UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CIENCIAS

# EQUIVALENCIA ENTRE EL AXIOMA DE ELECCIÓN Y LA EXISTENCIA DE BASES EN ESPACIOS VECTORIALES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICA

P R E S E N T A :

LIBERTAD BECERRA AZUARA

TUTOR:
DR. HUGO ALBERTO RINCÓN MEJÍA

FACULTAD DE CIENCIAS
U.N.A.M.

2009

A Yolanda quién me enseñó que el amor es la acción más bella y sincera que se da cada día y cada instante, sin importar la distancia, el tiempo ni los obstáculos, que se da a todo lo que tiene vida. Te amo mamá. Sería imposible agradecerte todo lo que me has dado. Siempre está a mi lado la belleza de tus ojos y la hermosura de tu alma…

A Antero quién me enseñó que a pesar de todos los problemas que se presenten se sigue adelante con alegría y valor, sin olvidar nunca la razón. Eres de los hombres valientes, fieles, bondadosos y nobles, que hacen diferente este mundo, por suerte eres mi papá, mi ejemplo favorito. Ti amo.

# Agradecimientos

Quiero agradecer en primer lugar a todos mis maestros, de todos los niveles escolares, gracias a todo su esfuerzo logré esto…

A la UNAM, mi segundo hogar.

A mis padres, quienes anhelaban con este momento.

A mi asesor, Hugo Alberto Rincón Mejía, quién siempre ha tenido la paciencia de enseñarme una y otra vez, sin él esto hubiera sido imposible.

A José Ríos Montes, Alejandro Alvarado García, Ernesto Mayorga Saucedo y a Fernando Vilchis Montalvo por todas sus observaciones y opiniones sobre este trabajo.

Al José Lino Samaniego Mendoza, por todo el apoyo, buenos consejos, amistad y por su ejemplo. Gracias Lino por creer en mí, cuando ni siquiera yo misma lo hacía.

A Ana M. Guzmán Gómez, por brindarme el espacio donde comencé a escribir este trabajo y por recibirme con afecto.

A Ana Irene Ramírez Galarza, por sus enseñanzas tanto dentro como fuera del aula.

A Alejandro R. Garciadiego Dantán, por esas clases que me ayudaron a disfrutar las matemáticas como un producto humano, en un espacio y tiempo determinados, con una significación profunda.

A mis amigos, gracias a ustedes aprendí que no sólo los buenos momentos tienen minutos, sino que junto a ustedes cada minuto es un buen momento. Gracias por las risas, el cariño, las verdades y muchas cosas más. Ustedes me hacen sentir que este mundo es el mejor. Los quiero muchísimo.

# Índice general

# Introducción

El objetivo principal de la tesis es dar la demostración de la equivalencia entre el axioma de elección y la existencia de bases en espacios vectoriales. Para la demostración, que está contenida en el último capítulo, se requieren algunos conocimientos de Álgebra y de Teoría de Conjuntos.

La tesis está dividida en cuatro capítulos. El primero corresponde a la contrucción y a algunas propiedades del anillo de polinomios. Para la realización de esta parte, se utilizó el libro *Basic Algebra I* de Nathan Jacobson.

Para el segundo capítulo, se usó principalmente *Numbers, sets and axioms: the Apparatus of Mathematics* de Hamilton. El contenido va desde el concepto de relación y conjunto ordenado, hasta el desrarrollo de los números ordinales y cardinales.

En el tercer capítulo se dan algunas equivalencias del axioma de elección.

Terminamos con la demostración de la equivalencia entre el axioma de elección y la existencia de bases para los espacios vectoriales. Esto se basa en *Axiom of Choice* de Herrlich.

# Capítulo 1

# Polinomios.

## 1.1. Construcción y definiciones.

**Definición 1** *Si $X$ es un conjunto no vacío y $*$, $* : X \times X \to X$, es una operación definida en $X$.*

*1. $(X, *)$ es un **semigrupo** si $*$ es asociativa.*

*2. Un **monoide** es una terna ordenada $(X, *, e)$ tal que $(X, *)$ es un semigrupo y $e \in X$ es un neutro para la operación $*$.*

*3. Un **grupo** $(X, *, e)$ es un monoide en el que cada elemento tiene inverso.*

*4.- Un monoide o grupo es **conmutativo** si su operación es conmutativa.*

**Definición 2** *Un **anillo** es una quinteta ordenada $(R, +, \cdot, 0, 1)$ tal que:*

*1.- $(R, +, 0)$ es un grupo abeliano,*

*2.- $(R, \cdot, 1)$ es un monoide,*

*3.- se satisfacen las leyes distributivas:*

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (b + c) \cdot a &= b \cdot a + c \cdot a \end{aligned}$$

$\forall a, b, c \in R$.

*El elemento $1$ es llamado **unidad**.*

**Definición 3** *Un anillo $R$ es llamado **conmutativo** si $(R, \cdot, 1)$ es conmutativo.*

**Definición 4** *Si $R$ es un anillo conmutativo y $\mathbb{N}$ el conjunto de los números naturales,*

$$\mathbf{R}^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to R\}.$$

**Definición 5** *Si $f \in R^{\mathbb{N}}$, el **soporte** de $f$ es sop $(f) = \{i \in \mathbb{N} \mid f(i) \neq 0\}$.*

**Definición 6** $\mathbf{R}[x] = \mathbf{R}^{(\mathbb{N})} =: \left\{f \in R^{\mathbb{N}} \mid sop\ (f)\ \text{es finito}\right\}$.

**Definición 7** *La **suma** de dos elementos de* $R[x]$, $+ : R[x] \times R[x] \to R[x]$,

está dada por $(f+g)(i) = f(i) + g(i)$.

**Observación 1** *La suma está bien definida.*

**Demostración.** Si $i \in sop\,(f+g)$, entonces $f(i) + g(i) = (f+g)(i) \neq 0$. Además, $f(i) + g(i) \neq 0$, implica que $f(i) \neq 0$ o $g(i) \neq 0$. Pero $f(i) \neq 0$ o $g(i) \neq 0$, si y sólo si, $i \in sop\,(f)$ o $i \in sop\,(g)$. Entonces $sop\,(f+g) \subseteq sop\,(f) \cup sop\,(g)$. Como $sop\,(f)$ y $sop\,(g)$ son finitos, entonces $sop\,(f) \cup sop\,(g)$ es finito. Por lo tanto $sop\,(f+g)$ es finito. ■

**Definición 8** *Llamamos **cero** al elemento* $\bar{0} \in R[x]$ *tal que* $\bar{0}(i) = 0\ \forall i \in \mathbb{N}$.

Notemos que $sop\,(\bar{0}) = \emptyset$ que es finito.

**Proposición 1** $(R[x], +, \bar{0})$ *es un grupo abeliano.*

**Demostración.** Sea $i \in \mathbb{N}$, entonces
(1) $(f+g)(i) = f(i) + g(i) = g(i) + f(i) = (g+f)(i)$.
(2)

$$(f + (g+h))(i) = f(i) + (g+h)(i) = f(i) + (g(i) + h(i)) =$$

$$= (f(i) + g(i)) + h(i) = (f+g)(i) + h(i) = ((f+g)+h)(i).$$

(3) $\left(f + \bar{0}\right)(i) = f(i) + \bar{0}(i) = f(i) + 0 = f(i)$.
(4) Si $f \in R[x]$ entonces $\exists\ -f \in R[x]$ : que $(-f)(i) = -f(i)\ \forall i \in \mathbb{N}$. Así,

$$(f + (-f))(i) = f(i) + (-f)(i) = f(i) + (-f(i)) = 0.$$

Por lo tanto, $f + (-f) = \bar{0}$. Además, note que $sop\,(-f) = sop\,(f)$.
Esto, implica que $-f \in R[x]$.
$\therefore \left(R[x], +, \bar{0}\right)$ es un grupo abeliano. ■

**Definición 9** *El **producto** (o **multiplicación**) en* $R[x]$, $\bullet : R[x] \times R[x] \to R[x]$, $(f,g) \longmapsto f \bullet g : \mathbb{N} \to R$ *se da por*

$$(f \bullet g)(i) = p(i) = \sum_{j+k=i} f(j)\, g(k).$$

Si $f(i) = 0$ para $i > n$ y $g(j) = 0$ para $j > m$, entonces $p(k) = 0$ para $k > m + n$.

**Observación 2** *El producto está bien definido.*

**Demostración.** Si $i \in sop\,(f \bullet g)$, entonces $0 \neq (f \bullet g)(i) = \sum_{j+k=i} f(j)\, g(k)$.

Ahora, $0 \neq \sum_{j+k=i} f(j)\, g(k)$, implica que $j \in sop\ (f)$ y $k \in sop\ (g)$ para alguna $j$ y alguna $k$ tales que $j + k = i$. Además,

$$\{j + k \mid j \in sop\,(f)\,,\ k \in sop\,(g)\}$$

es finito pues $sop\ (f)$ y $sop\ (g)$ son finitos. Entonces

$$sop\,(f \bullet g) \subseteq \{j + k \mid j \in sop\,(f)\,,\ k \in sop\,(g)\}$$

$\therefore sop\,(f \bullet g)$ es finito. ■

**Nota 1** *Si $f,\ g \in \mathbf{R}^{\mathbb{N}}$, $f \cdot g : \mathbb{N} \to R$ dada por*

$$(f \cdot g)(i) = \sum_{j+k=i} f(j)\, g(k)\,,$$

*está bien definida porque, dado $i \in \mathbb{N}$, el conjunto*

$$\{(k, l) \in \mathbb{N} \times \mathbb{N} \mid k + l = i\}$$

*es finito así que es una suma finita de elementos de $R$.*

**Definición 10** *El elemento **uno** es el $\overline{1} \in R[x]$ tal que $\overline{1}(0) = 1$, $\overline{1}(i) = 0$ $\forall i \neq 0$.*

**Proposición 2** $\left(R[x]\,, \bullet, \overline{1}\right)$ *es un monoide conmutativo.*

**Demostración.** Sea $i \in \mathbb{N}$, entonces

(1) $(f \bullet g)(i) = \sum_{j+k=i} f(j)\, g(k) = \sum_{k+j=i} g(k)\, f(j) = (g \bullet f)(i)$.

(2)

$$\begin{aligned}((f \bullet g) \bullet h)(i) &= \sum_{j+k=i} (f \bullet g)(j)\, h(k) = \sum_{j+k=i} \Big( \sum_{l+m=j} f(l)\, g(m) \Big) h(k) = \\ &= \sum_{l+m+k=i} f(l)\, g(m)\, h(k) = \sum_{l+p=i} f(l) \Big( \sum_{m+k=p} g(m)\, h(k) \Big) = \\ &= \sum_{l+p=i} f(l)\, (g \bullet h)(p) = (f \bullet (g \bullet h))(i)\,.\end{aligned}$$

(3) $\left(\overline{1} \bullet f\right)(i) = \sum_{k+j=i} \overline{1}(k)\, f(j) = \overline{1}(0)\, f(i) = (1)\, f(i) = f(i)$.

$\therefore \left(R[x]\,, \bullet, \overline{1}\right)$ es un monoide conmutativo. ■

**Proposición 3** $\left(R[x]\,, +, \overline{0}, \bullet, \overline{1}\right)$ *es un anillo conmutativo.*

**Demostración.** $\left(R[x], +, \bar{0}\right)$ es un grupo abeliano por la Proposición 1.

Por la Proposición 2, $\left(R[x], \bullet, \bar{1}\right)$ es un monoide conmutativo.

Además, se valen las propiedades distributivas, porque

$$\begin{aligned}(f \bullet (g+h))(i) &= \sum_{k+j=i} f(j)(g+h)(k) = \sum_{k+j=i} f(j)(g(k)+h(k)) = \\ &= \sum_{k+j=i} (f(j)g(k)) + (f(j)h(k)) = \\ &= \sum_{k+j=i} f(j)g(k) + \sum_{k+j=i} f(j)h(k) = (f \bullet g)(i) + (f \bullet h)(i).\end{aligned}$$

$$\text{Y, } (g+h) \bullet f = f \bullet (g+h) = f \bullet g + f \bullet h = g \bullet f + h \bullet f.$$

$\therefore \left(R[x], +, \bar{0}, \bullet, \bar{1}\right)$ es un anillo conmutativo. ■

**Nota 2** *Cuando no exista posibilidad de confusión en el producto podemos prescindir de* $\bullet$*, es decir, basta escribir* $fg$ *en vez de* $f \bullet g$*.*

**Notación 1** *Por definición de* $R[x]$*, cada* $f \in R[x]$ *está determinada por una sucesión de casi puros ceros. Así, podemos expresar a* $f \in R[x]$ *como* $(f(0), f(1), ..., f(n), ...)$*.*

*Además, si denotamos* $f(i) = a_i$*, para* $i = 0, 1, 2, ..., n$*, la expresión de cada función* $f \in R[x]$ *puede ser* $(a_0, a_1, ..., a_n, ...)$*. Es decir* $f(n) = 0$ *para casi toda* $n$*.*

**Nota 3** *Las sucesiones* $(a_0, a_1, ..., a_i, ...)$ *y* $(b_0, b_1, ..., b_i, ...)$ *son vistos como iguales si y sólamente si* $a_i = b_i$ *para todo* $i$*.*

**Observación 3** $\mathbf{R}^{\mathbb{N}}$ *con las operaciones definidas como en el anillo* $R[x]$*. También resulta ser un anillo conmutativo con uno, ya que para todo* $i \in \mathbb{N}$*,* $(f+g)(i) = f(i) + g(i) \in R$*, y por lo tanto* $f + g$ *está bien definida; además por la nota 1 sabemos que el producto también está bien definido. Así que realizando las operaciones de forma puntual para cada* $i \in \mathbb{N}$*,* $\mathbf{R}^{\mathbb{N}}$ *es un anillo.*

**Definición 11** *Una aplicación* $\phi$ *de un anillo* $R$ *en un anillo* $R'$ *es un* ***morfismo de anillos*** *si:*

*1.* $\phi(a+b) = \phi(a) + \phi(b)$ $\forall a, b \in R$*, (se dice que* $\phi$ *respeta la suma).*

*2.* $\phi(ab) = \phi(a)\phi(b)$ $\forall a, b \in R$*, (se dice que* $\phi$ *respeta el producto).*

*3.* $\phi(1) = \phi(1')$*, donde* $1$ *e* $1'$ *son las unidades de* $R$ *y de* $R'$*, respectivamente.*

**Definición 12** *1.- Si* $\phi$ *es inyectiva decimos que* $\phi$ *es un* ***monomorfismo****.*

*2.- Si* $\phi$ *es suprayectiva decimos que* $\phi$ *es un* ***epimorfismo****.*

*3.- Si* $\phi$ *es biyectiva entonces* $\phi$ *se llama* ***isomorfismo.*** *Además, decimos que los anillos* $R$ *y* $R'$ *son* ***isomorfos****.*

**Notación 2** *Si $R$ y $R'$ son isomorfos, lo denotamos por $R \cong R'$.*

**Definición 13** *Si $\phi : R \to R'$ es un morfismo de anillos, entonces el* ***kernel*** *es*

$$\ker\ f = \{r \in R \mid f(r) = 0\}.$$

**Proposición 4** *Si $\phi : R \to R[x]$ se define por $a \longmapsto f_a$, donde $f_a(0) = a$ , $f_a(i) = 0\ \forall\ i \neq 0$, entonces $\phi$ es un monomorfismo.*

**Demostración.** $\phi$ respeta la suma, porque

$$f_{a+b}(0) = a + b = f_a(0) + f_b(0),$$

$$f_{a+b}(i) = 0 = 0 + 0 = f_a(i) + f_b(i)\ \ \forall i \neq 0.$$

Así, $\phi(a+b) = f_{a+b} = f_a + f_b = \phi(a) + \phi(b)$.
También, $\phi$ respeta el producto, pues

$$f_{ab}(0) = ab = f_a(0) f_b(0),$$

$$f_{ab}(i) = 0 = 0(0) = f_a(i) f_b(i)\ \ \forall i \neq 0.$$

Así, $\phi(ab) = f_{ab} = f_a f_b = \phi(a)\phi(b)$.
Además, $\phi$ respeta el 1, ya que $f_1(0) = 1$, $f_1(i) = 1\ \forall i \neq 0$, $f_1$ coincide con $\overline{1}$. Así, $\phi(1) = f_1 = \overline{1}$.
Entonces $\phi$ es un morfismo de anillos.
Por último, veremos que $\phi$ es inyectiva.
$\phi(a) = \phi(b) \iff f_a = f_b$. Pero, $f_a = f_b \iff (a, 0, 0, ..) = (b, 0, 0, ..)$.
Además, $(a, 0, 0, ..) = (b, 0, 0, ..) \iff a = b$. Así, $\phi$ es inyectiva.
$\therefore \phi$ es un monomorfismo. ■

**Nota 4** *Por la Proposición 4, identificamos $R$ con su imagen*

$$R \cong \phi(R) = \{(r, 0, 0, ...) \mid r \in R\} \subset R[x],$$

entonces $R \underset{anillo}{\leq} R[x]$.

**Definición 14** *Llamamos $x$ al elemento de $R[x]$ tal que $x(1) = 1$,*

$x(i) = 0\ \forall\ i \neq 1$, es decir, $x = (0, 1, 0, ...)$.

**Proposición 5** $x^n = (\underbrace{0, ..., 0, 1}_{n+1}, 0, ....)\ \forall n \geq 2$, *es decir,* $x^n\ (n) = 1$, $x^n(i) = 0$ $\forall i \neq n$.

**Demostración.** Por inducción sobre $n$.
**Base.** Para $n = 2$.
$\left(x^2\right)(2) = (x \bullet x)(2) = \sum_{j+k=2} x(j)\, x(k) = x(1)\, x(1) = 1 \cdot 1 = 1.$
$\left(x^2\right)(i) = (x \bullet x)(i) = \sum_{\substack{j+k=i \\ j \neq 1}} x(j)\, x(k) = 0 \ \forall i \neq 2.$
Entonces, $x^2 = (\underbrace{0, 0, 1}_{2+1=3}, 0, ....)$.
**Hipótesis de inducción.** Supongamos válido para $n$, $x^n(n) = 1$,
$x^n(i) = 0 \ \forall i \neq n$, demostraremos que la afirmación es válida para $n+1$.
$\left(x^{n+1}\right)(n+1) = (x^n x)(n+1) = \sum_{j+k=n+1} x^n(j)\, x(k) = x^n(n)\, x(1) = 1 \cdot 1$
$= 1.$
$\left(x^{n+1}\right)(i) = (x^n x)(i) = \sum_{\substack{j+k=i \\ j \neq n}} x^n(j)\, x(k) = 0 \ \forall i \neq n+1.$
$\therefore x^n = (\underbrace{0, ..., 0, 1}_{n+1}, 0, ....) \ \forall n \geq 2.$ ■

**Definición 15** $x^0 = (1, 0, ....)$.

**Proposición 6** *Si $a \in R$, entonces $ax^n = (\underbrace{0, ..., 0, a}_{n+1}, 0, ...)$ $\forall n \geq 0$, es decir,* $(ax^n)(n) = a$, $(ax^n)(i) = 0 \ \forall i \neq n$.

**Demostración.** Por inducción sobre $n$.
**Base.** Para $n = 0$.
$\left(ax^0\right)(0) = \sum_{j+k=0} a(j)\, x^0(k) = a(0)\, x^0(0) = a \cdot 1 = a.$
$\left(ax^0\right)(i) = \sum_{\substack{j+k=i \\ j \neq 0}} a(j)\, x^0(k) = 0 \ \forall i \neq 0.$
Por lo que la afirmación se cumple para $n = 0$.
**Hipótesis de inducción.** Supongamos válido para $n$.
$(ax^n)(n) = a$, $(ax^n)(i) = 0 \ \forall i \neq n$.
Para $n+1$, se vale al firmación porque

$$\left(ax^{n+1}\right)(n+1) = (ax^n)(x)(n+1) = \sum_{j+k=n+1} (ax^n)(j)\, x(k) =$$

$$= (ax^n)(n)\, x(1) = a \cdot 1 = a.$$

$\left(ax^{n+1}\right)(i) = (ax^n)(x)(i) = \sum_{\substack{j+k=i \\ j \neq n}} ax^n(j)\, x(k) = 0 \quad \forall i \neq n+1.$
$\therefore ax^n = (\underbrace{0, ..., 0, a}_{n+1}, 0, ...).$ ■

**Proposición 7** $(f(0), f(1), ..., f(n), 0, 0, ...) = f(0) + f(1)\, x + ... + f(n)\, x^n$.

**Demostración.** Como $f(i) \in R$, entonces $f(i)\,x^i = (\underbrace{0,...,0,f(i)}_{i+1},0,...)$ $\forall i \in \mathbb{N}$, por la Proposición 6. Entonces $(f(0), f(1), ..., f(n), 0, 0...) =$
$= (f(0)\,0,0,0,...) + (0, f(1), 0, ...) + \cdots + (0,0,..., f(n), 0, ...)$
$= f(0)\,(1,0,0,...) + f(1)\,(0,1,0,...) + \cdots + f(n)\,(0,0,...,1,0,...)$
$= f(0)\,x^0 + f(1)\,x^1 + f(2)\,x^2 + \cdots + f(n)\,x^n = f(0) + f(1)\,x + ... + f(n)\,x^n$.
■

**Definición 16** *$R[x]$ es el **anillo de polinomios** sobre $R$ en una variable $x$ y cada elemento de $R[x]$ se llama **polinomio** con coeficientes en $R$ en una variable $x$. Decimos que $R[x]$ es el anillo obtenido de adjuntar el elemento $x$ a $R$.*

**Notación 3** *La Proposición 7, permite escribir a un polinomio en la forma*

$$f = a_0 + a_1x + ... + a_nx^n = \sum_{i=0}^{n} a_ix^i$$

donde $a_i \in R$, $a_n \neq 0$ y $a_i = 0$ para $i \geq n+1$. Por costumbre, se escribe $f(x)$.

**Definición 17** *Si $f$ es un polinomio distinto de cero, el **grado** de $f$, es*

$$\text{grad}\ (f) = \text{máx}\ \{n \mid f(n) \neq 0\}.$$

**Definición 18** *Si $f(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$.*
***(1)** Llamamos a los $a_i$ los **coeficientes** de $f(x)$.*
***(2)** $a_0$ es el **término constante.***
***(3)** $a_n$ es el **coeficiente principal** si $n = \text{grad}\ (f)$.*
***(4)** Si $a_n = 1$, entonces $f(x)$ es llamado **mónico.***
***(5)** Un elemento de $R$ es un **polinomio constante.***

**Nota 5** *Si $f(x) \in R[x]$ y grad $(f) = n$, podemos escribir $f(x) = \sum_{i=0}^{n} a_ix^i$.*

**Observación 4** *Sean $f, g \in R[x]$ con grad $(f) = n$ y grad $(g) = m$. $f = g$ si y sólamente si $n = m$ y $a_i = b_i\ \forall i$.*

**Demostración.** $f = g \iff (a_0, a_1, ..., a_n, 0, 0, ...) = (b_0, b_1, ..., b_m, 0, 0, ...)$. Además, $(a_0, a_1, ..., a_n, 0, 0, ...) = (b_0, b_1, ..., b_m, 0, 0, ...) \iff a_i = b_i\ \ \forall i \in \mathbb{N}$.
$\therefore f = g \iff a_i = b_i\ \forall i$. ■

**Observación 5** *Si $R$ es un anillo conmutativo y si $f, g \in R[x]$, entonces*

$$f + g = 0\ \text{ó}\ \text{grad}\ (f+g) \leq \text{máx}\ \{\text{grad}\ (f),\ \text{grad}\ (g)\}.$$

**Demostración.** Si $f,\, g \in R[x]$ con grad $(f) = n$ y grad $(g) = m$. Supongamos sin pérdida de generalidad que $n \leq m$ y que $f + g \neq 0$.

$$(f+g)(i) = f(i) + g(i) = 0 + 0 = 0 \text{ si } i > m$$

$\therefore$ grad $(f+g) \leq$ máx $\{\text{grad}\,(f), \text{grad}\,(g)\}$. ■

**Observación 6** *Si $R$ es un anillo conmutativo y si $f, g \in R[x]$, $f \neq \bar{0}$, $g \neq \bar{0}$, entonces*

$$fg = \bar{0} \;\; o \;\; \text{grad} \;\; (fg) \leq \text{grad} \;\; (f) + \text{grad} \;\; (g).$$

**Demostración.** Si $f,\, g \in R[x]$ con grad $(f) = n$ y grad $(g) = m$. Supongamos que $fg \neq \bar{0}$. Como $f \neq \bar{0}$, $g \neq \bar{0}$, entonces $f(i) = 0$ para $i > n$ y $g(j) = 0$ para $j > m$, entonces por la Definición 9, $p(k) = 0$ para $k > m + n$. Esto significa que grad $(fg) \leq n + m =$ grad $(f) +$ grad $(g)$.

