjuntos finitos, por hipótesis, entonces $Sop(f) \cup Sop(g)$ es un conjunto finito, entonces $Sop(f+g)$ es un conjunto finito. Por tanto, $f + g \in A^{(\mathbb{N}^n)}$.

(ii) $+$ es asociativa:

Es claro, por 3. de los **Ejemplos** 2.1.

(iii) $+$ es conmutativa:

Es claro, por 3. de los **Ejemplos** 2.1.

(iv) Existe neutro aditivo, 0:

Sea $f_0 : \mathbb{N}^n \longrightarrow A, \nu \longmapsto 0$. Notemos que $f_0 \in A^{(\mathbb{N}^n)}$ porque $Sop(f_0) = \emptyset$. Lo demás se sigue por 3. de los **Ejemplos** 2.1.

(v) Existe inverso aditivo para cualquier $f \in A^{(\mathbb{N}^n)}$:

Sea $f \in A^{(\mathbb{N}^n)}$. Entonces, $-f : \mathbb{N}^n \longrightarrow A, \nu \longmapsto -(f(\nu))$, es elemento de $A^{(\mathbb{N}^n)}$, pues $Sop(-f) = Sop(f)$, y cumple lo demás por 3. de los **Ejemplos** 2.1.

(vi) $\cdot$ está bien definido:

$f, g \in A^{(\mathbb{N}^n)}$ y $\nu \in Sop(f \cdot g)$, se cumple que $0 \neq (f \cdot g)(\nu) = \sum_{\mu+\rho=\nu} f(\mu)g(\rho)$, entonces existen $\mu_0, \rho_0 \in \mathbb{N}^n$ tales que $\mu_0 + \rho_0 = \nu$ y $f(\mu_0)g(\rho_0) \neq 0$, por lo que $\mu_0 \in Sop(f)$ y $\rho_0 \in Sop(g)$. Luego, como $Sop(f)$ y $Sop(g)$ son conjuntos finitos, también es finito el conjunto de productos $f(\mu)g(\rho)$ que sean distintos de cero, entonces $Sop(f \cdot g)$ es un conjunto finito. Por tanto, $f \cdot g \in A^{(\mathbb{N}^n)}$.

(vii) $\cdot$ es asociativo:

Sean $f, g, h \in A^{(\mathbb{N}^n)}$ y $\nu \in \mathbb{N}^n$. Entonces:

$$((fg)h)(\nu) = \sum_{\mu+\rho=\nu} (fg)(\mu)h(\rho) = \sum_{\mu+\rho=\nu} \Big(\sum_{\sigma+\tau=\mu} f(\sigma)g(\tau) \Big) h(\rho) = \sum_{\sigma+\tau+\rho=\nu} (f(\sigma)g(\tau))h(\rho).$$

Por otra parte, si calculamos $(f(gh))(\nu)$ obtendremos

$$(f(gh))(\nu) = \sum_{\sigma+\tau+\rho=\nu} f(\sigma)(g(\tau)h(\rho)).$$

Así, $((fg)h)(\nu) = (f(gh))(\nu)$, por la asociatividad de A. Por tanto, $(fg)h = f(gh)$.

(viii) $\cdot$ es conmutativo:

Sean $f, g \in A^{(\mathbb{N}^n)}$ y $\nu \in \mathbb{N}^n$. Entonces:

$$(fg)(\nu) = \sum_{\mu+\rho=\nu} f(\mu)g(\rho) = \sum_{\rho+\mu=\nu} g(\rho)f(\mu) = (gf)(\nu).$$

Así, $fg = gf$.

(ix) Existe neutro multiplicativo, 1:

Sea $f_1 : \mathbb{N}^n \longrightarrow A, \nu \longmapsto \begin{cases} 1 \quad si \quad \nu = (0, \ldots, 0) =: \bar{0} \\ \\ 0 \quad si \qquad\quad \nu \neq \bar{0} \end{cases}$

Así, $f_1 \in A^{(\mathbb{N}^n)}$. Ahora, si $g \in A^{(\mathbb{N}^n)}$ y $\nu \in \mathbb{N}^n$, entonces

$$(gf_1)(\nu) = \sum_{\mu+\rho=\nu} g(\mu)f_1(\rho) = g(\nu)f_1(\bar{0}) = g(\nu).$$

Luego, $gf_1 = g$.

(x) $\cdot$ se distribuye sobre $+$:

Sean $f, g, h \in A^{(\mathbb{N}^n)}$ y $\nu \in \mathbb{N}^n$. Entonces:

$$(f(g+h))(\nu) = \sum_{\mu+\rho=\nu} f(\mu)(g+h)(\rho) = \sum_{\mu+\rho=\nu} f(\mu)(g(\rho)+h(\rho)) =$$
$$\sum_{\mu+\rho=\nu} f(\mu)g(\rho) + f(\mu)h(\rho) = \sum_{\mu+\rho=\nu} f(\mu)g(\rho) + \sum_{\mu+\rho=\nu} f(\mu)h(\rho) = (fg)(\nu) + (fh)(\nu).$$

Así, $f(g+h) = fg + fh$.

Por tanto, $(A^{(\mathbb{N}^n)}, +, \cdot)$ es un anillo.

†

Observación 2.15. *Sea A un anillo. Para cada $a \in A$, sea $f_a : \mathbb{N}^n \longrightarrow A$, $\nu \longmapsto \begin{cases} a & si \quad \nu = \bar{0} \\ 0 & si \quad \nu \neq \bar{0} \end{cases}$.*

Entonces, para cada $a \in A$, $f_a \in A^{(\mathbb{N}^n)}$

Proposición 2.33. *Sea A un anillo. Entonces, $\iota : A \longrightarrow A^{(\mathbb{N}^n)}$, $a \longmapsto f_a$, es un morfismo inyectivo.*

Demostración. Sean $a, b \in A$. Primero, $\iota(a+b) = f_{a+b}$ y $\iota(a) + \iota(b) = f_a + f_b$, entonces si $\nu \in \mathbb{N}^n$, tenemos que $f_{a+b}(\nu) = a + b$ y $(f_a + f_b)(\nu) = f_a(\nu) + f_b(\nu) = a + b$ si $\nu = \bar{0}$ y $f_{a+b}(\nu) = 0$ y $(f_a + f_b)(\nu) = f_a(\nu) + f_b(\nu) = 0$ si $\nu \neq \bar{0}$, entonces, se concluye que $\iota(a+b) = \iota(a) + \iota(b)$. Ahora, $\iota(ab) = f_{ab}$ y $\iota(a)\iota(b) = f_a f_b$, por lo que si $\nu \in \mathbb{N}^n$, se tiene que $f_{ab}(\nu) = ab$ y $(f_a f_b)(\nu) = \sum_{\mu+\rho=\nu} f_a(\mu) f_b(\rho) = ab$ si $\nu = \bar{0}$ y $f_{ab}(\nu) = 0$ y $(f_a f_b)(\nu) = \sum_{\mu+\rho=\nu} f_a(\mu) f_b(\rho) = 0$ si $\nu \neq \bar{0}$, entonces, se tiene que $\iota(ab) = \iota(a)\iota(b)$. Por último, $\iota(1) = f_1$, que como se vio en la demostración de la proposición anterior, $f_1 = 1_{A^{(\mathbb{N}^n)}}$. Así, ι es un morfismo. Por último, sean $a, b \in A$ tales que $\iota(a) = \iota(b)$, entonces $f_a(\nu) = f_b(\nu)$ para todo $\nu \in \mathbb{N}^n$, particular, cuando $\nu = \bar{0}$, $a = f_a(\nu) = f_b(\nu) = b$, por lo que ι es inyectivo. Por tanto, $\iota : A \longrightarrow A^{(\mathbb{N}^n)}$, $a \longmapsto f_a$, es un morfismo inyectivo.

†

Observación 2.16. *Por la proposición anterior, $\iota|^{\iota[A]} : A \longrightarrow \iota[A]$ es un isomorfismo. Así, identificaremos a A como un subanillo de $A^{(\mathbb{N}^n)}$ y al morfismo ι, lo denotaremos por $A \hookrightarrow A^{(\mathbb{N}^n)}$.*

Ahora, introducimos una notación más conveniente para tratar a los elementos del anillo $A^{(\mathbb{N}^n)}$.

Sea $n \in \mathbb{N}$ no cero. Para cada $i = 1, \ldots, n$, sea $e_i := (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{N}^n$, es decir, e_i denota la n-tupla la cual tiene 1 en la i-ésima coordenada y 0 en las demás. Luego, si $k \in \mathbb{N}$, definimos $ke_i := (0, \ldots, 0, k, 0, \ldots, 0)$. Así, cada multiíndice $\nu \in \mathbb{N}^n$ se expresa de forma única como $\nu := (\nu_1, \ldots, \nu_n) = \nu_1 e_1 + \cdots + \nu_n e_n$.

Sean A un anillo y $n \in \mathbb{N}$ no cero. Para cada $1 \leq i \leq n$, sea $x_i : \mathbb{N}^n \longrightarrow A$ tal que $\nu \longmapsto \begin{cases} 1 & si \quad \nu = e_i \\ 0 & si \quad \nu \neq e_i \end{cases}$. Así, para cada $1 \leq i \leq n$, $x_i \in A^{(\mathbb{N}^n)}$. Ahora, dados $1 \leq i \leq n$ y $k \in \mathbb{N}$, de la

definición del producto en $A^{(\mathbb{N}^n)}$, tenemos que $x_i^k : \mathbb{N}^n \longrightarrow A$, $\nu \longmapsto \begin{cases} 1 & si \quad \nu = ke_i \\ \\ 0 & si \quad \nu \neq ke_i \end{cases}$.

Ahora, dado un multiíndice $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$, definimos $x^\nu := x_1^{\nu_1} \cdots x_n^{\nu_n}$, que cumple $x^\nu(\nu) := x_1^{\nu_1} \cdots x_n^{\nu_n}(\nu)$

$= 1$ y $x^\nu(\mu) = 0$ para todo $\mu \in \mathbb{N}^n$ tal que $\mu \neq \nu$. Así, si $f \in A^{(\mathbb{N}^n)}$ y si denotamos $a_\nu := f(\nu)$ para cada $\nu \in Sop(f) = \{ \nu \in \mathbb{N}^n \,|f(\nu) \neq 0 \}$, entonces

$$f = \sum_{\nu \in Sop(f)} a_\nu x^\nu$$

Notación 2.8. *Sean A un anillo y $n \in \mathbb{N}$ no cero. Entonces, denotaremos al anillo*

$$A^{(\mathbb{N}^n)} = \{ f : \mathbb{N}^n \longrightarrow A \mid f \text{ es función y } Sop(f) \text{ es un conjunto finito } \}$$

como

$$A[x_1, \ldots, x_n] = \left\{ \sum_\nu a_\nu x^\nu \mid \text{son sumas finitas y } a_\nu \in A \right\}$$

o como

$$A[x_1, \ldots, x_n] = \left\{ \sum_{\nu_1, \ldots, \nu_n \in \mathbb{N}} a_{\nu_1, \ldots, \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n} \mid \text{son sumas finitas y } a_{\nu_1, \ldots, \nu_n} \in A \right\}.$$

Definición 2.17. *Sean A un anillo y $n \in \mathbb{N}$ no cero. Entonces, al anillo $A[x_1, \ldots, x_n]$ le llamaremos* ***anillo de polinomios en n variables****.*

Observación 2.17. *Sean A un anillo y $n \in \mathbb{N}$ no cero. Consideremos al anillo de polinomios en n variables $A[x_1, \ldots, x_n]$. Entonces,*

1. *A los $x_i \in A[x_1, \ldots, x_n]$ para $i = 1, \ldots, n$ les llamaremos* ***variables o indeterminadas****.*
2. *Si $f \in A[x_1, \ldots, x_n]$ es tal que $f = \sum_{\nu_1, \ldots, \nu_n \in \mathbb{N}} a_{\nu_1, \ldots, \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n}$, entonces los $a_{\nu_1, \ldots, \nu_n}$ son los* ***coeficientes*** *de f.*
3. *Si $f = \sum_\nu a_\nu x^\nu$, $g = \sum_\nu b_\nu x^\nu \in A[x_1, \ldots, x_n]$, entonces $f = g$ si y solo si $a_\nu = b_\nu$ para todo ν.*

4. *Un polinomio del tipo ax^ν para cierto $\nu \in \mathbb{N}^n$ recibe el nombre de* ***monomio****. Este monomio se dice* ***nulo*** *si $a = 0$. Así, todo polinomio no nulo se escribe de modo único como suma de una cantidad finita de monomios no nulos.*

5. *Si $ax_1^{\nu_1} \cdots x_n^{\nu_n}$ es un monomio no nulo, entonces el* ***grado*** *del monomio será la suma $\nu_1 + \cdots + \nu_n$. Así, si $f \in A[x_1, \ldots, x_n]$ es un polinomio no nulo, entonces el grado de f, que denotaremos por ∂f, será el mayor de los grados de sus monomios. Si todos los monomios de f tienen el mismo grado, diremos que f es homogéneo. Un polinomio f se puede expresar de forma única como $f = f_0 + f_1 + \cdots + f_m$, donde cada f_i es cero o es homogéneo de grado i, y $f_m \neq 0$.*

Proposición 2.34. *Si A es un dominio entero, entonces el anillo de polinomios $A[x_1, \ldots, x_n]$ es un dominio entero.*

Demostración. Suponga que $f, g \in A[x_1, \ldots, x_n]$ son polinomios no nulos de grado p y q, respectivamente. Ahora, escribimos $f = f_0 + f_1 + \cdots + f_p$, con $f_p \neq 0$, y $g = g_0 + g_1 + \cdots + g_q$, con $g_q \neq 0$. Notemos que los f_i y g_j son cero u homogéneos de grado i y j, respectivamente. Luego, $fg = \sum_{k=0}^{p+q} h_k$, donde $h_k = \sum_{i+j=k} f_i g_j$. Ahora, como h_k es cero u homogéneo de grado k, entonces habremos probado la proposición si probamos que $h_{p+q} = f_p g_q \neq 0$. Para este propósito ordenaremos los monomios de algún grado r lexicográficamente, es decir, $x_1^{\mu_1} \cdots x_n^{\mu_n} < x_1^{\nu_1} \cdots x_n^{\nu_n}$ si $\mu_s < \nu_s$, donde s es el menor entero, $1 \leq s \leq n$, tal que $\mu_s \neq \nu_s$. Ahora, con respecto a este orden, y para $r = p$, sea $ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ el primero de los monomios que aparecen en f_p, $a \neq 0$. Similarmente, sea $bx_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ el primero de los monomios que aparecen en g_q, $b \neq 0$. Luego, entonces $abx_1^{\alpha_1+\beta_1} x_2^{\alpha_2+\beta_2} \cdots x_n^{\alpha_n+\beta_n}$ es el primer monomio que aparece en el producto $f_p g_q$, y como $ab \neq 0$, se sigue que $f_p g_q \neq 0$. Por tanto, $A[x_1, \ldots, x_n]$ es un dominio entero.

†

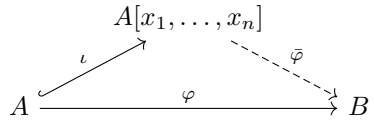
Corolario 2.6. *Si k es un campo, entonces el anillo de polinomios $k[x_1, \ldots, x_n]$ es un dominio entero.*

Demostración. Como k es un campo, entonces, por el **Corolario 2.1**, k es un dominio entero. Así, por la proposición anterior, $k[x_1, \ldots, x_n]$ es un dominio entero.

†

Proposición 2.35 (Propiedad universal del anillo de polinomios). *Sea A un anillo. Consideremos al anillo de polinomios en n variables $A[x_1, \ldots, x_n]$ y al morfismo inclusión $A \xhookrightarrow{\iota} A[x_1, \ldots, x_n]$. Ahora,*

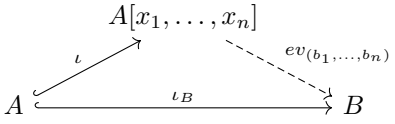
dado otro anillo B, un morfismo $\varphi : A \longrightarrow B$ y elementos $b_1, \ldots, b_n \in B$, existe un único morfismo $\bar{\varphi} : A[x_1, \ldots, x_n] \longrightarrow B$ tal que $\bar{\varphi} \circ \iota = \varphi$ y $\bar{\varphi}(x_i) = b_i$ para todo $i = 1, \ldots, n$.



Observación 2.18. *Sean B un anillo y A un subanillo de B. Consideremos al anillo $A[x_1, \ldots, x_n]$ y al morfismo inclusión $A \xhookrightarrow{\iota} A[x_1, \ldots, x_n]$. Ahora, consideremos al morfismo inclusión $A \xhookrightarrow{\iota_B} B$ y sean $b_1, \ldots, b_n \in B$, entonces, por la propiedad universal del anillo de polinomios, existe un único morfismo*

$$ev_{(b_1,\ldots,b_n)} : A[x_1, \ldots, x_n] \longrightarrow B$$

tal que $ev_{(b_1,\ldots,b_n)} \circ \iota = \iota_B$ y $ev_{(b_1,\ldots,b_n)}(x_i) = b_i$ para todo $i = 1, \ldots, n$.



*Al anterior morfismo lo llamaremos **morfismo de evaluación** en el punto $(b_1, \ldots, b_n)$. En lo sucesivo, si $f \in A[x_1, \ldots, x_n]$, entonces denotaremos por $f(b_1, \ldots, b_n)$ a $ev_{(b_1,\ldots,b_n)}(f)$.*

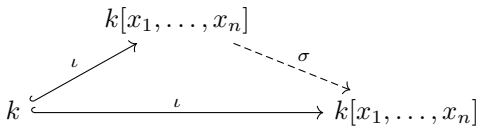
Veamos tres ejemplos los cuales engloban la propiedad universal del anillo de polinomios.

Ejemplos 2.10. *Sean k un campo, $n \in \mathbb{N}$ no cero y $a_1, \ldots, a_n \in k$.*

1. *Tenemos que $x_i - a_i \in k[x_1, \ldots, x_n]$. Ahora, por la propiedad universal del anillo de polinomios, existe un único morfismo*

   $$\sigma : k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n]$$

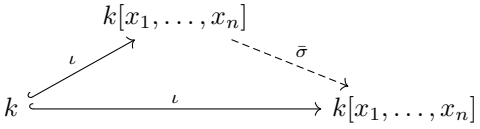
   tal que $\sigma \circ \iota = \iota$ y $\sigma(x_i) = x_i - a_i$.

   Ahora, $x_i + a_i \in k[x_1, \ldots, x_n]$. Así, por la propiedad universal del anillo de polinomios, existe un único morfismo

$$\bar{\sigma} : k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n]$$

tal que $\bar{\sigma} \circ \iota = \iota$ *y* $\bar{\sigma}(x_i) = x_i + a_i$.



Luego, $\iota = \sigma \circ \iota = \sigma \circ (\bar{\sigma} \circ \iota) = (\sigma \circ \bar{\sigma}) \circ \iota$*, entonces, por la unicidad del morfismo* $Id_{k[x_1,\ldots,x_n]}$, $\sigma \circ \bar{\sigma} = Id_{k[x_1,\ldots,x_n]}$. *Además,* $\iota = \bar{\sigma} \circ \iota = \bar{\sigma} \circ (\sigma \circ \iota) = (\bar{\sigma} \circ \sigma) \circ \iota$*, entonces, por la unicidad del morfismo* $Id_{k[x_1,\ldots,x_n]}$, $\bar{\sigma} \circ \sigma = Id_{k[x_1,\ldots,x_n]}$. *Por tanto,* σ *es un automorfismo con inversa* $\bar{\sigma}$.

2. *Consideremos el morfismo* $ev_{(0,\ldots,0)} : k[x_1, \ldots, x_n] \longrightarrow k$ *. Ahora, calculemos* $ker(ev_{(0,\ldots,0)})$. *En efecto,*

   $ker(ev_{(0,\ldots,0)}) = \{\ f \in k[x_1, \ldots, x_n] \mid f(0, \ldots, 0) = 0\ \} = \{\ f_1x_1 + \cdots + f_nx_n \mid f_i \in k[x_1, \ldots, x_n]\ \} = (x_1, \ldots, x_n)$.

3. *Consideremos el morfismo* $ev_{(a_1,\ldots,a_n)} : k[x_1, \ldots, x_n] \longrightarrow k$ *. Ahora, por 1. y 2., es fácil calcular* $ker(ev_{(a_1,\ldots,a_n)})$, *pues* $ev_{(a_1,\ldots,a_n)} = ev_{(0,\ldots,0)} \circ \bar{\sigma}$. *Así,* $ker(ev_{(a_1,\ldots,a_n)}) = \{f \in k[x_1, \ldots, x_n] | ev_{(a_1,\ldots,a_n)}(f) = 0\ \} = \{\ f \in k[x_1, \ldots, x_n] \mid ev_{(0,\ldots,0)}(\bar{\sigma}(f)) = 0\ \} = \{f \in k[x_1, \ldots, x_n] \mid \bar{\sigma}(f) \in ker(ev_{(0,\ldots,0)})\} = \{\ f \in k[x_1, \ldots, x_n] \mid f \in \sigma[ker(ev_{(0,\ldots,0)})]\ \} = \sigma[ker(ev_{(0,\ldots,0)})]$. *Luego, sabemos, por 2., que* $ker(ev_{(0,\ldots,0)}) = (x_1, \ldots, x_n)$, *entonces* $ker(ev_{(a_1,\ldots,a_n)}) = \sigma[ker(ev_{(0,\ldots,0)})] = \sigma[(x_1, \ldots, x_n)] = \{\sigma(f) | f \in (x_1, \ldots, x_n)\} = \{\sigma(f_1x_1 + \cdots + f_nx_n) | f_i \in k[x_1, \ldots, x_n]\} = \{\sigma(f_1)\sigma(x_1) + \cdots + \sigma(f_n)\sigma(x_n) | f_i \in k[x_1, \ldots, x_n]\} = \{g_1(x_1 - a_1) + \cdots + g_n(x_n - a_n) | g_i \in k[x_1, \ldots, x_n]\} = (x_1 - a_1, \ldots, x_n - a_n)$.

Proposición 2.36. *Sean* k *un campo y* $a_1, \ldots, a_n \in k$, *para algún* $n \in \mathbb{Z}^+$. *Entonces, el ideal* $(x_1 - a_1, \ldots, x_n - a_n)$ *es un ideal máximo de* $k[x_1, \ldots, x_n]$.

Demostración. Consideremos el morfismo $ev_{(a_1,\ldots,a_n)} : k[x_1, \ldots, x_n] \longrightarrow k$.
Luego, por 3. de los ejemplos anteriores, $ker(ev_{(a_1,\ldots,a_n)}) = (x_1 - a_1, \ldots, x_n - a_n)$, entonces, por el primer teorema de isomorfismo,

$$k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong ev_{(a_1,\ldots,a_n)}[k[x_1, \ldots, x_n]],$$

pero como $ev_{(a_1,\ldots,a_n)}$ es suprayectivo, entonces

$$k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong k,$$

lo cual implica que $(x_1 - a_1, \ldots, x_n - a_n)$ es un ideal máximo de $k[x_1, \ldots, x_n]$, por la **Proposición 2.28**

†

Definición 2.18. *1. Sean A un anillo, $a \in A$ y $f \in A[x]$. Diremos que a es una **raíz** (o un **cero**) de f si*

$$ev_a(f) := f(a) = 0.$$

*2. Sean k un campo y $f \in k[x]$ un polinomio. Un elemento $a \in k$ se llama un **cero de multiplicidad** $m \geq 1$ de f si $(x-a)^m | f$ pero $(x-a)^{m+1} \nmid f$.*

Ahora, ya definido el anillo de polinomios, es momento de continuar con nuestra exposición sobre extensiones de campos.

Teorema 2.3. *Sean k un campo y $f \in k[x]$ un polinomio de grado $n \geq 1$. Entonces, el número de raíces de f, contadas con su multiplicidad, en cualquier extensión L de k, es menor o igual que n.*

Demostración. Ver [Zal96, Teorema 2.10].

†

Definición 2.19. *Sea K/k una extensión. Un elemento $a \in K$ se llama **algebraico sobre** k, si existe un polinomio $p \in k[x]$ no cero, tal que $p(a) = 0$. En caso contrario, diremos que a es **trascendente sobre** k.*

Ejemplos 2.11. *1. Si K/k es cualquier extensión, entonces todo elemento $a \in k$ es algebraico sobre k, pues si $f := x - a \in k[x]$, entonces $f(a) = 0$.*

2. En la extensión $\mathbb{R}/\mathbb{Q}$ el elemento $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$ es algebraico sobre $\mathbb{Q}$, pues $g := x^2 - 2 \in \mathbb{Q}[x]$ y $g(\sqrt{2}) = 0$.

3. $\pi \in \mathbb{R}$ es trascendente sobre $\mathbb{Q}$.

4. $e \in \mathbb{R}$ es trascendente sobre $\mathbb{Q}$.

Observación 2.19. *Sean K/k una extensión y $a \in K$ algebraico sobre k. Entonces, existe un polinomio $p \in k[x]$ tal que $p(a) = 0$. Luego, si a_n es el coeficiente principal de p, entonces al multiplicar p por a_n^{-1} obtenemos un polinomio mónico, es decir, un polinomio p' con coeficiente principal igual a 1. Ahora, notemos*

que $p'(a) = 0$, pues $p' = a_n^{-1}p$. Así, si $a \in K$ es algebraico sobre k, entonces, por el principio del buen orden, existe un polinomio mónico en $k[x]$ de menor grado del cual a es raíz.

Lema 2.1. *Sean K/k una extensión y $a \in K$ algebraico sobre k. Entonces, el polinomio mónico de menor grado $m \in k[x]$ del cual $a \in K$ es raíz, es único. Más aún, m es irreducible, es decir, m no es una unidad y si $m = fg$, entonces f ó g es una unidad de $k[x]$, y m divide a cualquier otro polinomio $p \in k[x]$ del cual a es raíz.*

Demostración. Ver [Zal96, Lema 2.18].

†

Notación 2.9. *Sean K/k una extensión y $a \in K$ algebraico sobre k. Denotaremos al polinomio mónico irreducible de menor grado del cual a es raíz por $Irr(a, k) \in k[x]$.*

Proposición 2.37. *Sean K/k una extensión y $a \in K$ algebraico sobre k. Entonces,*

$$k(a) = \{p(a) |\ p \in k[x] \text{ y } \partial(p) < \partial(Irr(a, k))\ \}.$$

Demostración. Ver [Zal96, Lema 2.19].

†

Teorema 2.4. *Sean K/k una extensión y $a \in K$. Entonces, a es algebraico sobre k si y solo si la extensión $k(\alpha)/k$ es finita.*

Demostración. Ver [Zal96, Lema 2.20].

†

Corolario 2.7. *Sean K/k una extensión y $a \in K$. Si a es algebraico sobre k, entonces*

$$[k(a) : k] = \partial(Irr(a, k)).$$

Corolario 2.8. *Sean K/k una extensión y $a \in K$. Si a es algebraico sobre k, entonces todos los elementos de $k(a)$ son algebraicos.*

Demostración. En efecto, sea $m := Irr(a, k) \in k[x]$ con $n = \partial m$. Ahora, si $b \in K(a)$, entonces los $n + 1$ elementos $1, b, \ldots, b^n$ forman un conjunto linealmente dependiente, por lo que existen

$a_0, a_1, \ldots, a_n \in k$ no todos nulos tales que $a_0 1 + a_1 b + \cdots + a_n b^n = 0$. Luego, si $f := a_0 + a_1 x + \cdots + a_n x^n \in k[x]$, entonces $f(b) = 0$. Así, $b \in k(a)$ es algebraico sobre k.

†

Definición 2.20. *Una extensión K/k se llama **algebraica** si todos los elementos de K son algebraicos sobre k.*

Corolario 2.9. *Toda extensión finita K/k es algebraica.*

Proposición 2.38. *Sea K/k una extensión. Entonces, K/k es finita si y solo si es algebraica y existe un número finito de elementos $a_1, \ldots, a_m \in K$ tales que $K = k(a_1, \ldots, a_m)$.*

Definición 2.21. *Sea k un campo. Diremos que k es **algebraicamente cerrado** si todo polinomio de $k[x]$ tiene todas sus raíces en k.*

Observación 2.20. *El teorema fundamental del álgebra nos indica que $\mathbb{C}$ es un campo algebraicamente cerrado.*

Proposición 2.39. *Sea k un campo. Las siguientes afirmaciones son equivalentes:*

1. *k es algebraicamente cerrado.*
2. *Si L/k es una extensión algebraica, entonces $L = k$.*
3. *Si L/k es una extensión finita, entonces $L = k$.*

Demostración. Ver [Zal96, Proposición 2.39].