$\therefore fg = \bar{0}$ o grad $(fg) \leq$ grad $(f) +$ grad $(g)$. ■

## 1.2. Propiedad Universal del Anillo de Polinomios.

**Teorema 1** ***(Propiedad universal)***. *Sean $R$, $S$ anillos conmutativos, $u \in S$ y $\eta : R \to S$ un morfismo de anillos. Entonces $\exists!\ \eta_u : R[x] \to S$ morfismo de anillos tal que $\eta_u(x) = u$, y $\eta_u$ extiende a $\eta$.*

Decimos que $\eta$ tiene una y sólo una extensión a un morfismo $\eta_u$.
**Demostración.** Supongamos que $\exists\ \eta_u : R[x] \to S$ morfismo tal que
$\eta_u(x) = u$ y $\eta_u(a) = \eta(a) = a' \in S$, $\forall\ a \in R$.
Como $\eta_u(cd) = \eta_u(c)\,\eta_u(d)$, por ser $\eta_u$ un morfismo, tenemos

$$\eta_u(x^n) = \eta_u(\underbrace{x \cdots x}_{n}) = \underbrace{\eta_u(x) \cdots \eta_u(x)}_{n} = (\eta_u(x))^n = (u)^n.$$

Esto quiere decir, que $\eta_u(x^n) = u^n \quad \forall n \in \mathbb{N}$.
Si $f = \sum_{i=0}^{n} a_i x^i \in R[x]$,

$$\begin{aligned} \eta_u(f) &= \eta_u(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \eta_u\left(a_i x^i\right) = \sum_{i=0}^{n} \eta_u(a_i)\,\eta_u\left(x^i\right) = \\ &= \sum_{i=0}^{n} \eta(a_i)\,\eta_u\left(x^i\right) = \sum_{i=0}^{n} a_i' u^i \in S. \end{aligned}$$

Notemos que si se define $\eta_u(f) = \sum_{i=0}^{n} a_i' u^i \in S$, entonces se
satisfacen $\eta_u(x) = u$ y $\eta_u(a) = \eta(a) = a' \in S$, $\forall\ a \in R$.
Con esto obtenemos el morfismo de anillos.
Tomemos $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i \in R[x]$. Veremos que $\eta_u$ es un

morfismo de anillos.
Demostraremos que $\eta_u$ respeta el producto. Sabemos que $fg = \sum_{i=0}^{n+m} p_i x^i$ donde $p_i = \sum_{j+k=i} a_j b_k$. Entonces

$$\begin{aligned}\eta_u(fg) &= \eta_u(\sum_{i=0}^{n+m} p_i x^i) = \sum_{i=0}^{n+m} \eta_u\left(p_i x^i\right) = \sum_{i=0}^{n+m} \eta_u(p_i)\,\eta_u\left(x^i\right) = \\ &= \sum_{i=0}^{n+m} \eta(p_i)\,\eta_u\left(x^i\right) = \sum_{i=0}^{n+m} p_i' u^i, \text{ donde } p_i' = \sum_{j+k=i} a_j' b_k'.\end{aligned}$$

Por otro lado,

$$\eta_u(f)\,\eta_u(g) = \eta_u(\sum_{i=0}^{n} a_i x^i)\eta_u(\sum_{i=0}^{m} b_i x^i) = (\sum_{i=0}^{n} a_i' u^i)(\sum_{i=0}^{m} b_i' u^i) = \sum_{i=0}^{n+m} p_i' u^i.$$

Así, $\eta_u(fg) = \eta_u(f)\,\eta_u(g)$.
También $\eta_u$ respeta la suma. Como $f+g = \sum_{i=0}^{n} (a_i + b_i) x^i$, tenemos que

$$\eta_u(f+g) = \eta_u(\sum_{i=0}^{n} (a_i+b_i) x^i) = \sum_{i=0}^{n} \eta_u(a_i+b_i)\,\eta_u\left(x^i\right) =$$

$$= \sum_{i=0}^{n} (\eta_u(a_i) + \eta_u(b_i))\,\eta_u\left(x^i\right) = \sum_{i=0}^{n} \eta_u(a_i)\,\eta_u\left(x^i\right) + \eta_u(b_i)\,\eta_u\left(x^i\right) =$$

$$= \sum_{i=0}^{n} \eta_u(a_i)\,\eta_u\left(x^i\right) + \eta_u(b_i)\,\eta_u\left(x^i\right) = \sum_{i=0}^{n} a_i' u^i + b_i' u^i = \sum_{i=0}^{n} a_i' u^i + \sum_{i=0}^{n} b_i' u^i$$

$$= \eta_u(\sum_{i=0}^{n} a_i x^i) + \eta_u(\sum_{i=0}^{n} b_i x^i) = \eta_u(f) + \eta_u(g).$$

Así, $\eta_u(f+g) = \eta_u(f) + \eta_u(g)$.
Además, $\eta_u$ respeta el 1, pues para $1 \in R$, tenemos $\eta_u(1) = \eta(1) = 1'$.
Por lo anterior, $\eta_u : R[x] \to S$ es un morfismo de anillos tal que $\eta_u(x) = u$, y que extiende a $\eta$.
**Unicidad.** Supongamos que $\exists\ \gamma : R[x] \to S$ un morfismo con $\gamma \neq \eta_u$ tal que $\gamma(x) = u$. De $\eta_u(x) = u$ y $\gamma(x) = u$, tenemos que $\gamma(x) = \eta_u(x)$. Entonces $\gamma = \eta_u$, contradicción. Por lo tanto, $\eta_u$ es único.
$\therefore \exists!\ \eta_u : R[x] \to S$ morfismo tal que $\eta_u(x) = u$. ■

**Definición 19** *Llamamos **sustitución** de $u \in R$ en lugar de $x$ en $f$ ( o del valor de $f$ para $x = u$) a la aplicación del morfismo de $R[x]$ en $R$ que extiende la función identidad sobre $R$ y envía $x$ en $u$. Así, la imagen de un polinomio $f(x)$, bajo este homomorfismo se puede denotar por $f(u)$.*

**Definición 20** *$R[u]$ es el subanillo de $R$ generado por $R$ y $u$.*

**Proposición 8** *Si $R, S$ son anillos conmutativos y se cumple la propiedad universal, entonces $R[u] = \text{Im } \eta_u$.*

**Demostración.** $\text{Im } \eta_u = \{s \in S \mid s = \eta_u(f),\ f \in R[x]\}$.
($\subseteq$) Si $f \in R[u]$, entonces $f = \sum a_i u^i$, donde $a_i \in R$. Entonces

$$f = \sum a_i u^i = \eta_u(\sum a_i x^i) \in \text{Im}\, \eta_u.$$

($\supseteq$) Si $s \in S$, entonces $s = \eta_u(f)$, para $f \in R[x]$. Entonces

$$s = \eta_u(\sum a_i x^i) = \sum a_i u^i \in R[u].$$

$\therefore R[u] = \text{Im}\, \eta_u$. ■

**Definición 21** *Un **ideal** en un anillo conmutativo $R$ es un subconjunto $I$ tal que*
*a) $0 \in I$,*
*b) si $a, b \in I$, entonces $a + b \in I$,*
*c) si $a \in I$ y $r \in R$, entonces $ra \in I$.*

**Notación 4** *$I$ ideal de $R$ se denota por $I \underset{ideal}{\leq} R$.*

**Corolario 1** *$R[u] \cong R[x]/I$ donde $I$ es un ideal en $R[x]$ tal que $I \cap R = \langle 0 \rangle$.*

**Demostración.** Si $I = Ker\ \eta_u$, entonces $I \underset{ideal}{\leq} R[x]$. Además, como $\eta_{u|_R} = 1_R$ es la inclusión, tenemos que es mono, entonces $R \cap Ker\ \eta_u = \langle 0 \rangle$, es decir, $R \cap I = \langle 0 \rangle$. Así, por el Teorema fundamental sobre morfismos de anillos[1], tenemos $R[u] \cong R[x]/I$.
$\therefore R[u] \cong R[x]/I$. ■

**Observación 7** *El homomorfismo $f(x) \longmapsto f(u)$ es un monomorfismo si y sólo si $f(u) = 0$ implica que $f(x) = 0$, esto es, $a_0 + a_1 u + ... + a_n u^n = 0$ implica que cada $a_i = 0$, para $i \in \{1, ..., n\}$.*

**Definición 22** *Si $R \underset{anillo}{\leq} S$. Un elemento $u \in S$ se llama **algebraico** sobre $R$ si $f(u) = 0$ para algún $f \in R[x]$. Y si cumple con la observación 7 decimos que $u$ es **trascendente** sobre $R$. Si $R = \mathbb{Q}$ y $S = \mathbb{C}$, simplemente se habla de **números algebraicos** y **trascendentes.***

[1] Teorema fundamental sobre morfismos de anillos: Si $\eta$ es un morfismo de un anillo $R$ en un anilllo $R'$ y $K$ el kernel. Entonces $K$ es un ideal en $R$ y existe un único morfismo $\overline{\eta}$ de $R/K$ en $R'$ tal que $\eta = \overline{\eta}\ \upsilon$ donde $\upsilon$ es el morfismo natural de $R$ en $R/K$. Más aún, $\upsilon$ es un epimorfismo y $\overline{\eta}$ es un monomorfismo. Además, cualquier imagen de un morfismo de un anillo $R$ es isomorfa al anillo $R/K$.

**Ejemplo 1** *El número complejo* $\omega = -\frac{1}{2}+\frac{1}{2}\sqrt{3}i$ $\left(i=\sqrt{-1}\right)$ *es algebraico (sobre* $\mathbb{Q}$*).*

**Demostración.** Si $p(x) = x^2+x+1 \in \mathbb{Q}[x]$, entonces

$$\begin{aligned} p(\omega) &= \omega^2+\omega+1 = \left(-\frac{1}{2}+\frac{1}{2}\sqrt{3}i\right)^2+\left(-\frac{1}{2}+\frac{1}{2}\sqrt{3}i\right)+1 = \\ &= \frac{1}{4}-\frac{\sqrt{3}}{2}i-\frac{3}{4}+\frac{\sqrt{3}}{2}i+1 = -\frac{2}{4}-\frac{1}{2}+1 = 0. \end{aligned}$$

$\therefore \omega$ es algebraico sobre $\mathbb{Q}$. ■

**Definición 23** *Si* $R$ *es un anillo conmutativo y* $x$ *e* $y$ *son indeterminadas, tomando* $A = R[x]$*, podemos formar el anillo de polinomios* $A[y]$*. Este anillo se llama el* ***anillo de polinomios sobre*** $R$ ***en dos indeterminadas*** $x$ *e* $y$*, y se denota por* $R[x,y]$*. Así,* $R[x,y]$ *es el anillo de polinomios en* $y$ *con coeficientes que son polinomios en* $x$*.*

**Ejemplo 2** $ax^2+bxy+cy^2+dx+ey+f = cy^2+(bx+e)y+\left(ax^2+dx+f\right)$*, es un polinomio en* $y$ *con coeficientes en* $R[x]$*.*

**Definición 24** *Por inducción definimos el* ***anillo*** *conmutativo* $R[x_1,x_2,...,x_n]$*,* ***de polinomios sobre*** $R$ ***en*** $n$ ***indeterminadas*** $x_i$*:*

$$R[x_1,x_2,...,x_n] = (R[x_1,x_2,...,x_{n-1}])[x_n].$$

**Observación 8** *Por la construcción de* $R[x_1,x_2,...,x_n]$*, podemos decir que* $f \in (R[x_1,x_2,...,\overset{\wedge}{x_j},...,x_n])[x_j]$*, es un polinomio sobre* $R[x_1,x_2,...,\overset{\wedge}{x_j},...,x_n]$ *en la indeterminada* $x_j$*, para alguna* $j \in \{1,...,n\}$*, donde* $\overset{\wedge}{x_j}$ *significa que a la indeterminada* $x_j$ *se ha omitido en la anillo* $R[x_1,x_2,...,x_n]$*. Esto significa que* $R[x_1,x_2,...,\overset{\wedge}{x_j},...,x_n]$ *tiene* $n-1$ *indeterminadas.*

**Teorema 2** *Si* $R$ *es un anillo conmutativo y* $n \in \mathbb{N}$*, entonces existe un anillo* $R[x_1,x_2,...,x_n]$ *con la siguiente propiedad universal. Si* $S$ *es un anillo y* $\eta : R \to S$ *homomorfismo y* $f : \{1,2,...,n\} \to S$ *tal que* $f(i) = u_i$*, entonces existe una única extensión* $\eta_{u_1,...,u_n} : R[x_1,...,x_n] \to S$ *que envía* $x_i \longmapsto u_i$ $\forall i \in \{1,2,...,n\}$*.*

**Demostración.** Por inducción sobre $n$.

**Base.** Para $n=1$. $R[x_1]$ es el anillo de polinomios en una indeterminada $x_1$ sobre $R$. Por el Teorema 1, $\exists!$ $\eta_{u_1} : R[x_1] \to S$ morfismo que extiende $\eta$, tal que $\eta_{u_1}(x_1) = u_1$. Por lo que la afirmación se cumple para $n=1$.

**Hipótesis de Inducción.** Supongamos que $\exists!$ $\eta_{u_1,...,u_{n-1}} : R[x_1,...,x_{n-1}] \to S$ morfismo que extiende $\eta$, y envía $x_i \longmapsto u_i$ $\forall i \in \{1,2,...,n-1\}$, demostraremos que la afirmación se cumple para $n$. Por hipótesis de inducción y sustituyendo

en el Teorema 1, el anillo $R$ por $R[x_1, ..., x_{n-1}]$ ,y el morfismo $\eta$ por $\eta_{u_1,...,u_{n-1}}$, y como

$$R[x_1, ..., x_n] = R[x_1, ..., x_{n-1}][x_n],$$

encontramos el morfismo $\eta_{u_1,...,u_n} = \left(\eta_{u_1,...,u_{n-1}}\right) u_n$, que envía $x_n \longmapsto u_n$.

Por lo tanto, $\eta_{u_1,...,u_n} : R[x_1, ..., x_n] \to S$ es una extensión de $\eta$, tal que

$$x_i \longmapsto u_i \ \forall i \in \{1, 2, ..., n\}.$$

**UNICIDAD.** La unicidad de $\eta_{u_1,...,u_n}$ queda totalmente determinada por su imagen sobre los elementos $x_i$, $\forall i \in \{1, 2, ..., n\}$, que generan a $R[x_1, ..., x_n]$. ■

**Teorema 3** *Si $R[x_1, ..., x_n]$ y $\pi \in S_n$ es una permutación que actúa en $\{1, ..., n\}$, entonces existe un único automorfismo $\bar{\pi}$, que es la identidad sobre $R$ y tal que*

$$\bar{\pi}(x_i) = x_{\pi(i)}$$

$\forall i \in \{1, ..., n\}$.

**Demostración.** Sutituyamos en el Teorema 2, $S = R[x_1, ..., x_n]$, $u_i = x_{\pi^{-1}(i)}$ $\forall i \in \{1, ..., n\}$, y sea $\eta = 1_S \mid_R$, la restricción de la aplicación de la identidad $1_S$ en $R$.

Así, $\exists!\ \bar{\pi} = \eta_{u_1,...,u_n} : R[x_1, ..., x_n] \to R[x_1, ..., x_n]$ que es un endomorfismo que cumple con las hipótesis. ■

**Notación 5** *Si $(i) = (i_1, ..., i_n) \in \mathbb{N}^{(n)}$, esto es, una n-ada de enteros no negativos, entonces cualquier $f \in R[x_1, ..., x_n]$, tiene la forma*

$$f = \sum_{(i)}^{n} a_{(i)} x^{(i)},\ a_{(i)} \in R,$$

donde $x^{(i)} = x_1^{i_1} \cdots x_n^{i_n}$.

**Definición 25** *$x^{(i)} = x_1^{i_1} \cdots x_n^{i_n}$ es un **monomio.** Así un polinomio $f$ es una combinación lineal de monomios con coeficientes $a_{(i)}$ en $R$.*

**Observación 9** *A veces conviene consider al monomio como $x^{(i)} = \lambda x_1^{i_1} \cdots x_n^{i_n}$ donde $\lambda = a_{(i)} \in R$. Si llamamos $p_i = x^{(i)}$, entonces podemos escribir a $f$ de la siguiente forma*

$$f = \sum_{i=1}^{n} p_i.$$

**Observación 10** *Todos los coficientes $a_{(i)}$, a excepción de un número finito de ellos, son iguales a cero. Tenemos $(x_1^{i_1}\cdots x_n^{i_n})(x_1^{j_1}\cdots x_n^{j_n}) = x_1^{i_1+j_1}\cdots x_n^{i_n+j_n}$. Si $(i_1,...,i_n) \neq (j_1,...,j_n)$, entonces $x_1^{i_1}\cdots x_n^{i_n} \neq x_1^{j_1}\cdots x_n^{j_n}$. Ahora, dos polinomios $f, g \in R[x_1,...,x_n]$ son iguales si coinciden todos sus coeficientes para todos los monomios.*

**Observación 11** $f = \sum_{(i)}^{n} a_{(i)}x^{(i)} = 0 \Longleftrightarrow a_{(i)} = 0.$

**Definición 26** *El **grado del polinomio** $f$ **con relación** a $x_k$, es*

$$\text{grad}_{x_k}\ (f) = \text{grad}\ (f),$$

*donde $f \in (R[x_1, x_2, ..., \overset{\wedge}{x_j}, ..., x_n])[x_j]$, visto en la observación 8.*

**Ejemplo 3** *Si $f = 1 + x + xy^3 + x^2y^2$, entonces $\text{grad}_x\ (f) = 2$ y $\text{grad}_y\ (f) = 3$.*

**Definición 27** *El **grado total** $x_1^{i_1}\cdots x_n^{i_n}$ es*

$$\text{grad}\ (x_1^{i_1}\cdots x_n^{i_n}) = \sum_{j=1}^{n} i_j.$$

**Definición 28** *Si $f \in R[x_1,...,x_n]$, el **grado** de $f$, se define como*

$$\text{grad}\ (f) = \text{máx}\left\{m \mid m = \text{grad}\ \left(x_1^{i_1}\cdots x_n^{i_n}\right)\right\}.$$

**Observación 12** *Para cualquier $R[u_1,...,u_n]$ el morfismo $\eta_{u_1,...,u_n}$ de $R[x_1,...,x_n]$ en $R[u_1,...,u_n]$, es un isomorfismo si: $\sum_{(i)}^{n} a_{(i)}u^{(i)} = 0$ si y sólo si $a_{(i)} = 0$.*

**Definición 29** *Si $u_i$, para $i = 1, ...n$, satisfacen la Observación (12), decimos que $u_1, ..., u_n$ son **algebraicamente independientes sobre** $R$.*

**Observación 13** *Hasta ahora, hemos visto el caso en que $R$ es un anillo conmutativo. Sin embargo, las construcciones de $R[x]$ y $R[x_1,...,x_n]$ son válidas también para $R$ no necesariamente conmutativo. Al hacer la construcción de dichos conjuntos se satisfacen todas las condiciones de anillo, excepto la conmutatividad del producto. Por tanto, $R[x]$ y $R[x_1,...,x_n]$ son anillos no necesariamente conmutativos.*

**Proposición 9** *Si $R$ es un anillo, entonces $x_i \in C(R[x_1,...,x_n]), \forall i = 1, 2, ..., n$.*[2]

[2] $C(R) = \{r \in R \mid rx = xr\ \forall x \in R\}$ se llama el **centro** del anillo $R$.

**Demostración.** Por inducción sobre $n$.

**Base.** Para $n = 1$, veremos que $x \in C(R[x])$. Por definición de $x$, tenemos que $x(1) = 1$ y $x(i) = 0\ \forall i \neq 1$. Ahora, si $f \in R[x]$,entonces

$$\begin{aligned}(xf)(i) &= \sum_{j+k=i} x(j) f(k) = x(1) f(i-1) = (1) f(i-1) = f(i-1) \\ &= f(i-1)(1) = \sum_{k+j=i} f(k) x(1) = (fx)(i).\end{aligned}$$

Por lo tanto, $x \in C(R[x])$, es decir, la afirmación es válida para $n = 1$.

**Hipótesis de Inducción.** Supongamos válido para $n-1$,

$$\{x_1, ..., x_{n-1}\} \in C(R[x_1, ..., x_{n-1}]),$$

demostraremos la afirmación para $n$. Sustituyendo en el caso para $n = 1$, $R[x_1, ..., x_{n-1}]$ en vez de $R$ y $x$ por $x_n$, obtenemos que

$$x_n \in C(R[x_1, ..., x_{n-1}][x_n]).$$

Como $R[x_1, ..., x_{n-1}] \subseteq R[x_1, ..., x_n]$, entonces

$$C(R[x_1, ..., x_{n-1}]) \subseteq C(R[x_1, ..., x_n]).$$

Por esto y por hipótesis de inducción,

$$\{x_1, ..., x_{n-1}\} \subseteq C(R[x_1, ..., x_n]).$$

Entonces

$$\{x_1, ..., x_n\} = \{x_1, ..., x_{n-1}\} \cup \{x_n\} \in C(R[x_1, ..., x_n]).$$

$\therefore x_i \in C(R[x_1, ..., x_n])$, para $i = 1, 2, ...n$. ■

**Nota 6** *En la proposición no se supone que $R$ sea conmutativo.*

Los siguientes dos ejemplos son los análogos a los Teoremas 1 y 2, pero para anillos no conmutativos.

**Observación 14** *Para que se cumpla la propiedad universal, es necesario enviar a $x$ a algún elemento $u \in S$. Sabemos que al multiplicar $x$ conmuta con todo $f = (a_0, a_1, a_2, ...) \in R[x]$, en particular conmuta con todo $a_i \in R$. Entonces $\eta(a_i)$ debe conmutar con $u$, por tanto es necesario que $u \in C(\eta(R))$.*

**Ejemplo 4** *Si $R$ y $S$ son anillos, $\eta : R \to S$ morfismo, $u \in C(\eta(R)) \subseteq S$. Entonces $\exists!\ \eta_u : R[x] \to S$ tal que $\eta_u(x) = u$.*

**Demostración.** Si $A = \sum_{i=0}^{n} a_i x^i \in R[x]$, entonces $\eta_u(A) = \sum_{i=0}^{n} \eta(a_i) u^i = \sum_{i=0}^{n} a'_i u^i$.

Ahora, si $B = \sum_{i=0}^{n} b_i x^i \in R[x]$, se satisfacen los siguientes incisos:

i) $\eta_u(A+B) = \eta_u(\sum_{i=0}^{n}(a_i+b_i)x^i) = \sum_{i=0}^{n} \eta(a_i+b_i) u^i = \sum_{i=0}^{n} (\eta(a_i)+\eta(b_i)) u^i = \sum_{i=0}^{n} \left[\eta(a_i)u^i + \eta(b_i)u^i\right] = (\sum_{i=0}^{n} a'_i u^i) + (\sum_{i=0}^{m} b'_i u^i) = \eta_u(A) + \eta_u(B)$.

ii) $\eta_u(AB) = \eta_u(\sum_{i=0}^{n+m} p_i x^i)$, donde $p_i = \sum_{j+k=i} a_j b_k$, entonces

$$\eta_u(AB) = \sum_{i=0}^{n+m} \eta(p_i) u^i = \sum_{i=0}^{n+m} p'_i u^i.$$

Por otro lado,

$$\eta_u(A)\eta_u(B) = (\sum_{i=0}^{n} a'_i u^i)(\sum_{i=0}^{m} b'_i u^i).$$

Como $u^i \in C(\eta(R))$, entonces $\eta_u(A)\eta_u(B) = \sum_{i=0}^{n+m} p'_i u^i$.

Por lo tanto, $\eta_u(AB) = \eta_u(A)\eta_u(B)$.

iii) $\eta_u\left(\overline{1}\right) = \eta(1_S) = 1_S$.

Por (i), (ii) y (iii), $\eta_u$ es un morfismo de anillos.

Por último, supongamos que $\exists\ \gamma : R[x] \to S$ tal que $\gamma(x) = u$ y $\gamma \neq \eta_u$. Entonces $\gamma(x) = u = \eta_u(x)$, contradicción. Así que $\eta_u$ es único.

$\therefore \exists!\ \eta_u : R[x] \to S$ tal que $\eta_u(x) = u$. ■

**Ejemplo 5** *Para cualquier anillo $R$ y cualquier entero positivo $n$, $\exists$ un anillo $R[x_1, ..., x_n]$, con la siguiente propiedad: Si $S$ es cualquier morfismo de anillos $\eta : R \to S$, tal que $i \longmapsto u_i$ para $u_i \in C(\eta(R))$, para $i = 1, ..., n$, entonces $\exists!$ $\eta_{u_1 \cdots u_n} : R[x_1, ..., x_n] \to S$ tal que $x_i \longmapsto u_i$, $1 \leq i \leq n$.*

**Demostración.** Por inducción sobre $n$.

**Base.** Para $n = 1$. Por el ejemplo anterior, sabemos que $\exists!\ \eta_u : R[x] \to S$ tal que $\eta_u(x) = u$. Así que es válido para $n = 1$.

**Hipótesis de Inducción.** Supongamos válido para $n$, entonces

$\exists!\ \eta_{u_1 \cdots u_{n-1}} : R[x_1, ..., x_{n-1}] \to S$ tal que $x_i \longmapsto u_i$, $1 \leq i \leq n-1$.