†

Proposición 2.40. *Todo campo algebraicamente cerrado es infinito.*

Demostración. Sea K un campo algebraicamente cerrado. Ahora, si $K = \{a_1, \ldots, a_n\}$ fuera finito, entonces el polinomio $f = (x - a_1) \cdots (x - a_n) + 1 \in K[x]$ no tendría raíces en K, contradicción. Por tanto, K es infinito.

†

Definición 2.22. *Sean K/k una extensión y $a_1, \ldots, a_n \in K$ trascendentes sobre k. Diremos que $a_1, \ldots, a_n$ son **algebraicamente independientes sobre** k si no existe un polinomio no cero $p \in k[x_1, \ldots, x_n]$ tal que $p(a_1, \ldots, a_n) = 0$. En caso contrario, diremos que son **algebraicamente dependientes**.*

Observación 2.21. *La definición anterior es equivalente a que el morfismo*

$$k[x_1, \ldots, x_n] \longrightarrow k[a_1, \ldots, a_n]$$

$$x_i \longmapsto a_i$$

$$A \ni a \longmapsto a$$

es un isomorfismo.

2.1.3 Anillos noetherianos

En esta sección definimos una clase particular de anillos, los anillos noetherianos. El nombre de estos anillos es en honor a Emmy Noether; ella fue quien introdujo en 1921 el concepto de condiciones de cadena.

Definición 2.23. *Un anillo A es **noetheriano** si todo ideal de A es finitamente generado.*

Lo que sigue es demostrar un par de equivalencias de los anillos noetherianos, pero para esto, necesitamos hacer la siguiente:

Definición 2.24. *Sea A un anillo.*

1. *Decimos que A satisface la **condición de la cadena ascendente**, si toda cadena ascendente de ideales en A se estaciona; es decir, si $\{I_j\}_{j\in\mathbb{Z}^+}$ es una cadena ascendente en A, entonces existe $N \in \mathbb{Z}^+$ tal que para toda $n > N$, $I_N = I_n$.*
2. *Decimos que A satisface la **condición máxima** si toda familia no vacía de ideales de A tiene elemento máximo; esto es, en toda $\mathcal{F}$, familia no vacía de ideales de A, existe $I_0 \in \mathcal{F}$ para el cual no existe $I \in \mathcal{F}$ tal que $I_0 \subsetneq I$.*

Observación 2.22. *Si A es un anillo que satisface la condición de la cadena ascendente, entonces con **CCA** abreviamos este último hecho.*

Ahora si, enunciemos y demostremos lo antes mencionado.

Proposición 2.41. *Sea A un anillo. Las siguientes condiciones son equivalentes:*

1. *A es noetheriano.*

2. *A satisface la CCA.*

3. *A satisface la condición máxima.*

Demostración. (1. $\implies$ 2.) Si $\{I_j\}_{j\in\mathbb{Z}^+}$ es una cadena ascendente de ideales de A, por la **Proposición 2.17**, $J := \bigcup_{n\geq 1} I_n \leq A$. Así, por hipótesis, existen $a_1, a_2, \ldots, a_l \in A$, para algún $l \in \mathbb{Z}^+$, tal que $(a_1, a_2, \ldots, a_l) = \bigcup_{n\geq 1} I_n$. Notemos que $a_i \in J$, para todo $i \in \{1, \ldots, l\}$. Por tanto, para cada $i \in \{1, \ldots, l\}$, existe I_{n_i} ideal en la cadena tal que $a_i \in I_{n_i}$. Por último, si N es el elemento más grande de $\{n_i \mid i \in \{1, \ldots, l\}\}$, entonces la cadena se estaciona en N. En efecto, sea $M > N$ entero. Luego, $I_N \subseteq I_M$; la cadena es ascendente. Ahora, si $x \in I_M \subseteq J$, entonces $x = r_1a_1 + \cdots + r_la_l$, para algunos $r_1, \ldots, r_l \in A$, y por la definición de N, $a_1, \ldots, a_l \in I_N$, entonces por el **Corolario 2.12**, $x = r_1a_1 + \cdots + r_la_l \in I_N$. Por tanto, A satisface la CCA.

(2. $\implies$ 3.) Supongamos lo contrario; es decir, supongamos que existe $\mathcal{F}'$, familia no vacía de ideales de A, tal que no tiene elemento máximo. Luego, sea $I_1 \in \mathcal{F}'$, entonces existe $I_2 \in \mathcal{F}'$ tal que $I_1 \subsetneq I_2$. Ahora, supongamos que $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n$, para algún $n \geq 2$ entero, entonces existe $I_{n+1} \in \mathcal{F}'$ tal que $I_n \subsetneq I_{n+1}$. Así queda determinada, por inducción, una cadena ascendente de ideales de A tal que nunca se estaciona, contradicción. Por tanto, A satisface la condición máxima.

(3. $\implies$ 1.) Sea $I \leq A$ y $\mathcal{F} := \{J \leq A \mid J \text{ es finitamente generado y } J \subseteq I\}$. Luego, $\mathcal{F} \neq \emptyset$ pues $0 \in \mathcal{F}$ y por tanto, existe $M \in \mathcal{F}$ elemento máximo. Afirmamos que $M = I$. Si pasara que $M \neq I$, existiría $a \in I$ tal que $a \notin M$ e implicaría que $\{ra + m \mid r \in A \text{ y } m \in M\} = (a, 1) \in \mathcal{F}$; $(a, 1) \leq A$, $(a, 1)$ es finitamente generado y $(a, 1) \subseteq I$, y $M \subsetneq (a, 1)$; es decir, M no sería elemento máximo de $\mathcal{F}$, contradicción. Así, I es finitamente generado. Por tanto, A es noetheriano.

†

Teorema 2.5 (Teorema de la base de Hilbert). *Si A es un anillo noetheriano, entonces $A[t]$ es noetheriano.*

Demostración. Procedamos por contradicción; es decir, supongamos que existe I ideal de $A[t]$ tal que no es finitamente generado. Luego, $I \neq 0$, entonces sea $f_1 \in I$ de grado mínimo y definamos, inductivamente, $f_{n+1} \in I \setminus (f_1, \ldots, f_n)$ de grado mínimo. Ahora, notemos que $gr(f_1) \leq gr(f_2) \leq \cdots \leq gr(f_n) \leq \cdots$. Luego, denotemos con a_n el coeficiente principal de f_n, para todo $n \in \mathbb{Z}^+$. Además, $(a_1) \subseteq (a_1, a_2) \subseteq \cdots \subseteq (a_1, a_2, \ldots, a_n) \subseteq \cdots$ es una cadena ascendente de ideales

en A, entonces existe $N \in \mathbb{Z}^+$ tal que $(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_N)$ para todo $n > N$, en particular, $(a_1, a_2, \ldots, a_{N+1}) = (a_1, a_2, \ldots, a_N)$ y por tanto, $a_{N+1} = b_1a_1 + b_2a_2 + \cdots + b_Na_N$ para algunos $b_i \in A$ con $i \in \{1, 2, \ldots, N\}$. Ahora, sea $g := f_{N+1} - (\sum_{i=1}^{N} b_i t^{d_{N+1}-d_i} f_i)$, donde $d_i := gr(f_i)$ para todo $i \in \{1, 2, \ldots, N\}$. Notemos que $g \in I \setminus (f_1, f_2, \ldots, f_N)$; de lo contrario $f_{N+1} \in (f_1, f_2, \ldots, f_N)$, lo cual contradice nuestra elección de f_{N+1}. Por tanto, $gr(g) \geq gr(f_{N+1})$.

Ahora, desarrollemos un poco g. Para esto, notemos que $f_{N+1} = a_{N+1}t^{d_{N+1}} +$ **(términos de grado menor)** y $f_i = a_it^{d_i} +$ **(términos de grado menor)**, para todo $i \in \{1, 2, \ldots, N\}$. Así,

$$g = a_{N+1}t^{d_{N+1}} + \textbf{(términos de grado menor)} - \sum_{i=1}^{N} b_i t^{d_{N+1}-d_i}(a_it^{d_i} + \textbf{(términos de grado menor)}),$$

donde $\sum_{i=1}^{N} b_i t^{d_{N+1}-d_i}(a_it^{d_i} +$ **(términos de grado menor)** es un polinomio con coeficiente principal a_{N+1}. Por tanto, al realizar la resta, obtenemos que g es un polinomio con $gr(g) < N + 1$, contradicción; $f_{N+1} \in I \setminus (f_1, f_2, \ldots, f_N)$ es de grado mínimo. Luego, todo ideal de $A[t]$ es finitamente generado.

Por tanto, $A[t]$ es noetheriano.

†

Corolario 2.10. *1. Si A es un anillo noetheriano, entonces $A[t_1, t_2, \ldots, t_n]$ es noetheriano, para todo $n \in \mathbb{Z}^+$.*

2. Si k es un campo, entonces $k[t_1, t_2, \ldots, t_n]$ es noetheriano, para todo $n \in \mathbb{Z}^+$.

Demostración. 1. Procedamos por inducción matemática sobre n. En efecto, para el caso cuando $n = 1$ es cierto; es el **teorema de la base de Hilbert**. Ahora, supongamos que la proposición es verdadera para todo $k \in \{1, \ldots, n-1\}$, para algún $n \in \mathbb{Z}^+$. Demostremos que es cierta para $k = n$. En efecto, como $A[t_1, \ldots, t_{n-1}][t_n] \cong A[t_1, t_2, \ldots, t_n]$, entonces hacemos $A' = A[t_1, \ldots, t_{n-1}]$ que por hipótesis inductiva es noetheriano y aplicando el **teorema de la base de Hilbert**, tenemos que $A'[t_n] = A[t_1, \ldots, t_{n-1}][t_n]$ es noetheriano. Por tanto, $A[t_1, t_2, \ldots, t_n]$ es noetheriano. Luego, por el principio de inducción matemática, la proposición es verdadera para todo $n \in \mathbb{Z}^+$.

2. En este caso notemos que como k es un campo, entonces por 2. de la **Proposición 2.24**, 0 y k son sus únicos ideales; los cuales son finitamente generados por 0 y 1, respectivamente. Luego, k es noetheriano. Así, por 1. $k[t_1, t_2, \ldots, t_n]$ es noetheriano, para todo $n \in \mathbb{Z}^+$.

†

2.2 Módulos, submódulos y morfismos

Definición 2.25. *Sea A un anillo. Diremos que M es un A-**módulo** si:*

1. *M es un grupo abeliano.*
2. *Existe una operación*

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & am \end{array}$$

*llamada **multiplicación escalar**, tal que satisface:*

   (i) Asociatividad: $a_1(a_2m) = (a_1a_2)m$, para cualesquiera $a_1, a_2 \in A$ y cualquier $m \in M$.

   (ii) Distributividad: $a(m_1+m_2) = am_1+am_2$ y $(a_1+a_2)m = a_1m+a_2m$, para cualesquiera $a, a_1, a_2 \in A$ y cualesquiera $m, m_1, m_2 \in M$.

   (iii) Elemento unitario: $1m = m$, para cualquier $m \in M$.

Ejemplos 2.12. *Sea A un anillo.*

1. *A es un A-módulo.*
2. *Si I es un ideal de A, entonces I es un A-módulo.*
3. *El anillo cociente A/I es un A-módulo con la operación escalar:*

$$\cdot : A \times A/I \longrightarrow A/I, (a, a' + I) \longmapsto aa' + I.$$

Proposición 2.42. *Sea A un anillo. Entonces, en cualquier A-módulo M, se cumplen:*

1. *$0_Am = 0_M$ y $a0_M = 0_M$, para todo $a \in A$ y todo $m \in M$.*
2. *$-(am) = a(-m) = (-a)m$, para todo $a \in A$ y todo $m \in M$.*

Definición 2.26. *Sean A un anillo y M un A-módulo. Diremos que un subconjunto N de M es un* ***submódulo*** *de M si:*

1. $0 \in N$.
2. *Si* $n_1, n_2 \in N$, *entonces* $n_1 + n_2 \in N$.
3. *Si* $a \in A$ *y* $n \in N$, *entonces* $an \in N$.

Ejemplos 2.13. *Sean A un anillo y M un A-módulo.*

1. *M posee los submódulos triviales 0 y M.*
2. *Sea* $m_0 \in M$. *Entonces,* $Am_0 := \{am_0 \mid a \in A\}$ *es un submódulo de M, llamado submódulo* ***cíclico generado*** *por* m_0.

Demostración. 2. En efecto, sea ${}_AM$ y $m_0 \in M$. Luego, por 1. de la **Proposición 2.42** $0 = 0m_0 \in Am_0$. Ahora, sean $am_0, a'm_0 \in Am_0$, entonces $am_0 + a'm_0 = (a + a')m_0 \in Am_0$. Por último, si $a \in A$ y $a'm_0 \in Am_0$, entonces $a(a'm_0) = (aa')m_0 \in Am_0$. Por tanto, Am_0 es un submódulo de M.

†

Proposición 2.43. *Sean A un anillo y M un A-módulo. Si Γ es una familia no vacía de submódulos de M, entonces $\bigcap \Gamma$ es un submódulo de M.*

Convención 2.3. *Sean A un anillo y M un A-módulo. Si Γ es la familia vacía de submódulos de M, entonces $\bigcap \Gamma = M$.*

Corolario 2.11. *Sean A un anillo y M un A-módulo. Si Γ es una familia de submódulos de M, entonces $\bigcap \Gamma$ es un submódulo de M.*

Definición 2.27. *Sean A un anillo, M un A-módulo y X un subconjunto de M. Definimos el submódulo* ***generado*** *por X, denotado por $\langle X \rangle$, como*

$$\langle X \rangle = \begin{cases} \left\{ \sum_{finita} a_j x_j | a_j \in A, x_j \in X \right\} & si \quad X \neq \emptyset \\ 0 & si \quad X = \emptyset \end{cases}$$

Proposición 2.44. *Sean A un anillo, M un A-módulo y X un subconjunto de M. Se cumplen:*

1. $\langle X \rangle$ *es un submódulo de* M.
2. *Si* $X = \{x_1, \ldots, x_t\}$ *es finito,* $\langle X \rangle = \left\{ \sum_{j=1}^{t} a_j x_j \mid a_1, \ldots, a_t \in A \right\}$.
3. $\langle X \rangle = \bigcap \Gamma$, *donde* $\Gamma := \{N \subseteq M \mid N$ *es submódulo de* M *y* $X \subseteq N\}$.