Sustituyendo en la base, $R[x_1, ..., x_{n-1}]$ en vez de $R$ y $x$ por $x_n$, obtenemos

$\exists! \eta_{u_1 \cdots u_n} : R[x_1, ..., x_n] = R[x_1, ..., x_{n-1}][x_n] \to S$

tal que $x_i \longmapsto u_i$, $1 \leq i \leq n$. ■

**Ejemplo 6** *Si $R$ es un anillo conmutativo, $I \underset{ideal}{\leq} R$ y si $I[x_1, ..., x_n]$ denota el subconjunto de $R[x_1, ..., x_n]$ de polinomios con coeficientes contenidos en $I$. Entonces:*

**1)** $I[x_1,...,x_n] \underset{ideal}{\leq} R[x_1,...,x_n]$.

**2)** $R[x_1,...,x_n]/I[x_1,...,x_n] \cong (R/I)[y_1,...,y_n]$, donde $y_i$ son indeterminadas en $R/I$.

**Demostración.** Para ambos incisos usaremos inducción sobre $n$.

**1)**

**Base.** Para $n=1$, veremos que $I[x] \underset{ideal}{\leq} R[x]$.

i) Si $I \underset{ideal}{\leq} R$, entonces $0 \in I$. Así, $a_i = 0\ \forall i$, implica que $\sum a_i x^i = \bar{0}$. Entonces $\bar{0} \in I[x]$.

ii) Si $f = \sum a_i x^i$, $g = \sum b_i x^i \in I[x]$, entonces

$$h = f + g = \sum c_i x^i,$$

donde $c_i = a_i + b_i \in I$, porque $a_i, b_i \in I$. Así, $h \in I[x]$.

iii) Si $f = \sum a_i x^i \in I[x]$, $g = \sum b_j x^j \in R[x]$, entonces

$$h = fg = \sum c_k x^k,$$

donde $c_k = \sum_{i+j=k} a_i b_j$. Como $a_i \in I\ \forall i$ y $b_j \in R\ \forall j$, entonces $a_i b_j \in I$. Así, $c_k \in I[x]$, es decir, $h \in I[x]$.

$$\therefore I[x] \underset{ideal}{\leq} R[x].$$

**Hipótesis de Inducción.** Supongamos válido para $n-1$,

$$I[x_1,...,x_{n-1}] \underset{ideal}{\leq} R[x_1,...,x_{n-1}].$$

Por hipótesis de inducción, sustituyendo en la base, a $I$ por $I[x_1,...,x_{n-1}]$, la indeterminada $x$ por $x_n$ y $R[x_1,...,x_{n-1}]$ en vez de $R$, obtenemos

$$I[x_1,...,x_n] = I[x_1,...,x_{n-1}][x_n] \underset{ideal}{\leq} R[x_1,...,x_{n-1}][x_n] = R[x_1,...,x_n].$$

$$\therefore\ I[x_1,...,x_n] \underset{ideal}{\leq} R[x_1,...,x_n].$$

**2)**

**Base.** Para $n=1$, mostraremos que $R[x]/I[x] \cong (R/I)[y]$. Sea

$$\varphi : (R/I)[y] \to R[x]/I[x]$$

$$\sum (r_i + I) y^i \longmapsto \sum r_i x^i + I[x].$$

Veremos que $\varphi(A+B) = \varphi(A) + \varphi(B)\ \ \forall\ A, B \in (R/I)[y]$.

$$\varphi((\sum (a_i + I)y^i) + (\sum (b_i + I)y^i)) = \varphi(\sum (a_i + I + b_i + Iy^i)) =$$

$$= \varphi(\sum((a_i + b_i) + I)y^i) = \sum(a_i + b_i)x^i + I[x].$$

Por otro lado,

$$\begin{aligned}\varphi\left(\sum (a_i + I)\, y^i\right) + \varphi\left(\sum (b_i + I)\, y^i\right) &= \\ \left(\sum a_i x^i + I[x]\right) + \left(\sum b_i x^i + I[x]\right) &= \sum (a_i + b_i)\, x^i + I[x].\end{aligned}$$

Por lo tanto, $\varphi(A + B) = \varphi(A) + \varphi(B) \ \ \forall\ A, B \in (R/I)[y]$.
Demostraremos que $\varphi(AB) = \varphi(A)\varphi(B) \ \forall\ A, B \in (R/I)[y]$.

$$\varphi((\sum(a_i + I)y^i)(\sum(b_i + I)y^i)) = \varphi(\sum d_i y^i) =$$

$$= \varphi(\sum(c_i + I)y^i) = \sum c_i x^i + I[x]$$

donde $d_i = \sum\limits_{j+k=i} (a_j + I)(b_k + I) = \sum\limits_{j+k=i} a_j b_k + I = c_i + I$
Por otro lado,

$$\varphi(\sum(a_i + I)y^i)\varphi(\sum(b_i + I)y^i) = (\sum a_i x^i + I[x])(\sum b_i x^i + I[x]) =$$

$$= (\sum a_i x^i)(\sum b_i x^i) + I[x] = \sum c_i x^i + I[x].$$

Por lo tanto, $\varphi(AB) = \varphi(A)\varphi(B) \ \forall\ A, B \in (R/I)[y]$.
Además, $\varphi(1 + I) = \overline{1} + I[x]$.
Como consecuencia de lo anterior, $\varphi$ es un morfismo de anillos.
Ahora, veremos que $\varphi$ es inyectiva. Si $\sum a_i x^i + I[x] = \sum b_i x^i + I[x]$, entonces $\sum a_i x^i = \sum b_i x^i + p(x)$, para $p(x) \in I[x]$. Entonces $\sum (a_i - b_i)\, x^i = \sum a_i x^i - \sum b_i x^i = p(x) \in I[x]$. Como $p(x) \in I[x]$, debe de cumplirse que $a_i - b_i \in I$. Esto significa que $a_i - b_i = u_i$, donde $u_i \in I$. Así, $a_i = b_i + u$, para $u \in I$, lo que implica que $a_i + I = b_i + I$. Por lo que, $\sum (a_i + I)\, x^i = \sum (b_i + I)\, x^i$. Entonces $\varphi$ es inyectiva.
Por último checaremos que $\varphi$ es suprayectiva. Si $A = \sum r_i x^i + I[x] \in R[x]/I[x]$, entonces $\exists\ B \in (R/I)[y]$: que

$$\varphi(B) = \varphi\left(\sum (r_i + I)\, y^i\right) = \sum r_i x^i + I[x] = A.$$

Entonces $\varphi$ es suprayectiva.
Por lo tanto, $\varphi$ es un isomorfismo, es decir, $R[x]/I[x] \cong (R/I)[y]$.
**Hipótesis de Inducción.** Asumamos válido para $n - 1$,

$$R[x_1, ..., x_{n-1}]/I[x_1, ..., x_{n-1}] \cong (R/I)[y_1, ..., y_{n-1}].$$

Sustituyendo en la base**,** $R[x]$ por $R[x_1, ..., x_{n-1}]$, $I[x]$ por $I[x_1, ..., x_{n-1}]$ y $x$ por $x_n$, obtenemos que

$$R[x_1, ..., x_{n-1}][x_n]/I[x_1, ..., x_{n-1}][x_n]$$

es isomorfo a

$$(\ R[x_1,...,x_{n-1}]\diagup I[x_1,...,x_{n-1}])[y_n].$$

Entonces

$$R[x_1,...,x_n]\diagup I[x_1,...,x_n] \cong (\ R[x_1,...,x_{n-1}]\diagup I[x_1,...,x_{n-1}])[y_n].$$

Aplicando la hipótesis de inducción, tenemos que

$$\begin{array}{rcl}(\ R[x_1,...,x_{n-1}]\diagup I[x_1,...,x_{n-1}])[y_n] & \cong & (R\diagup I)[y_1,...,y_{n-1}][y_n] = \\ & & (R\diagup I)[y_1,...,y_n].\end{array}$$

$\therefore\ R[x_1,...,x_n]\diagup I[x_1,...,x_n] \cong (R\diagup I)[y_1,...,y_n]$. ■

**Ejemplo 7** $M_n(R[x_1,...,x_r]) \cong M_n(R)[x_1,...,x_r]$.

**Demostración.** Por inducción sobre $r$.
**Base.** Para $r=1$. Sea

$$\varphi : M_n(R)[x] \to M_n(R[x])$$

$$\sum_{s=0}^{k} A_s x^s \to B$$

donde $A_s \in M_n(R)$ para $s=1,...,k$, y además
$(B)_{l,m} = \sum\limits_{s=0}^{k} (A_s)_{l,m} x^s$, para $l,m \in \{1,...,n\}$.
i) $\varphi\left(\left(\sum A_i x^i\right)+\left(\sum B_i x^i\right)\right) = \varphi\left(\left(\sum (A_i+B_i)\, x^i\right)\right) = C$,
donde $(C)_{l,m} = \sum \left(\left(A_{i_{l,m}} + B_{i_{l,m}}\right) x^i\right)$.
Por otro lado,

$$\varphi\left(\sum A_i x^i\right) + \varphi\left(\sum B_i x^i\right) = D+E,$$

donde $(D+E)_{l,m} = \sum A_{i_{l,m}} x^i + \sum B_{i_{l,m}} x^i = \sum \left(\left(A_{i_{l,m}} + B_{i_{l,m}}\right) x^i\right)$.
Por lo que,

$$\varphi(P+Q) = \varphi(P) + \varphi(Q)\ \ \forall P,Q \in M_n(R)[x].$$

ii) $\varphi\left(\left(\sum A_i x^i\right)\left(\sum B_i x^i\right)\right) = \varphi\left(\left(\sum C_i x^i\right)\right) = C$,
donde $C_{i_{l,m}} = \sum\limits_{u_{l,m}+v_{l,m}=i_{l,m}} A_{u_{l,m}} B_{v_{l,m}}$.
Entonces

$$(C)_{a,b} = \left(A_{u_{l,m}} B_{v_{l,m}}\right)_{a,b} = \sum_{z=1}^{k} A_{u_{a,z}} B_{v_{z,b}}.$$

Por otro lado,

$$\varphi\left(\sum A_i x^i\right)\varphi\left(\sum B_i x^i\right) = DE = F,$$

donde $(D)_{l,m} = \sum A_{i_{l,m}} x^i$, $(E)_{l,m} = \sum B_{i_{l,m}} x^i$.
Entonces $F = \sum C_{i_{l,m}} x^i$ donde $C_{i_{l,m}} = \sum_{u_{l,m}+v_{l,m}=i_{l,m}} A_{u_{l,m}} B_{v_{l,m}}$.

Entonces

$$\left(A_{u_{l,m}} B_{v_{l,m}}\right)_{a,b} = \sum_{z=1}^{k} A_{u_{a,z}} B_{v_{lz,b}} = (C)_{a,b}\,.$$

Así, $\varphi(PQ) = \varphi(P)\,\varphi(Q)\ \forall\ P, Q \in M_n(R)[x]$.
iii) $\varphi\left(I_{M_n(R)[x]}\right) = B$,
Si $l = m$, entonces $(B)_{l,m} = (I_n)_{l,m} = \overline{1}$.
Si $l \neq m$, entonces $(B)_{l,m} = (O)_{l,m} = 0$.
Entonces, $B = 1_{M_n(R[x])}$.
Así, por (i), (ii) y (iii), $\varphi$ es un morfismo de anillos.
iv) Veremos que $\varphi$ es inyectiva.

$$A = \varphi\left(\sum L_i x^i\right) = \varphi\left(\sum M_i x^i\right) = B \Longleftrightarrow (A)_{l,m} = (B)_{l,m}\,.$$

Pero, $(A)_{l,m} = (B)_{l,m} \Longleftrightarrow \sum L_{i_{l,m}} x^i = \sum M_{i_{l,m}} x^i$. Además, $\sum L_{i_{l,m}} x^i = \sum M_{i_{l,m}} x^i \Longleftrightarrow L_{i_{l,m}} = M_{i_{l,m}}$. Por lo tanto $L = (L)_{l,m} = (L)_{l,m} = M$.
Así, $\varphi$ es inyectiva.
v) Ahora, si $B \in M_n(R[x])$, se cumple $(B)_{l,m} = \sum A_{i_{l,m}} x^i$ entonces $\exists$ $P = \sum A_i x^i \in M_n(R)[x]$ tal que $\varphi(P) = B$. Por lo tanto, $\varphi$ es suprayectiva.
Entonces por (iv) y (v), $\varphi$ es biyectiva.

$$\therefore M_n(R[x]) \cong M_n(R)[x]\,.$$

**Hipótesis de Inducción.** Supongamos válido para $r-1$,

$$M_n(R[x_1, ..., x_{r-1}]) \cong M_n(R)[x_1, ..., x_{r-1}]\,.$$

Sustituyendo en la base, $R[x_1, ..., x_{r-1}]$ en vez de $R$ y $x$ por $x_r$, obtenemos

$$M_n(R[x_1, ..., x_r]) = M_n(R[x_1, ..., x_{r-1}][x_r]) \cong M_n(R[x_1, ..., x_{r-1}])[x_r]\,.$$

Aplicando la hipótesis de inducción, tenemos

$$M_n(R[x_1, ..., x_{r-1}])[x_r] \cong M_n(R)[x_1, ..., x_{r-1}][x_r] = M_n(R)[x_1, ..., x_r]\,.$$

$\therefore M_n(R[x_1, ..., x_r]) \cong M_n(R)[x_1, ..., x_r]$. ■

**Ejemplo 8** *Si $R$ es un anillo conmutativo y $R[[x]]$ es el conjunto de las sucesiones en $R$, es decir, $(a_0, a_1, a_2, ...)$, para $a_i \in R$. $R[[x]]$ se llama el* ***anillo de las series de potencias ( enteras) formales.*** *Un elemento de $R[[x]]$ se denota por $f(x) = \sum_{i\geq 0} a_i x^i$. Las operaciones con las series de potencias formales de $R[[x]]$ se efectúan con las mismas reglas que para las operaciones con polinomios:*

$$\left(\sum a_i x^i\right) + \left(\sum b_i x^i\right) = \sum (a_i + b_i)\, x^i,$$

$$\left(\sum a_i x^i\right)\left(\sum b_j x^j\right) = \sum c_k x^k$$

donde $c_k = \sum_{i+j=k} a_i b_j$.

**Teorema 4** $\left(R\left[[x]\right], +, \bar{0}, \cdot, \bar{1}\right)$ *es un anillo conmutativo.*

**Demostración. Nota:** Por la observación 3 podemos concluir que $\left(R\left[[x]\right], +, \bar{0}, \cdot, \bar{1}\right)$ es un anillo conmutativo. Sin embargo, se realiza explícitamente, a continuación.

Primero veremos que $\left(R\left[[x]\right], +, \bar{0}, \right)$ es un grupo abeliano.

i) $((\sum a_i x^i) + (\sum b_i x^i)) + (\sum c_i x^i) = (\sum (a_i + b_i)x^i) + \sum b_i x^i$
$= \sum((a_i + b_i) + c_i)x^i = \sum(a_i + (b_i + c_i))x^i = \sum a_i x^i + (\sum(b_i + c_i)x^i)$
$= \sum a_i x^i + ((\sum b_i x^i) + (\sum c_i x^i))$.

ii) $(\sum a_i x^i) + (\sum b_i x^i) = \sum(a_i + b_i)x^i = \sum(b_i + a_i)x^i = (\sum b_i x^i) +$
$(\sum a_i x^i)$.

iii) $(\sum a_i x^i) + \bar{0} = \sum(a_i + 0)x^i = \sum a_i x^i$.

iv) Si $\sum a_i x^i \in R\left[[x]\right]$, entonces $\exists - \sum a_i x^i := \sum(-a_i)x^i \in R\left[[x]\right]$, tal que $(\sum a_i x^i) + (-\sum a_i x^i) = (\sum a_i x^i) + (\sum(-a_i)x^i) = \sum(a_i + (-a_i))x^i$
$= \sum(0)x^i = \bar{0}$.

Entonces $\left(R\left[[x]\right], +, \bar{0}, \right)$ es un grupo abeliano.

Ahora, veremos que $\left(R\left[[x]\right], \cdot, \bar{1}\right)$ es un monoide conmutativo.

i) $((\sum a_i x^i)(\sum b_j x^j))(\sum c_l x^l) = (\sum d_k x^k)(\sum c_l x^l) = \sum e_m x^m$
donde $d_k = \sum_{i+j=k} a_i b_j$ y $e_m = \sum_{k+l=m} d_k c_l = \sum_{k+l=m} (\sum_{i+j=k} a_i b_j) c_l = \sum_{i+j+l=m} a_i b_j c_l$.

Por otro lado,

$$(\sum a_i x^i)((\sum b_j x^j)(\sum c_l x^l)) = (\sum a_i x^i)(\sum f_{\tilde{n}} x^{\tilde{n}}) = \sum h_p x^p$$

donde $f_{\tilde{n}} = \sum_{j+l=\tilde{n}} b_j c_l$ y
$h_p = \sum_{i+\tilde{n}=p} a_i f_{\tilde{n}.} = \sum_{i+\tilde{n}=p} a_i (\sum_{j+l=\tilde{n}} b_j c_l) = \sum_{i+j+l=p} a_i b_j c_l$.
Por lo anterior, concluimos que $m = p$ y $e_m = h_p$.
Entonces

$$((\sum a_i x^i)(\sum b_j x^j))(\sum c_l x^l) = (\sum a_i x^i)((\sum b_j x^j)(\sum c_l x^l)).$$

ii) $\left(\sum a_i x^i\right)\left(\sum b_j x^j\right) = \left(\sum c_k x^k\right)$ donde $c_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i$. Entonces

$$\sum c_k x^k = (\sum b_j x^j)(\sum a_i x^i).$$

iii) $(\sum a_i x^i)(\bar{1}) = \sum c_k x^k$ donde $c_k = \sum_{i+j=k} a_i \bar{1}_j$.

Si $k = i$, entonces $c_i = \sum_{\substack{i+j=k \\ j=0}} a_i \bar{1}_j = a_i \bar{1}_0 = a_i\,(1) = a_i$.

Si $k \neq i$, entonces $c_i = \sum\limits_{\substack{i+j=k \\ j\neq 0}} a_i \bar{1}_j = 0$.

Entonces

$$\sum c_k x^k = \sum a_i x^i.$$

Por lo tanto, $\left(R\left[[x]\right], \cdot, \bar{1}\right)$ es un monoide conmutativo.

Por último, comprobaremos las leyes distributivas.
$\sum a_i x^i((\sum b_j x^j) + (\sum c_j x^j)) = \sum a_i x^i(\sum (b_j + c_j)x^j) = \sum d_k x^k$,
donde $d_k = \sum\limits_{i+j=k} a_i(b_j + c_j) = \sum\limits_{i+j=k} a_i b_j + \sum\limits_{i+j=k} a_i c_j$.
Por otro lado,

$$(\sum a_i x^i)(\sum b_j x^j) + (\sum a_i x^i)(\sum c_j x^j) = \sum e_k x^k + \sum h_k x^k,$$

donde $e_k = \sum\limits_{i+j=k} a_i b_j$ y $h_k = \sum\limits_{i+j=k} a_i c_j$, entonces $e_k + h_k = d_k$.
Así, $\sum a_i x^i((\sum b_j x^j) + (\sum c_j x^j)) = (\sum a_i x^i)(\sum b_j x^j) + (\sum a_i x^i)(\sum c_j x^j)$.
Por lo anterior y por la conmutatividad del producto, tenemos

$$((\sum b_j x^j) + (\sum c_j x^j))(\sum a_i x^i) = (\sum a_i x^i)((\sum b_j x^j) + (\sum c_j x^j)) =$$

$$= (\sum a_i x^i)(\sum b_j x^j) + (\sum a_i x^i)(\sum c_j x^j) =$$

$$= (\sum b_j x^j)(\sum a_i x^i) + (\sum c_j x^j)(\sum a_i x^i).$$

Por lo que se satisfacen las leyes distributivas.
$\therefore \left(R\left[[x]\right], +, \bar{0}, \cdot, \bar{1}\right)$ es un anillo conmutativo. ■

**Definición 30** *$R\left[[x]\right]$ se llama el* ***anillo de polinomios de las series de potencias en una indeterminada.***

**Observación 15** $R[x] \underset{anillo}{\leq} R\left[[x]\right]$.

**Demostración.** Por las definiciones de $R[x]$ y $R\left[[x]\right]$, tenemos que $R[x] \subseteq R\left[[x]\right]$. Como $R[x]$ es un anillo bajo las mismas operaciones que $R\left[[x]\right]$, y el neutro aditivo y multiplicativo son los mismos, entonces $R[x] \underset{anillo}{\leq} R\left[[x]\right]$. ■

**Ejemplo 9** *Si $M$ es un monoide, $R$ un anillo conmutativo y*

$$R[M] = \{f : M \to R \mid f(m) = 0 \text{ para casi toda } m\}.$$

*Definamos adición, multiplicación, $\bar{0}$ y $\bar{1}$ en $R[M]$ por*

$$(f+g)(m) = f(m) + g(m)$$

$$(f \cdot g)(m) = \sum_{pq=m} f(p)\, g(q)$$

$$\overline{0}(m) = 0$$

$$\overline{1}(1) = 1,\ \overline{1}(m) = 0 \text{ si } m \neq 1.$$

Entonces se cumplen los siguientes afirmaciones:

**1.** $R[M]$ es un anillo.
**2.** Si $A = \{a' \in R[M] \mid a'(1) = a,\ a'(m) = 0 \text{ si } m \neq 1\}$, entonces

$$A \underset{anillo}{\leq} R[M] \text{ y } A \cong R.$$

**3.** Si $B = \{m' \in R[M] \mid m'(m) = 1,\ m'(n) = 0 \text{ si } n \neq m\}$, entonces

$$B \underset{monoide}{\leq} R[M] \text{ y } B \cong M.$$

**4.** $R \subseteq C(R[M])$.
**5.** Si $f \in R[M]$ entonces $f = \sum_i r_i m_i'$, $r_i \in R$, $m_i \in M$.
**6.** $\sum_i r_i m_i' = \overline{0} \Longleftrightarrow r_i = 0$.
**7**. Si $\sigma : R \to S$ morfismo de anilllos tal que $\sigma(R) \subseteq C(S)$,
y $\tau : M \to S$ es un morfismo de monoides, entonces $\exists! \gamma : R[M] \to S$
morfismo de anillos que cumple $\gamma_{|_R} = \sigma$ y $\gamma_{|_M} = \tau$.

**Demostración. 1.** Primero veremos que $(R[M], +, \overline{0})$ es un grupo aditivo.
a) $((f+g)+h)(m) = (f+g)(m) + h(m) = (f(m) + g(m))\, h(m) =$
b) $f(m) + (g(m) + h(m)) = f(m) + (g+h)(m) = (f + (g+h))(m)$.
c) $(f+g)(m) = f(m) + g(m) = g(m) + f(m) = (g+f)(m)$.
$(\overline{0} + f(m) = \overline{0}(m) + f(m) = 0 + f(m) = f(m)$.
d) Si $f \in R[M]$ entonces $\exists\, -f \in R[M]$: que $(-f)(m) = -f(m)$, $((-f)+f)(m) = (-f)(m) + f(m) = -f(m) + f(m) = 0$.

Así, $\left(R[M], +, \overline{0}\right)$ es un grupo aditivo.

Ahora, checaremos que $\left(R[M], \cdot, \overline{1}\right)$ es un monoide.

a)

$$\begin{aligned}((fg)h)(m) &= \sum_{pq=m} (fg)(p)\, h(q) = \sum_{pq=m} \Big(\sum_{lr=p} f(l)\,(g)\,(r)\Big) h(q) = \\ &= \sum_{lrq=m} f(l)\, g(r)\, h(q) = \sum_{lw=m} f(l) \Big(\sum_{rq=w} g(r)\, h(q)\Big) = \\ &= \sum_{lw=m} f(l)\,(gh)(w) = (f(gh))(m).\end{aligned}$$

b) $(f\bar{1})(m) = \sum_{pq=m} f(p)\,\bar{1}(q) = f(m)\,\bar{1}(1) = f(m)(1) = f(m)$.

$\left(\bar{1}f\right)(m) = \sum_{pq=m} \bar{1}(p)\ f(q) = \bar{1}(1)\ f(m) = f(m)(1) = f(m)$.

Por esto, $\left(R[M], \cdot, \bar{1}\right)$ es un monoide.

Por último, mostraremos que se satisfacen las leyes distributivas.

a)

$$\begin{aligned}(f(g+h))(m) &= \sum_{pq=m} f(p)(g+h)(q) = \sum_{pq=m} f(p)(g(q)+h(q)) = \\ &= \sum_{pq=m} f(p)g(q) + f(p)h(q) = \sum_{pq=m} f(p)g(q) + \\ \sum_{pq=m} f(p)h(q) &= (fg)(m) + (fh)(m) = (fg+fh)(m).\end{aligned}$$

b)

$$\begin{aligned}((g+h)f)(m) &= \sum_{pq=m} (g+h)(p)f(q) = \sum_{pq=m} (g(p)+h(p))f(q) \\ &= \sum_{pq=m} (g(p)f(q)+h(p)f(q)) = \sum_{pq=m} g(p)f(q) + \sum_{pq=m} h(p)f(q) \\ &= (gf)(m) + (hf)(m) = (gf+hf)(m).\end{aligned}$$

$$\therefore \left(R[M], +, \bar{0}, \cdot, \bar{1}\right) \text{ es un anillo.}$$

**2.**

Sea $\alpha : R \to R[M]$ tal que $r \longmapsto r'$.

Antes de continuar, hay que destacar dos observaciones:

Primera: $r_1' r_2' = (r_1 r_2)'$.

Porque

$(r_1' r_2')(1) = \sum_{pq=1} r_1'(p)\, r_2'(q) = r_1'(1)\, r_2'(1) = (r_1)(r_2) = r_1 r_2 = (r_1 r_2)'(1)$,

$(r_1' r_2')(m) = \sum_{pq=m} r_1'(p)\, r_2'(q) = r_1'(1)\, r_2'(m) = (r_1)(0) = 0 = (r_1 r_2)'(m)$

$\forall m \neq 1$.

Segunda Observación: $(r_1 + r_2)' = r_1' + r_2'$.

Porque

$(r_1 + r_2)'(1) = r_1 + r_2 = (r_1')(1) + (r_2')(1) = (r_1' + r_2')(1)$,

$(r_1 + r_2)'(m) = 0 = (r_1')(m) + (r_2')(m) = (r_1' + r_2')(m) \quad \forall m \neq 1$.

Entonces $\alpha$ satisface los siguientes incisos.

(a) $\alpha(r_1 + r_2) = (r_1 + r_2)' = r_1' + r_2' = \alpha(r_1) + \alpha(r_2)$,

(b) $\alpha(r_1 r_2) = (r_1 r_2)' = r_1' r_2' = \alpha(r_1)\,\alpha(r_2)$,

(c) $\alpha(1) = 1'$,

Por (a), (b) y (c), $\alpha$ es un morfismo de anillos.

También, $\alpha$ es inyectiva, ya que, si $r_1 \neq r_2$, implica que

$r_1' \neq r_2'$ $(r_1'(1) = r_1 \neq r_2 = r_2'(1))$.

Además, como $\alpha(R) \underset{anillo}{\leq} R[M]$ y $\alpha(R) = A$, entonces $\alpha$ es biyectiva.

$$\therefore R \cong A \text{ y } A \underset{anillo}{\leq} R[M].$$

**3**.
Sea $\beta : M \to R[M]$ que envía $m \longmapsto m'$.
Notemos que $m_1' m_2' = (m_1 m_2)'$.

Ya que

$$\begin{aligned}(m_1' m_2')(m_1 m_2) &= \sum_{pq=m_1 m_2} m_1'(p)\, m_2'(q) = \sum_{pq=m_1 m_2} m_1'(m_1)\, m_2'(m_2) = 1 \cdot 1 \\ &= 1 = (m_1 m_2)'(m_1 m_2).\end{aligned}$$

Si $n \neq m_1 m_2$ entonces $(m_1' m_2')(n) = \sum_{pq=n} m_1'(p)\, m_2'(q) = \sum_{\substack{pq=n \\ q \neq m_2}} m_1'(m_1)\, m_2'(q)$

$= 1 \cdot 0 = 0 = (m_1 m_2)'(n)$
Así, tenemos que $\beta$ es un morfismo de monoides, porque:
i) $\beta(m_1 m_2) = (m_1 m_2)' = m_1' m_2' = \beta(r_1)\beta(r_2)$,
ii) $\beta(1) = 1'$.
Además, $\beta$ es inyectiva, pues si $m_1' = m_2'$, entonces
$m_1 = m_2$ $(1 = m_1'(m_1) = m_2'(m_1) \Leftrightarrow m_1 = m_2)$.
Y, como $\beta(M) \underset{monoide}{\leq} R[M]$ y $\beta(M) = B$ entonces $\beta$ es biyectiva.

$$\therefore B \cong M \text{ y } B \underset{monoide}{\leq} R[M].$$

**4.**
Por **2,** $R \cong A$ entonces basta mostrar que $A \subseteq C(R[M])$.
Si $a \in A$, $f \in R[M]$, entonces

$$\begin{aligned}(af)(m) &= \sum_{pq=m} a(p)f(q) = a(1)f(m) = af(m) = \\ &= f(m)a = f(m)a(1) = \sum_{pq=m} f(p)a(1) = (fa)(m).\end{aligned}$$

$$\therefore R \subseteq C(R[M]).$$

**5.**
Si $f \in R[M]$ tal que $sop\ f = \{m_1, m_2, ..., m_n\}$, entonces $f = \sum_i r_i m_i = \sum_i r_i' m_i' = \sum_i f(m_i)' m_i'$. Ahora,

$$(\sum_{i=1}^{n} f(m_i)' m_i')(m_j) = \sum_{i=1}^{n} f(m_i)(m_i'(m_j)) = f(m_j)(1) = f(m_j).$$

Además,

$$(\sum_{i=1}^{n} f\left(m_i\right)' m_i'\left(u\right)) = \sum_{i=1}^{n} f\left(m_i\right)\left(m_i'\left(u\right)\right) = 0 \quad \forall u \notin sopf.$$

$$\therefore f = \sum_i r_i m_i', \ r_i \in R, \ m_i \in M.$$

**6.**

$(\Longleftarrow)$ Si $r_i = 0 \ \forall i$, entonces $f(m) = (\sum_i r_i m_i')(m) = r_i m_i'(m) = (0)(m_i'(m)) = 0 \ \forall m$. Así, $\sum_i r_i m_i' = \bar{0}$.

$(\Longrightarrow)$ Si $\sum_i r_i m_i' = \bar{0}$, entonces $(\sum_i r_i m_i')(m) = 0 \ \forall m$. Así, $\sum_i r_i\left(m_i'\left(m_j\right)\right) = 0$. Entonces $r_j = r_j(1) = 0 \ \forall j$. Por lo tanto, $r_i = 0 \ \forall i$.

$$\therefore \sum_i r_i m_i' = \bar{0} \Longleftrightarrow r_i = 0.$$

**7.**

Sea $\gamma : R[M] \to S$ tal que $f = \sum_i r_i m_i \longmapsto \sum_i \sigma\left(r_i\right)\tau\left(m_i\right)$.

Veremos que $\gamma$ cumple con las condiciones de morfismo.

Si $f = \sum_i r_i m_i$, $g = \sum_j a_j m_j \in R[M]$.

(i)

$$\begin{aligned}
\gamma(fg) &= \gamma((\sum_i r_i m_i)(\sum_j a_j m_j)) = \gamma(\sum_k (\sum_{m_i m_j = m_k} r_i a_j m_k)) = \\
&= \sum_k (\sum_{m_i m_j = m_k} \sigma(r_i a_j)\tau(m_k)) = \sum_k (\sum_{m_i m_j = m_k} \sigma(r_i)\sigma(a_j)\tau(m_k)) \\
&= \sum_k (\sum_{m_i m_j = m_k} \sigma(r_i)\sigma(a_j)\tau(m_i)\tau(m_j)).
\end{aligned}$$

Por otro lado,

$$\begin{aligned}
\gamma(f)\gamma(g) &= (\sum_i \sigma\left(r_i\right)\tau\left(m_i\right))(\sum_j \sigma\left(a_j\right)\tau\left(m_j\right)) = \\
&= \sum_k (\sum_{m_i m_j = m_k} \sigma\left(r_i\right)\tau\left(m_i\right)\left(\sigma\left(a_j\right)\tau\left(m_j\right)\right)) = \\
&= \sum_k (\sum_{m_i m_j = m_k} \sigma(r_i)\sigma(a_j)\tau(m_i)\tau(m_j)).
\end{aligned}$$

Entonces, $\gamma(fg) = \gamma(f)\gamma(g)$.

(ii) $\gamma(f+g) = \gamma(\sum_i r_i m_i + \sum_j a_j m_j) = \gamma(\sum_k l_k m_k) = \sum_k \sigma\left(l_k\right)\tau\left(m_k\right)$

para $k = i + j$, $l_k \in \{r_i, a_j\}$, $m_k \in \{m_i, m_j\}$.

Por otro lado,

$$\begin{aligned}\gamma(f)+\gamma(g) &= \gamma(\sum_i r_i m_i)+\gamma(\sum_j a_j m_j)= \\ &= (\sum_i \sigma(r_i)\tau(m_i))+(\sum_j \sigma(a_j)\tau(m_j))=\sum_k \sigma(l_k)\tau(m_k)\end{aligned}$$

para $k=i+j$, $l_k \in \{r_i, a_j\}, m_k \in \{m_i, m_j\}$.
Así, $\gamma(f+g)=\gamma(f)+\gamma(g)$.
(iii) $\gamma\left(\overline{1}\right)=\gamma(1)=\gamma((1)(1))=\sigma(1)\tau(1)=(1_S)(1_S)=1_S$.
Por tanto, $\gamma$ es un morfismo de anillos.
Por último, mostraremos que $\gamma$ es único.
Supongamos que $\exists\ \theta : R[M]\to S$, $\gamma\neq\theta$, con $\theta(f)=\sum_i \sigma(r_i)\tau(m_i)$. Pero $\gamma(f)=\sum_i \sigma(r_i)\tau(m_i)$, entonces $\theta(f)=\gamma(f)$, así, $\theta=\gamma$, contradicción. ■

**Definición 31** *Si $M$ es un grupo, $R[M]$ es llamado el **álgebra de grupo de** $M$ sobre $R$.*

**Ejemplo 10** *Sea $R$ un anillo y sea $\mathbb{N}^{(r)}$ un monoide conmutativo con $r$ generadores $x_i$. Entonces $R[\mathbb{N}^{(r)}]$ es isomorfo a $R[x_1,...,x_r]$, para $x_i$ indeterminadas, $1\leq i\leq r$.*

**Demostración.** Si $\{M_i\}_{i\in I}$, $M_i$ monoide $\forall i$ y el producto como $\prod_i\{M_i\}=\{f: I\to \cup_i\{M_i\} \mid f(i)\in M_i\}$. Definamos la operación binaria, $\cdot$, en $\prod_i\{M_i\}$ por $(f\cdot g)(i)=f(i)g(i)$, y la unidad 1, como $(1)(i)=1_i$. Veremos que $(\prod_i\{M_i\},\cdot,1)$ es un monoide.
(i)

$$\begin{aligned}((f\cdot g)\cdot h)(i) &= (f\cdot g(i))h(i)=(f(i)g(i))h(i)\\ &= f(i)(g(i)h(i))=f(i)(g\cdot h)(i)=(f\cdot(g\cdot h))(i).\end{aligned}$$

(ii) $(f\cdot 1)(i)=f(i)1(i)=f(i)1_i=f(i)$, $(1\cdot f)(i)=1(i)f(i)=1_i f(i)=f(i)$ $\forall\ f\in\prod_i\{M_i\}$.

$$\therefore (\prod_i\{M_i\},\cdot,1) \text{ es un monoide.}$$

Notemos las siguientes observaciones:
1) Si $M_i$ es conmutativo $\forall i$ entonces $(\prod_i\{M_i\},\cdot,1)$ es un monoide conmutativo. Porque $(f\cdot g)(i)=f(i)g(i)=g(i)f(i)=(g\cdot f)(i)$.
2) Si $M_i=M$ entonces $\prod_i\{M_i\}=M^I$.
3) En particular $\mathbb{N}^r$ es un monoide conmutativo pues $\mathbb{N}$ es un monoide conmutativo.
Definimos el **coproducto** de la siguiente forma $\coprod_i\{M_i\}=\{f\in\prod_i\{M_i\} \mid f(i)=1_i \text{ para casi toda } i\}$.

4) Si $M_i = M$ entonces $\coprod_i \{M_i\} = M^{(I)}$.

5) $\mathbb{N}^{(r)}$ es un monoide conmutativo con $r$ generadores. Además de las observaciones anteriores, sabemos que:

(i) $R[M] = \left\{ f \in R^M \mid f(m) = 0 \text{ para casi toda } m \right\}$.

(ii) $R[x_1, x_2] = (R[x_1])[x_2]$.

(iii) $R[x] = R^{(\mathbb{N})}$.

(iv) $R[x_1, x_2] = (R[x_1])^{(\mathbb{N})} = (R^{(\mathbb{N})})^{(\mathbb{N})} = R^{(\mathbb{N}\times\mathbb{N})} = R^{(\mathbb{N}^2)}$.

Para demostrar el ejemplo aplicaremos inducción sobre r:

**Base.** Si $r = 1$. Entonces$R[\mathbb{N}] = \left\{ f \in R^{\mathbb{N}} \mid f(m) = 0 \text{ para casi toda } m \right\}$ y $R[x] = \left\{ f \in R^{\mathbb{N}} \mid sop\ f \text{ es finito} \right\}$. Así, $R[x] = R[\mathbb{N}]$.

Por lo tanto, $R[x] \cong R[\mathbb{N}]$.

Antes de proseguir, mostraremos que para $r = 2$ tenemos que $R\left[\mathbb{N}^2\right] \cong R[x_1, x_2]$.

Sea $\varphi : R\left[\mathbb{N}^2\right] \to \left(R^{(\mathbb{N})}\right)^{(\mathbb{N})}$ que envía $g \longmapsto \overline{g}$ por medio de $\left(\overline{g}(i)\right)(j) := g(i,j)$.

Veremos que $\varphi$ es un morfismo de anillos.

(i)

$$\left(\left(\overline{f+g}\right)(i)\right)(j) = (f+g)(i,j) = f(i,j) + g(i,j) =$$

$$= \left(\overline{f}(i)\right)(j) + \left(\overline{g}(i)\right)(j) = \left(\overline{f}(i) + \overline{g}(i)\right)(j) = \left(\left(\overline{f} + \overline{g}\right)(i)\right)(j).$$

$$\therefore \left(\overline{f+g}\right)(i) = \overline{f}(i) + \overline{g}(i) \text{ pues es válido } \forall j$$

$$\therefore \overline{f+g} = \overline{f} + \overline{g} \text{ pues es válido } \forall i$$

(ii)

$$\begin{aligned}
\left(\left(\overline{fg}\right)(i)\right)(j) &= (fg)(i,j) = \sum_{(k,l)+(s,t)=(i,j)} f(k,l)\, g(s,t) = \\
&= \sum_{k+s=i} \Big( \sum_{l+t=j} \left(\overline{f}(k)\right)(l) \left[\left(\overline{g}(s)\right)(t)\right] \Big) = \\
&= \sum_{k+s=i} \left(\overline{f}(k)\, \overline{g}(s)\right)(j) = \left(\left(\overline{f}\,\overline{g}\right)(i)\right)(j).
\end{aligned}$$

$$\therefore \left(\overline{fg}\right)(i) = \left(\overline{f}\,\overline{g}\right)(i) \quad \text{pues es válido } \forall j$$

$$\therefore \overline{fg} = \overline{f}\,\overline{g} \text{ pues es válido } \forall i.$$

(iii) También se cumple que $\varphi(1) = \overline{1}$, ya que

$$\left(\overline{1}(i)\right)(j) = 1(i,j) = \begin{cases} 0 \text{ si } (i,j) \neq (0,0) \\ 1 \text{ si } (i,j) = (0,0) \end{cases}.$$

$$\therefore \varphi \text{ es un homomorfismo de anillos.}$$

Mostraremos que $\varphi$ tiene inversa.

Sea $\varphi^{-1} : (R^{(\mathbb{N})})^{(\mathbb{N})} \longrightarrow R[\mathbb{N}^2]$ tal que $f' \longmapsto f$ donde $f(i,j) := (\ f'(i))(j)$.
$f'(i,j) = (f'(i))\,(j) = f(i,j)$.
Por otro lado $(g'(i))(j) = g'(i,j) = (g(i))(j)$.

$$\therefore \varphi \text{ tiene inversa.}$$

$$\therefore \varphi \text{ es biyectiva.}$$

$$\therefore\ R[\mathbb{N}^2] \cong R[x_1, x_2].$$

**Hipótesis de inducción.** Supongamos válido para $r-1$.

$$R\left[x_1, ..., x_{r-1}\right] \cong R\left[\mathbb{N}^{(r-1)}\right],$$

veremos que la afirmación es válida para $r$.
Si en la base sustituimos $R$ por $R\left[x_1, ..., x_{r-1}\right]$ y $x$ por $x_r$, obtenemos

$$R\left[x_1, ..., x_r\right] = \left(R\left[x_1, ..., x_{r-1}\right]\right)\left[x_r\right] \cong \left(R\left[x_1, ..., x_{r-1}\right]\right)\left[\mathbb{N}\right].$$

Además por hipótesis de inducción, tenemos que

$$\left(R\left[x_1, ..., x_{r-1}\right]\right)\left[\mathbb{N}\right] \cong R\left[\mathbb{N}^{(r-1)}\right]\left[\mathbb{N}\right].$$

Sin embargo, por las observaciones anteriores, sabemos que

$$\left(R\left[\mathbb{N}^{(r-1)}\right]\right)\left[\mathbb{N}\right] = \left\{f \in \left(R\left[\mathbb{N}^{(r-1)}\right]\right)^{(\mathbb{N})} \mid f\left(m\right) = 0 \text{ para casi toda } m\right\}.$$

Por la observación 5 inciso (iv), $\left(R\left[\mathbb{N}^{(r-1)}\right]\right)^{(\mathbb{N})} = R^{\mathbb{N}^{(r)}}$.
Entonces
$\left(R\left[\mathbb{N}^{(r-1)}\right]\right)\left[\mathbb{N}\right] = \left\{f \in \left(R\left[\mathbb{N}^{(r-1)}\right]\right)^{(\mathbb{N})} \mid f\left(m\right) = 0 \text{ para casi toda } m\right\}$
$= \left\{f \in R^{\mathbb{N}^{(r)}} \mid f\left(m\right) = 0 \text{ para casi toda } m\right\} = R\left[\mathbb{N}^{(r)}\right]$.
Entonces,

$$\left(R\left[x_1, ..., x_{r-1}\right]\right)\left[\mathbb{N}\right] \cong R\left[\mathbb{N}^{(r)}\right].$$

Por lo tanto,
$R\left[x_1, ..., x_r\right] \cong \left(R\left[x_1, ..., x_{r-1}\right]\right)\left[\mathbb{N}\right] \cong R\left[\mathbb{N}^{(r)}\right]$. ■

## 1.3. Algunas Propiedades de los Anillos de Polinomios.

**Definición 32** *Un anillo $R$ es llamado un* ***dominio*** *si el conjunto $R^{\cdot}$ de elementos no cero de $R$ es un submonoide de $(R, \cdot, 1)$.*

**Proposición 10** *Si $D$ es un dominio, $f, g \in D[x] \setminus \{\bar{0}\}$, entonces*

$$\text{grad}\ \ (fg) = \text{grad}\ \ (f) + \text{grad}\ \ (g).$$

**Demostración.** Si $f = \sum a_i x^i, g = \sum b_j x^j \in D[x]$, con grad $(f) = n$ y grad $(g) = m$, entonces $a_n \neq 0$ y $b_m \neq 0$. Como $a_n, b_m \in D$, no son divisores de cero, $a_n b_m \neq 0$. Por lo tanto, grad $(fg) = n + m =$ grad $(f) +$ grad $(g)$. ■

**Teorema 5** *Si $D$ es un dominio, entonces $D[x_1, ..., x_n]$ es un dominio. Además, las unidades de $D[x_1, ..., x_n]$ son las unidades de $D$.*

**Demostración.** Por inducción sobre $n$.

**Base.** Para $n = 1$, se considera $D[x]$. Si $f(x) = \sum a_i x^i$, $g(x) = \sum b_j x^j \in D[x]$, tal que $f(x) g(x) = \bar{0}$. Por la Proposición 10,

$$0 = \text{grad } (\bar{0}) = \text{grad } (fg) = \text{grad } (f) + \text{grad } (g).$$

Como grad $(f)$, grad $(g) \in \mathbb{N}$, entonces grad $(f) = 0 =$ grad $(g)$. Esto implica que $f(x), g(x) \in D$, es decir, $f(x) = a_0$ y $g(x) = b_0$, para $a_0, b_0 \in D$. Así, tenemos que $a_0 \cdot b_0 = 0$, lo que implica que $a_0 = 0$ o $b_0 = 0$ ya que $D$ es un dominio. Entonces $f(x) = \bar{0}$ o $g(x) = \bar{0}$. Por lo tanto, $D[x]$ es un dominio.

Ahora, si $f(x)$ es una unidad en $D[x]$, entonces existe $g(x) \in D[x]$ tal que $f(x) g(x) = 1$. Esto implica que grad $(f) \cdot$ grad $(g) = 0$,

así que el grad $(f) = 0$ o el grad $(g) = 0$. Entonces $f(x) = d_1$ y $g(x) = d_2$, donde $d_1, d_2 \in D$, tales que $d_1 d_2 = 1$.Así, si $f(x)$ es una unidad en $D[x]$, entonces $f(x) \in D$ es una unidad en $D$, al igual que su inversa.

Por otro lado, si $d_1$ es una unidad en $D$, entonces existe $d_2 \in D$ tal que $d_1 d_2 = 1$. Como $D \hookrightarrow D[x]$, entonces existen $f(x), g(x) \in D[x]$ tales que $f(x) = d_1$ y $g(x) = d_2$, que satisfacen que $1 = d_1 d_2 = f(x) g(x)$. Entonces $d_1 = f(x)$ es una unidad en $D[x]$.

Por tanto, las unidades en $D[x]$ son la unidades en $D$.

**Hipótesis de Inducción.** Supongamos que $D[x_1, ..., x_{n-1}]$ es un dominio y que sus unidades son las unidades de $D$.

Si en la base sustituimos $D$ por $D[x_1, ..., x_{n-1}]$, y, $x$ por $x_n$, obtenemos que $[Dx_1, ..., x_{n-1}][x_n]$ es un dominio y como $D[x_1, ..., x_{n-1}][x_n] = D[x_1, ..., x_n]$, hemos terminado.

Por lo tanto $D[x_1, ..., x_n]$ es un dominio y las unidades de $D[x_1, ..., x_n]$ son las unidades de $D$. ■

**Teorema 6** ***(Algoritmo de la división).*** *Si $R$ es un anillo conmutativo. Si $f(x), g(x) \in R[x]$, $g(x) \neq \bar{0}$, el* grad $(g) = m$ *y $b_m$ es el coeficiente principal de $g(x)$. Entonces $\exists\ k \in \mathbb{N}$, $q(x), r(x) \in R[x]$ con* $0 \leq$ grad $(r) <$ grad $(g)$ *o $r(x) = \bar{0}$, tal que*

$$b_m^k\ f(x) = q(x) g(x) + r(x).$$

**Demostración.** Por casos:

**(a)** Si grad $(f) <$ grad $(g)$, entonces $f(x) = \bar{0} \cdot g(x) + f(x)$, es decir, $q(x) = \bar{0}$, $r(x) = f(x)$.

**(b)** Si $m = \text{grad}\,(g) \leq \text{grad}\,(f) = n$ y $a_n$ es el coeficiente principal de $f(x)$. Sea

$$b_m\ f(x) - a_n x^{n-m} g(x) = f_1(x)\ \ldots\ (*)$$

Los coeficientes principales correspondientes a $x^n$ en $b_m\ f(x)$ y $a_n x^{n-m} g(x)$ son iguales: $a_n b_m$. Por esto,

$$\text{grad}(f_1(x)) = \text{grad}(b_m f(x) - a_n x^{n-m} g(x)) < n.$$

Usaremos inducción sobre el grado de $f$.

**Base.** Si $n = 0$, como $0 = n \geq m$, implica que $m = 0$, es decir,

$g(x) = b_0$ para algún $b_0 \in R$. Entonces $r(x) = \overline{0} = f_1(x)$, $k = 1$ y $q(x) = a_0$, así

$$b_0\ f(x) = q(x)\, g(x) + r(x) = a_0\ g(x) + \overline{0}.$$

**Hipótesis de inducción.** Suponemos que $\exists\ k_1 \in \mathbb{N}$, $q_1(x)$, $r(x) \in R[x]$ con grad $(r) <$ grad $(g)$,

$$b_m^{k_1}\ f_1(x) = q_1(x)\, g(x) + r(x)$$

Como

$$b_m^{k_1+1}\ f(x) = b_m^{k_1}(b_m\ f(x)).$$

Aplicando la ecuación (*), obtenemos

$$\begin{aligned} b_m^{k_1+1}\ f_1(x) &= b_m^{k_1}\left(f_1(x) + a_n x^{n-m} g(x)\right) = \\ & \quad b_m^{k_1}\ f_1(x) + b_m^{k_1}\ a_n x^{n-m} g(x). \end{aligned}$$

Así, por la ecuación (*) y por la hipótesis de inducción, tenemos que

$$\begin{aligned} b_m^{k_1+1}\ f_1(x) &= b_m^{k_1}\ a_n x^{n-m} g(x) + q_1(x)\, g(x) + r(x) = \\ & \quad g(x)\,(b_m^{k_1}\ a_n x^{n-m} + q_1(x)) + r(x). \end{aligned}$$

donde $q(x) = b_m^{k_1}\ a_n x^{n-m} + q_1(x)$.

$\therefore\ b_m^k\ f(x) = q(x)\, g(x) + r(x)$. ■

**Corolario 2** ***(Teorema del Residuo).*** *Si $f(x) \in R[x]$ y $a \in R$, entonces* $\exists!$ *$q(x) \in R[x]$ tal que*

$$f(x) = (x-a)\, q(x) + f(a).$$

**Demostración.** Si $f(x) \in R[x]$ y $g(x) = x - a \in R[x]$, por el Teorema 6 $\exists\ k \in \mathbb{N}$, $q(x)$, $r(x) \in R[x]$ con grad $(r) <$ grad $(g)$ tal que

$$f(x) = (1)^k\ f(x) = q(x)\,(x-a) + r(x).$$

$1 =$ grad $(g) >$ grad $(r)$. Entonces grad $(r) = 0$. Por lo tanto $r(x) = r \in R$. Esto implica que

$$f(x) = (x-a)\, q(x) + r.$$

Entonces $f(a) = (a-a)\,q(a) + r = r$. Así,

$$f(x) = (x-a)\,q(x) + f(a).$$

Por último, supongamos que $q(x)$ no es único, entonces $\exists\ q_1(x) \in R[x]$, $q(x) \neq q_1(x)$, tal que $f(x) = (x-a)\,q_1(x) + f(a)$. Entonces

$$(x-a)\,q(x) + f(a) = (x-a)\,q_1(x) + f(a).$$

Así, $(x-a)\,(q(x) - q_1(x)) = (x-a)\,q(x) - (x-a)\,q_1(x) = \bar{0}$.

Como $(x-a) \neq \bar{0}$, entonces $q(x) - q_1(x) = \bar{0}$, es decir, $q(x) = q_1(x)$, absurdo.

Por lo tanto, $q(x)$ es único.

$\therefore \exists!\ q(x) \in R[x]$ tal que $f(x) = (x-a)\,q(x) + f(a)$. ■

**Corolario 3** ***(Teorema del Factor).*** $(x-a) \mid f(a)$ *($(x-a)$ es un factor de* $f(x) \Longleftrightarrow f(a) = 0$*).*

**Demostración.** ($\Longrightarrow$) Si $(x-a) \mid f(x)$, entonces $f(x) = q(x)\,(x-a)$, para alguna $q(x) \in R[x]$. Por otro lado, por el Corolario 2, $\exists!\ q(x) \in R[x]$ tal que $f(x) = (x-a)\,q(x) + f(a)$. Entonces $q(x)\,(x-a) = (x-a)\,q(x) + f(a)$.

Por lo tanto, $f(a) = 0$.

($\Longleftarrow$) Supongamos que $f(a) = 0$.

Por el Corolario 2, $\exists!\ q(x) \in R[x]$ tal que $f(x) = (x-a)\,q(x) + f(a)$. Entonces

$f(x) = (x-a)\,q(x) + 0 = f(x) = (x-a)\,q(x)$.

Así, $(x-a) \mid q(x)$.

$\therefore (x-a) \mid f(a)$. ■

**Definición 33** *Si $R$ es una anillo conmutativo y $a \in R$, entonces el ideal $I = \{ra \mid r \in R\}$, se llama* ***ideal principal generado por*** *$a$ y se denota por $\langle a \rangle$. Un ideal $I$ de $R$ es un* ***ideal principal*** *si $I = \langle a \rangle$ para alguna $a \in R$.*

**Definición 34** *Un dominio $D$ es un* ***Dominio de Ideales Principales (DIP)*** *si cada ideal $I$ de $D$ es principal.*

**Teorema 7** *Si $F$ es un campo entonces $F[x]$ es un DIP.*

**Demostración.** Si $F$ es un campo entonces $F[x]$ es un dominio, por el Teorema 5. Ahora, si $I \underset{ideal}{\leq} F[x]$, tenemos los siguientes casos:

**(i)** $I = 0$ implica que $I = \left\langle \bar{0} \right\rangle$.

**(ii) Si** $I \neq 0$, entonces $\exists\ g(x) \in I$, $g(x) \neq \bar{0}$, así, si defino el conjunto

$$A = \left\{ h(x) \in I \mid h(x) \neq \bar{0} \right\},$$

entonces $A \neq \emptyset$.

Sea $g(x) \in I$ tal que grad $(g) = men\ \{\text{grad}\ (h) \mid h \in A\}$. Si $f(x) \in I$, entonces $f(x) \in F[x]$, aplicando el algoritmo de la división obtenemos $f(x) = q(x)\,g(x) + r(x)$ donde grad $(r) <$ grad $(g)$ o $r(x) = \overline{0}$. Como $I$ es un ideal y $f(x)$, $g(x) \in I$, entonces $r(x) = f(x) - q(x)\,g(x) \in I$.

Ahora, si $r(x) \neq \overline{0}$, entonces $r(x) \in A$ tal que grad $(r) <$ grad $(g)$, absurdo.

Entonces $r(x) = \overline{0}$, así $f(x) = q(x)\,g(x)$.

Por lo tanto cada elemento de $I$ es un múltiplo de $g(x)$, es decir, $I = \langle g(x) \rangle$.

$\therefore F[x]$ es un DIP. ■

**Definición 35** *Si $F$ es un campo. El campo de fracciones de $F[x]$, denotado por $F(x)$, es llamado el* ***campo de funciones racionales*** *sobre $F$.*

Si $F$ es un campo, entonces los elementos de $F(x)$ tienen la forma $f(x) \diagup g(x)$, donde $f(x)$, $g(x) \in F[x]$ y $g(x) \neq \overline{0}$.

**Observación 16** *Si $F$ es un campo, tenemos el epimorfismo $f(x) \to f(u)$ de $F[x]$ a $F[u]$, cuyo kernel es un ideal $I$ tal que $I \cap F = \langle 0 \rangle$. Así, $I = \langle g(x) \rangle$ pero $g(x)$ no es una unidad pues $I \cap F = \langle 0 \rangle$. Entonces $g(x) = 0$ o* grad $(g) > 0$. *En el primer caso $I = \langle 0 \rangle$, así el epimorfismo es un isomorfismo y $u$ es trascendente sobre $F$. Si* grad $(g) > 0$, *asumimos que es el generador mónico de $I$.*

**Definición 36** *Un polinomio $g(x)$ es* ***el polinomio mínimo sobre*** *$F$ de el elemento (algebraico) $u$, si satisface el segundo caso de la Observación 16.*

**Definición 37** *Si $F$ es un campo. Un polinomio no constante $f(x) \in F[x]$ es* ***irreducible sobre*** *$F$ si $f(x)$ no puede expresarse como el producto $g(x)\,h(x)$ de dos polinomios $g(x)$ y $h(x)$ en $F[x]$, ambos de grado menor que el grado de $f(x)$.*

**Observación 17** *Por el Teorema 5, las unidades en $F[x]$ son precisamente los elementos diferentes de cero de $F$. Así, podemos definir un polinomio irreducible $f(x)$, como un polinomio no constante, tal que si $f(x) = g(x)\,h(x)$ en $F[x]$, entonces $g(x)$ es unidad o $f(x)$ es unidad.*

**Definición 38** *Una* ***raíz*** *de $f(x)$* ***en*** *$F[x]$ en $F$ es un elemento $u \in F$ tal que $f(u) = 0$.*

**Lema 1** *Son equivalentes para cada anillo conmutativo $R \neq 0$ :*

*i) $R$ es un campo.*

*ii) Los únicos ideales de $R$ son $\{0\}$ y $R$.*

**Demostración.** (i)$\Longrightarrow$(ii)

Si $R$ es un campo, sabemos que $\{0\} \underset{ideal}{\leq} R$.