Notación 2.10. *Sean A un anillo, M un A-módulo y $X = \{x_1, \ldots, x_n\}$ un subconjunto finito de M. Denotaremos al submódulo de M generado por X como $\langle x_1, \ldots, x_n \rangle$, en vez de $\langle X \rangle = \langle \{x_1, \ldots, x_n\} \rangle$.*

Definición 2.28. *Sean A un anillo y M un A-módulo.*

1. *Diremos que X, un subconjunto de M, es un* ***conjunto generador*** *de M si $\langle X \rangle = M$.*
2. *Diremos que M es* ***finitamente generado*** *si existe un conjunto generador finito.*

Definición 2.29. *Sean A un anillo y M, N A-módulos. Una función $f : M \longrightarrow N$ es un morfismo de A-módulos o simplemente un A-morfismo si cumple:*

(i) $f(m + m') = f(m) + f(m')$ *para todo* $m, m' \in M$.

(ii) $f(am) = af(m)$ *para todo* $a \in A$ *y todo* $m \in M$.

2.2.1 Álgebras

Sean $f : A \longrightarrow B$ un morfismo de anillos y M un B-módulo. Definimos la siguiente acción:

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & f(a)m \end{array}$$

Proposición 2.45. *Sean $f : A \longrightarrow B$ y M un B-módulo. Entonces, con la acción anterior, M es un A-módulo.*

Demostración. M es un grupo abeliano porque M es B-módulo. Así, solo resta probar que la acción antes definida cumple con los axiomas de la **Definición 2.25**. En efecto, sean $a, a' \in A$ y $x, y \in M$. Luego, tenemos:

(i) Asociatividad: $(aa')x = f(aa')x = (f(a)f(a'))x = f(a)(f(a')x) = f(a)(a'x) = a(a'x)$.

(ii) Distributividad: $a(x+y) = f(a)(x+y) = f(a)x + f(a)y = ax + ay$ y $(a+a')x = f(a+a')x = (f(a)+f(a'))x = f(a)x + f(a')x = ax + a'x$.

(iii) Elemento unitario: $1_A x = f(1_A)x = 1_B x = x$.

Por tanto, M es un A-módulo. Más aún, diremos que el B-módulo M se vuelve un A-módulo por **cambio de anillos** o **restricción de escalares**.

†

Corolario 2.12. *Si $f : A \longrightarrow B$ es un morfismo de anillos, entonces el B-módulo B se vuelve un A-módulo, por restricción de escalares.*

Observación 2.23. *Si $f : A \longrightarrow B$ es un morfismo de anillos, por el corolario anterior, B tiene dos estructuras algebraicas, es un anillo y un A-módulo. Así, ambas estructuras son compatibles.*

Demostración. La conclusión se refiere al producto porque el grupo aditivo es el mismo. En efecto, si $b \in f[A]$, $b = f(a)$ para algún $a \in A$, entonces para todo $x \in B$, $ax = f(a)x = bx$, donde ax es el producto como A-módulo y bx es el producto como anillo.

†

Definición 2.30. *Sea A un anillo. Una A-álgebra es un anillo B junto con un morfismo de anillos $f : A \longrightarrow B$.*

Ejemplos 2.14.

Observación 2.24. *Sean B un anillo y A un subanillo de B. Notemos que B es una A-álgebra, vía el morfismo inclusión, $\iota : A \longrightarrow B$, definido por $\iota(a) = a$.*

Convención 2.4. *Sean B un anillo y A un subanillo de B. En lo sucesivo, por la observación anterior, si mencionamos que B es una A-álgebra, se estará considerando el morfismo inclusión, $\iota : A \longrightarrow B$.*

Definición 2.31. *Sean B un anillo y A un subanillo de B.*

1. *Diremos que B es una A-álgebra **finita** si B es finitamente generado como A-módulo.*
2. *Diremos que B es una A-álgebra de **tipo finito sobre** A si existen $n \in \mathbb{Z}^+$ y $\alpha_1, \ldots, \alpha_n \in B$ tal que $B = A[\alpha_1, \ldots, \alpha_n]$.*

Ejemplos 2.15.

Definición 2.32. *Sean $f : A \longrightarrow B$ y $g : A \longrightarrow C$ morfismos de anillos. Diremos que $h : B \longrightarrow C$ es un **morfismo de A-álgebras** si h es un morfismo de anillos y un A-morfismo.*

Proposición 2.46. *Sean $f : A \longrightarrow B$, $g : A \longrightarrow C$ y $h : B \longrightarrow C$ morfismos de anillos. Entonces, $h : B \longrightarrow C$ es un morfismo de A-álgebras si y solo si $h \circ f = g$.*

Demostración. ($\Longrightarrow$) Si $a \in A$, $(h \circ f)(a) = h(f(a)) = h(f(a)1_B) = h(a1_B) = ah(1_B) = a1_C = g(a)1_C = g(a)$. Así, $h \circ f = g$.

($\Longleftarrow$) Si $a \in A$ y $x \in B$, $h(ax) = h(f(a)x) = h(f(a))h(x) = g(a)h(x) = ah(x)$. Así, h es un A-morfismo.
Por tanto, $h : B \longrightarrow C$ es un morfismo de A-álgebras si y solo si $h \circ f = g$.

†

2.3 Integridad

Definición 2.33. *Sean B un anillo y A un subanillo de B.*

1. *Diremos que $b \in B$ es **entero sobre** A si existe un polinomio mónico*

$$f = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in A[x]$$

   tal que $0 = ev_b(f) = b^m + a_{m-1}b^{m-1} + \cdots + a_1b + a_0$.

2. *Diremos que B es **entero sobre** A si todo elemento de B es entero sobre A.*

Lema 2.2. *Sean B un anillo, A un subanillo de B y $\alpha \in B$. Son equivalentes:*

1. *α es entero sobre A.*

2. *El subanillo $A[\alpha] \subseteq B$ es finitamente generado como A-módulo.*

3. *Existe un subanillo C, con $A \subseteq C \subseteq B$, tal que $\alpha \in C$ y C es finitamente generado como A-módulo.*

Demostración. (1. $\Longrightarrow$ 2.) En efecto, $A[\alpha]$ es un subanillo de B que contiene a A y α, por 2. de la **Observación 2.2**. Así, A es un subanillo de $A[\alpha]$. Luego, $A[\alpha]$ es un A-módulo. Ahora, $A[\alpha] = \left\{ \sum_{j=0}^{n} a_j \alpha^j \mid n \in \mathbb{Z}^+ \cup \{0\}, a_j \in A \right\}$, por la **Proposición 2.8**. Así, $A[\alpha] = \langle \{\alpha^i \mid i \in \mathbb{Z}^+ \cup \{0\}\}\rangle$, por la **Proposición ??**. Ahora, por hipótesis, existe $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$ tal que $ev_\alpha(f) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Luego, $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 1)$. Ahora, sabemos que, $1, \alpha, \ldots, \alpha^{n-1} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$. Luego, afirmamos que $\alpha^{n+s} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$, para todo $s \in \mathbb{Z}^+$. En efecto, para $s = 1$, tenemos: $\alpha^{n+1} = \alpha^n\alpha = -(a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0 1)\alpha = -(a_{n-1}\alpha^n+\cdots+a_1\alpha^2+a_0\alpha) = (-a_{n-1})(-(a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0 1)) + (-a_{n-2})\alpha^{n-1} + \cdots + (-a_1)\alpha^2 + (-a_0)\alpha) = (a_{n-1}^2 - a_{n-2})\alpha^{n-1} + (a_{n-1}a_{n-2} - a_{n-3})\alpha^{n-2} + \cdots + (a_{n-1}a_1 - a_0)\alpha + (a_{n-1}a_0)1$. Así, $\alpha^{n+1} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$. Ahora, supongamos que para $s \in \mathbb{Z}^+$, $s \geq 2$, se cumple que $\alpha^{n+s} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$. Demostremos que $\alpha^{n+s+1} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$. En efecto, como $\alpha^{n+s} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$, entonces $\alpha^{n+s} = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 1$, para algunos $b_{n-1}, \ldots, b_1, b_0 \in A$. Así, $\alpha^{n+s+1} = \alpha^{n+s}\alpha = (b_{n-1}\alpha^{n-1}+\cdots+b_1\alpha+b_0 1)\alpha$, que sabiendo que $\alpha^n = -(a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0 1)$ y procediendo de forma análoga al caso $s = 1$, se concluye que $\alpha^{n+s+1} = (b_{n-1}(-a_{n-1}) + b_{n-2})\alpha^{n-1} + \cdots + (b_{n-1}(-a_1) + b_0)\alpha + (b_{n-1}(-a_0))1$. Luego, $\alpha^{n+s+1} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$. Así, por el principio de inducción matemática, $\alpha^{n+s} \in \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$, para todo $s \in \mathbb{Z}^+$. Así, $\{\alpha^i \mid i \in \mathbb{Z}^+\cup\{0\}\} \subseteq \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$, entonces $\langle\{\alpha^i \mid i \in \mathbb{Z}^+\cup\{0\}\}\rangle \subseteq \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$. Además, es claro que, $\{1, \alpha, \ldots, \alpha^{n-1}\} \subseteq \langle\{\alpha^i \mid i \in \mathbb{Z}^+ \cup \{0\}\}\rangle$, entonces $\langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle \subseteq \langle\{\alpha^i \mid i \in \mathbb{Z}^+ \cup \{0\}\}\rangle$. Así, $\langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle = \langle\{\alpha^i \mid i \in \mathbb{Z}^+ \cup \{0\}\}\rangle$. Por tanto, $A[\alpha] = \langle\{1, \alpha, \ldots, \alpha^{n-1}\}\rangle$.

(2. $\Longrightarrow$ 3.) Sabemos que $A \subseteq A[\alpha] \subseteq B$ y $\alpha \in A[\alpha]$, por 2. de la **Observación 2.2** y por la **Definición 2.4**. Además, por hipótesis, $A[\alpha]$ es un A-módulo finitamente generado. Así, si $C := A[\alpha]$, se obtiene lo deseado.

(3. $\Longrightarrow$ 1.) Supongamos que $C = Ay_1 + \cdots + Ay_n$. Si $\alpha \in C$, entonces $\alpha y_j \in C$ para todo $1 \leq j \leq n$. Así,

$$\alpha y_i = a_{i1}y_1 + \cdots + a_{in}y_n, \text{ con } a_{ij} \in A \text{ y } 1 \leq i \leq n$$

y la igualdad anterior se puede escribir como

$$\sum_{j=1}^{n} (\delta_{ij}\alpha - a_{ij})y_j = 0 \text{ con } 1 \leq i \leq n \text{ y } \delta_{ij} \text{ una delta de Kronecker}$$

que es un sistema de n ecuaciones lineales homogéneas en $y_1, \ldots, y_n$. Por la regla de Cramer se tiene que $det(\delta_{ij}\alpha - a_{ij}) \cdot y_j)$ para todo j, y como C está generado por los y_j se sigue que $det(\delta_{ij}\alpha - a_{ij}) \cdot C = 0$ y así para $1 \in C$ se tiene que $det(\delta_{ij}\alpha - a_{ij}) \cdot 1 = 0$, es decir, $det(\delta_{ij}\alpha - a_{ij}) = 0$. Finalmente, desarrolando $det(\delta_{ij}\alpha - a_{ij})$, poniendo la indeterminada x en lugar de α, se obtiene un polinomio con coeficientes en A que se anula en α y este polinomio es mónico porque el término de grado x^n proviene del producto de los elementos de la diagonal principal $(x - a_{11}) \cdots (x - a_{nn})$. Por tanto, α es entero sobre A.

†

Proposición 2.47. *Sean C un anillo y A, B subanillos de C tales que $A \subseteq B \subseteq C$. Entonces, si C es un B-módulo finitamente generado y B es un A-módulo finitamente generado, se cumple que C es un A-módulo finitamente generado.*

Corolario 2.13. *Sean B un anillo, A un subanillo de B y $\alpha_1, \ldots, \alpha_n \in B$ enteros sobre A. Entonces, $A[\alpha_1, \ldots, \alpha_n]$ es un A-módulo finitamente generado.*

Demostración. Procedamos por inducción matemática sobre n. En efecto, para $n = 1$, $A[\alpha_1]$ es un A-módulo finitamente generado, por la equivalencia $1. \Leftrightarrow 2.$ del **Lema 2.2**. Ahora, supongamos que para $n \in \mathbb{Z}^+$, $n \geq 2$, se cumple que $A[\alpha_1, \ldots, \alpha_n]$ es un A-módulo finitamente generado, donde $\alpha_1, \ldots, \alpha_n \in B$ son enteros sobre A. Demostremos que $A[\alpha_1, \ldots, \alpha_n, \alpha_{n+1}]$ es un A-módulo finitamente generado, donde $\alpha_1, \ldots, \alpha_n, \alpha_{n+1} \in B$ son enteros sobre A. En efecto, como $\alpha_{n+1} \in B$ es entero sobre A, existe $f \in A[x]$ tal que $ev_{\alpha_{n+1}}(f) = 0$. Luego, como $A \subseteq A[\alpha_1, \ldots, \alpha_n]$, entonces $f \in A[\alpha_1, \ldots, \alpha_n][x]$ y $ev_{\alpha_{n+1}}(f) = 0$, por lo que, $\alpha_{n+1} \in B$ es entero sobre $A[\alpha_1, \ldots, \alpha_n]$, entonces, por la equivalencia $1. \Leftrightarrow 2.$ del **Lema 2.2**, $A[\alpha_1, \ldots, \alpha_n][\alpha_{n+1}] = A[\alpha_1, \ldots, \alpha_n, \alpha_{n+1}]$ es un $A[\alpha_1, \ldots, \alpha_n]$-módulo finitamente generado. Ahora, como $A[\alpha_1, \ldots, \alpha_n]$ es un A-módulo finitamente generado, por hipótesis inductiva, se tiene que $A[\alpha_1, \ldots, \alpha_n, \alpha_{n+1}]$ es un A-módulo finitamente generado, por la **Proposición 2.47**. Por tanto, por el principio de inducción matemática, se cumple que, para todo $n \in \mathbb{Z}^+$, $A[\alpha_1, \ldots, \alpha_n]$ es un A-módulo finitamente generado si $\alpha_1, \ldots, \alpha_n \in B$ son enteros sobre A.