Supongamos que $\{0\} \neq I \underset{ideal}{\leq} R$.

Si $a \in I$, $a \neq 0$, entonces $1 = aa^{-1} \in I$. Pero, si $1 \in I$, entonces

$x1 = x \in I \ \forall \ x \in R$, es decir, que el único ideal que contiene al 1 es $R$.
Por lo tanto, $I = R$

$$\therefore \{0\} \text{ y } R \text{ son los únicos ideales de } R.$$

(ii)$\Longrightarrow$(i)
Si $R$ es un anillo conmutativo $\neq 0$, cuyos únicos ideales son $\{0\}$ y $R$.
Si $0 \neq a \in R$, entonces $\langle a \rangle \neq \{0\}$, entonces $\langle a \rangle = R$. Así, $1 \in \langle a \rangle$,
entonces hay un $x \in R$ tal que $ax = 1$. Esto significa que cada elemento de $R$ diferente de cero es invertible.
$\therefore R$ es un campo. ■

**Teorema 8** *Si $u$ es algebraico sobre $F$, $F$ campo, con polinomio mínimo $g(x)$. Entonces $F[u]$ es un campo si $g(x)$ es irreducible en $F[x]$ , es decir, no puede escribirse como $g(x) = f(x)h(x)$ donde* grad $(f) > 0$ *y* grad $(h) > 0$. *En otras palabras, si $g(x)$ es reducible entonces $F[u]$ no es un dominio.*

**Demostración.** Por la Propiedad Universal $\exists!\ \eta_u : F[x] \to F[u]$, si $I = \ker(\eta_u)$, entonces $F \cap I = 0$. Cualquier ideal de $F[x]/I$ tiene la forma $J/I$ donde $J \underset{ideal}{\leq} F[x]$ que contiene a $I = \langle g(x) \rangle$. Entonces $J = \langle f(x) \rangle$ y $g(x) = f(x)h(x)$ donde $f(x)$, $h(x) \in F[x]$. Como $g(x)$ es irreducible entonces $f(x)$ o $h(x)$ es una unidad.

Si $f(x)$ es una unidad, entonces demostraremos que $J = F[x]$.
($\subseteq$) Sabemos que $\langle f(x) \rangle \subseteq F[x]$.
($\supseteq$) Si $q(x) \in F[x]$, entonces

$$q(x)\,\overline{1} = q(x)f(x)f^{-1}(x) = (q(x)f^{-1}(x))f(x) = l(x)f(x),$$

esto significa que $q(x) \in \langle f(x) \rangle = J$.
Entonces, $J = F[x]$.
Si $h(x)$ es una unidad, entonces veremos que $J = I$.
($\subseteq$) Por hipótesis, $I \subseteq J$.
($\supseteq$) Como $h(x)$ es una unidad y $g(x) = f(x)h(x)$, entonces $g(x)h^{-1}(x) = f(x)$. Entonces

$$p(x) = l(x)g(x)h^{-1}(x) = (l(x)h^{-1}(x))g(x) = m(x)g(x).$$

Así, $p(x) \in \langle g(x) \rangle = I$.
Por lo que $J = I$.
Ahora, si $J = f[x]$, entonces $F[x]/I = J/I \underset{ideal}{\leq} F[x]/I$.
Cuando $J = I$, entonces $J/I = I/I = 0$.
Por esto, los únicos ideales de $F[x]/I$ son el 0 y el mismo.
Por otro lado, por el Corolario 1, tenemos que $F[u] \cong F[x]/I$.
Como los únicos ideales de $F[x]/I$ son 0 y $F[x]/I$, tenemos que $F[x]/I$ es un campo.

Además, si $g(x) = f(x)h(x)$ donde grad $(f) > 0$ y grad $(h) > 0$, entonces grad $(f) <$ grad $(g)$ y grad $(h) <$ grad $(g)$. Como $g(x)$ es el polinomio mínimo

sobre $F$ del elemento algebraico $u$, entonces $f(u) \neq 0$ y $h(u) \neq 0$. Como $g(u) = 0$, entonces $0 = g(u) = f(u) \cdot h(u)$. Así, $F(u) \neq 0$ tiene divisores de cero diferentes de cero.

$\therefore F[u]$ no es un dominio. ■

**Teorema 9** *Si $f(x) \in F[x]$, grad $(f) = n > 0$, $F$ campo. Entonces $f(x)$ tiene a lo más $n$ raíces distintas en $F$.*

**Demostración.** Demostraremos por inducción sobre $r$, la siguiente afirmación: Si $a_1, ..., a_r$ son raíces distintas de $f(x)$, entonces $\Pi_1^r (x - a_j) \mid f(x)$.

**Base**. Para $r = 1$. Si $a_1$ es una raíz de $f(x)$, entonces $(x - a_1) \mid f(x) \Longleftrightarrow f(a_1) = 0$, por el Teorema del Factor.

**Hipótesis de Inducción.** Asumimos válido para $r - 1$,

demostraremos que la afirmación es válida para $r$. Por hipótesis de inducción,

$$f(x) = \Pi_1^{r-1} (x - a_j) h(x), \text{ para alguna } h(x) \in F[x].$$

Para la raíz $a_r$ se cumple que

$$0 = f(a_r) = \Pi_1^{r-1} (a_r - a_j) h(a_r).$$

Como $a_r \neq a_j$, para $j \in \{1, ..., r-1\}$, $a_r - a_j \neq 0$, entonces $h(a_r) = 0$. Así, por la base, $h(x) = (x - a_r) k(x)$.

Entonces

$$f(x) = \Pi_1^{r-1} (x - a_j) h(x) = \Pi_1^{r-1} (x - a_j) ((x - a_r) k(x)) = \Pi_1^r (x - a_j) k(x).$$

Así, se cumple la afirmación.

Como $f(x) = \Pi_1^r (x - a_j) k(x)$, entonces grad $(\Pi_1^r (x - a_j)) \leq$ grad $(f)$.

$\therefore r \leq n$. ■

# Capítulo 2

# Números Ordinales y Números Cardinales.

## 2.1. Relaciones y Conjuntos Ordenados.

**Definición 39** *Si $X, Y$ son conjuntos, una **relación** de $X$ a $Y$ es un subconjunto $R$ del producto cartesiano $X \times Y$. Una **relación** en $X$ es un subconjunto de $X \times X$. Si $R$ es una relación y $(x, y) \in R$, decimos que $x$ está relacionado con $y$.*

**Notación 6** *Empleamos $xRy$ para indicar que $x$ está relacionado con $y$ por medio de la relación $R$ Para decir que $(x, y) \notin R$, escribimos $x \not R y$.*

**Observación 18** *Decir que $aRb$ significa que $(a, b) \in R$.*

**Definición 40** *Una **relación** $\mathbf{n}$-aria es un subconjunto de $X_1 \times X_2 \times \cdots \times X_n$.*

**Definición 41** *Una relación $R$ es **reflexiva** si $xRx$ $\forall x \in X$.*

**Definición 42** *Una relación $R$ es **simétrica** si $xRy$ implica $yRx$ $\forall x, y \in X$.*

**Definición 43** *Una relación $R$ es **transitiva** si $xRy$ y $yRz$ implica $xRz$ $\forall x, y, z \in X$.*

**Definición 44** *Una **relación es de equivalencia** en un conjunto $X$ si es una relación binaria de $X$ a $X$ (es decir un subconjunto de $X \times X$) que es reflexiva, simétrica y transitiva.*

**Proposición 11** *Sea $\{R_i\}_{i \in I}$ una familia de relaciones en $X$, entonces $\underset{i \in I}{\cap} \{R_i\}$ es una relación en $X$.*

**Demostración.** Como $R_i \subseteq X \times X \ \forall\ i \in I$, entonces $\bigcap\limits_{i\in I}\{R_i\} \subseteq X \times X$.

$\therefore \bigcap\limits_{i\in I}\{R_i\}$ es una relación en $X$. ■

**Proposición 12** *Sea $\{R_i\}_{i\in I}$ una familia de relaciones reflexivas en $X$, entonces $\bigcap\limits_{i\in I}\{R_i\}$ es una relación reflexiva en $X$.*

**Demostración.** Como $(a,a) \in R_i\ \forall i \in I$, entonces $(a,a) \in \bigcap\limits_{i\in I}\{R_i\}$.

$\therefore \bigcap\limits_{i\in I}\{R_i\}$ es reflexiva en $X$. ■

**Proposición 13** *Sea $\{R_i\}_{i\in I}$ una familia de relaciones simétricas en $X$, entonces $\bigcap\limits_{i\in I}\{R_i\}$ es una relación simétrica en $X$.*

**Demostración.** Si $(a,b) \in \bigcap\limits_{i\in I}\{R_i\}$, entonces $(a,b) \in R_i\ \forall i \in I$. Como $R_i$ es simétrica $\forall i \in I$, entonces $(b,a) \in R_i\ \forall i \in I$, es decir, $(b,a) \in \bigcap\limits_{i\in I}\{R_i\}$.

$\therefore \bigcap\limits_{i\in I}\{R_i\}$ es simétrica en $X$. ■

**Proposición 14** *Sea $\{R_i\}_{i\in I}$ una familia de relaciones transitivas en $X$, entonces $\bigcap\limits_{i\in I}\{R_i\}$ es una relación transitiva en $X$.*

**Demostración.** Si $(a,b) \in \bigcap\limits_{i\in I}\{R_i\}$ y $(b,c) \in \bigcap\limits_{i\in I}\{R_i\}$, entonces $(a,b) \in R_i$ y $(b,c) \in R_i\ \forall i \in I$. Como $R_i$ es transitiva $\forall i \in I$, entonces $(a,c) \in \bigcap\limits_{i\in I}\{R_i\}$.

$\therefore \bigcap\limits_{i\in I}\{R_i\}$ es transitiva en $X$. ■

**Proposición 15** *Sea $\{R_i\}_{i\in I}$ una familia de relaciones de equivalencia en $X$, entonces $\bigcap\limits_{i\in I}\{R_i\}$ es una relación de equivalencia en $X$.*

**Demostración.** Por las Proposiciones: 11, 12, 13, y, 14, $\bigcap\limits_{i\in I}\{R_i\}$ es una relación de equivalencia en $X$. ■

**Proposición 16** *Si $R$ es una relación en $X$, entonces existe una menor relación de equivalencia $R'$ en $X$ que contiene a $R$.*

**Demostración.** Sea

$$\mathcal{F} = \{R^* \mid R^* \text{ es una relación de equivalencia en } X \text{ y } R \subseteq R^*\},$$

como $R \subseteq X \times X$, entonces $\mathcal{F} \neq \emptyset$. Por la Proposición 15, $\cap\mathcal{F}$ es una relación de equivalencia en $X$. Además, como $R \subseteq R^*$ tenemos que $R \subseteq \cap\{R^*\} = \cap\mathcal{F}$.

Ahora, si $R^{**}$ es una relación de equivalencia de $X$ que contiene a $R$, entonces $R^{**} \in \mathcal{F}$, esto implica que $\cap\mathcal{F} \subseteq R^{**}$.

Por lo tanto, existe $R' = \cap\mathcal{F}$ una menor relación de equivalencia en $X$ que contiene a $R$. ■

**Definición 45** *Una relación $R$ es **antisimétrica** si $xRy$ y $yRx$ implica $x = y$ $\forall x, y \in X$.*

**Definición 46** *Una relación binaria $R$ de un conjunto $X$ es un **orden (parcial)** si $R$ es reflexiva, antisimétrica y transitiva. Decimos que $X$ es un conjunto ordenado por $R$, o bien, que $X$ es un **conjunto parcialmente ordenado (COPO)**.*

**Notación 7** *Usamos $(X, R)$ para expresar que $X$ es un conjunto parcialmente ordenado por $R$.*

**Definición 47** *Si $R$ es una relación binaria en un conjunto $X$ y si $Y \subseteq X$. La **restricción** de $R$ a $Y$ es el conjunto*

$$R\mid_Y = \{(a, b) \in R \mid a \in Y \ y\ b \in Y\}.$$

**Teorema 10** *Si $(X, R)$ es un COPO y $Y \subseteq X$, entonces $R\mid_Y$ es una relación de orden en $Y$.*

**Demostración.** Si $a \in Y$, como $Y \subseteq X$ y $R$ es reflexiva, entonces $(a, a) \in R$. Entonces $(a, b) \in R\mid_Y$ .

Si $(a, b) \in R\mid_Y$ y $(b, a) \in R\mid_Y$ entonces por definición de $R\mid_Y$, tenemos que $(a, b) \in R$ y $(b, a) \in R$. Así, por la antisimetría de $R$,

se cumple que $a = b$ $\forall a, b \in Y$. Entonces $R\mid_Y$ es antisimétrica.

Si $(a, b) \in R\mid_Y$ y $(b, c) \in R\mid_Y$ entonces por definición de $R\mid_Y$, tenemos que $(a, b) \in R$ y $(b, c) \in R$. Por la transitividad de $R$,

$(a, c) \in R$ $\forall a, b, c \in Y$, entonces $(a, c) \in R\mid_Y$, es decir, $R\mid_Y$

es transitiva.

$\therefore (X, R\mid_Y)$ es un COPO. ■

**Definición 48** *Si $R$ es una relación binaria en un conjunto $X$, llamamos al conjunto*

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}$$

*la **inversa** de la relación $R$.*

**Teorema 11** *La inversa de una relación de orden es una relación de orden.*

**Demostración.** Si $R$ es una relación de orden en el conjunto $X$, por ser reflexiva tenemos

que $(x, x) \in R$, así que $(x, x) \in R^{-1}$ $\forall x \in X$, entonces $R^{-1}$ es reflexiva.

Ahora, si $(x, y) \in R^{-1}$ y $(y, x) \in R^{-1}$, entonces $(y, x) \in R$ y $(x, y) \in R$

como $R$ es antisimétrica tenemos que $x = y$. Entonces $R^{-1}$ es antisimétrica.

Por último, si $(x, y) \in R^{-1}$ y $(y, z) \in R^{-1}$. Entonces $(y, x) \in R$ y $(z, y) \in R$ y como $R$ es transitiva, se tiene que $(z, x) \in R$, y entonces $(x, z) \in R^{-1}$. Entonces $R^{-1}$ es una relación de orden. ■

**Definición 49** *$(X, R)$ es un **conjunto totalmente ordenado (COTO)**, si $R$ es un orden y cualesquiera dos elementos de $X$ son comparables.*[1]

**Definición 50** *Si $(X, R)$ es un conjunto parcialmente ordenado y $A \subseteq X$. Decimos que $m \in A$ es el **elemento menor** de $A$ si $mRa$ $\forall a \in A$. Es el **elemento mayor** de $A$ si $aRm$ $\forall a \in A$.*

**Notación 8** *$m = men\ A$, denota al elemento menor $m$ de $A$.*

**Definición 51** *Si $(X, R)$ es un conjunto parcialmente ordenado y $A \subseteq X$. Una **cota superior** para $A$ es un elemento $x \in X$ tal que $aRx$ $\forall a \in A$. Si $xRa$ $\forall a \in A$ decimos que $x \in X$ es una **cota inferior** para $A$.*

**Definición 52** *Si $(X, R)$ es un conjunto parcialmente ordenado y $A \subseteq X$. El **supremo** de $A$ es el elemento menor del conjunto de todas las cotas superiores de $A$ (si existe). El elemento mayor del conjunto de todas las cotas inferiores de $A$, es el **ínfimo** de $A$ (si existe).*

**Notación 9** *$a = \sup(A)$ denota el supremo de $A$ y $b = ínf\ (A)$ denota el ínfimo de $A$.*

## 2.2. Conjuntos Bien Ordenados y Números Ordinales.

**Definición 53** *Si $(X, R)$ es COTO, $(X, R)$ se llama un conjunto **bien ordenado (COBO)** si cada $B \subseteq X$, $B \neq \emptyset$, tiene elemento menor, en este caso a $R$ se le llama **buen orden.***

**Definición 54** *Un **número ordinal** u **ordinal** es un COBO, en el que cada elemento es igual al conjunto de todos sus predecesores, es decir cada $x \in X$, cumple que*

$$x = \{y \in X \mid yRx,\ y \neq x\}.$$

**Notación 10** *Usamos las letras del alfabeto griego $\alpha$,$\beta$,$\gamma$,..., para denotar números ordinales.*

**Ejemplo 11** *Si $n \in \mathbb{N}$, entonces $n = \{0, 1, 2, ..., n-1\}$. Como $(\mathbb{N}, \leq)$ es un COBO y cada $n \in \mathbb{N}$ es igual al conjunto de todos sus predecesores, se satisface la definición de número ordinal. Así, todo número natural es un número ordinal.*

**Definición 55** *Si $(X, R)$ es un COBO. El **segmento inicial** de $X$ determinado por un elemento $a \in X$ es*

$$X_a = \{y \in X \mid yRa,\ y \neq a\}.$$

[1] Dos elementos $x, y$ de un conjunto ordenado parcialmente por $R$ son **comparables** si: $xRy$ o $yRx$.

**Ejemplo 12** $\mathbb{N}_n = \{0, 1, ..., n-1\} = n$ *es el segmento inicial de* $\mathbb{N}$ *determinado por* $n \in \mathbb{N}$.

**Definición 56** *Si* $(A, R)$ *y* $(B, S)$ *son COBOS, decimos que* $(A, R)$ *y* $(B, S)$ *son* ***isomorfos (o del mismo tipo de orden),*** *si existe* $f : A \to B$ *biyectiva que preserva el orden, es decir, que*

$$a_1 R a_2 \text{ si y sólo si } f(a_1)\, S f(a_2)$$

*para todo* $a_1, a_2 \in A$. *Llamamos a una* $f$ *con la propiedad anterior* ***isomorfismo de orden*** *entre* $(A, R)$ *y* $(B, S)$.

**Nota 7** *A lo largo del capítulo, usaremos las palabra isomorfismo en vez de isomorfismo de orden.*

**Notación 11** ***1.*** $(A, R) \cong (B, S)$, *significa que* $(A, R)$ *y* $(B, S)$ *son isomorfos. Cuando* $R = S$, *escribimos* $A \cong B$.

*2.* $(A, R) \ncong (B, S)$ *denota que* $(A, R)$ *y* $(B, S)$ *no son isomorfos.*

**Observación 19** *Si* $(X, R)$ *es un COBO, entonces* $(X_a, R\,|_{X_a})$ *es un COBO.*

**Demostración.** Supongamos lo contrario, entonces existe $Y \subseteq X_a$, $Y \neq \emptyset$, que no tiene elemento menor. Sin embargo, $Y \subseteq X_a \subseteq X$, contradiciendo que $(X, R)$ es un COBO.

$\therefore (X_a, R)$ es un COBO. ■

**Observación 20** *Si* $a \in X$, $b \in X_a$, *entonces* $(X_a)_b = X_b$.

**Demostración.** Demostraremos que $(X_a)_b \subseteq X_b$ y que $(X_a)_b \supseteq X_b$.

$(\subseteq)$ Si $p \in (X_a)_b$, entonces $p \in X_a$ es tal que $pRb$, $p \neq b$. Así, $p \in X$, por la definición de $X_a$. Por lo tanto, $p \in X_b$.

$(\supseteq)$ Si $p \in X_b$, entonces $p \in X$ es tal que $pRb$, $p \neq b$. Como también $b \in X_a$, tenemos que $b \in X$, $bRa$ y $b \neq a$. Consecuentemente $pRa$, por la transitividad de $R$. Además $p \neq a$ ($p = a \Longrightarrow aRp$. $aRp$ y $pRb \Longrightarrow aRb$. De $aRb$ y $bRa$ tendríamos que $a = b$.). Así, $p \in (X_a)_b$.

$\therefore (X_a)_b = X_b$. ■

**Observación 21** *Si* $(X, R)$ *es un COBO entonces* $a = men\,(X \setminus X_a)$ $\forall\, a \in X$.

**Demostración.** Por definición de segmento inicial, $a \notin X_a$, lo que implica que $a \in (X \setminus X_a)$. Si $p \in X \setminus X_a$, entonces $p \not R a$ o $p = a$. Por ser $R$ un orden total, $p \not R a$ implica que $aRp$

$\therefore a = men\,(X \setminus X_a)$. ■

**Observación 22** *Si* $a, b \in X$, $aRb$ *si y sólo si* $X_a \subseteq X_b$.

**Demostración.** ($\Longrightarrow$) Supongamos $aRb$. Si $p \in X_a$, entonces $p \in X$, $pRa$, $p \neq a$. Así, $pRb$, por transitividad. Además, $p \neq b$ ($p = b \Longrightarrow bRp$. Pero, $bRp$ y $aRb \Longrightarrow aRp$. Como $pRa$,entonces $p = a$). Por lo tanto $p \in X_b$. Es decir, $X_a \subseteq X_b$.

($\Longleftarrow$) Si $X_a \subseteq X_b$, supongamos que $bRa$ y $b \neq a$, entonces $b \in X_a \subseteq X_b$. Así, $bRb$ y $b \neq b$, absurdo. Entonces $aRb$. ■

**Teorema 12** *Si $(X, R)$ es un COBO y $Y \subseteq X$ es tal que $X_b \subseteq Y$ $\forall b \in Y$, entonces $Y = X$ o $Y = X_c$ para algún $c \in Y$.*

**Demostración.** Supongamos que $Y \neq X$, entonces $X \diagdown Y \neq \emptyset$. Sea $c = men\,(X \diagdown Y)$. Veremos que $Y = X_c$. Para esto mostraremos $Y \subseteq X_c$ y $Y \supseteq X_c$.

($\subseteq$) Si $p \in Y$. Supongamos que $p \notin X_c$, entonces $cRp$ o $c = p$. Si $cRp$ y $c \neq p$, entonces $c \in X_p \subseteq Y$, contradiciendo que $c \in (X \diagdown Y)$. Ahora, si $c = p$, entonces $c \in Y$, absurdo. Por lo anterior, $p \in X_c$.

($\supseteq$) Si $p \in X_c$, entonces $pRc$, $p \neq c$. Supongamos que $p \notin Y$, entonces $p \in (X \diagdown Y)$, así que $cRp$. De $pRc$ y $cRp$ tenemos que $c = p$, contradicción. Por lo tanto, $p \in Y$.

Consecuentemente $Y = X_c$.

$\therefore Y = X$ o $Y = X_c$ para algún $c \in Y$. ■

**Nota 8** *Observe que $c = men\,(X \diagdown Y)$.*

**Teorema 13** *Sean $(X, R)$, $(Y, S)$ COBOS.*

*(i) Si $f : X \to X$ es inyectiva y preserva el orden, entonces $pR(f(p))$ $\forall$ $p \in X$.*

*(ii) $X \overset{f}{\cong} X \Longrightarrow f = 1_X$.*

*(iii) $X \overset{f}{\cong} Y$ y $X \overset{g}{\cong} Y \Longrightarrow f = g$.*

*(iv) $X \ncong X_a$ $\forall$ $a \in X$.*

**Demostración.** (i) Supongamos que para algún $p \in X$, no se satisface la condición. Tenemos que $(f(p))Rp$ y $p \neq f(p)$, ya que $R$ es un orden total. Como $f$ es inyectiva $f(p) \neq f(f(p))$. Y, como preserva el orden $(f(f(p)))R(f(p))$. Llamamos $f^n(p) = (\underbrace{f(f(\cdots f}_{n}(p))))$ $\forall n \in \mathbb{N}$. Recursivamente generamos una sucesión $..., f^n(p), ..., f^3(p), f^2(p), f(p)$. Así obtenemos

$$B = \{f^n(p) \mid n \in \mathbb{N}\} \subseteq X,$$

con $B \neq \emptyset$ y sin primer elemento, lo que es una contradicción.

$$\therefore pR(f(p)), \forall p \in X.$$

(ii) Si $X \overset{f}{\cong} X$, entonces $X \overset{f^{-1}}{\cong} X$. Por (i), $pR(f(p))$ y $(f(p))R(f^{-1}(f(p)) = p)$. Consecuentemente, $p = f(p)$ por la antisimetría de $R$.

$$\therefore f = 1_X.$$

(iii) Si $X \overset{f}{\cong} Y$ y $X \overset{g}{\cong} Y$, entonces $X \overset{f}{\cong} Y$ y $Y \overset{g^{-1}}{\cong} X$. Esto implica que $X \overset{g^{-1}f}{\cong} X$. Por el inciso (ii), $g^{-1}f = 1_X$.

$$\therefore g = f.$$

(iv) Supongamos que $X \overset{f}{\cong} X_a$ para algún $a \in X$, entonces $f$ es inyectiva y preserva el orden. Por (i) $aR(f(a))$. Además, $f(a) \in X_a$, entonces $f(a)\, Ra$ y $f(a) \neq a$. De $aR(f(a))$ y $(f(a))Ra$, tenemos que $f(a) = a$, contradicción.

$\therefore \nexists\ f$ tal que $X \overset{f}{\cong} X_a\ \forall\ a \in X$. ■

**Teorema 14** *Si $(X, R)$, $(Y, S)$ son COBOS, entonces $X \cong Y$ o $X \cong Y_b$ para algún $b \in Y$, o $Y \cong X_a$ para algún $a \in X$.*

**Demostración.** Supongamos que $X \ncong Y$. Por casos:

**a)** $X = \emptyset$, $Y \neq \emptyset \Longrightarrow X \cong Y_a$, donde $a = men\ Y$.

**b)** $Y = \emptyset$, $X \neq \emptyset \Longrightarrow Y \cong X_b$, donde $b = men\ X$.

**c)** $X \neq \emptyset$, $Y \neq \emptyset$. Sean $x_0 = men\ X$ , $y_0 = men\ Y$. Así $X_{x_0} = \emptyset = Y_{y_0}$, entonces $X_{x_0} \cong Y_{y_0}$.

Por lo anterior podemos determinar $A \neq \emptyset$,

$$A = \{a \in X \mid \exists b \in Y \text{ y } X_a \cong Y_b\} \subseteq X.$$

Notemos que $b$ es único para cada $a \in A$. De lo contrario, existiría $b^* \in Y$, $b^* \neq b$, tal que $X_a \cong Y_{b^*}$, entonces $Y_b \cong Y_{b^*}$. Como $S$ es un orden total, sucedería que $bSb^*$ o $b^*Sb$. Por esto y por $Y_b \cong Y_{b^*}$, habría un conjunto isomorfo a un segmento inicial de sí mismo, contradiciendo el Teorema 13 (iv).

Definimos

$$\begin{aligned} \varphi &: A \to Y \\ \varphi(a) &= b \text{ si } X_a \cong Y_b. \end{aligned}$$

Ahora, $\varphi(a_1) = \varphi(a_2) \iff b_1 = b_2$. Así, $X_{a_1} \cong Y_{b_1} \cong X_{a_2} \Longrightarrow a_1 = a_2$. Entonces $\varphi$ es inyectiva.

Veamos que $\varphi$ preserva el orden. Si $a, c \in A$ con $aRc$, tenemos dos casos:

**(i)** $a = c$. En este caso $\varphi(a) = \varphi(c)$.

**(ii)** $a \neq c$. En este caso $a \in X_c$. Como $c \in A$, existe $g$ tal que $X_c \overset{g}{\cong} Y_{\varphi(c)}$. Además, $X_a \subseteq X_c$ por la Observación 22. Así, $X_a \overset{g|_{X_a}}{\cong} Y_{g(a)}$ con $g(a) \in Y_{\varphi(c)}$. Entonces $(g(a))S(\varphi(c))$. Por unicidad, $g(a) = \varphi(a)$, por lo que $X_a \cong Y_{\varphi(a)}$. Por lo tanto $(\varphi(a))S(\varphi(c))$.

En cada caso $\varphi$ preserva el orden.

Mostraremos que $A = X$ y $\varphi(A) = Y_b$ para algún $b \in Y$, o bien que, $\varphi(A) = Y$ y $A = X_a$ para algún $a \in A$.

Antes de continuar, observemos que $X_a \subseteq A\ \forall a \in A$. Porque, si $a \in A$ y $x \in X_a$, como $\exists\ f$ tal que $X_a \overset{f}{\cong} Y_b$ para algún $b \in Y$, entonces $f(x) \in Y_b$. Así, $X_x \overset{f_{|_{X_x}}}{\cong} Y_{f(x)}$. Entonces $x \in A$.

Como se satisfacen las hipótesis del Teorema 12, tenemos que: **(a)** $A = X$, o bien **(b)** $A = X_{x_0}$ para algún $x_0 \in X$.

Si **(a),** entonces $\varphi(A) \neq Y$, así, $Y \backslash \varphi(A) \neq \emptyset$. Sea $p = men\ (Y \backslash \varphi(A))$. Comprobaremos que $\varphi(A) = Y_p$.

**(⊆)** Si $l \in \varphi(A)$, entonces, no $pSl$. Como $\varphi(A) \subseteq Y$, $(\varphi(A), S)$ es un COBO, por Observación 19. Como $S$ es un orden total, $lSp$ y $l \neq p$, es decir, $l \in Y_p$. Así, $\varphi(A) \subseteq Y_p$.

**(⊇)** Si $m \in Y_p$, entonces $m \in Y$ es tal que $mSp$, $m \neq p$. Así, $m \notin (Y \backslash \varphi(A))$, es decir, $m \in \varphi(A)$. Entonces $\varphi(A) \supseteq Y_p$.

Consecuentemente $\varphi(A) = Y_p$.

Por último, comprobemos que **(b)** implica $\varphi(A) = Y$. Pues si $\varphi(A) \neq Y$, entonces $\varphi(A) = Y_{y_0}$ para $y_0 = men\ (Y \backslash \varphi(A))$. Por otro lado, como $(X \diagdown A) \neq \emptyset$, sabemos que $x_0 = men\ (X \diagdown A)$, por la nota 8. Así, $X_{x_0} \overset{\varphi}{\cong} Y_{y_0}$. Entonces $x_0 \in A$, contradicción. Por lo tanto, $\varphi(A) = Y$.

Como $\varphi$ es inyectiva, preserva el orden. Además se cumple que o bien $X = A$ y $\varphi(A)$ es un segmento inicial de $Y$, o bien que $A$ es un segmento inicial de $X$ y $\varphi(A) = Y$.

Obtenemos:

$$X \overset{\varphi}{\cong} Y_b \text{ para algún } b \in Y, \text{ o } Y \overset{\varphi}{\cong} X_a \text{ para algún } a \in X.$$

$\therefore X \cong Y$, $X \cong Y_b$ para algún $b \in Y$, o , $Y \cong X_a$ para algún $a \in X$. ■

**Teorema 15** *(a) Si $\alpha$ es un ordinal, entonces $\alpha_a$ es un ordinal $\forall a \in \alpha$ . Equivalentemente, $a$ es un ordinal $\forall a \in \alpha$.*

*(b) La relación de orden en un ordinal es siempre $\subseteq$ .*

*(c) Si $\alpha$ y $\beta$ son ordinales y $\alpha \cong \beta$, entonces $\alpha = \beta$.*

*(d) Si $\alpha$ y $\beta$ son ordinales, entonces:*

$$\alpha = \beta,\ \alpha \in \beta\ o\ \beta \in \alpha.$$

**Demostración.** (a) Si $\alpha$ es un ordinal y $x \in \alpha$, entonces por definición, $x = \{y \in \alpha : yRx,\ y \neq x\} = \alpha_x$. Ahora, si $y \in \alpha_x$, entonces $y \in \alpha$, así, $y = \alpha_y$. También, $\alpha_y = (\alpha_x)_y$ por la Observación 20. Como consecuencia, $y = \alpha_y = (\alpha_x)_y = x_y \subseteq x$.

$$\therefore x \text{ es un número ordinal.}$$

(b) Si $\alpha$ es un ordinal y $R$ su relación de orden, por la Observación 22: $aRb \iff \alpha_a \subseteq \alpha_b$, $\forall a, b \in \alpha$. También $a = \alpha_a$ y $b = \alpha_b$, por ser $\alpha$ un ordinal. Por lo que, $aRb \iff a \subseteq b\ \forall\ a, b \in X$.

$$\therefore R = \ \subseteq .$$

(c) Si $\alpha$ y $\beta$ son ordinales y $\alpha \overset{f}{\cong} \beta$. Supongamos que $f \neq 1_\alpha$, entonces $B = \{x \in \alpha \mid f(x) \neq x\} \neq \emptyset$. Sea $x_0 = men\ B$. Ahora, $f(x) = x\ \forall x \subsetneqq x_0$. Además, $\alpha_{x_0} \overset{f}{\cong} \beta_{f(x_0)}$. De $f(x) = x\ \forall x \subsetneqq x_0$ y $\alpha_{x_0} \overset{f}{\cong} \beta_{f(x_0)}$, obtenemos que $\alpha_{x_0} = \beta_{f(x_0)}$, esto significa que $x_0 = f(x_0)$, contradicción. Entonces $f = 1_\alpha$.

$$\therefore \alpha = \beta.$$

(d) Si $\alpha$ y $\beta$ son ordinales. Por el Teorema 14, tenemos tres casos:
**(i)** $\alpha \cong \beta$.
**(ii)** $\alpha \cong \beta_y$ para algún $y \in \beta$.
**(iii)** $\alpha_x \cong \beta$ para algún $x \in \alpha$.
Si **(i),** entonces $\alpha = \beta$, por el inciso (c).
Si **(ii),** entonces $\alpha \cong \beta_y = y$ para algún $y \in \beta$, por el inciso (a). Y, nuevamente por (c), obtenemos $\alpha = y$.Así, $\alpha \in \beta$.
Análogamente, si **(iii),** $x = \alpha_x \cong \beta$, para $x \in \alpha$,por (a). Y, por (c), $\beta = x \in \alpha$.
$\therefore \alpha = \beta$, $\alpha \in \beta$ o $\beta \in \alpha$. ■

**Corolario 4** *Si $\alpha$ y $\beta$ son ordinales tal que $\alpha \subsetneqq \beta$, entonces $\alpha \in \beta$.*

**Demostración.** Si $\alpha \neq \beta$, entonces $\alpha \in \beta$ o $\beta \in \alpha$, por el Teorema 15(d).
Supongamos que $\beta \in \alpha$, esto implica que $\beta = \alpha_\beta$, por el Teorema 15 (a). Como, $\alpha_\beta \subseteq \alpha$, también $\beta \subseteq \alpha$. De $\alpha \subsetneqq \beta$ y $\beta \subseteq \alpha$, tenemos que $\alpha = \beta$, lo que contradice nuestra hipótesis.
$\therefore \alpha \in \beta$. ■
Por el ejemplo 11, sabemos que los números naturales son números ordinales. Así, cualquier conjunto finito que sea un número ordinal es un número natural, por el Teorema 15 (c).

**Definición 57** *Si $\alpha$ es un ordinal, entonces $\alpha^+ = \alpha \cup \{\alpha\}$ es el sucesor de $\alpha$.*

**Teorema 16** *Si $\alpha$ es un ordinal entonces $\alpha^+$ es un ordinal.*

**Demostración. (1)** Comprobaremos que $(\alpha^+, \subseteq)$ es un COTO.
Si $x, y \in \alpha^+$, tenemos los siguientes casos:
**(i)** $x = y \Longrightarrow x \subseteq y$ y $y \subseteq x$.
**(ii)** $x, y \in \alpha \Longrightarrow x \subseteq y$ o $y \subseteq x$.
**(iii)** $x \in \alpha$ y $y = \alpha \Longrightarrow x = \alpha_x \subseteq \alpha = y$.
**(iv)** $y \in \alpha$ y $x = \alpha \Longrightarrow y = \alpha_y \subseteq \alpha = x$.
Como consecuencia de los incisos, $(\alpha^+, \subseteq)$ es un COTO. Note que las implicaciones de **(ii)** a **(iv)** se deben al Teorema 15 (b).
**(2)** Veremos que $(\alpha^+, \subseteq)$ es un COBO.
Si $X \subseteq \alpha^+$ y $X \neq \emptyset$, entonces $X = \{\alpha\}$ o $X \cap \alpha \neq \emptyset$. Si $X = \{\alpha\}$, tenemos que $\alpha = men\ X$. Ahora, si $\emptyset \neq X \cap \alpha \subseteq \alpha$, llamemos $x_0 = men\ (X \cap \alpha)$. Como $x_0 \subseteq x\ \forall x \in X \cap \alpha$, entonces $x_0 \subseteq x\ \forall x \in X$ y $\forall x \in \alpha$. Por lo anterior, $x_0 = men\ (X)$. En ambos casos, $X$ tiene primer elemento, es decir, $(\alpha^+, \subseteq)$ es un COBO.

**(3)** Solo falta ver que cada elemento de $\alpha^+$ es un ordinal. Si $x \in \alpha^+$, entonces $x = \alpha$ o $x \neq \alpha$. Cuando $x = \alpha$, sucede que $(\alpha \cup \{\alpha\})_x = (\alpha \cup \{\alpha\})_\alpha = \{p \in \alpha \cup \{\alpha\} \mid pR\alpha,\ p \neq \alpha\} = \alpha = x$.

Por último, $x \neq \alpha$, implica $x = \alpha_x$. Así, $(\alpha \cup \{\alpha\})_x = \alpha_x = x$. Por lo tanto, todo elemento de $\alpha^+$ es un ordinal.

$\therefore$Por **(1), (2) y (3),** $\alpha^+$ es un ordinal. ■

**Teorema 17** *Si $X$ es un conjunto en que cada elemento $x$ es un ordinal, entonces*

*(a) $(X, \subseteq)$ es un COBO.*

*(b) $\cup X$ es un ordinal.*

**Demostración.** (a) Primero veremos que $(X, \subseteq)$ es un COTO. Si $\alpha, \beta \in X$, entonces por el Teorema 15 (d) se tiene que $\alpha = \beta$, $\alpha \in \beta$ o $\beta \in \alpha$. Si $\alpha \in \beta$, entonces tenemos que $\alpha = \beta_\alpha \subseteq \beta$. Y si $\beta \in \alpha$, entonces $\beta = \alpha_\beta \subseteq \alpha$. Entonces $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$, es decir, $(X, \subseteq)$ es un COTO.

Ahora, si $Y \subseteq X$, $Y \neq \emptyset$, sea $\gamma \in Y$ y supongamos que $\gamma \neq men\ Y$. Si $\delta \in Y$, y $\delta \subsetneqq \gamma$, entonces $\delta \in \gamma$, por el Corolario 4. Así, $\gamma \cap Y \neq \emptyset$, pero $\gamma \cap Y \subseteq \gamma$, por lo que $\exists\ \alpha = men\,(\gamma \cap Y)$. Por definición de elemento menor, $\alpha \subseteq \beta$, $\forall \beta \in \gamma \cap Y$. Consecuentemente $\alpha = men\ (Y)$.

$$\therefore (X, \subseteq) \text{ es un COBO.}$$

(b) Por definición de la unión, si $x \in \cup X$, entonces $x \in \alpha$ para algún $\alpha \in X$. Esto significa que $x$ es un ordinal. Así, $(\cup X, \subseteq)$ es un COBO, por el inciso (a).

Afirmamos que $x \subseteq \cup X$ , $\forall x \in \cup X$. Porque si $y \in x$, entonces $y = x_y$, por ser $x$ un ordinal. Además, como $x \in \cup X$ , tenemos que $x \in \alpha$ para algún $\alpha \in X$. Así, $x = \alpha_x$. Entonces $y = x_y \subseteq x = \alpha_x \subseteq \alpha$. Por lo tanto, $y \in \cup X$, cumpliéndose la afirmación.

Ahora, si $x \in \cup X$,

$$(\cup X)_x = \{p \in \cup X : p \subseteq x,\ p \neq x\} = \{p \in \cup X : p \in x\}.$$

Como $\cup X$ es un conjunto de ordinales, entonces $(\cup X)_x = (\cup X) \cap x = x$, pues $x \subseteq \cup X$. Así $(\cup X)_x = x$, $\forall x \in \cup X$.

$\therefore \cup X$ es un ordinal. ■

**Ejemplo 13** *Si denotamos*

$$\omega = \{0, 1, 2, ..., n, n+1, ...\},$$

*podemos suponer que $\omega$ es el primer número más grande que cualquier número natural. Como cada $n \in \mathbb{N}$ es un ordinal, entonces $(\omega, \subseteq)$ es un COBO, por el Teorema 15 (a). Entonces $\omega$ es también un número ordinal.*

**Corolario 5** *Si $X$ es un conjunto de ordinales, entonces $\cup X = \sup X$.*

**Demostración.** Por Teorema 17 (b), $\cup X$ es un ordinal.

Por otro lado, si $\alpha \in X$, entonces $\alpha \subseteq \cup X$ por definición de unión. Así, $\cup X$ es una cota superior de $X$.

Ahora, si $\beta$ es una cota superior de $X$, demostraremos que $\cup X \subseteq \beta$. Si $\gamma \in \cup X$, entonces $\gamma \in \alpha$ para algún $\alpha \in X$. Además $\alpha \subseteq \beta$, por ser $\beta$ cota superior. Así $\gamma \in \beta$, con lo que queda terminada la demostración.

$\therefore \cup X = \sup X$. ■

**Ejemplos 14** ***1.*** *Si* $X = \{n_1, n_2, ..., n_k\}$, *entonces* $\cup X = n_k$.

***2.*** *Si* $X = \omega$, *entonces* $\cup X = \omega$.

***3.*** $\omega^+$, $(\omega^+)^+$, $\left((\omega^+)^+\right)^+$, .... *son ordinales, porque* $\omega$ *es un ordinal y por el Teorema 16. Se denotan por* $\omega + 1$, $\omega + 2$, $\omega + 3$, ..., *respectivamente.*

***4.*** *El ejemplo anterior, implica que* $\{\omega + n : n \in \omega\}$ *es un conjunto de ordinales, entonces* $\cup \{\omega + n : n \in \omega\} = \omega 2$ *es un ordinal, por el Teorema 17 (b).*

***5.*** $\omega 2^+$, $(\omega 2^+)^+$, $\left((\omega 2^+)^+\right)^+$, .... *son ordinales, porque* $\omega 2$ *es un ordinal y por el Teorema 16. Se denotan por* $\omega 2 + 1$, $\omega 2 + 2$, $\omega 2 + 3$, ..., *respectivamente.*

***6.*** $\cup \{\omega 2 + n : n \in \omega\} = \omega 3$ *es un ordinal, por el Teorema 17 (b).*

***7.*** *Continuando así, obtenemos* $\{\omega n : n \in \omega\}$ *es un conjunto de ordinales, entonces* $\cup \{\omega n : n \in \omega\} = \omega^2$ *es nuevamente un ordinal por el Teorema 17 (b).*

***8.*** *Por lo anterior, si tenemos una sucesión creciente de ordinales* $\alpha_i$, $i \in \mathbb{Z}^+$, *podemos construir un ordinal más grande* $\cup \{\alpha_i : i \in \mathbb{Z}^+\}$, *y encontrar una nueva sucesión de ordinales.*

**Definición 58** *Un ordinal* $\alpha \neq 0$ *es un* ***ordinal sucesor*** *si* $\alpha = \beta^+$, *para algún ordinal* $\beta$. *En caso contrario,* $\alpha$ *es un* ***ordinal límite****. Un ordinal límite no tiene predecesor inmediato.*

**Ejemplos 15** ***1.*** $\omega$, $\omega 2$, $\omega 3$, $\omega^2$ *son ordinales límite.*

***2.*** $\omega + 1$, $\omega + 2$, $\omega + 3$, ..., *al igual que,* $\omega 2^+$, $(\omega 2^+)^+$, $\left((\omega 2^+)^+\right)^+$, ...., *son ordinales sucesores.*

***3.*** 0 *es un ordinal límite.*

***4.*** *Los números naturales diferentes de cero son ordinales sucesores.*

**Teorema 18** *No existe el conjunto de todos los ordinales.*

**Demostración.** Realizaremos la demostración por contradicción. Supongamos que $X$ es el conjunto de todos los ordinales, entonces $\cup X$ es un ordinal, por el Teorema 17 (b). También $(\cup X)^+$ es un ordinal por el Teorema 16. Si llamamos $\alpha = (\cup X)^+$, debe cumplirse que $\cup X \in X$ y $\alpha \in X$.

Si $\gamma \in X$, entonces $\gamma \subseteq \cup X \subseteq \cup X \cup \{\cup X\} = (\cup X)^+$. Esto implica que $\gamma \in \cup X$ o $\gamma = \cup X$. Si $\gamma \in \cup X$, entonces $\gamma = (\cup X)_\gamma \subseteq \cup X$ para algún $\gamma \in \cup X$, pues $\cup X$ es un ordinal. Como también $\cup X \subseteq (\cup X)^+$, obtenemos $\gamma = (\cup X)_\gamma \subseteq (\cup X)^+$ para algún $\gamma \in (\cup X)^+$. Por ser $(\cup X)^+$ ordinal, entonces $\gamma = (\cup X)^+_\gamma \subseteq (\cup X)^+$ para algún $\gamma \in (\cup X)^+$. Ahora, si $\gamma = UX$, tenemos $\gamma \subsetneq (\cup X)^+$. Por

el Corolario 4, $\gamma \in (\cup X)^+$. Nuevamente, $\gamma = (\cup X)_\gamma \subseteq (\cup X)^+$ para algún $\gamma \in (\cup X)^+$. Entonces, en ambos casos, $\gamma$ es un segmento inicial de $\alpha$ y $\gamma \neq \alpha$. Por tanto, $\alpha \notin X$, contradicción. ■

**Teorema 19** *Si $(X, R)$ es un COBO, entonces $\exists!$ $\alpha$ ordinal tal que $\alpha \cong X$. Éste es llamado el número ordinal de $(X, R)$ y es denotado por ord $(X, R) = \alpha$.*

**Demostración.** Primero demostraremos la unicidad. Si $\alpha$ y $\beta$ son ordinales tal que $\alpha \cong X$ y $\beta \cong X$, entonces $\alpha \cong \beta$, así que por el Teorema 15 (c), $\alpha = \beta$.

En lo siguiente, demostraremos la existencia.

Si $X$ es un conjunto y si $\alpha$ es un ordinal, por el Teorema 14, tenemos tres casos:

**(1)** $X \cong \alpha$.

**(2)** $X \cong \alpha_a$ para algún $a \in \alpha$.

**(3)** $\alpha \cong X_x$ para algún $x \in X$.

Si **(1)** no hay nada que demostrar.

Si **(2),** por el Teorema 15 (a) $\alpha_a = \beta$ ordinal. Entonces $X \cong \beta$.

Ahora, supongamos que $(X, R) \ncong \alpha$. Entonces se cumple **(3),** para cada ordinal $\alpha$.

Sea

$$B = \{Y \in \wp(X) \mid Y = X_x \text{ para algún } x \in X \text{ y } Y \cong \gamma \text{ para algún } \gamma \text{ ordinal}\}.$$

Si P(x,y) es la siguiente afirmación: $x \in B$ y $y \cong x$, $y$ ordinal,
por el Axioma de Reemplazo,

$$A = \{y \mid (\exists x)\ \text{P(x,y)}\}$$

es un conjunto. Entonces $A$ contiene a todos los ordinales, esto contradice el Teorema 18.

$\therefore \exists!$ $\alpha$ ordinal tal que $\alpha \cong X$. ■

**Notación 12** *Usamos la relación $\leq$, para los ordinales de la siguiente forma:*
*Si $\alpha, \beta$ son ordinales,*
*(i)$\alpha \leq \beta$, si $\alpha \subseteq \beta$,*
*(ii)$\alpha < \beta$, si $\alpha \subsetneq \beta$.*

## 2.3. Recursión Transfinita.

**Definición 59** *Dos conjuntos $A$ y $B$ son **equipotentes** si hay una biyección de $A$ a $B$.*

**Observación 23** *Si $X$ es un conjunto y $\alpha$ un ordinal, una biyección $f : \alpha \to X$ induce un buen orden $R$ en $X$: para $x, y \in X$, definimos $(x, y) \in R$ si y solamente si $f^{-1}(x) \leq f^{-1}(y)$.*

**Definición 60** *Una* ***sucesión transfinita*** *es una función $f$ cuyo dominio es un número ordinal. Si $\alpha$ es el dominio de $f$, decimos que $f$ es una* ***sucesión transfinita de longitud*** *$\alpha$.*

**Nota 9** *$f$ no necesariamente es inyectiva.*

**Ejemplos 16** *Las siguientes funciones son sucesiones transfinitas*

***1.*** *La biyección $f : \omega \to \omega$ tal que $f(n) = n$.*

***2.*** *La biyección $f : \omega^+ \to \omega$ tal que $f(n) = n + 1$, para $n \in \omega$, y $f(\omega) = 0$.*

***3.*** *La biyección $f : \omega 2 \to \omega$ tal que $f(n) = 2n$, para $n \in \omega$, y $h(\omega + n) = 2n + 1$, para $n \in \omega$.*

**Teorema 20** ***(Principio de Inducción Transfinita).*** *Sea $(X, R)$ un COBO, $X \neq \emptyset$. Si $A \subseteq X$, $A \neq \emptyset$, satisface:*

$$X_a \subseteq A \Longrightarrow a \in A, \text{ para cada } a \in X,$$

*entonces $A = X$.*

**Demostración.** Como $A \subseteq X$, basta demostrar que $X \subseteq A$. Supongamos que $X \nsubseteq A$, entonces $\exists\, x \in X$ tal que $x \in (X \diagdown A)$. Así, $X_x \subseteq A$. Entonces, por hipótesis, $x \in A$, contradicción. Por lo que, $X \subseteq A$.

$\therefore X = A$. ■

**Corolario 6** ***( Principio de Inducción Transfinita para Ordinales)***[2] *Sea $\alpha$ un ordinal $\neq 0$. Si $\emptyset \neq A \subseteq \alpha$ satisface.*

$$\gamma \subseteq A \Longrightarrow \gamma \in A, \forall \gamma < \alpha,$$

*entonces $A = \alpha$.*

**Demostración.** Si $\gamma < \alpha$ entonces $\gamma \in \alpha$ y $\gamma = \alpha_\gamma \subseteq \alpha$, por ser $\gamma$ y $\alpha$ ordinales. Por el Teorema 20, $A = \alpha$. ■

**Teorema 21** ***(Recursión Transfinita).*** *Si $\alpha$ es un ordinal, $X$ es un conjunto y $\mathcal{L}^\alpha$ es el conjunto de todas las sucesiones transfinitas de longitud menor que $\alpha$ de elementos de $X$, (es decir, $\mathcal{L}^\alpha = \{f \mid f : \beta \to X$, para algún $\beta < \alpha\}$), entonces dada cualquier $h : \mathcal{L}^\alpha \to X$, $\exists!\ g : \alpha \to X$, tal que $g(\gamma) = h\left(g_{|_\gamma}\right)$, para cada $\gamma < \alpha$, donde $g_{|_\gamma}$ es la restricción de $g$ a $\gamma$, (y como tal es miembro de $\mathcal{L}^\alpha$).*

**Demostración.** Primero demostraremos la unicidad, suponiendo que existe dicha función $g$. Si $g : \alpha \to X$ y $g' : \alpha \to X$ satisfacen

$$g(\gamma) = h\left(g_{|_\gamma}\right) \text{ y } g'(\gamma) = h\left(g'_{|_\gamma}\right) \ \forall\, \gamma < \alpha,$$

demostraremos que $g = g'$ por medio de inducción transfinita.

[2] También se conoce como el Segundo Principio de Inducción.

Sea

$$T = \{\gamma \mid \gamma < \alpha \text{ y } g(\gamma) = g'(\gamma)\}.$$

Notemos que $T \subseteq \alpha$, debido a que $(T, \subseteq)$ es un COBO. Además, $T \neq \emptyset$ porque $g(0) = g'(0) = h(\emptyset)$.

Si $\gamma < \alpha$ y $\gamma \subseteq T$, entonces $g(\delta) = g'(\delta) \ \ \forall\ \delta \in \gamma$, es decir, $g_{|\gamma} = g'_{|\gamma}$. Así, $g(\gamma) = h\left(g_{|\gamma}\right) = h\left(g'_{|\gamma}\right) = g'(\gamma)$. Esto quiere decir que $\gamma \in T$. Por el Segundo Principio de Inducción, $T = \alpha$. Consecuentemente, $g(\gamma) = g'(\gamma)\ \forall\ \gamma < \alpha$. Por lo tanto, $g = g'$ .