†

Corolario 2.14. *Sean B un anillo, A un subanillo de B. Si $\alpha, \beta \in B$ son enteros sobre A, entonces $\alpha + \beta$, $\alpha - \beta$ y $\alpha\beta$ son enteros sobre A.*

Demostración. En efecto, como $\alpha, \beta \in B$ son enteros sobre A, tenemos que $A[\alpha, \beta]$ es un A-módulo finitamente generado, por el **Corolario 2.13**. Así, se tiene que $A \subseteq A[\alpha, \beta] \subseteq B$, inclusión de subanillos, $\alpha + \beta, \alpha - \beta, \alpha\beta \in A[\alpha, \beta]$ y $A[\alpha, \beta]$ es un A-módulo finitamente generado, entonces, por la equivalencia 3. $\Leftrightarrow$ 1. del **Lema 2.2**, aplicada tres veces, tenemos que $\alpha + \beta, \alpha - \beta, \alpha\beta \in B$ son enteros sobre A.

†

Definición 2.34. *Sean B un anillo y A un subanillo de B. Definimos la **cerradura entera** de A en B, denotada como $\bar{A}$, como*

$$\bar{A} = \{\alpha \in B \mid \alpha \text{ es entero sobre } A\}.$$

Corolario 2.15. *Sean B un anillo y A un subanillo de B. Entonces, $\bar{A}$ es un anillo y $A \subseteq \bar{A} \subseteq B$.*

Demostración. En efecto, por definición de $\bar{A}$, $\bar{A} \subseteq B$. Ahora, como $A \subseteq B$ y todo elemento de A es entero sobre A, pues si $a \in A$, entonces $x - a \in A[x]$ y $ev_a(x - a) = a - a = 0$, se tiene que $A \subseteq \bar{A}$. Luego, como A es un subanillo de B, $1 \in A$, entonces $1 \in \bar{A}$. Por último, si $\alpha, \beta \in \bar{A}$, entonces, por el **Corolario 2.14**, $\alpha - \beta, \alpha\beta \in \bar{A}$. Por tanto, por la **Definición 2.3**, $\bar{A}$ es un (sub)anillo.

†

Definición 2.35. *Sean B un anillo y A un subanillo de B.*

1. *Si $\bar{A} = A$, diremos que A es **integralmente cerrado** en B.*
2. *Si A es un dominio entero y $\bar{A} = A$ en su campo de fracciones k, diremos que A es **normal**.*

Corolario 2.16. *Sean B un anillo y A un subanillo de B. Son equivalentes:*

1. *B es una A-álgebra finita.*
2. *B es una A-álgebra de tipo finito y entera sobre A.*

Demostración. (1.$\Longrightarrow$2.) Toda A-álgebra finita es de tipo finito. Más aún, como B es finitamente generado como A-módulo , por 3. del **Lema 2.2**, B es entera sobre A.

(2.$\Longrightarrow$1.) Por hipótesis existen $\alpha_1, \ldots, \alpha_n \in B$ tales que $B = A[\alpha_1, \ldots, \alpha_n]$, y como los α_i son enteros sobre A, entonces, por el **Corolario 2.13**, $B = A[\alpha_1, \ldots, \alpha_n]$ es un A-módulo finitamente generado.

†

Corolario 2.17. *Sean C un anillo y A, B subanillos de C tales que $A \subseteq B \subseteq C$. Ahora, si C es entero sobre B y B es entero sobre A, entonces C es entero sobre A.*

Capítulo 3

Nullstellensatz

Álgebra lineal, una parte, se ocupa de encontrar la solución a un sistema de ecuaciones lineales dado; la teoría desarrolla una descripción completa del conjunto de soluciones de dicho sistema. **Geometría algebraica**, desde un punto de vista clásico, se ocupa de estudiar el conjunto de soluciones de un sistema de ecuaciones polinomiales en varias variables dado, llamado **conjunto algebraico**.

Mencionado lo anterior, para garantizar que estos espacios algebraicos sean no vacíos, hacemos la siguiente:

Convención 3.1. *En lo sucesivo, la palabra* ***campo*** *significará* ***campo algebraicamente cerrado****.*

Definición 3.1. *Sea k un campo y $n \in \mathbb{Z}^+$.*

1. *Definimos el* ***espacio afín de dimensión*** n ***sobre*** k*, denotado por $\mathbb{A}_k^n$, como*

$$\mathbb{A}_k^n = \{(a_1, ..., a_n) \mid a_i \in k\}.$$

2. *Sea $f \in k[x_1, \ldots, x_n]$. Definimos el conjunto cero de f, denotado por $\mathcal{V}(f)$, como*

$$\mathcal{V}(f) = \{P \in \mathbb{A}_k^n \mid f(P) = 0\}.$$

3. *Más generalmente, si $T \subseteq k[x_1, \ldots, x_n]$, definimos el conjunto* ***cero*** *de T, denotado por $\mathcal{V}(T)$, como*

$$\mathcal{V}(T) = \{P \in \mathbb{A}_k^n \mid f(P) = 0 \text{ para toda } f \in T\}.$$

4. *Sea $Y \subseteq \mathbb{A}_k^n$. Decimos que Y es un conjunto* ***algebraico afín*** *en $\mathbb{A}_k^n$ si existe $T \subseteq k[x_1, \ldots, x_n]$ tal que $\mathcal{V}(T) = Y$.*

Por 3. de la definición anterior, podemos afirmar que basta con considerar el ideal generado por T, (T). Formalmente, tenemos la siguiente:

Proposición 3.1. *Sea k un campo y $T \subseteq k[x_1, \ldots, x_n]$. Si $I := (T)$, entonces $\mathcal{V}(T) = \mathcal{V}(I)$. Más aún, existen $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, para algún $r \in \mathbb{Z}^+$, tal que $\mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_r) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$.*

Demostración. Primero, demostremos que $\mathcal{V}(T) = \mathcal{V}(I)$. ($\subseteq$): Si $P \in \mathcal{V}(T)$ y $f \in I$, entonces $g(P) = 0$ para todo $g \in T$ y $f = h_1 g_1 + \cdots + h_n g_n$, con $h_i \in k[x_1, \ldots, x_n]$, $g_i \in T$ y $n \in \mathbb{Z}^+$. Así, $f(P) = h_1 g_1(P) + \cdots + h_n g_n(P) = h_1(P) g_1(P) + \cdots + h_n(P) g_n(P) = h_1(P)0 + \cdots + h_n(P)0 = 0$. Luego, $P \in \mathcal{V}(I)$. Por tanto, $\mathcal{V}(T) \subseteq \mathcal{V}(I)$. ($\supseteq$): Si $P \in \mathcal{V}(I)$ y $f \in T$, se tiene que $g(P) = 0$ para todo $g \in I$ y $f \in I$, porque $T \subseteq (T) = I$, entonces $f(P) = 0$. Así, $P \in \mathcal{V}(T)$. Por tanto, $\mathcal{V}(I) \subseteq \mathcal{V}(T)$. Luego, se cumple que $\mathcal{V}(T) = \mathcal{V}(I)$.
Segundo, demostremos que existen $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, para algún $r \in \mathbb{Z}^+$, tal que $\mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_m)$. Para la existencia, por 2. del **Corolario 2.10**, A es noetheriano; es decir, todo ideal de $k[x_1, \ldots, x_n]$ es finitamente generado. Así, existen $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, para algún $r \in \mathbb{Z}^+$, tal que $I = (f_1, \ldots, f_r)$. Por tanto, $\mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_m)$.
Por último, demostremos que $\mathcal{V}(f_1, \ldots, f_r) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$. ($\subseteq$): Si $P \in \mathcal{V}(f_1, \ldots, f_r)$, se cumple que $f(P) = 0$ para todo $f \in (f_1, \ldots, f_r)$. Luego, en particular, $f_i \in (f_1, \ldots, f_r)$, para todo $i \in \{1, \ldots, r\}$, entonces $f_i(P) = 0$, para todo $i \in \{1, \ldots, r\}$. Así, $P \in \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$. Por tanto, $\mathcal{V}(f_1, \ldots, f_r) \subseteq \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$. ($\supseteq$): Si $P \in \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$ y $f \in (f_1, \ldots, f_r)$, se cumple que $f_i(P) = 0$, para todo $i \in \{1, \ldots, r\}$, y $f = g_1 f_1 + \cdots + g_r f_r$, para algunos $g_i \in k[x_1, \ldots, x_n]$, con $i \in \{1, \ldots, r\}$. Luego, $f(P) = g_1 f_1(P) + \cdots + g_r f_r(P) = g_1(P) f_1(P) + \cdots + g_r(P) f_r(P) = g_1(P)0 + \cdots + g_r(P)0 = 0$. Así, $P \in \mathcal{V}(f_1, \ldots, f_r)$. Por tanto, $\mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r) \subseteq \mathcal{V}(f_1, \ldots, f_r)$. Luego, $\mathcal{V}(f_1, \ldots, f_r) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$.

†

De la proposición anterior, concluimos que, los conjuntos algebraicos afines son conjuntos de ceros comunes de un conjunto finito de polinomios.

Proposición 3.2. *Sea k un campo. Si $f \in k[x_1, \ldots, x_n]$, con $f \neq 0$, entonces $\mathcal{V}(f) \neq \mathbb{A}_k^n$.*

Demostración. Procedamos por inducción matemática sobre n. Para el caso $n = 1$ es porque si $f \in k[x]$, con $f \neq 0$, entonces el número de raíces de f, en k, es menor o igual que su grado, por el **Teorema 2.3**, pero como k es algebraicamente cerrado, entonces k es infinito, entonces $\mathcal{V}(f) \neq \mathbb{A}^1_k$. Supongamos ahora que el lema es válido para menor o igual $n-1$ variables, con $n \geq 2$; es decir, se cumple que si $f \in k[x_1, \ldots, x_{n-1}]$, con $f \neq 0$, entonces $\mathcal{V}(f) \neq \mathbb{A}^{n-1}_k$. Demostremos que si $f \in k[x_1, \ldots, x_n]$, con $f \neq 0$, entonces $\mathcal{V}(f) \neq \mathbb{A}^n_k$. En efecto, sea $f \in k[x_1, \ldots, x_n]$, con $f \neq 0$. Primero, notemos que si $L : \mathbb{A}^{n-1}_k \longrightarrow \mathbb{A}^n_k$, $(\alpha_1, \ldots, \alpha_{n-1}) \longmapsto (\alpha_1, \ldots, \alpha_{n-1}, 0)$, entonces L es inyectiva, y por tanto, $\mathbb{A}^{n-1}_k \cong L(\mathbb{A}^{n-1}_k) \subseteq \mathbb{A}^n_k$, es decir, podemos pensar que $\mathbb{A}^{n-1}_k \subseteq \mathbb{A}^n_k$. Ahora, factorizando las potencias x_n^i en los monomios de f, escribimos

$$(*) \qquad f = a_k(x_1, \ldots, x_{n-1})x_n^k + \cdots$$

Notemos que si no aparece la variable x_n en f, entonces $f \in k[x_1, \ldots, x_{n-1}]$, y por hipótesis de inducción, existe un punto $(\alpha_1, \ldots, \alpha_{n-1}, 0) \in \mathbb{A}^{n-1}_k \subseteq \mathbb{A}^n_k$ tal que $f(\alpha_1, \ldots, \alpha_{n-1}, 0) \neq 0$, entonces $\mathcal{V}(f) \neq \mathbb{A}^n_k$. Podemos entonces suponer que x_n aparece en f, entonces $a_k(x_1, \ldots, x_{n-1}) \neq 0$ (no es el polinomio cero). Así, por hipótesis de inducción, existe un punto $(\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{A}^{n-1}_k$ tal que $a_k(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Luego, sustituyendo el punto $(\alpha_1, \ldots, \alpha_{n-1})$ en todos los coeficientes a_i de $(*)$, se obtiene el polinomio en una variable

$$\tilde{f} = a_k(\alpha_1, \ldots, \alpha_{n-1})x_n^k + \cdots \in k[x_n],$$

donde el coeficiente $a_k(\alpha_1, \ldots, \alpha_{n-1})x_n^k \neq 0$ y por lo tanto el número de raíces de $\tilde{f}$ es menor o igual que su grado, entonces $\tilde{f}$ no se puede anular en todo k, lo que implica que existe $\alpha_n \in k$ tal que $0 \neq \tilde{f}(\alpha_n) = f(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$, es decir, f no se anula en todo $\mathbb{A}^n_k$. Por tanto, $\mathcal{V}(f) \neq \mathbb{A}^n_k$.

†

Observación 3.1. *Sea k un campo y $n \in \mathbb{Z}^+$. Entonces,*

$$\begin{array}{rccc} \mathcal{V}: & \{J \leq k[x_1, \ldots, x_n]\} & \longrightarrow & \{Y \subseteq \mathbb{A}^n_k | \, Y \ \textit{es un conjunto algebraico en} \ \mathbb{A}^n_k\} \\ & J & \longmapsto & \mathcal{V}(J) \end{array}$$

es una función sobreyectiva, pero no inyectiva.

Ahora, tenemos la construcción recíproca:

Definición 3.2. *Sea k un campo, $n \in \mathbb{Z}^+$ y $X \subseteq \mathbb{A}_k^n$. Definimos el conjunto $\mathcal{I}(X)$ como*

$$\mathcal{I}(X) = \{f \in k[x_1, \ldots, x_n] \mid f(P) = 0 \text{ para todo } P \in X\}.$$

Proposición 3.3. *Sea k un campo, $n \in \mathbb{Z}^+$ y $X \subseteq \mathbb{A}_k^n$. Entonces, $\mathcal{I}(X) \leq k[x_1, \ldots, x_n]$.*

Demostración. Primero, por definición, $\mathcal{I}(X) \subseteq k[x_1, \ldots, x_n]$. Luego, $0 \in \mathcal{I}(X)$, pues $0(P) = 0$, para todo $P \in X$. Ahora, si $f, g \in \mathcal{I}(X)$, se tiene que $f(P) = 0$ para todo $P \in X$ y $g(P) = 0$ para todo $P \in X$, entonces, si $P \in X$, $(f + g)(P) = f(P) + g(P) = 0 + 0 = 0$. Así, $f + g \in \mathcal{I}(X)$. Por último, si $h \in k[x_1, \ldots, x_n]$ y $f \in \mathcal{I}(X)$, entonces $h \in k[x_1, \ldots, x_n]$ y $f(P) = 0$ para todo $P \in X$, por lo que si $P \in X$, $hf(P) = h(P)f(P) = h(P)0 = 0$. Luego, $hf \in \mathcal{I}(X)$. Por tanto, $\mathcal{I}(X) \leq k[x_1, \ldots, x_n]$.

†

Observación 3.2. *Sea k un campo y $n \in \mathbb{Z}^+$. Entonces,*

$$\begin{array}{rccc} \mathcal{I}: & \{X \subseteq \mathbb{A}_k^n\} & \longrightarrow & \{J \leq k[x_1, \ldots, x_n]\} \\ & X & \longmapsto & \mathcal{I}(X) \end{array}$$

es una función.

Demostremos algunas propiedades básicas que cumplen las funciones $\mathcal{V}$ e $\mathcal{I}$.

Lema 3.1. *Las funciones $\mathcal{V}$ e $\mathcal{I}$ cumplen:*

1. *Si $E \subseteq E' \subseteq k[x_1, \ldots, x_n]$, entonces $\mathcal{V}(E') \subseteq \mathcal{V}(E)$.*
2. *$\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$, para todo $I \leq k[x_1, \ldots, x_n]$.*
3. *$\mathcal{V}(k[x_1, \ldots, x_n]) = \emptyset$.*
4. *$\mathcal{V}(0) = \mathbb{A}_k^n$.*
5. *$\mathcal{V}(J_1) \cup \mathcal{V}(J_2) = \mathcal{V}(J_1 \cap J_2)$, para cualesquiera $J_1, J_2 \leq k[x_1, \ldots, x_n]$.*
6. *$\bigcap_{j \in \Lambda} \mathcal{V}(J_j) = \mathcal{V}(\sum_{j \in \Lambda} J_j)$, para toda $\{J_j\}_{j \in \Lambda}$ familia de ideales de $k[x_1, \ldots, x_n]$.*
7. *Si $X \subseteq Y \subseteq \mathbb{A}_k^n$, entonces $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$.*

8. $\mathcal{I}(\emptyset) = k[x_1, \ldots, x_n]$.

9. $\mathcal{I}(\mathbb{A}_k^n) = 0$.

10. *Si* $X \subseteq \mathbb{A}_k^n$*, entonces* $\sqrt{\mathcal{I}(X)} = \mathcal{I}(X)$*, es decir,* $\mathcal{I}(X)$ *es un ideal radical.*

11. $J \subseteq \mathcal{I}(\mathcal{V}(J))$*, para todo* $J \leq k[x_1, \ldots, x_n]$.

12. $X \subseteq \mathcal{V}(\mathcal{I}(X))$*, para todo* $X \subseteq \mathbb{A}_k^n$*. Más aún,* $X = \mathcal{V}(\mathcal{I}(X))$ *si y solo si* X *es un conjunto algebraico afín.*

Demostración. 1. Si $P \in \mathcal{V}(E')$, se cumple que $f(P) = 0$ para todo $f \in E'$. Luego, como $E \subseteq E'$, se tiene que $f(P) = 0$ para todo $f \in E$, entonces $P \in \mathcal{V}(E)$. Por tanto, $\mathcal{V}(E') \subseteq \mathcal{V}(E)$.

2. ($\supseteq$): Como $I \subseteq \sqrt{I}$, entonces, por 1., $\mathcal{V}(\sqrt{I}) \subseteq \mathcal{V}(I)$. ($\subseteq$): $P \in \mathcal{V}(I)$ implica que $f(P) = 0$ para todo $f \in I$. Luego, si $f \in \sqrt{I}$ se implica que existe $r \in \mathbb{Z}^+$ tal que $f^r \in I$, entonces $f^r(P) = 0$. Así, si $r = 1$, se cumple que $f(P) = 0$, en otro caso, $f^r = f \cdots f$ (r veces), que como $k[x_1, \ldots, x_n]$ es un dominio entero, se tiene que $f(P) = 0$, por lo que $P \in \mathcal{V}(\sqrt{I})$. Así, $\mathcal{V}(I) \subseteq \mathcal{V}(\sqrt{I})$. Por tanto, $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.

3. Si $\mathcal{V}(k[x_1, \ldots, x_n]) \neq \emptyset$, entonces existiría $P \in \mathbb{A}_k^n$ tal que $f(P) = 0$ para todo $f \in k[x_1, \ldots, x_n]$. Así, como $k \subseteq k[x_1, \ldots, x_n]$, en particular, $1_k = 1(P) = 0$, contradicción, pues k es un campo. Luego, $\mathcal{V}(k[x_1, \ldots, x_n]) = \emptyset$

4. ($\subseteq$): Por definición, $\mathcal{V}(0) \subseteq \mathbb{A}_k^n$. ($\supseteq$): Si $P \in \mathbb{A}_k^n$, entonces $0(P) = 0$. Así, $P \in \mathcal{V}(0)$. Luego, $\mathbb{A}_k^n \subseteq \mathcal{V}(0)$. Por tanto, $\mathcal{V}(0) = \mathbb{A}_k^n$.

5. ($\subseteq$): Como $J_1 \cap J_2 \subseteq J_1, J_2$, entonces, por 1., $\mathcal{V}(J_1), \mathcal{V}(J_2) \subseteq \mathcal{V}(J_1 \cap J_2)$. Así, $\mathcal{V}(J_1) \cup \mathcal{V}(J_2) \subseteq \mathcal{V}(J_1 \cap J_2)$. ($\supseteq$): Si $P \notin \mathcal{V}(J_1)$ y $P \notin \mathcal{V}(J_2)$, entonces existe $f \in J_1$ tal que $f(P) \neq 0$ y existe $g \in J_2$ tal que $g(P) \neq 0$. Ahora, notemos que $fg \in J_1$ y $fg \in J_2$, es decir, $fg \in J_1 \cap J_2$. Luego, $fg(P) = f(P)g(P) \neq 0$, pues como k es campo, entonces k es dominio entero. Así, $P \notin \mathcal{V}(J_1 \cap J_2)$. Luego, se sigue que $\mathcal{V}(J_1 \cap J_2) \subseteq \mathcal{V}(J_1) \cup \mathcal{V}(J_2)$. Por tanto, $\mathcal{V}(J_1) \cup \mathcal{V}(J_2) = \mathcal{V}(J_1 \cap J_2)$.

6.($\subseteq$): Si $P \in \mathcal{V}(J_j)$ para toda $j \in \Lambda$, entonces para todo $f \in \sum_{j \in \Lambda} J_j$, escribiendo $f = \sum_{\text{finita}} g_j f_j$ con $g_j \in k[x_1, \ldots, x_n]$ y $f_j \in J_j$, se tiene que $f(P) = \sum_{\text{finita}} g_j(P) f_j(P) = 0$. Así, $P \in \mathcal{V}(\sum_{j \in \Lambda} J_j)$. ($\supseteq$): Si $P \in \mathcal{V}(\sum_{j \in \Lambda} J_j)$, como cada $J_j \subseteq \sum_{j \in \Lambda} J_j$, entonces $P \in \mathcal{V}(J_j)$ para todo $j \in \Lambda$, por lo que $P \in \bigcap_{j \in \Lambda} \mathcal{V}(J_j)$.

7. Si $f \in \mathcal{I}(Y)$, se cumple que $f(P) = 0$ para todo $P \in Y$, entonces, como $X \subseteq Y$, se tiene que $f(P) = 0$ para todo $P \in X$, entonces $f \in \mathcal{I}(X)$. Así, $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$.

8. Si $\mathcal{I}(\emptyset) \neq k[x_1, \ldots, x_n]$, entonces existiría $f \in k[x_1, \ldots, x_n]$ tal que $f \notin \mathcal{I}(\emptyset)$, es decir, existiría $P \in \emptyset$ tal que $f(P) \neq 0$, contradicción. Por tanto, $\mathcal{I}(\emptyset) = k[x_1, \ldots, x_n]$.

9. ($\subseteq$): Si $f \in \mathcal{I}(\mathbb{A}_k^n)$, entonces, por la contrarecíproca de la **Proposición 3.2**, $f = 0$. ($\subseteq$): Es claro. Por tanto, $\mathcal{I}(\mathbb{A}_k^n) = 0$.

10. ($\subseteq$): Si $f \in \sqrt{\mathcal{I}(X)}$, existe $r \in \mathbb{N}$ no nulo tal que $f^r \in \mathcal{I}(X)$, entonces $f^r(P) = 0$ para todo $P \in X$, es decir, $(f(P))^r = 0$, entonces $f(P) = 0$, es decir, $f \in \mathcal{I}(X)$. Así, $\sqrt{\mathcal{I}(X)} \subseteq \mathcal{I}(X)$. ($\supseteq$): Por la **Proposición 2.18**.

11. Si $f \in J$ y para todo $P \in \mathcal{V}(J)$, se cumple que $f(P) = 0$, entonces $f \in \mathcal{I}(\mathcal{V}(J))$. Por tanto, $J \subseteq \mathcal{I}(\mathcal{V}(J))$.

12. Si $P \in X$ y para todo $f \in \mathcal{I}(X)$, se cumple que $f(P) = 0$, entonces $P \in \mathcal{V}(\mathcal{I}(X))$. Así, $X \subseteq \mathcal{V}(\mathcal{I}(X))$. Para la otra parte, si $X = \mathcal{V}(\mathcal{I}(X))$, por definición, se sigue que X es algebraico. Ahora, si X es algebraico, entonces $X = \mathcal{V}(J)$ para algún ideal J de $k[x_1, \ldots, x_n]$. Luego, por 11., $J \subseteq \mathcal{I}(X)$, entonces, por 1., $\mathcal{V}(\mathcal{I}(X)) \subseteq \mathcal{V}(J) = X$, por lo que $X = \mathcal{V}(\mathcal{I}(X))$.

†

Debido a 3., 4., 5. y 6. del lema anterior, tenemos la siguiente:

Proposición 3.4. *Sea k un campo y $n \in \mathbb{Z}^+$. Entonces, $(\mathbb{A}_k^n, \{Y \subseteq \mathbb{A}_k^n \mid Y$ es algebraico en $\mathbb{A}_k^n\})$ es un espacio topológico.*

Observación 3.3. *A la topología $\{Y \subseteq \mathbb{A}_k^n \mid Y$ es algebraico en $\mathbb{A}_k^n\}$ en $\mathbb{A}_k^n$ se le conoce como topología de **Zariski**.*

Ahora, es tiempo de enunciar una serie de resultados que nos ayudaran con la demostración del Nullstellensatz. En efecto, comenzamos con el primer:

Lema 3.2. *Si k es un campo y $f \in k[x_1, \ldots, x_n]$ es un polinomio no nulo de grado d, entonces existe un cambio de variables lineal $x_i' = x_i - a_i x_n$, para $1 \leq i \leq n-1$, y con $a_i \in k$, tales que el polinomio*

$$f(x_1' + a_1 x_n, \ldots, x_{n-1}' + a_{n-1} x_n, x_n) \in k[x_1', \ldots, x_{n-1}', x_n]$$

tiene un término de la forma cx_n^d, *con* $c \in k$.

Demostración. Escriba $x_i' = x_i - a_i x_n$, para alguna elección de $a_i \in k$, $1 \leq i \leq n-1$. Se probará que existe una elección de las a_i que satisfacen el lema. Sea f_d la componente homogénea de f de grado d y escriba $f = f_d + g$, con g de grado menor o igual a $d-1$. Entonces,

$$f(x_1'+a_1x_n, \ldots, x_{n-1}'+a_{n-1}x_n, x_n) = f_d(a_1, \ldots, a_{n-1}, 1)x_n^d + \text{términos de grado menor en } x_n$$

ya que cada monomio de grado d en f_d es de la forma $m_d = ax_1^{e_1} \cdots x_n^{e_n}$ con $\sum e_i = d$, y al substituir x_i por $x_i = x_i' + a_i x_n$, $1 \leq i \leq n-1$ el monomio m_d queda de la forma

$$a(x_1' + a_1x_n)^{e_1} \cdots (x_{n-1}' + a_{n-1}x_n)^{e_{n-1}} x_n^{e_n}$$

donde al expandir los binomios notamos que al juntar los términos de mayor grado en x_n queda

$$a(a_1^{e_1}x_n^{e_1} \cdots a_{n-1}^{e_{n-1}}x_n^{e_{n-1}}x_n^{e_n}) = a(a_1^{e_1} \cdots a_{n-1}^{e_{n-1}} \cdot 1)x_n^d = m_d(a_1, \ldots, a_{n-1}, 1)x_n^d$$

porque $\sum e_i = d$, de donde se sigue la afirmación con $f_d = \sum m_d$. Finalmente, notamos ahora que $f_d(x_1, \ldots, x_{n-1}, 1)$ es un polinomio en $x_1, \ldots, x_{n-1}$ que no es nulo, porque de lo contrario f no tendría grado d; se sigue que $\mathcal{V}(f_d) \neq k^{n-1}$ por la **Proposición 3.2**. Así, existen $a_1, \ldots, a_{n-1} \in k$ tales que $f_d(a_1, \ldots, a_{n-1}, 1) \neq 0$ y poniendo $c = f_d(a_1, \ldots, a_{n-1}, 1)$ se sigue la conclusión del lema.