Ahora, demostraremos la existencia de $g$. Supongamos que dados $\alpha$ y $h$, dicha función no existe. Sea

$$B = \left\{\beta \leq \alpha \mid \nexists\ g : \beta \to X \text{ con } g(\gamma) = h\left(g_{|\gamma}\right)\ \ \forall\ \gamma < \beta\right\},$$

Llamemos $\beta_0 = men\ B$. Para cada $\delta < \beta_0$, $\exists\ g_\delta : \delta \to X$ tal que $g_\delta(\gamma) = h\left(g_{\delta|\gamma}\right)\ \forall\ \gamma < \delta$. La función $g_\delta$ es única, por lo visto anteriormente. Si $\beta_0 = \emptyset$, entonces $\emptyset \xrightarrow{\emptyset} X$ cumple con la condición por vacuidad. Ahora, si $\beta_0 \neq \emptyset$, tenemos que $\beta_0 = \delta^+$ para algún $\delta$ ordinal, o bien, $\beta_0$ es un ordinal límite. Para $\beta_0 = \delta^+$, hay una función $g_\delta : \delta \to X$ tal que

$$g_\delta(\gamma) = h\left(g_{\delta|\gamma}\right) \quad \forall\ \gamma < \delta.$$

Como $dom\ h = \delta$, extendemos $g_\delta$ a la función $g : \delta \to X$ con

$$g(\gamma) = g_\delta(\gamma) = h\left(g_{\delta|\gamma}\right) = h\left(g_{|\gamma}\right)\ \ \forall\ \gamma < \delta$$

$$\text{y } g(\delta) = h(g_\delta) = h\left(g_{|\delta}\right).$$

Por ambas afirmaciones:

$$g(\gamma) = h\left(g_{|\gamma}\right) \quad \forall\ \gamma < \beta_0.$$

Entonces $\beta_0 \notin B$, contradicción.

Como $\beta_0$ no es un ordinal sucesor, entonces es un ordinal límite. Consideremos las funciones $g_\delta : \delta \to X \ \ \forall\ \delta < \beta_0$. Supongamos que $\delta < \xi < \beta_0$, entonces para

$$g_\xi : \xi \to X \text{ y } g_{\xi|\delta} : \delta \to X$$

se satisface que si $\gamma < \delta$ entonces

$$g_{\xi|\delta}(\gamma) = g_\xi(\gamma) = h\left(g_{\xi|\gamma}\right) = h\left(\left(g_{\xi|\delta}\right)_{|\gamma}\right).$$

Por unicidad, $g_\xi = g_{\xi|\delta}$ para $\delta < \xi < \beta_0$. Ahora, definamos

$$g : \beta_0 \to X \text{ por}$$

$$g(\delta) = g_{\delta^+}(\delta)\ \ \forall\ \delta < \beta_0.$$

Observe que $\delta^+ < \beta_0$, por ser $\beta_0$ un ordinal límite. Por lo tanto $g$ extiende cada función $g_\delta$. Pues si $\lambda < \delta$, entonces $g(\lambda) = g_{\lambda^+}(\lambda) = g_\delta(\lambda)$. Y si $\gamma < \beta_0$, obtenemos que $g(\gamma) = g_{\gamma^+}(\gamma) = h\left(g_{\gamma^+|\gamma}\right)\ \forall\ \gamma < \alpha$. ■

## 2.4. Números Cardinales.

**Definición 61** *Un número ordinal infinito $\alpha$ es un* ***aleph*** *(u* ***ordinal inicial****) si $\alpha$ no es equipotente con cualquier ordinal menor.*

**Ejemplos 17** ***1)*** *$\omega$ es el aleph más pequeño, ya que no es equipotente a cualquier número natural. Se denota por $\aleph_0$.*

***2)*** *$\omega+1$ no es un ordinal inicial porque es equipontente a $\omega$, como vimos en el ejemplo 16 (2). Similarmente, $\omega 2$ no lo es.*

**Definición 62** *Si $X$ es un conjunto, el* ***número cardinal*** *de $X$, es el número ordinal menor que es equipotente con $X$.*

**Notación 13** *Si el cardinal de $X$ es $\alpha$, escribimos $|X| = \alpha$.*

**Nota 10** *Para la existencia de el número cardinal de un conjunto $X$, es necesario el Teorema 23 del capítulo 3.*

**Observación 24** *Todos los números ordinales finitos y todos los alephs son números cardinales, y no hay otros cardinales.*

**Teorema 22** *Si $X$ y $Y$ son conjuntos se tiene que:*
*(i) $|X| = |Y| \Longleftrightarrow X$ y $Y$ son equipotentes.*
*(ii) $|X| \leq |Y| \Longleftrightarrow f : X \overset{inyectiva}{\rightarrow} Y$.*

**Demostración.** (i)
($\Longrightarrow$) Si $|X| = \alpha = |Y|$, significa que $\exists\ f : X \to \alpha$, $g : Y \to \alpha$ biyectivas. Entonces $g^{-1} \circ f : X \to Y$ es biyectiva. Por lo tanto, $X$ y $Y$ son equipotentes.
($\Longleftarrow$) Si $X$ y $Y$ son equipotentes, entonces para cualquier ordinal $\alpha$ tal que $f : \alpha \to X$ es biyectiva debe cumplirse también que $g : \alpha \to Y$ es biyectiva. Así, para el menor $\alpha$ tal que $f : \alpha \to X$ es biyectiva también $\alpha$ es el menor ordinal tal que $g : \alpha \to Y$ es biyectiva. Por lo tanto, $|X| = \alpha = |Y|$.

$$\therefore |X| = |Y| \Longleftrightarrow X \text{ y } Y \text{ son equipotentes.}$$

(ii)
($\Longrightarrow$) Supongamos que $\alpha = |X| \leq |Y| = \beta$. Entonces $\alpha \subseteq \beta$. Así podemos definir $f : X \to Y$ inyectiva por medio de $g : X \to \alpha$ biyectiva, la inclusión $i : \alpha \hookrightarrow \beta$, y $h : \beta \to Y$ biyectiva, donde $f = h \circ i \circ g$. Por lo tanto, $f : X \to Y$ inyectiva.
($\Longleftarrow$) Si $f : X \to Y$ inyectiva, $|X| = \alpha$ y $|Y| = \beta$, sea $\delta = |f(X)|$. Tenemos que $\alpha = \delta$, pues hay una biyección entre $X$ y $f(X)$. Sabemos también, que hay un buen orden $R$ tal que $ord(Y, R) = \beta$. Como $f(X) \subseteq Y$, $ord(f(X), R) \leq ord(Y, R)$. Entonces

$$\alpha = |X| = |f(X)| \leq ord(f(X), R) \leq ord(Y, R) = \beta.$$

$\therefore |X| \leq |Y| \Longleftrightarrow \exists\ f : X \overset{inyectiva}{\rightarrow} Y$. ■

### 2.4.1. El Número de Hartogs.

**Definición 63** *Si $X$ es un conjunto, el número ordinal menor que no es equipotente con ningún subconjunto de $X$ es llamado el* ***número de Hartogs*** *de $X$ y se denota por $\aleph$. En otras palabras, el número de Hartogs es el ordinal menor $\aleph$ tal que $\aleph \nleq |X|$.*

**Lema 2** *Si $X$ es un conjunto, entonces el número de Hartogs de $X$ es un aleph.*

**Demostración.** Sea $X$ un conjunto y $\aleph$ el número de Hartogs de $X$. Supongamos que $\aleph$ no es un ordinal inicial, entonces para algún $\beta < \aleph$ tenemos que $|\beta| = |\aleph|$. Como $\beta < \aleph$, entonces $\beta$ es equipotente a un subconjunto de $X$. Además, como $|\beta| = |\aleph|$, $\beta$ es equipotente a $\aleph$. Por lo anterior, $\aleph$ es equipotente a un subconjunto de $X$, esto contradice la definición del número de Hartogs. Por lo tanto, $\aleph$ es un ordinal inicial. ■

**Lema 3** *El número de Hartogs existe para todo conjunto $X$.*

**Demostración.** Sea $X$ un conjunto. Si $Y \subseteq X$ es tal que $(Y, R)$ es un COBO, entonces $\exists!$ $\alpha$ ordinal tal que $\alpha \cong Y$, por el Teorema 19. Así, para cada $R \in \wp(X \times X)$ que sea un buen orden $\exists!$ $\alpha$ tal que $\alpha \cong (Y, R)$. Entonces considero el conjunto $A = \{R \mid \alpha \cong (Y, R),\ \alpha \text{ ordinal}\}$.

Si P(x,y) es la afirmación: $x \in b$ y $y \cong x$ para un ordinal $y$, entonces por el Axioma de Reemplazo,[3]

$$B = \{y \mid (\exists x)\ \text{P(x,y)}\} \text{ es un conjunto.}$$

Entonces $B$ contiene a todos los ordinales equipotentes a un subconjunto de $X$. Ahora, si $f$ es una función inyectiva de $\alpha$ en $X$ y si denotamos $F = im\ f$, entonces $R = \{(f(\beta), f(\gamma)) \mid \beta < \gamma < \alpha\} \subseteq F \times F \subseteq X \times X$. Así, $R \subseteq X \times X$ es un conjunto bien ordenado isomorfo a $\alpha$.

Por último, si $P(x)$ es la propiedad de que $x$ es un ordinal equipotente a un subconjunto de $X$, aplicamos el Axioma de Especificación,[4] obtenemos el conjunto

$$\aleph = \{x \in B \mid x \text{ es un ordinal equipotente a un subconjunto de } X\}.$$

∴El número de Hartogs existe. ■

[3] Axioma (Esquema de Remplazo). Sea $P(x, y)$ una fórmula tal que para todo $x$ existe un único $y$ para el cual $P(x, y)$ se satisface.

Para cada conjunto $A$, existe un conjunto $B$ tal que, para todo $x \in A$, existe $y \in B$ para el cual $P(x, y)$ se satisface.

[4] Axioma (de especificación). Si $X$ es un conjunto y $p$ es una propiedad, los elementos de $X$ que tienen la propiedad $p$ forman un conjunto.

# Capítulo 3

# Axioma de Elección.

## 3.1. Formulación del Axioma de Elección.

**Definición 64** *Si* $\{X_i\}_{i\in I}$ *es una familia de conjuntos con* $X_i \neq \emptyset$, $\forall\ i \in I$, *una* ***función de elección*** *(o,* ***de selección****) para esta familia es una función* $f : I \to \underset{i\in I}{\cup}\{X_i\}$ *tal que* $f(i) \in X_i\ \forall\ i \in I$.

**Definición 65** *Si* $\{X_i\}_{i\in I}$ *es una familia de conjuntos con* $X_i \neq \emptyset\ \forall\ i \in I$, *su* ***producto cartesiano*** *es el conjunto* $\underset{i\in I}{\prod} X_i$, *formado por todas las funciones de elección* $f$ *para esta familia. En otras palabras,*

$$\underset{i\in I}{\prod} X_i = \{f : I \to \underset{i\in I}{\cup}\{X_i\} \mid f(i) \in X_i \forall i \in I\}.$$

El **Axioma de Elección (AE)**, establece que para cada familia $\{X_i\}_{i\in I}$, $I \neq \emptyset$, $X_i \neq \emptyset$, $\forall\ i \in I$, el producto $\underset{i\in I}{\prod} X_i \neq \emptyset$.

**Observación 25** *El Axioma de Elección también puede enunciarse como sigue:*

***1.*** *Existe una función de elección para cada familia no vacía de conjuntos no vacíos.*

***2.*** *Si* $X \neq \emptyset$ *es un conjunto, entonces existe* $f : \wp(X) \setminus \{\emptyset\} \to X$ *tal que* $f(A) \in A\ \forall A \in \wp(X) \setminus \{\emptyset\}$. *(En este caso, vemos a* $I = \wp(X) \setminus \{\emptyset\}$ *y la famila correspondiente sería* $\{A_B\}_{B\in I} = \{A_B \mid A_B = B \subseteq \wp(X) \setminus \{\emptyset\}\}$,*así por el axioma de elección* $\exists\ f : I \to X = \cup\{A_B\}_{B\in I}$ *con* $f(A_B) \in A_B\ \forall B \in I$.*).*

## 3.2. Algunas equivalencias del Axioma de Elección.

**Teorema 23** *Son equivalentes:*

**(1)** El **Axioma de Elección**.

**(2)** El **Teorema del Buen Orden (TBO)**: Todo conjunto puede bien ordenarse.

**Demostración.** (1) $\Longrightarrow$ (2)

Si $X$ es un conjunto entonces, por el AE, existe $f : \wp(X) \setminus \{\emptyset\} \to X$ tal que $f(A) \in A$, $\forall\ A \in \wp(X) \setminus \{\emptyset\}$. Por el Teorema de Recursión Transfinita, construimos mediante la aplicación sucesiva de $f$ la función $g : \alpha \to X$ con $g(\gamma) = f(X \setminus \{g(\delta) \mid \delta < \gamma\})\ \forall\ \gamma < \alpha$. Ahora, elegiremos $\alpha$ de manera adecuada. Para obtenerlo, consideremos $B = \{R \mid (C, R)$ es un COBO para $C \subseteq X\}$. Por el Teorema 19 (Capítulo 2), si $R \in B$, $\exists!\ ord\,(C, R)$ tal que $ord\,(C, R) \cong C$. Así, podemos definir $h : B \to ord$[1] con $h(R) = ord\,(C, R)\ \forall R \in B$. Así a cada relación $R$ le asigno un único ordinal $\alpha \in \text{Im}\,(h)$.

Ahora, si P(x,y) es la afirmación: $x \in B$ y $y = h(x)$, por el Teorema de Remplazamiento, existe un conjunto $D = \{y \mid (\exists x)\ \text{P(x,y)}\}$. También se tiene que $D = \{\varepsilon \text{ ordinal} \mid \varepsilon = h(R)\ \forall R \in B\}$. Por el Teorema 18, sabemos que no existe un conjunto de todos los ordinales, entonces existe un ordinal $\gamma \notin D$.

Definimos

$$E = \{\delta \text{ ordinal} \mid \delta \leq \gamma,\ \delta \notin D\},$$

entonces $E \neq \emptyset$, además por el Teorema 17 $E$ es un COBO, por lo tanto existe el ordinal menor $\alpha$ que no está en $D$.

Sin embargo, con esta elección de $\alpha$, surge un problema en la construcción. Ya que puede suceder que $(X \setminus \{g(\delta) \mid \delta < \gamma\}) = \emptyset$ para algún $\gamma < \alpha$, esto implicaría que no existiría $f(X \setminus \{g(\delta) \mid \delta < \gamma\})$. Para evitar dicha situación, damos un valor arbitario $b$ a $f$ en el valor $\emptyset$, es decir, $f(\emptyset) = b$ para algún $b \notin A$. Antes de proseguir, haremos dos observaciones:

**(a)** Si $\gamma < \alpha$ y $g(\gamma) \neq b$, entonces para $\xi < \gamma$, $g(\xi) \neq g(\gamma)$, ya que $g(\gamma) \notin \{g(\xi) \mid \xi < \gamma\}$.

**(b)** Si $g(\gamma) = f(\emptyset) = b$ para algún $\gamma < \alpha$, entonces $g(\gamma') = b\ \forall\ \gamma < \gamma' < \alpha$.

Entonces hay dos casos a considerar:

(i) $g(\gamma) \neq b\ \forall\ \gamma < \alpha$.

(ii) $g(\gamma) = b$ para algún $\gamma < \alpha$.

Si sucediera (i), tenemos que $\{g(\gamma) \mid \gamma < \alpha\} \subseteq X$. Por (a), sabemos que $\{g(\gamma) \mid \gamma < \alpha\}$ es inyectiva. Entonces $g$ es una biyección entre $\alpha$ y $\{g(\gamma) \mid \gamma < \alpha\}$. Así, por la Observación 23 del Capítulo 2, $\{g(\gamma) \mid \gamma < \alpha\}$ es un conjunto bien ordenado. Entonces $\{g(\gamma) \mid \gamma < \alpha\} \cong \alpha$. Por lo que $\alpha \in D$, contradicción.

En el caso (ii), sea $\beta = mín\ \{\gamma \in ord \mid g(\gamma) = b\}$. Se cumple que $\{g(\delta) \mid \delta < \beta\} = X$. (Porque $g(\beta) = b \Longrightarrow (X \setminus \{g(\delta) \mid \delta < \beta\}) = \emptyset$. Así, $\{g(\delta) \mid \delta < \beta\} = X$). Como $\beta$ es el menor de los ordinales tal que $g(\beta) = b$, todo $\delta < \beta$ cumple que $g(\delta) \neq \emptyset$. Por esto, también $g$ es inyectiva de $\beta$ a $\{g(\delta) \mid \delta < \beta\}$. Esto se ve si sustituimos en (a), $\gamma$ por $\delta$ y $\alpha$ por $\beta$. Entonces, $X$ está bien ordenado con el orden inducido por la biyección $g$ entre $X$ y $\beta$. Así, $X \cong \beta$.

Por lo tanto, $X$ se puede bien ordenar.

**(2) $\Longrightarrow$ (1)**

[1] *ord* denota la clase de los ordinales.

Si $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$, $\forall\, i \in I$. Como cada $X_i$ puede bien ordenarse y $X_i \neq \emptyset$, $\forall\, i \in I$, puedo elegir $men\,(X_i) = x_i$, $\forall\, i \in I$. Si $f : I \to \cup\{X_i\}$, $i \mapsto x_i$, entonces $f \in \prod_I \{X_i\}$ Por lo tanto se cumple AE.

$$\therefore \prod_I \{X_i\} \neq \emptyset.$$

$\therefore$ AE y TBO son equivalentes. ■

**Teorema 24** *Son equivalentes:*

**(1)** El Axioma de Elección.

**(2)** Si $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$, $\forall i \in I$, con $X_i \cap X_j = \emptyset$, entonces $\exists\, Y$ conjunto con $|Y \cap X_i| = 1\ \forall\ i \in I$.

**Demostración. (1) $\Longrightarrow$ (2)**

Si $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$, $\forall i \in I$, con $X_i \cap X_j = \emptyset$. Sea $X = \bigcup_{i\in I} \{X_i\}$, entonces $\{X_i\}_{i\in I} \subseteq \wp(X)$. Por AE, $\exists : \wp(X) \setminus \{\emptyset\} \to X$ tal que $f(A) = a \in A$ $\forall A \in \wp(X) \setminus \{\emptyset\}$. Ahora, si $Y = f(\{X_i\}_{i\in I}) = \{f(X_i) = x_i \mid i \in I\}$, tenemos que $Y \cap X_j = f(\{X_i\}_{i\in I}) \cap X_j = \{x_j\}$. Como $|Y \cap X_j| = |\{x_j\}|$ y $|\{x_j\}| = 1$, concluimos la demostración.

$$\therefore \exists Y \text{ tal que } |Y \cap X_i| = 1\ \forall i \in I.$$

**(2) $\Longrightarrow$ (1)**

Si $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$, $\forall i \in I$. Definimos la familia

$$\{A_i\}_{i\in I} = \{\{i\} \times X_i \mid i \in I\}.$$

Como $X_i \neq \emptyset$, $\forall i \in I$, entonces $A_i \neq \emptyset$. Además, si $i \neq j$, tenemos que $A_i \cap A_j = (\{i\} \times X_i) \cap (\{j\} \times X_j) = \emptyset$. Así, por **(2),** $\exists\, Y$ tal que $Y \cap (\{i\} \times X_i) = \{(i, x_i)\}$ $\forall i \in I$. Entonces, $f = \{(i, x_i) \mid i \in I\}$ es una función, es decir, $\exists$ $f : I \to \bigcup_{i\in I} \{X_i\}$ tal que $f(i) = x_i \in X_i$. ■

**Definición 66** *Si $A$ es un conjunto y $B \subseteq A$. Decimos que $B$ es una* ***cadena,*** *si cualesquiera dos elementos de $B$ son comparables.*

*Si cualesquiera dos elementos de $B$ son incomparables, $B$ se llama* ***anticadena.***

**Ejemplos 18** *Si tomamos la divisibilidad en $\mathbb{N}$, entonces:*

***1.*** *$A = \{3^n \mid n \in \mathbb{N}\}$ es una cadena.*

***2.*** *$B = \{p \mid p$ primo$\}$ es una anticadena.*

**Observación 26** *El conjunto $\emptyset$, por vacuidad, es una cadena y una anticadena.*

**Proposición 17** *Si $K$ es una cadena y si $A \subseteq K$, entonces $A$ es una cadena.*

**Demostración.** Es claro. ■

**Proposición 18** *Si $B \subseteq A$ y $A$ es una anticadena, entonces $B$ es una anticadena.*

**Demostración.** Si $b_1, b_2 \in B \subseteq A$, como $A$ es una anticadena, entonces $b_1, b_2$ no son comparables. Así, $B$ es una anticadena. ■

**Definición 67** *Una familia de conjuntos $\mathcal{F}$ se llama de **carácter finito,** si*

$$A \in \mathcal{F} \text{ si y sólo si } B \in \mathcal{F} \text{ para cada } B \subseteq A,\ B \text{ finito.}$$

**Lema 4** *Si $\mathcal{F}$ es una familia de carácter finito y si $K$ es una cadena en $\mathcal{F}$ con respecto a $\subseteq$, entonces $\cup K \in \mathcal{F}$.*

**Demostración.** Por la Definición 67, basta mostrar que $A \in \mathcal{F}$, $\forall\ A \subseteq \cup K$, $A$ finito. Si $A = \{a_1, ..., a_n\} \subseteq \cup K$, entonces $\exists\ A_i \in K$ tal que $x_i \in A_i$ $\forall\ i \in \{1, ..., n\}$. Ahora, como $K$ es una cadena hay un $j \in \{1, ..., n\}$ tal que $A_i \subseteq A_j\ \forall\ i \in \{1, ..., n\}$. Así, $a_i \in A_j\ \forall\ i \in \{1, ..., n\}$. Entonces $A \subseteq A_j$. Además, $A_j \in \mathcal{F}$.

$A \in \mathcal{F}$ si y sólo si $B \in \mathcal{F}\ \forall B \subseteq A$, $B$ finito. Como $A$ es un subconjunto finito de $A_j$ y $A_j \in \mathcal{F}$, entonces $A \in \mathcal{F}$. ■

**Teorema 25** *Son equivalentes:*

***(1)*** *AE.*

***(2) Condición de la Cadena Máxima de Hausdorff:*** *Cada conjunto parcialmente ordenado contiene una cadena máxima.*

***(3) Lema de Zorn:*** *Si en un conjunto parcialmente ordenado $X$ cada cadena tiene una cota superior, entonces $X$ tiene un elemento máximo.*

***(4) Lema de Teichmüller-Tukey:*** *Si una subcolección no vacía $\mathcal{L}$ de $\wp(X)$ es de caracter finito, entonces $\mathcal{L}$ contiene un elemento máximo, con respecto a $\subseteq$.*

***(5)*** *Cada conjunto preordenado[2] contiene una anticadena máxima.*

**Demostración. (1)$\Longrightarrow$ (2)**

Si $X$ es finito la afirmación es inmediata.

Supongamos que $X$ es un conjunto infinito parcialmente ordenado que no contiene una cadena máxima. Si $K$ es una cadena en $X$ llamamos $C(K) = \{x \in (X \setminus K) \mid K \cup \{x\} \text{ es una cadena}\}$. Observemos que $C(K) \neq \emptyset$, porque $K$ no es una cadema máxima en $X$. Por AE, $\exists\ f : \wp(X) \setminus \{\emptyset\} \to X$ con $f(A) \in A$, $\forall\ A \in \wp(X) \setminus \{\emptyset\}$. Si $\aleph$ es el número de Hartogs de $X$ entonces, por recursión transfinita, definimos $g : \aleph \to X$ tal que $g(\alpha) = f(C(\{g(\beta) \mid \beta < \alpha\}))$.

Mostraremos que $g$ es inyectiva y por lo tanto $\aleph \leq |X|$, contradiciendo la elección de $\aleph$.

Mostraremos que $\{g(\beta) \mid \beta < \alpha\}$ es una cadena también por Inducción Transfinita:

(i) Si $\alpha = 0$, entonces $g(0) = \emptyset$ que es una cadena por la Observación 20.

[2] $X$ es un **conjunto preordenado** si tiene definida una relación $R$ que es reflexiva y transitiva. A $R$ se le llama **preorden.**

(ii) Si $\alpha = \delta^+$. Supongamos que si $\beta < \alpha$, se cumple que $\{g(\xi) \mid \xi < \beta\}$ es una cadena. Como $\delta < \alpha = \delta \cup \{\delta\}$, tenemos que $\{g(\beta) \mid \beta < \delta\}$ es una cadena. Ahora, supongamos que para algún $\beta < \delta$, $g(\beta)$ es incomparable con $g(\delta)$, entonces $\delta \geq \alpha$, contradiciendo la elección de $\alpha$. Entonces $g(\delta)$ es comparable con $g(\beta)\ \forall\ \beta < \delta$. Por lo tanto, $\{g(\beta) \mid \beta < \alpha\} = \{g(\beta) \mid \beta < \delta\} \cup \{g(\delta)\}$ es una cadena.

(iii) Si $\alpha$ es un ordinal límite. Supongamos que $\{g(\delta) \mid \delta < \beta\}$ es una cadena, $\forall \beta < \alpha$. Si $\delta < \alpha$, entonces también $\delta^+ < \alpha$, por ser $\alpha$ un ordinal límite.

Si $\beta_1 < \beta_2 < \alpha$ entonces $\beta_1 < \beta_2 < \beta_2^+ < \alpha$ y $\left\{g(\beta) \mid \beta < \beta_2^+\right\}$ es una cadena por hipótesis.

$$\therefore g(\beta_1) \text{ y } g(\beta_2) \text{ son comparables.}$$

De (i), (ii) y (iii), concluimos que $\{g(\beta) \mid \beta < \alpha\}$ es una cadena ( y por lo tanto $g$ está bien definida).

Por último, veremos que $g$ es inyectiva. Si $g(\alpha_1) = g(\alpha_2)$. Supongamos que $\alpha_1 \neq \alpha_2$. Sin pérdida de generalidad consideremos $\alpha_1 < \alpha_2$. Llamemos $K_{\alpha_i} = \{g(\beta) \mid \beta < \alpha_i\}$ para $i = 1, 2$. Como $\alpha_1 < \alpha_2$, entonces $g(\alpha_1) \in K_{\alpha_2}$. Por otro lado, $g(\alpha_2) = f(C(K_{\alpha_2})) \in C(K_{\alpha_2})$, es decir, $g(\alpha_2) \in (X \setminus K_{\alpha_2})$. De $g(\alpha_1) = g(\alpha_2)$ y $g(\alpha_2) \in (X \setminus K_{\alpha_2})$, tenemos que $g(\alpha_1) \in (X \setminus K_{\alpha_2})$, contradicción. Entonces $\alpha_1 = \alpha_2$. Por lo tanto, $g$ es inyectiva.

$\aleph \xrightarrow{g} X$ inyectiva implica que $\aleph \leq |X|$, contradiciendo que $\aleph$ es el número de Hartogs de $X$.

**(2) $\Longrightarrow$ (3)**

Si $(X, R)$ es un COPO en el que cada cadena $K$ tiene una cota superior. Por **(2),** existe una cadena máxima $K'$en $X$. Sea $k' \in X$, la cota superior de $K$. Demostraremos que $k'$ es un elemento máximo de $X$. De lo contrario, existiría algún $y \in X$ tal que $k < y$, entonces $K \cup \{y\}$ sería una cadena. Además, como $K' \subseteq K' \cup \{y\}$, tendríamos que $K'$ no es máxima, contradicción. Por lo tanto, $k'$ es máximo en $X$.

**(3)$\Longrightarrow$ (4)**

Si $\mathcal{L}$ es una subcolección de $\wp(X)$ con $\mathcal{L} \neq \emptyset$ y $\mathcal{L}$ de carácter finito. Como $\subseteq$ es un orden parcial en $\wp(X)$, entonces $(\mathcal{L}, \subseteq)$ es un COPO. Ahora, denotemos $A = \{K \subseteq \mathcal{L} \mid K \text{ es una cadena en } \mathcal{L}\}$. Por la Observación 26, $\emptyset$ es una cadena, entonces $A \neq \emptyset$. Tenemos que cada elemento $K$ de $\mathcal{L}$ está acotado superiormente por $\cup K$, por el Lema 4**,** $\cup K \in \mathcal{L}$. Todo lo anterior muestra que se satisfacen las hipótesis del Lema de Zorn, así que $\mathcal{L}$ tiene un elemento máximo.

**(4) $\Longrightarrow$ (5)**

Si $X$ es un conjunto preordenado. Definamos

$$\mathcal{L} = \{A \subseteq X \mid A \text{ es una anticadena}\}.$$

Como $\emptyset$ es una anticadena (Observación 26), entonces $\mathcal{L} \neq \emptyset$. A continuación, mostraremos que $\mathcal{L}$ es de carácter finito. Si $A \in \mathcal{L}$, y $B \subseteq A$, $B$ finito, entonces $B$ es una anticadena, por la Proposición 18. Por esto $B \in \mathcal{L}$. Ahora, si $B \subseteq A$, $B$ finito y $B \in \mathcal{L}$, tenemos que $A \in \mathcal{L}$. Pues si $a_1, a_2 \in A$, entonces

$B = \{a_1, a_2\} \subseteq A$ con $a_1, a_2$ incomparables. Por lo tanto $\mathcal{L}$ es de carácter finito. Por **(4),** $\mathcal{L}$ contiene un elemento máximo.

$$\therefore X \text{ contiene una anticadena máxima.}$$

**(5) $\Longrightarrow$ (1)**

Sea $I \neq \emptyset$ y $\{X_i\}_{i\in I}$, $X_i \neq \emptyset, \forall i \in I$. Consideremos $X = \{(x,i) \mid i \in I,\ x \in X_i\}$. Definimos una relación $R$ en $X$ de la siguiente forma: $(x,i)\,R\,(y,j) \Longleftrightarrow i = j$. Notemos que $R$ cumple:

(i) $(x,i)\,R\,(x,i)$.

(ii) $(x,i)\,R\,(y,j)$ y $(y,j)\,R\,(z,k) \Longrightarrow i = j$ y $j = k \Longrightarrow (x,i)\,R\,(z,k)$.

Por (i) y(ii), $R$ es reflexiva y transitiva, entonces $R$ es un preorden. Así, $(X,R)$ es un conjunto preordenado. Por **(5),** $X$ contiene una anticadena máxima que es de la forma $K = \{(x_i,i) \mid i \in I\}$. Así, para cada $i \in I$, $x_i \in X_i\ \forall i \in I$, entonces definimos $f : I \to \underset{i\in I}{\cup}\{X_i\}$ tal que $f(i) = x_i\ \forall\ i \in I$. ■

**Teorema 26** *Son equivalentes:*

***(1)** AE.*

***(2)** El **Axioma de Elección Múltiple (AEM):** Dado $I \neq \emptyset$ para cada $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$, $\forall\ i \in I$, $\exists\ \{F_i\}_{i\in I}$, $F_i \neq \emptyset$, $F_i$ finito con $F_i \subseteq X_i\ \ \forall\ i \in I$.*

***(3) Condición de la Anticadena Máxima de Kurepa**: Cada conjunto parcialmente ordenado contiene una anticadena máxima.*

**Demostración. (1) $\Longrightarrow$ (2)**

Si $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$, $\forall\ i \in I$. Por el AE, $\exists\ f : I \to \underset{i\in I}{\cup}\{X_i\}$ tal que $f(i) = x_i \in X_i\ \forall\ i \in I$. Tomando $F_i = \{x_i\}$, $i \in I$. Entonces $F_i \neq \emptyset\ \forall\ i \in I$ y $F_i$ finito con $F_i \subseteq X_i\ \ \forall\ i \in I$.

$$\therefore \text{ se cumple el AEM.}$$

**(2) $\Longrightarrow$ (3)**

Si $X$ es un conjunto parcialmente ordenado. Por AEM, $\exists\ f : \wp(X) \setminus \{\emptyset\} \to \{B \in \wp(X) \mid B \text{ finito}\}$ tal que $f(A) \subseteq A\ \forall\ A \in \wp(X) \setminus \{\emptyset\}$. Tomamos $g(A) = \{x \mid x \text{ es mínimo de } f(A)\}$. Cada $g(A) \neq \emptyset$, ya que $f(A)$ es un conjunto finito. Como los elementos de $g(A)$ son mínimos, estos son incomparables entre ellos, y así $g(A)$ es una anticadena finita no vacía.

Por otro lado, para una anticadena $K$ de $X$, llamamos $C(K) = \{x \in (X \setminus K) \mid K \cup \{x\}\}$ es una anticadena$\}$. Supongamos que $X$ no contiene un anticadena máxima, entonces $C(K) \neq \emptyset$. Si $\aleph$ es el número de Hartogs de $\wp(X)$, definimos $h : \aleph \to \wp(X)$ por recursión transfinita:

$$h(\alpha) = \underset{\beta<\alpha}{\cup} h(\beta) \cup g(C(\underset{\beta<\alpha}{\cup} h(\beta))).$$

Para ver que h está bien definida, notemos que

i) $h(0) = \emptyset \cup g(C(\emptyset)) = \emptyset \cup g(X) = g(X)$, que es independiente finito y $\neq 0$.

ii) $g(C(\underset{\beta<\alpha}{\cup} h(\beta))$ es finito no vacío y no está contenido en $\underset{\beta<\alpha}{\cup} h(\beta)$.

iii) Por definición, $\beta < \alpha \Longrightarrow h(\beta) \subsetneqq h(\alpha)$.

Usando ii) y iii) por inducción cada $h(\alpha)$ es independiente.
iv) $\alpha < \beta \Longrightarrow h(\alpha) \neq h(\beta)$.

$$\therefore h : \aleph \to \wp(X) \text{ es inyectiva. Lo que contradice.}$$

**(3) $\Longrightarrow$ (1)**
Si $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$ $\forall i \in I$, $I \neq \emptyset$. Llamamos $X = \{X_i\}_{i\in I}$ y $Y = \{(X_i, x_i) \mid X_i \subseteq X \text{ y } x_i \in X_i\}$. Definimos una relación $R$ por la siguiente regla:

$$(X_i, x_i)R(X_j, x_j) \Longleftrightarrow X_i = X_j \text{ y } x_i \leq x_j \text{ en } X.$$

Ahora, se satisface:
(i) $(X_i, x_i)R(X_i, x_i)$.
(ii) $(X_i, x_i)R(X_j, x_j)$ y $(X_j, x_j)R(X_k, x_k) \Longrightarrow (X_i = X_j \text{ y } x_i \leq x_j \text{ en } X)$ y $(X_j = X_k \text{ y } x_j \leq x_k \text{ en } X)$. Esto sucede, sólo si $X_i = X_k$ y $x_i \leq x_k$ en $X$, lo que significa que $(X_i, x_i)R(X_k, x_k)$. Así, $R$ es transitiva.
(iii) $(X_i, x_i)R(X_j, x_j)$ y $(X_j, x_j)R(X_i, x_i) \Longrightarrow (X_i = X_j \text{ y } x_i \leq x_j \text{ en } X)$ y $(X_j = X_i \text{ y } x_j \leq x_i \text{ en } X)$. Entonces, $X_i = X_j$ y $x_i = x_j$ en $X$, por lo que $(X_i, x_i) = (X_j, x_j)$. Lo que significa, que $R$ es antisimétrica.

Por lo tanto, $R$ es un orden parcial. Entonces, por **(3)**, $Y$ contiene una anticadena máxima. Una anticadena $K$ de $Y$ tiene la forma $K = \{(X_i, x(X_i)) \mid X_i \subseteq X\}$ donde cada $x(X_i)$ es un distinguido elemento de $X_i$ para cada $i \in I$. Es decir, $\exists\, x : I \to \cup\{X_i\}_{i\in I}$ tal que $x(X_i) \in X_i \;\forall\; i \in I$. ■

## 3.3. Espacios Vectoriales y el Axioma de Elección.

### 3.3.1. Espacios Vectoriales.

**Definición 68** *Si $K$ es un campo. Un **espacio vectorial** es una quinteta $(V, \tilde{+}, \bar{0}, K, \cdot : K \times V \to V)$, tal que:*

***1.*** *$(V, \tilde{+}, \bar{0})$ es un grupo abeliano.*
***2.*** *$\cdot : K \times V \to V$ satisface:*
***a)*** $1 \cdot v = v$, $\forall v \in V$.
***b)*** $(cd) \cdot v = c \cdot (d \cdot v)$, $\forall c, d \in K$, $\forall v \in V$.
***c)*** $(c + d) \cdot v = c \cdot v + d.c$, $\forall c, d \in K$, $\forall v \in V$.
***d)*** $c \cdot (v \tilde{+} w) = c \cdot v + c \cdot w, \forall c \in K$, $\forall v, w \in V$.

*Los elementos de $V$ se llaman **vectores,** los elementos de $K$ se llaman **escalares,** y cuando sea claro como se definieron las operaciones, escribiremos ${}_KV$ en lugar de toda la quinteta ordenada. ${}_KV$ se lee: $V$ es un espacio vectorial sobre el campo $K$.*

**Definición 69** *Si ${}_KV$ es un espacio vectorial y $\emptyset \neq U \subseteq {}_KV$. Un vector $v \in {}_KV$ es llamado una **combinación lineal** de vectores de $U$ si existe $\{u_1, ..., u_n\} \subseteq$*

*$U$ y $\{k_1, ..., k_n\} \subseteq K$ tales que*

$$v = \sum_{i=1}^{n} k_i u_i.$$

**Definición 70** *Si ${}_K V$ es un espacio vectorial y $\emptyset \neq G \subseteq {}_K V$. Entonces el conjunto **generado** por $G$, es el conjunto que consiste en todas las combinaciones lineales de los vectores en $G$. Se denota como $\langle G \rangle$. Si $A = \langle G \rangle$, decimos que $G$ **genera** a $A$.*

**Definición 71** *Si ${}_K V$ es un espacio vectorial y $U \subseteq {}_K V$, entonces $U$ es llamado **linealmente dependiente** si existen $\{u_1, ..., u_n\} \subseteq U$, con $u_i \neq u_j$, $\forall i, j \in \{1, ..., n\}$, y $\{k_1, ..., k_n\} \subseteq K$, con $k_i \neq 0$ para al menos una $i \in \{1, ..., n\}$, tales que*

$$\sum_{i=1}^{n} k_i u_i = 0.$$

**Definición 72** *Si ${}_K V$ es un espacio vectorial y $U \subseteq {}_K V$ y no es linealmente dependiente entonces decimos que $U$ es **linealmente independiente.***

**Observación 27** *Si $A$ es un subconjunto linealmente independiente en un espacio vectorial ${}_K V$ y si $v \in {}_K V$, $v \notin A$. Entonces $A \cup \{v\}$ es linealmente dependiente si y sólo si $v \in \langle A \rangle$.*

**Demostración.** Se omite. ■

**Definición 73** *Si ${}_K V$ es un espacio vectorial y $A \subseteq {}_K V$. Un **subconjunto linealmente independiente máximo** $B$ de $A$, es un $B \subseteq A$ que satisface:*

***(a)** $B$ es un conjunto linealmente independiente.*

***(b)** El único conjunto linealmente independiente de $A$ que contiene a $B$ es el mismo $B$.*

**Definición 74** *Si ${}_K V$ es un espacio vectorial, $\beta \subseteq {}_K V$ es una **base** para ${}_K V$ si $\beta$ es linealmente independiente y $\langle \beta \rangle = {}_K V$.*

**Teorema 27** *Si ${}_K V$ es un espacio vectorial y $\beta = \{u_1, ..., u_n\} \subseteq {}_K V$. Entonces $\beta$ es una base para ${}_K V$ si y sólo si cada $v \in {}_K V$ puede expresarse de forma única como combinación lineal de vectores de $\beta$,*

$$v = \sum_{i=1}^{n} k_i u_i, \ u_i \in \beta$$

*para escalares únicos $k_i$ para $i = 1, ..., n$.*

**Demostración.** ($\Longrightarrow$) Si $\beta$ es una base para ${}_KV$. Si $v \in {}_KV$, entonces $v \in \langle\beta\rangle$, es decir que $v$ es una combinación lineal de vectores de $\beta$. Ahora, supongamos que

$$v = \sum_{i=1}^{n} k_i u_i \text{ y } v = \sum_{i=1}^{m} l_i u_i$$

para $k_i$, $l_i \in K$. Agregando unos cuántos ceros podemos suponer que $n = m$ y que las $u_i$ son las mismas de cada lado, entonces

$$\sum_{i=1}^{n} k_i u_i = \sum_{i=1}^{n} l_i u_i,$$

esto implica

$$\sum_{i=1}^{n} (k_i - l_i) u_i = 0.$$

Como $\beta$ es linealmente independiente por ser una base, tenemos que $k_i - l_i = 0 \ \forall i \in \{1, ..., n\}$. Entonces $k_i = l_i \ \forall i \in \{1, ..., n\}$. Por lo tanto la expresión de $v$ como combinación lineal de vectores de $\beta$ es única.

($\Longleftarrow$) Que ${}_KV = \langle\beta\rangle$, se sigue directamente de la hipótesis.

Si $\beta$ fuera linealmente dependiente

$$\exists 0 \neq k_1 u_1 + ... + k_n u_n \text{ con } u_i \in \beta \text{ y } k_i \neq 0 \ \forall i.$$

Si $n > 1$, entonces

$$k_n u_n = -k_1 u_1 - ... - k_{n-1} u_{n-1},$$

contradiciendo la unicidad.

Si $n = 1$, entonces $k_1 u_1 = 0$, con $k_1 \neq 0$ y $u_1 \in \beta$.

$$u_1 = 0 \in \beta.$$

Hay dos casos:

(i) $\beta = \{0\}$.

(ii) $\beta \neq \{0\}$.

Si (i). Entonces $0 = 1 \cdot 0 = 2 \cdot 0$, contradiciendo la unicidad.

Si (ii), sea $0 \neq u \in \beta$. Entonces $u = u + 1 \cdot 0$, nuevamente contradiciendo la unicidad. ■

**Observación 28** *Notemos que una base $\beta$ es un subconjunto linealmente independiente máximo, porque:*

***1.*** *$\beta$ es un conjunto linealmente independiente.*

***2.*** *Si $v \in {}_KV$ y $v \notin \beta$, entonces $\beta \cup \{v\}$ es linealmente dependiente pues $\langle\beta\rangle = {}_KV$, por la Observación 27.*

### 3.3.2. El AE es equivalente a que cada espacio vectorial tiene una base.

**Teorema 28** *Son equivalentes:*

***1.*** *Cada espacio vectorial tiene una base.*

***2.*** *AE*

**Demostración.** (1) $\Longrightarrow$ (2)

Por el Teorema 26, sabemos que el AE es equivalente al AEM, así que basta mostrar que (1) implica el AEM.

Si $\{X_i\}_{i\in I}$, $X_i \neq \emptyset$, $X_i \cap X_j = \emptyset$, $\forall i \in I \neq \emptyset$. Sea $X = \underset{i\in I}{\cup}\{X_i\}$. Si $K$ es un campo, denotemos por $K(X)$ es el campo de funciones racionales en las variables $x \in X$ sobre $K$.

Consideremos los monomios $p \in K[X]$, como en la Observación 9 del Capítulo 1 (pág. 12). Definimos el $i$-**grado** de un monomio $p = \lambda x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m}$ como el grado total del monomio (Definición 27, pág. 13) para cada $i \in I$, es decir, el $i$-grado de $p$ como $d_i(p) = \sum\limits_{x_k \in X_i} n_k$.

Si $h \in K(X)$ entonces $h = \frac{f}{g}$ donde $f, g \in K[X]$ y $g(x) \neq \bar{0}$. Tenemos que $h = \frac{p_1+\ldots+p_n}{q_1+\ldots+qm}$ donde $p_k$, $q_k$ son monomios de $K[X]$. Cuando cada $q_k$ tiene el mismo $i$-grado, $d_1$, y cada $p_k$ es del mismo $i$-grado $d_2$, decimos que el elemento $h \in K(X)$ es $i$-**homogéneo de grado** $d = d_2 - d_1$.

Tomemos

$$A = \{a \in K(X) \mid a \text{ es } i\text{-homogéneo de grado 0 para cada } i \in I\} \cup \{0\}.$$

Notemos que si $a = \frac{p_1+\ldots+p_n}{q_1+\ldots+q_m} \in A$ es $i$-homogéneo de grado 0 entonces $d_1 = d_2$, esto significa que todos los monomios $p_k$ y $q_k$ son del mismo $i$-grado.

Ahora, demostraremos que $A \underset{campo}{\leq} K(X)$.

Si $a = \frac{p_1+\ldots+p_n}{q_1+\ldots+q_m}$, $b = \frac{p'_1+\ldots+p'_{n'}}{q'_1+\ldots+q'_{m'}} \in K(X)$, vemos que:

**(i)**

$$\begin{aligned} a+b &= \frac{p_1+\ldots+p_n}{q_1+\ldots+q_m} + \frac{p'_1+\ldots+p'_{n'}}{q'_1+\ldots+q'_{m'}} = \\ &= \frac{(p_1+\ldots+p_n)(q'_1+\ldots+q'_{m'}) + (q_1+\ldots+q_m)(p'_1+\ldots+p'_{n'})}{(q_1+\ldots+q_m)(q'_1+\ldots+q'_{m'})} = \\ &= \frac{c}{e}. \end{aligned}$$

Pero $d_i(p_k) = d_i(q_k) = d_1$ y $d_i(p'_k) = d_i(q'_k) = d_2$, entonces

$$d_i(p_k q'_k) = d_1 + d_2 = d_i(q_k p'_k), y, d_i(q_k q'_k) = d_1 + d_2.$$

Como $d_i(p_k q'_k) = d_i(q_k p'_k) = d_1 + d_2$, implica que $d_i(c) = d_1 + d_2$. De $d_i(c) = d_i(e)$, tenemos que $a + b$ es $i$-homogénea de grado 0.

Entonces $a + b \in A$.

**(ii)** Entonces $\bar{0} \in A$, por definición de $A$.

**(iii)** $a = \frac{p_1+\ldots+p_n}{q_1+\ldots+q_n} \Longrightarrow -a = \frac{(-p_1)+\ldots+(-p_n)}{q_1+\ldots+q_n} = \frac{-(p_1+\ldots+p_n)}{q_1+\ldots+q_n}$

donde $-p_k = -\lambda x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m}$ para $\lambda \in K$. Así, $d_i(p_k) = d_i(-p_k)$. Además, como $d_i(p_k) = d_i(q_k)$, entonces $d_i(p_k) = d_i(q_k) = d_i(-p_k)$.

Entonces $-a \in A \ \forall a \in A$.

Por **(i), (ii)** y **(iii),** $(A, +, \bar{0})$ es un subgrupo abeliano de $(K(X), +, \bar{0})$.

**(iv)** $ab = (\frac{p_1+\ldots+p_n}{q_1+\ldots+q_m})(\frac{p'_1+\ldots+p'_{n'}}{q'_1+\ldots+q'_{m'}}) = \frac{(p_1+\ldots+p_n)(p'_1+\ldots+p'_{n'})}{(q_1+\ldots+q_m)(q'_1+\ldots+q'_{m'})}$.

Como $d_i(p_k) = d_i(q_k) = d_1$ y $d_i(p'_k) = d_i(q'_k) = d_2$, entonces

$$d_i(p_s p'_t) = d_1 + d_2 = d_i(q_s q'_t).$$

Así, $ab \in A$.

**(v)** $\bar{1} = \frac{r_1+\ldots+r_s}{r_1+\ldots+r_s}$, entonces $\bar{1}$ es $i$-homogéneo de grado 0.

**(vi)** $a = \frac{p_1+\ldots+p_n}{q_1+\ldots+q_n} \Longrightarrow a^{-1} = \frac{q_1+\ldots+q_n}{p_1+\ldots+p_n}$, por lo que $a^{-1}$ es $i$-homogénea de grado 0.

Por los incisos **(iv)-(vi),** tenemos que $(A, \cdot, \bar{1})$ es un subgrupo de $(K(X), \cdot, \bar{1})$.

Por lo tanto, $(A, +, \bar{0}, \bullet, \bar{1})$ es un subcampo de $K(X)$, y tenemos la cadena de campos $K \underset{campo}{\leq} A \underset{campo}{\leq} K(X)$.

Como $(K(X), +, \bar{0})$ es un grupo abeliano y es un subcampo de $K(X)$ tenemos que $K(X)$ es un espacio vectorial sobre $A$.

Por (1), $K(X)$ tiene una base $\beta$. Entonces cada elemento de $K(X)$ puede expresarse de forma única de acuerdo al Teorema 27. Así, cada monomio $x \in X \subseteq K(x)$, se puede expresar como combinación lineal de vectores de $\beta$,

$$x = \sum_{b \in \beta(x)} \lambda_b(x) \cdot b$$

donde $\beta(x) \subseteq \beta$, $\beta(x)$ es finito, y $\lambda_b(x) \in A \setminus \{0\}$.

Si $i \in I$ y si $x, y \in X_i$, tenemos que

$$x = \sum_{b \in \beta(x)} \lambda_b(x) \cdot b \text{ y } y = \sum_{b \in \beta(y)} \lambda_b(y) \cdot b.$$

Además, $y = \frac{y}{x} \cdot x$, y así obtenemos que

$$y = \frac{y}{x}\Big(\sum_{b \in \beta(x)} \lambda_b(x) \cdot b\Big) = \sum_{b \in \beta(x)} \frac{y}{x} \lambda_b(x) \cdot b,$$

entonces

$$\sum_{b \in \beta(y)} \lambda_b(y) \cdot b = y = \sum_{b \in \beta(x)} \frac{y}{x} \lambda_b(x) \cdot b.$$

Ahora,

(i) $\frac{y}{x} \in A$.

(ii) $\beta(x) = \beta(y)$. Ya que, $\beta(x), \beta(y) \subseteq \beta$ y al ser $\beta$ una base, la combinación lineal es única.

(iii) $\frac{\lambda_b(y)}{y} = \frac{\lambda_b(x)}{x}$. Pues por la unicidad de los escalares se cumple que

$$\lambda_b(y) = \frac{y}{x}\lambda_b(x).$$

Ahora $\lambda_b(y) = \frac{y}{x}\lambda_b(x) \Longleftrightarrow \frac{\lambda_b(y)}{y} = \frac{\lambda_b(x)}{x}$.

Por lo anterior, notamos que todos los conjuntos $\beta(x)$ y los elementos $\frac{\lambda_b(x)}{x}$ dependen sólamente de $i$, y no dependen $x$.

Ahora, como $\lambda_b(x) \in A \setminus \{0\}$, entonces $\lambda_b(x)$ es $i$-homogéneo de grado 0.

Denotamos $\beta_i = \beta(x)$ y $\alpha(b,i) = \frac{\lambda_b(x)}{x}$.

$\alpha(b,i)$ es $i$-homogéneo de grado $d = -1$. (Pues $d = d_i(\lambda_b(x)) - d_i(x) = 0 - 1 = -1$). Por eso, si $\alpha(b,i) \in K(X)$ se expresa en su forma reducida, forzosamente alguna $x \in X_i$ se encuentra en el denominador.

Definimos

$F_i = \{x \in X_i \mid x$ aparece en el denominador de la expresión reducida de $\alpha(b,i)\}$. $F_i \subseteq X_i$ es finito y no vacío, por lo tanto, se satisface el AEM.

(2) $\Longrightarrow$ (1)

Por el Teorema 25, el AE es equivalente al Lema de Zorn. Así, que basta demostrar que el Lema de Zorn implica que cada espacio vectorial tiene una base.

Si $V$ es un espacio vectorial, consideremos

$$\mathcal{F} = \{A \subseteq V \mid A \text{ es linealmente independiente}\}.$$

$\mathcal{F}$ está parcialmente ordenado por $\subseteq$.

Si $K$ es una cadena en $\mathcal{F}$, demostraremos que $\cup K \in \mathcal{F}$. Si $\{v_i\}_{i=1}^n \subseteq \cup K$ y $a_i$ son escalares, para $i = 1, ..., n$, tales que

$$a_1 v_1 + ... + a_n v_n = 0$$

entonces $\exists\, C_i \in K$ con $v_i \in C_i\ \forall i \in \{1, ..., n\}$. Como $K$ es una cadena para $\{C_i \mid i = 1, ..., n\}$, tomamos $C_j = \text{máx}\{C_i \mid i = 1, ..., n\}$, entonces $v_i \in C_j$, para $i = 1, ..., n$. Por ser $C_j$ un conjunto linealmente independiente, tenemos que $a_i = 0\ \forall i \in \{1, ..., n\}$. Entonces $\cup K$ es un conjunto linealmente independiente, es decir, $\cup K \in \mathcal{F}$. Esto significa que cada cadena $K$ de $\mathcal{F}$ tiene una cota superior $\cup K$. Por el Lema de Zorn, $\mathcal{F}$ tiene un elemento máximo $B$. Entonces $B \subseteq V$ es un conjunto linealmente independiente máximo. Por la Observación 28, $B$ es una base de $V$. ■

**Nota 11** *Para (2) $\Longrightarrow$ (1), se puede simplemente usar el Teorema 25, que muestra la equivalencia de AE con el Lema de Teichmüller-Tukey y notar que la familia de subconjuntos linealmente independientes de ${}_FV$ es una subcolección no vacía de carácter finito. ( Un conjunto es linealmente independiente, si y sólo si, cada uno de sus subconjuntos finitos es linealmente independiente ).*

# Bibliografía


[1] Bravo A., Rincón H., Rincón C., "Álgebra Superior", U.N.A.M. Facultad de Ciencias, México, 2006.

[2] Friedberg S., Insel A., Spence L., "Linear Algebra", Pearson Education, New Jersey, 2003.

[3] Hamilton A., "Number, sets and axioms: the Apparatus of Mathematics", Cambridge University Press, Cambridge, 1982.

[4] Hernández F., "Teoría de Conjuntos", Sociedad Matemática Mexicana, México, 1998.

[5] Herrlich, H., Axiom of Choice", Springer, Germany, 2006.

[6] Jacobson N., "Basic Algebra I", Freeman, New York, 1985.

[7] Rincón H., "Álgebra lineal", U.N.A.M., Facultad de Ciencias, México, 2006.