†

Teorema 3.1 (Normalización de Noether). *Sean* k *un campo y* $A = k[a_1, \ldots, a_n]$ *una* k*-álgebra de tipo finito sobre* k. *Entonces existen* $y_1, \ldots, y_m \in A$, *con* $m \leq n$, *tal que*

1. $y_1, \ldots, y_m$ *son algebraicamente independientes sobre* k.
2. A *es una* $k[y_1, \ldots, y_m]$*-álgebra finita.*

Demostración. Se probará este resultado por inducción sobre n. En efecto, sea $k[x_1, \ldots, k_n]$ el anillo de polinomios en n variables, consideremos el morfismo:

$$k[x_1, \ldots, x_n] \xrightarrow{\psi} k[a_1, \ldots, a_n] = A$$

$$x_i \longmapsto a_i$$

$$k \ni a \longmapsto a$$

y sea $I := ker(\psi)$. Si $I = 0$, podemos tomar $m = n$ y $y_1 = a_1, \ldots, y_n = a_n$, y claramente se cumplen 1. y 2. Si $I \neq 0$, entonces existe $f \in I$ no cero. Si $n = 1$, tenemos que $f(a_1) = 0$, y por tanto el resultado se cumple por el **Lema 2.2** con $m = 0$. Ahora, supongamos que $n > 1$ y que el resultado es cierto para $n - 1$. Luego, por el **Lema 3.2** existen $\alpha_1, \ldots, \alpha_{n-1} \in k$ tal que, si $a'_i := a_i - \alpha_i a_n$ y $A' := k[a'_1, \ldots, a'_{n-1}] \subseteq A$, tenemos que para algún $c \in k$ el polinomio

$$F(x_n) := \tfrac{1}{c} f(a'_1 + \alpha_1 x_n, \ldots, a'_{n-1} + \alpha_{n-1} x_n, x_n)$$

es un polinomio mónico en $A'[x_n]$, y $F(a_n) = 0$. Así, por el **Lema 2.2** se cumple que a_n es entero sobre A'. Ahora, por la hipótesis inductiva, existen $y_1, \ldots, y_m \in A'$ tales que cumplen:

(i) $y_1, \ldots, y_m$ son algebraicamente independientes sobre k,

(ii) A' es una $k[y_1, \ldots, y_m]$-álgebra finita.

Por el **Lema 2.2** tenemos que $A = A'[a_n]$ es una A'-álgebra finita, y que por el **Lema 2.2**, también se cumple que A es una $k[y_1, \ldots, y_m]$-álgebra finita.

†

Lema 3.3. *Sean A un campo y B un subanillo de A tal que A es una B-álgebra finita. Entonces B es campo.*

Demostración. Sea $b \in B$ no cero. Ahora, como A es un campo, entonces existe $b^{-1} \in A$. Demostremos que $b^{-1} \in B$. En efecto, como A es una B-álgebra finita, entonces, por el **Corolario 2.16** A es entera sobre B, entonces

$$b^{-n} + b_{n-1} b^{-(n-1)} + \cdots + b_1 b^{-1} + b_0 = 0, \text{ para algunos } b_i \in B.$$

Multiplicando por b^{n-1} obtenemos:

$$b^{-1} = -(b_{n-1} + b_{n-2} b + \cdots + b_0 b^{n-1}) \in B.$$

†

Teorema 3.2 (Zariski). *Sean k un campo y $A = k[a_1, \ldots, a_n]$ una k-álgebra de tipo finito sobre k. Si A es un campo, entonces A es algebraica sobre k.*

Demostración. En efecto, sean k un campo y $A = k[a_1, \ldots, a_n]$ una k-álgebra de tipo finito sobre k tal que A es un campo. Ahora, por el **Teorema de Normalización de Noether**, existen $y_1, \ldots, y_m \in A$, con $m \leq n$, tal que $y_1, \ldots, y_m$ son algebraicamente independientes sobre k y A es una $k[y_1, \ldots, y_m]$-álgebra finita. Así, por el lema anterior, $k[y_1, \ldots, y_m]$ es un campo. Pero esto solo puede pasar si $m = 0$. Por tanto, A es una k-álgebra finita, es decir, A es finitamente generado como k-módulo, es decir, A es un k-espacio vectorial de dimensión finita. Luego, se sigue que A/k es finita, entonces, por la **Proposición 2.38**, A/k es algebraica.

†

Teorema 3.3 (Nullstellensatz). *Si k es un campo, se cumplen:*

1. *Los ideales máximos del anillo $k[x_1, \ldots, x_n]$ son de la forma*

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) = \mathcal{I}(P),$$

   para algún $P = (a_1, \ldots, a_n) \in \mathbb{A}^n_k$.

2. *Si I es un ideal propio de $k[x_1, \ldots, x_n]$, entonces $\mathcal{V}(I) \neq \emptyset$.*

3. *Para todo ideal I de $k[x_1, \ldots, x_n]$, se tiene que $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.*

Demostración. 1. Si $a_1, \ldots, a_n \in k$, entonces, por la **Proposición 2.36**, $(x_1 - a_1, \ldots, x_n - a_n)$ es un ideal máximo de $k[x_1, \ldots, x_n]$. Ahora, si $\mathfrak{m}$ es un ideal máximo de $k[x_1, \ldots, x_n]$, entonces $K := k[x_1, \ldots, x_n]/\mathfrak{m}$ es un campo extensión de k, pues tenemos:

$$k \xhookrightarrow{\iota} k[x_1, \ldots, x_n] \xrightarrow{\pi} k[x_1, \ldots, x_n]/\mathfrak{m} =: K \ ,$$

donde K es de tipo finito sobre k, pues $K = k[x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m}]$, y por el **Teorema de Zariski**, K/k es algebraica, pero como k es algebraicamente cerrado, entonces, por 2. de la **Proposición 2.39**, $K = k$. Luego, para todo $1 \leq i \leq n$ y para $x_i + \mathfrak{m} \in K$ existe $a_i \in k$ tal que $x_i + \mathfrak{m} = a_i$, es decir, $x_i - a_i \in \mathfrak{m}$ y por lo tanto $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}$, y como el ideal $(x_1 - a_1, \ldots, x_n - a_n)$ es máximo, entonces $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$.

2. Si I es un ideal propio de $k[x_1, \ldots, x_n]$, entonces, por el **Corolario** 2.5 existe un ideal máximo $\mathfrak{m}$ tal que $I \subseteq \mathfrak{m}$, entonces, por 1. del **Lema** 3.1, $\mathcal{V}(\mathfrak{m}) \subseteq \mathcal{V}(I)$. Ahora, por 1., $\mathcal{V}(\mathfrak{m}) = \mathcal{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\} \neq \emptyset$. Así, $\mathcal{V}(I) \neq \emptyset$.

3. ($\supseteq$): Si $f \in \sqrt{I}$, se cumple que existe $m \in \mathbb{N}$ no nulo tal que $f^m \in I$, y por lo tanto para todo $P \in \mathcal{V}(I)$ se tiene que $0 = f^m(P) = (f(P))^m$ y así $f(P) = 0$, es decir, $f \in \mathcal{I}(\mathcal{V}(I))$. Por tanto, $\mathcal{I}(\mathcal{V}(I)) \supseteq \sqrt{I}$.

   ($\subseteq$): Sea $f \in \mathcal{I}(\mathcal{V}(I))$ y sea $I := (h_1, \ldots, h_r)$. Queremos mostrar que $f^N \in I$ para algún $N \in \mathbb{N}$ no cero. Para esto, se usará el truco de Rabinowitsch, el cual consiste en introducir una variable adicional t y considerar el ideal de polinomios $I_f = (h_1, \ldots, h_r, ft - 1) \subseteq k[x_1, \ldots, x_n, t]$ que contiene a I. Entonces, $\mathcal{V}(I_f) \subseteq \mathbb{A}_k^{n+1}$ consiste de los ceros comunes de los h_i (notemos que como los h_i no tienen la variable t, los ceros comunes de los h_i deben ser de la forma (P, b) con $P \in \mathcal{V}(I)$ y $b \in k$ arbitrario) que además son ceros de $ft - 1$, es decir, $f(P) - 1 = 0$ por lo que $f(P) \neq 0$, una contradicción porque $f \in \mathcal{I}(\mathcal{V}(I))$ y $P \in \mathcal{V}(I)$. Se sigue que $\mathcal{V}(I_f) = \emptyset$, que por la parte 2., se implica que $I_f = (1) = k[x_1, \ldots, x_n, t]$ y por lo tanto existen $g_i \in k[x_1, \ldots, x_n, t]$ tales que

$$1 = \sum_{i=1}^{r} g_i h_i + g_0(ft - 1) \in k[x_1, \ldots, x_n, t].$$

   Poniendo $t = \frac{1}{f}$ en la anterior ecuación (lo cual cancela el sumando con g_0) y limpiando denominadores, la anterior ecuación toma la forma

$$(*) \qquad 1 = \sum_{i=1}^{r} g_i(x_1, \ldots, x_n, 1/f)h_i = \frac{1}{f^N} \sum_{i=1}^{r} \widetilde{g}_i(x_1, \ldots, x_n, 1)h_i,$$

   donde N es tal que t^N es la mayor potencia de t que aparece en todos los polinomios g_i y los $\widetilde{g}_i$ son polinomios obtenidos al multiplicar los monomios de g_i por las potencias correspondientes de f; así, los $\widetilde{g}_i$ son polinomios de $k[x_1, \ldots, x_n]$. Multiplicando $(*)$ por f^N se sigue que

$$f^N = \sum_{i=1}^{r} \widetilde{g}_i(x_1, \ldots, x_n, 1)h_i \in I.$$

†

Ya alcanzado nuestro primer objetivo, ahora emprendemos camino hacia la demostración de nuestro segundo, y último, objetivo, la demostración de la equivalencia de las categorías de variedades algebraicas afines sobre un campo algebraicamente cerrado K y la categoría opuesta de K-álgebras

conmutativas finitamente generadas reducidas. Así, para este fin, nos resta definir los morfismos entre variedades algebraicas afines y una ley de composición entre estos.

Convención 3.2. *En este trabajo, convenimos en que las palabras* ***conjunto algebraico*** *y* ***variedad algebraica (variedad afín)*** *significan lo mismo.*

Definición 3.3. *Sea $V \subseteq \mathbb{A}_k^n$ una variedad algebraica.*

1. *El* ***anillo de coordenadas*** *de V es definido por*

$$k[V] := k[x_1, \ldots, x_n]/\mathcal{I}(V).$$

2. *Una* ***función polinomial*** *en V es una función $f : V \longrightarrow k$ tal que existe un polinomio $F \in k[x_1, \ldots, x_n]$ con $f(P) = F(P)$ para todo $P \in V$.*

Proposición 3.5. *Sea $V \subseteq \mathbb{A}_k^n$ una variedad algebraica. Se cumplen:*

1. *$k^V = \{f : V \longrightarrow k \mid f$ es función $\}$ es un anillo.*
2. *Sea $k_{\mathcal{P}}^V := \{f : V \longrightarrow k \mid f$ es función polinomial $\}$. Entonces, $k_{\mathcal{P}}^V$ es un subanillo de k^V tal que contiene a k.*
3. *Sea $L : k[x_1, \ldots, x_n] \longrightarrow k^V$ la función que restringe un polinomio F a una función polinomial $F|_V : V \longrightarrow k$. Entonces, L es un morfismo de anillos, $ker(L) = \mathcal{I}(V)$, $L[k[x_1, \ldots, x_n]] = k_{\mathcal{P}}^V$ y $k[V] \cong k_{\mathcal{P}}^V$.*

Demostración. 1. Si $+ : k^V \times k^V \longrightarrow k^V$, $(f, g) \longmapsto f(P) + g(P)$, y $\cdot : k^V \times k^V \longrightarrow k^V$, $(f, g) \longmapsto f(P)g(P)$, entonces, por 3. de los **Ejemplos** 2.1, $(k^V, +, \cdot)$ es un anillo.

2. Por definición, $k_{\mathcal{P}}^V \subseteq k^V$. Ahora, sea $l : k \longrightarrow k_{\mathcal{P}}^V$, $a \longmapsto a(P) = a$. Así, l está bien definida, pues $k \subseteq k[x_1, \ldots, x_n]$. Luego, l es inyectiva, pues si $a, b \in k$ son tales que $l(a) = l(b)$, entonces $a(P) = b(P)$, para todo $P \in V$, entonces $a = b$. Así, $l[k] \cong S$, para algún S subconjunto de $k_{\mathcal{P}}^V$. Así, $k \subseteq k_{\mathcal{P}}^V$. Ahora, veamos que $k_{\mathcal{P}}^V$ es un subanillo de k^V. En efecto, como $1_{k^V} \equiv 1 : V \longrightarrow k$, $P \longmapsto 1_k$ y $k \subseteq k_{\mathcal{P}}^V$, entonces $1_{k^V} \in k_{\mathcal{P}}^V$. Ahora, si $f, g \in k_{\mathcal{P}}^V$, entonces existen $F, G \in k[x_1, \ldots, x_n]$ tales que $f(P) = F(P)$ y $g(P) = G(P)$ para todo $P \in V$. Así, si $P \in V$, entonces $(f - g)(P) = f(P) - g(P) = F(P) - G(P) = (F - G)(P) \in k_{\mathcal{P}}^V$ y $(fg)(P) = f(P)g(P) = F(P)G(P) = (FG)(P) \in k_{\mathcal{P}}^V$. Luego, $k_{\mathcal{P}}^V$ es un subanillo de k^V. Por tanto, $k_{\mathcal{P}}^V$ es un subanillo de k^V tal que contiene a k.

3. Primero, veamos que L es morfismo. En efecto, si $F, G \in k[x_1, \ldots, x_n]$, entonces:

- $L(F+G) = (F+G)|_V$ y $L(F) + L(G) = F|_V + G|_V$. Así, si $P \in V$, entonces $(F+G)|_V(P) = F|_V(P) + G|_V(P)$. Luego, $L(F+G) = L(F) + L(G)$.
- $L(FG) = (FG)|_V$ y $L(F)L(G) = F|_V G|_V$. Ahora, si $P \in V$, entonces $(FG)|_V(P) = F|_V(P)G|_V(P)$. Así, $L(FG) = L(F)L(G)$.
- $L(1) = 1|_V = 1_{k_{\mathcal{P}}^V}$.

Así, L es morfismo.
Ahora, $ker(L) = \{F \in k[x_1, \ldots, x_n] \mid L(F) = 0|_V\} = \{F \in k[x_1, \ldots, x_n] \mid F(a) = 0 \forall a \in V\} = \mathcal{I}(V)$. Por último, es claro que $L[k[x_1, \ldots, x_n]] = k_{\mathcal{P}}^V$. Luego, por el **primer teorema de isomorfismo**, $k[V] = k[x_1, \ldots, x_n]/\mathcal{I}(V) \cong k_{\mathcal{P}}^V$.

†

Sea $V \subseteq \mathbb{A}_k^n$ una variedad algebraica. Entonces, gracias a la última parte de 3. de la proposición anterior, podemos hacer la siguiente identificación:

$$k[V] = \{f : V \longrightarrow k \mid f \text{ es función polinomial }\}.$$

Observación 3.4. *Sea $V \subseteq \mathbb{A}_k^n$ una variedad algebraica.*

1. *La composición de los morfismos naturales:*

$$k \hookrightarrow k[x_1, \ldots, x_n] \twoheadrightarrow k[x_1, \ldots, x_n]/\mathcal{I}(V) = k[V]$$

   hace del anillo $k[V]$ una k-álgebra.

2. *Las coordenadas $x_1, \ldots, x_n \in k[V] = k[x_1, \ldots, x_n]/\mathcal{I}(V)$ las podemos ver como funciones $x_i : V \longrightarrow k$, $P = (a_1, \ldots, a_n) \longmapsto a_i$, es decir, asignan a cada punto P de V su i-ésima coordenada.*

3. *El anillo $k[V]$ es el menor anillo de funciones en V que contiene a las funciones coordenadas y al campo k. Más aún, el anillo $k[V]$ está generado, como k-álgebra, por las funciones coordenadas, de ahí el nombre de anillo de coordenadas.*

Proposición 3.6. *Sea $V \subseteq \mathbb{A}_k^n$ una variedad algebraica. Entonces, el anillo $k[V]$ es reducido.*

Demostración. En efecto, como $k[V] = k[x_1, \ldots, x_n]/\mathcal{I}(V)$ e $\mathcal{I}(V)$ es un ideal radical, por 10. del **Lema 3.1** entonces, por la **Proposición 2.25**, $k[V] = k[x_1, \ldots, x_n]/\mathcal{I}(V)$ es reducido.

†

Ahora, definamos los morfismos entre variedades algebraicas.

Definición 3.4. *Sean $V \subseteq \mathbb{A}_k^n$ y $W \subseteq \mathbb{A}_k^m$ variedades algebraicas. Una función $f : V \longrightarrow W$ se dice que es una **aplicación polinomial** si existen polinomios $F_1, \ldots, F_m \in k[x_1, \ldots, x_n]$ tales que para todo $P \in V$ se cumple que $f(P) = (F_1(P), \ldots, F_m(P))$.*

Proposición 3.7. *Sean $V \subseteq \mathbb{A}_k^n$, $W \subseteq \mathbb{A}_k^m$ variedades algebraicas y denotemos a los anillos polinomiales de los espacios afines correspondientes por $k[x_1, \ldots, x_n]$ y $k[y_1, \ldots, y_m]$. Entonces, $f : V \longrightarrow W$ es una aplicación polinomial si y solo si $y_j \circ f \in k[V]$, para todas las funciones coordenadas $y_j \in k[W]$.*

Demostración. ($\Longrightarrow$): Si $f : V \longrightarrow W$ es una aplicación polinomial, existen polinomios $F_1, \ldots, F_m \in k[x_1, \ldots, x_n]$ tales que para todo $P \in V$ se cumple que $f(P) = (F_1(P), \ldots, F_m(P))$. Luego, si $P \in V$, entonces, para todo $j \in \{1, \ldots, m\}$, se tiene que $y_j \circ f(P) = y_j(F_1(P), \ldots, F_m(P)) = F_j(P)$, pero como F_j es un polinomio, entonces $F_j|_V \in k[V]$. Por tanto, $y_j \circ f \in k[V]$ para todo $j \in \{1, \ldots, m\}$.

($\Longleftarrow$): Sea $f := (f_1, \ldots, f_m)$. Luego, $f_j = y_j \circ f \in k[V]$ para todo $j \in \{1, \ldots, m\}$ implica que existen $F_j \in k[x_1, \ldots, x_n]$ tales que para todo $P \in V$, $f_j(P) = F_j(P)$. Así, para todo $P \in V$, $f(P) = (F_1(P), \ldots, F_m(P))$. Así, $f : V \longrightarrow W$ es una aplicación polinomial.

†

Observación 3.5. *Sea $X \subseteq \mathbb{A}_k^n$ una variedad algebraica. La función identidad $Id_X : X \longrightarrow X$, $P \longmapsto P$, es una aplicación polinomial.*

Definición 3.5. *Sean $X \subseteq \mathbb{A}_k^n$, $Y \subseteq \mathbb{A}_k^m$ y $Z \subseteq \mathbb{A}_k^r$ variedades algebraicas. Ahora, si $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ son aplicaciones polinomiales, con $f := (f_1, \ldots, f_m)$ y $g := (g_1, \ldots, g_r)$, entonces $g \circ f : X \longrightarrow Z$, que viene dada por $g \circ f = (g_1(f_1, \ldots, f_m), \ldots, g_r(f_1, \ldots, f_m))$, es polinomial.*

3.0.1 La categoría de variedades afines y aplicaciones polinomiales

Sea k un campo. Entonces, de lo anterior, tenemos que las variedades algebraicas junto con las aplicaciones polinomiales forman una categoría.

Notación 3.1. *Con $Af(k)$ denotaremos a la categoría de variedades algebraicas sobre un campo k y con morfismos las aplicaciones polinomiales.*

Observación 3.6. *Sea k un campo. Notemos que las k-álgebras reducidas y de tipo finito junto con los morfismos de k-álgebras forman una categoría, la cual denotaremos por k-álg-red.*

Teorema 3.4. *Sean $X \subseteq \mathbb{A}_k^n$, $Y \subseteq \mathbb{A}_k^m$ variedades algebraicas.*

1. *Si $f : X \longrightarrow Y$ es una aplicación polinomial, entonces f induce el morfismo de k-álgebras $f^\sharp : k[Y] \longrightarrow k[X]$.*
2. *Recíprocamente, cualquier morfismo de k-álgebras $\varphi : k[Y] \longrightarrow k[X]$ es de la forma $\varphi = f^\sharp$ para una única aplicación polinomial $f : X \longrightarrow Y$. En otras palabras, se tiene una biyección:*

   $$\{\text{aplicaciones polinomiales } f : X \longrightarrow Y\} \longleftrightarrow Hom_{k\text{-álg}}(k[Y], k[X]) \text{ dada por } f \longleftrightarrow f^\sharp$$

3. *La correspondencia de 1. es contravariante, es decir, si $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ son aplicaciones polinomiales, entonces $(g \circ f)^\sharp = f^\sharp \circ g^\sharp$.*
4. *Una consecuencia inmediata es que $f : X \longrightarrow Y$ es un isomorfismo si y solo si $f^\sharp : k[Y] \longrightarrow k[X]$ es un isomorfismo de k-álgebras.*

Demostración. 1. Si $f : X \longrightarrow Y$ es una aplicación polinomial, entonces f induce a $f^\sharp : k[Y] \longrightarrow k[X]$ por medio de la composición con f, es decir, si $\alpha \in k[Y]$ la vemos como una función polinomial $\alpha : Y \longrightarrow k$, entonces $f^\sharp(\alpha) = \alpha \circ f : X \longrightarrow k$. Ahora, se afirma que $f^\sharp$ es un k-morfismo, pues si $\alpha_1, \alpha_2 \in k[Y]$ y $a \in k$, entonces tenemos:

   - $f^\sharp(\alpha_1 + \alpha_2) = (\alpha_1 + \alpha_2) \circ f = \alpha_1 \circ f + \alpha_2 \circ f = f^\sharp(\alpha_1) + f^\sharp(\alpha_2)$.
   - $f^\sharp(\alpha_1\alpha_2) = (\alpha_1\alpha_2) \circ f = (\alpha_1 \circ f)(\alpha_2 \circ f) = f^\sharp(\alpha_1)f^\sharp(\alpha_2)$.
   - $f^\sharp(a) = a \circ f = a$.

2. Sean $\bar{y}_j = y_j + \mathcal{I}(Y) \in k[Y] = k[y_1, \ldots, y_m]/\mathcal{I}(Y)$ las funciones coordenadas. Calculando el morfismo dado $\varphi : k[Y] \longrightarrow k[X]$ en las $\bar{y}_j$ obtenemos que $\varphi(\bar{y}_j) \in k[X]$ y se pone $f_j =$

$\varphi(\bar{y}_j) \in k[X]$. Entonces, la función $f : X \longrightarrow \mathbb{A}_k^m$ dada por $f(P) = (f_1(P), \ldots, f_m(P))$ es una aplicación polinomial porque las f_j son funciones polinomiales.Verifiquemos que su imagen está en Y. Para ésto, suponga que $g \in \mathcal{I}(Y) \subseteq k[y_1, \ldots, y_m]$; entonces, en $k[Y]$ se tiene que $g(\bar{y}_1, \ldots, \bar{y}_m) = 0 \in k[Y]$ pues $g \in \mathcal{I}(Y)$. Se sigue que $\varphi(g(\bar{y}_1, \ldots, \bar{y}_m)) = 0 \in k[X]$ porque φ es morfismo. Como g tiene coeficientes en k y φ es k-morfismo, entonces

$$0 = \varphi(g(\bar{y}_1, \ldots, \bar{y}_m)) = g(\varphi(\bar{y}_1), \ldots, \varphi(\bar{y}_m)) = g(f_1, \ldots, f_m),$$

donde $g(f_1, \ldots, f_m) \in k[X]$ es la función $P \longmapsto g(f_1(P), \ldots, f_m(P))$, la cual hemos visto que se anula para todo $g \in \mathcal{I}(Y)$, y como Y es el conjunto de ceros de $\mathcal{I}(Y)$, se sigue que $(f_1(P), \ldots, f_m(P)) \in Y$, es decir, $f(P) \in Y$, como se quería. Resta probar que para la aplicación polinomial f anterior se tiene que $f^\sharp = \varphi : k[Y] \longrightarrow k[X]$. Para ésto, basta verificarlo en los generadores $\bar{y}_j$ del dominio. Ahora, como $f = (f_1, \ldots, f_m)$ y los $f_j = \varphi(\bar{y}_j)$, entonces

$$f^\sharp(\bar{y}_j) = \bar{y}_j \circ f = f_j = \varphi(\bar{y}_j).$$

El mismo argumento prueba que f es única con la propiedad de que $f^\sharp(\bar{y}_j) = \varphi(\bar{y}_j)$.

3. Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ aplicaciones polinomiales. Si $\alpha \in k[Z]$, entonces

$$(g \circ f)^\sharp(\alpha) = \alpha \circ (g \circ f) = (\alpha \circ g) \circ f = g^\sharp(\alpha) \circ f = f^\sharp(g^\sharp(\alpha)) = (f^\sharp \circ g^\sharp)(\alpha).$$

4. Es claro.

†

En lenguaje categórico precisamos todo lo anterior:

Se tiene un funtor contravariante:

$$Af(k) \xrightarrow{F} k\text{-álg-red}$$

tal que

(i) En objetos: $X \longmapsto k[X]$

(ii) En morfismos: $f : X \longrightarrow Y \longmapsto f^\sharp : k[Y] \longrightarrow k[X]$

Ahora, tenemos un funtor contravariante en dirección opuesta:

$$k\text{-álg-red} \xrightarrow{G} Af(k)$$

tal que

(i) En objetos:

Sea A una k-álgebra de tipo finito y reducida. Escogiendo generadores $\alpha_1, \ldots, \alpha_n \in A$, tenemos el morfismo:

$$\psi : k[x_1, \ldots, x_n] \longmapsto A = k[\alpha_1, \ldots, \alpha_n]$$

$$x_i \longmapsto \alpha_i$$

$$k \ni a \longmapsto a$$

el cual resulta ser suprayectivo. Así, por el **primer teorema de isomorfismo**,

$$k[x_1, \ldots, x_n]/ker(\psi) \cong A,$$

entonces si $I := ker(\psi)$, I resulta ser un ideal radical, entonces, por 3. del **Nullstellensatz**, a I le corresponde un único, salvo isomorfismo, subconjunto algebraico $X = \mathcal{V}(I)$. Así, se define $G(A) = X$.

(ii) En morfismos:

Por la parte 2. del **Teorema 3.4**, a cada morfismo $\varphi : A \longrightarrow A'$ de k-álgebras de tipo finito y reducidas le corresponde un único morfismo de conjuntos algebraicos afines $f : X' = \mathcal{V}(I') \longrightarrow X = \mathcal{V}(I)$ tal que $f^\sharp = \varphi$.

Más aún, los funtores F y G definen una equivalencia natural de categorías:

$$F : Af(k) \longleftrightarrow k\text{-álg-red} : G \ ,$$

es decir, existen transformaciones naturales

$$\eta : G \circ F \longrightarrow Id_{Af(k)} \qquad \text{y} \qquad \vartheta : F \circ G \longrightarrow Id_{k\text{-álg-red}}.$$

Bibliografia

[AM80] Michael Francis Atiyah and Ian Grant Macdonald. *Introducción al álgebra conmutativa*. Reverté, 1980.

[Bla11] Paul E Bland. Rings and their modules. In *Rings and Their Modules*. de Gruyter, 2011.

[Bor94] Francis Borceux. *Handbook of categorical algebra: volume 1, Basic category theory*, volume 1. Cambridge University Press, 1994.

[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[Hul03] Klaus Hulek. *Elementary algebraic geometry*. Number 20. American Mathematical Soc., 2003.

[Hun12] Thomas W Hungerford. *Algebra*, volume 73. Springer Science & Business Media, 2012.

[Jac12] Nathan Jacobson. *Basic algebra I*. Courier Corporation, 2012.

[Kas82] Friedrich Kasch. *Modules and rings*, volume 17. Academic press, 1982.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*. Number 8. Cambridge university press, 1989.

[ML13] Saunders Mac Lane. *Categories for the working mathematician*, volume 5. Springer Science & Business Media, 2013.

[RM88] Miles Reid and Reid Miles. *Undergraduate algebraic geometry*, volume 12. Cambridge University Press, 1988.

[RM95] Miles Reid and Reid Miles. *Undergraduate commutative algebra*. Number 29. Cambridge University Press, 1995.

[Rot10] Joseph J Rotman. *Advanced modern algebra*, volume 114. American Mathematical Soc., 2010.

[Sha87] David Sharpe. *Rings and factorization*. CUP Archive, 1987.

[Sha00] Rodney Y Sharp. *Steps in commutative algebra*. Number 51. Cambridge university press, 2000.

[Zal96] Felipe Zaldívar. *Teoría de Galois*. Number 3. Anthropos Editorial, 1996.

[Zal14] Felipe Zaldívar. *Introducción a la teoría de números*. Fondo de Cultura Económica, 2014.

[Zal20] Felipe Zaldívar. *Introducción al álgebra conmutativa*. 2020.

[Zal21] Felipe Zaldívar. *Introducción a la geometría algebraica*. 2021.

[ZS62] Oscar Zariski and Pierre Samuel. *Commutative algebra*, volume 1. Springer, 1962.